SOC 3® Report

Description of Ultimate Kronos Group Incorporated’s UKG Dimensions HCM System relevant to Security, Availability, Processing Integrity and Confidentiality

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

MANAGEMENT’S REPORT OF ITS ASSERTIONS ON THE EFFECTIVENESS OF ITS CONTROLS OVER THE ULTIMATE KRONOS GROUP INCORPORATED’S UKG DIMENSIONS HCM SYSTEM BASED ON THE TRUST SERVICES CRITERIA FOR SECURITY, AVAILABILITY, PROCESSING INTEGRITY, AND CONFIDENTIALITY ............................................. 1

REPORT OF INDEPENDENT ACCOUNTANTS ............................................................................................................................... 2

SYSTEM DESCRIPTION OF THE UKG DIMENSIONS HCM SYSTEM ......................................................................................... 4
   Product overview and service................................................................................................................................................... 4
   Components of the system..................................................................................................................................................... 5
   Service commitments and requirements............................................................................................................................... 6
November 16, 2021

We, as management of, Ultimate Kronos Group 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 SendGrid, an external subservice organization to provide SMTP relay services, and Twilio, an external subservice organization, to provide SMS open-shift scheduling. 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, 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, processing integrity, 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 Assertions of the Effectiveness of Its Controls over the UKG Dimensions HCM System (Assertion), that Ultimate Kronos Group Incorporated’s (UKG) controls over the UKG Dimensions HCM System (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, processing integrity, 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 Dimensions HCM 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 UKG Dimensions HCM System (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 SendGrid, an external subservice organization to provide SMTP relay services, and Twilio, an external subservice organization, to provide SMS open-shift scheduling. 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, processing integrity, 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 16, 2021
Boston, Massachusetts
System Description of the UKG Dimensions HCM 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 UKG Management Assertion and the guidance for a description of a service organization's system set forth in the AICPA Attestation Standards.

Product overview and service

The UKG Dimensions HCM System is a provider of Software as a Service (SaaS) based workforce management applications with a major focus in delivering solutions that support timekeeping, scheduling, leave and attendance, human resources (HR), and payroll. UKG has added services to the Custom Function Cloud (CFC). The CFC is an environment designed to host additional modules that can be more tailored for a Customer’s specific business needs. These solutions are available to Customers as add-on modules to their existing UKG Dimensions environment. The CFC modules communicate with UKG Dimensions via publicly available Application Programming Interfaces (API's). The list of CFC modules is included in section “Application” 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 leverages SendGrid as a service to provide
SMTP relay to Customers; reports from UKG Dimensions will leverage this service to send emails to customer users as well as internal alerting. UKG Dimensions is available any time, from anywhere through a front-end interface. Customers of UKG Dimensions receive 24x7 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 Dimensions 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 Dimensions 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 Dimensions 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.

Software

The applicable software supporting the UKG Dimensions 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 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 timekeeping, scheduling, leave and attendance, HR, and payroll. Dell Boomi is a tool utilized for the integration between the UKG Dimensions application and customer third-party systems. The Dell Boomi tool manages key APIs within the UKG Dimensions ecosystem, as well as the APIs with external client environments. The UKG Dimensions application comes with Dell Boomi accounts that allow Customers to create, deploy, and manage APIs to 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.

<table>
<thead>
<tr>
<th>Module</th>
<th>United States</th>
<th>Australia</th>
<th>Canada</th>
<th>Europe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timekeeping</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Scheduling</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Leave &amp; Attendance</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Forecasting</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Work</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Healthcare Analytics</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>HR</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payroll</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Module</td>
<td>United States</td>
<td>Australia</td>
<td>Canada</td>
<td>Europe</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------</td>
<td>-----------</td>
<td>---------------------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Microsoft Outlook Add-on¹</td>
<td>X</td>
<td>X</td>
<td>X (Beginning on October 30, 2020)</td>
<td></td>
</tr>
<tr>
<td>SMS Open ShiftFill¹</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gaming¹</td>
<td></td>
<td></td>
<td>X (Beginning on February 10, 2021)</td>
<td></td>
</tr>
<tr>
<td>Rotation Schedule¹</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

¹ Denotes a module available through the CFC

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

UKG will only make changes to customer environments at the 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 and tracked 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 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 or Secure File Transmission Protocol (SFTP). 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.

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, processing integrity, 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 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.
- Processing of transactions in accordance with the system documentation and requirements.
• 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.
Subservice organization complementary controls

UKG utilizes the following subservice organizations as it relates to the UKG Dimensions system:

- **Google Cloud**: Google Cloud is utilized for computing and hosting services to store and maintain UKG Dimensions customer data.
- **SendGrid**: SendGrid provides the SMTP relay that allows UKG and UKG Dimensions 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 Dimensions regions: Canada; US as of February 5, 2021; Europe as of March 17, 2021; Australia as of July 21, 2021. Instead, UKG is now managing SMTP relay services.
- **Twilio**: Twilio provides SMS services for open-shift scheduling through the use of the SMS Open ShiftFill application.

UKG has implemented various monitoring activities to monitor the services provided by Google, SendGrid and Twilio 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 SendGrid Twilio</td>
<td>P4.2, P6.4, P6.7, CC1.1, CC6.1</td>
<td>The entity implements processes to monitor and protect customer data.</td>
</tr>
<tr>
<td>Google Cloud SendGrid Twilio</td>
<td>P6.3, P6.4, P6.5, P6.6, CC2.2, CC7.3</td>
<td>The entity will notify UKG of any incidents or breaches.</td>
</tr>
<tr>
<td>Google Cloud SendGrid Twilio</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>Google Cloud SendGrid Twilio</td>
<td>P6.3, P6.4, CC6.6, CC7.2, CC1.2</td>
<td>Controls to address that the entity’s network is monitored and security mechanisms exist to protect from external threats and interruptions.</td>
</tr>
<tr>
<td>Google Cloud SendGrid Twilio</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 perform authorