SOC 3® Report

Description of UKG Ready and UKG Ready Partner Network System and Services relevant to Security, Availability, and Confidentiality

For the Period October 1, 2020 to September 30, 2021
# Table of Contents

**Management’s Report of its Assertion on the Effectiveness of Its Controls Over the UKG Ready and UKG Ready Partner Network System and Services** ............................................................ 1 

**Report of Independent Accountants** ......................................................................................................................... 2 

**System Description of the UKG Ready and UKG Ready Partner Network System and Services System** .......................................................................................................................... 4 

*Product overview and service* ................................................................................................................................................. 4  

*Components of the system* .................................................................................................................................................... 5  

*Service Commitments and Requirements* .......................................................................................................................... 6  

**Subservice Organization Complementary Controls** ........................................................................................................ 8  

**Complementary User Entity Controls** ............................................................................................................................. 9
Management’s Report of its Assertion on the Effectiveness of Its Controls Over the UKG Ready and UKG Ready Partner Network System and Services System Based on the Trust Services Criteria for Security, Availability, and Confidentiality

November 19, 2021

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

- Identifying the UKG Ready and UKG Ready Partner Network System and Services (System) and describing the boundaries of the System, which are presented in the section below titled System Description of the UKG Ready and UKG Ready Partner Network System and Services.
- 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 Ready and UKG Ready Partner Network System and Services System.
- Identifying, designing, implementing, operating, and monitoring effective controls over the UKG Ready and UKG Ready Partner Network System and Services (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 SendGrid, an external subservice organization to provide Simple Mail Transfer Protocol (SMTP) relay 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 Google Cloud Platform and SendGrid. 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 sub-service 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, 2020 to September 30, 2021, 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 Ultimate Kronos Group Incorporated
Report of Independent Accountants

To the Board of Directors
Ultimate Kronos Group Incorporated

Scope
We have examined management’s assertion, contained within the accompanying Management’s Report of its Assertion on the Effectiveness of Its Controls Over the UKG Ready and UKG Ready Partner Network System and Services (Assertion), that Ultimate Kronos Group Incorporated’s (UKG) controls over the UKG Ready and UKG Ready Partner Network System and Services (System) were effective throughout the period October 1, 2020 to September 30, 2021, 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 Ready and UKG Ready Partner Network System and Services (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 UKG Ready and UKG Ready Partner Network System and Services (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirement.

UKG uses Google Cloud Platform, an external subservice organization, to provide various services including hosting and cloud computing. Additionally, UKG uses SendGrid, an external subservice organization to provide Simple Mail Transfer Protocol (SMTP) relay 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 suitable designed and operating effectively throughout the period October 1, 2020 to September 30, 2021.

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. 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.

**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, 2020 to September 30, 2021, 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, 2020 to September 30, 2021.

*Ernst & Young LLP*

November 19, 2021
System Description of the UKG Ready and UKG Ready Partner Network System and Services 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 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 Kronos Management Assertion 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 Ready and UKG Ready Partner Network for Customers in the United States (US), 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 Ready and UKG Ready Partner Network (collectively referred to as UKG Ready) is a provider of Software as a Service (SaaS) based workforce management applications with a major focus in delivering solutions that support human resources (HR), payroll (PR), and time and labor management (TLM). Each solution can be used individually, as a complete suite, or in conjunction with other third-party applications, content, and/or services. UKG delivers the platform for applications and third-party offerings.
to be accessed within one interface. The UKG Ready solution is offered to UKG’s Customers subscribing to one or more of the product’s core modules. UKG Ready is hosted on the Google Cloud Platform (hereafter referred to as GCP) providing Customers with the benefit of high availability within the public cloud. UKG Ready is available any time, from anywhere through a front-end interface. Customers of UKG Ready receive 24x7 access to their solution without having to purchase hardware, operating systems, or database licenses. UKG Ready provides Customers with valuable peace of mind, knowing that experienced UKG technical consultants are managing their applications and employee data. UKG Ready is a choice for organizations to help them achieve their human capital management goals without exceeding their capital equipment budgets or placing additional demands on their in-house IT staff.

Components of the system

Infrastructure

The infrastructure supporting the UKG Ready 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. UKG Ready 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 Ready environment located in GCP, in any of the regions depicted in the scope depending on the origin 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 SSL VPN tool with multi-factor authentication (MFA). Customer specific configurations and data are segmented logically within the database. Further, a small subset of administrative users have direct access to the GCP portal.

For the period October 1, 2020 through September 29, 2021, UKG Ready leveraged SendGrid as a service to provide Simple Mail Transfer Protocol (SMTP) relay to Customers; reports from UKG Ready leveraged this service to send emails to Customer users as well as internal alerting. SendGrid services are no longer used in the United States as of July 28, 2021, Australia as of September 22, 2021 and Europe as of September 29, 2021. In place, UKG is now managing SMTP relay services.

Software

The applicable software supporting the UKG Ready environment includes various utilities that are used by UKG personnel in managing and monitoring the environment. These utilities include items such as high availability and replication, backups and redundancy, patch management, cloud automation and deployment, environment monitoring, antivirus, automation testing and database management software. Access to and use of these utilities is restricted to appropriate personnel who require such access to complete their job responsibilities.

Application

The UKG Ready application is designed, deployed, and maintained by UKG resources to be delivered to Customers using the public internet. Dell Boomi is a tool utilized for the integration between the UKG Ready application and Customer third-party systems. The Dell Boomi tool manages key APIs (Application Programming Interface) within the UKG Ready environments. The UKG Ready application is a human capital management suite that is compiled from the modules in the table below:

---

1 Customers throughout the report encompass Direct Customers, Partners and Partner’s Customers, unless otherwise stated.
<table>
<thead>
<tr>
<th>Module</th>
<th>United States</th>
<th>Europe</th>
<th>Australia</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Accruals</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Affordable Care Act (ACA)</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analytics</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attestation</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Benefits Center</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compensation</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Human Resources</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Leave of Absence</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payroll</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performance Management</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Payroll Powered by Payroll Metrics</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scheduler</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Talent Acquisition</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Time &amp; Labor Management</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

The solutions can be utilized individually, as a complete suite, or in conjunction with other third-party applications, content, and services. Customers have the flexibility to choose which modules they would like to purchase to meet the unique needs of their organization.

3.2.2.4 Data

Customer data is held in accordance with applicable data protection and other regulations set out in Customer contracts and limits access to electronically held Customer data on a least privileged basis. Customer data is held in a database management system, which is managed by the Cloud Operations team. Data in transmission is encrypted using Transport Layer Security (TLS) sessions. Access to Customer data in the relevant UKG products is limited to authorized personnel and is granted in accordance with UKG system security administration policies.

Procedures

In support of the environment, UKG has documented policies and procedures to support the operations and controls over its infrastructure and application systems. Relevant policies and procedures are made available to employees through the corporate intranet sites. Control activities in support of these policies and procedures have also been designed.

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 security, availability, and confidentiality 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 access restrictions to help ensure that logical and physical access to programs, data, and IT resources is restricted to appropriately authorized users and that access is restricted to performing appropriately authorized actions.

2 Partner Network Customers may only have a subset of these modules available to them.
- Implementing technical and non-technical controls, along with safeguards, to help ensure the availability of data in accordance with the system documentation and requirements.
- Applying 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.
- Assessing risk continuously as UKG products and processes evolve, utilizing the Data Inventory and Classification system.
- Inventorying data in a way to achieve accurate reporting of processing activities conducted on behalf of Customers.
Subservice Organization Complementary Controls

UKG utilizes the following subservice organizations as it relates to the UKG Ready System:

- **Google Cloud**: Google Cloud is utilized for computing and hosting services to store and maintain UKG Ready Customer data.
- **SendGrid**: SendGrid provides the SMTP relay that allows UKG and UKG Ready Customers to receive report content and alerts, if they are configured in various tools that support environment monitoring and backups. SendGrid services are no longer used in the following UKG Ready regions: United States as of July 28, 2021, Australia as of September 22, 2021 and Europe as of September 29, 2021. Instead, UKG is now managing SMTP relay services.

UKG has implemented various monitoring activities to monitor the described services provided by Google Cloud and SendGrid through their vendor management process, which confirms that contractual commitments are being met and effective controls exist over third-party services.

It is expected that the subservice organizations have implemented the following controls to support achievement of the associated criteria:

<table>
<thead>
<tr>
<th>Subservice provider(s)</th>
<th>Criteria</th>
<th>Expected subservice organization controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Cloud</td>
<td>CC1.1, CC6.1</td>
<td>The entity implements processes to monitor and protect customer data.</td>
</tr>
<tr>
<td>SendGrid</td>
<td>CC2.2, CC7.3</td>
<td>The entity will notify UKG of any incidents or breaches.</td>
</tr>
<tr>
<td>Google Cloud</td>
<td>CC8.1</td>
<td>Controls to address the handling and protection of confidential data during the system development lifecycle.</td>
</tr>
<tr>
<td>SendGrid</td>
<td>CC6.6, CC7.2, C1.2</td>
<td>Controls to address network is monitored and security mechanisms exist to protect from external threats and interruptions.</td>
</tr>
<tr>
<td>Google Cloud</td>
<td>CC6.1, CC6.2, CC6.3</td>
<td>Controls to address logical access to application software, system software, databases, and network components is restricted to authorized and appropriate users to performing authorized and appropriate actions.</td>
</tr>
<tr>
<td>SendGrid</td>
<td>CC6.1</td>
<td>Controls to address user authentication mechanisms (i.e., passwords).</td>
</tr>
<tr>
<td>Google Cloud</td>
<td>CC6.4</td>
<td>Controls to address physical access and environment protections to computer equipment and storage media are established.</td>
</tr>
<tr>
<td>Google Cloud</td>
<td>CC2.2, CC7.2</td>
<td>Google provides a process to internal users for reporting security, confidentiality, and privacy failures, incidents, and concerns, and other complaints.</td>
</tr>
<tr>
<td>SendGrid</td>
<td>CC2.2, CC2.3</td>
<td>System changes that may affect security, privacy, or confidentiality are communicated to management and users who will be affected.</td>
</tr>
<tr>
<td>Google Cloud</td>
<td>CC6.7</td>
<td>Google does not permit equipment from leaving Google data centers without being subject to Google’s sanitization process.</td>
</tr>
<tr>
<td>SendGrid</td>
<td>A1.1, A1.2, A1.3</td>
<td>Controls to address the entity’s ability to maintain continuous operations and react to availability incidents are in place.</td>
</tr>
<tr>
<td>Google Cloud</td>
<td>CC6.1, CC6.6, A1.2</td>
<td>Data that is uploaded or created in the Google Cloud is encrypted at rest.</td>
</tr>
</tbody>
</table>
Complementary user entity controls

The controls at UKG were designed with the assumptions that certain controls would be implemented by user entities. The application of certain controls by user entities is necessary to achieve the criteria identified in this report.

This section describes certain controls that the user entities should consider for achievement of the criteria identified in this Description. The complementary user entity controls presented below should not be regarded as a comprehensive list of all controls that should be employed by user entities:

- User entities are responsible for determining that the functionality within the UKG Ready application meets their requirements and notifying UKG timely with any required changes or enhancements. (CC2.3)
- 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. (CC6.1, CC6.2, and CC6.6)
- 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. (CC2.2 and CC2.3)
- User entities are responsible for adequately securing and disposing of any system output provided by the System. (CC6.6 and CC6.7)
- User entities are responsible for appropriately securing transmissions of data to UKG and informing UKG of any necessary changes to the System. (CC6.7)
- User entities are responsible for implementing processes and controls to prevent and detect unauthorized or malicious software and unauthorized access to the system or activity. (CC5.1 and CC6.8)
- 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. (C1.1, C1.2 and CC6.3)
- User entities are responsible for reviewing changes to their data to help ensure that all changes are appropriate and authorized. (C1.1 and CC8.1)
- User entities are responsible for reviewing notifications from UKG of changes to the UKG Ready environment and communicating any concerns to UKG. (CC2.2)
- 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. (CC2.2)
- User entities are responsible for communicating any identified incidents impacting the security, availability, or confidentiality of the system to UKG on a timely basis. (CC2.3 and CC7.1)
- User entities are responsible for reviewing application audit trails and notifying UKG of any discrepancies or unauthorized activity. (CC4.1 and CC7.2)
- 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. (C1.1 and C1.2)
- User entities are responsible for maintaining servers supporting the time-clock systems and restricting access to authorized individuals. (CC6.4, CC6.5 and CC6.6)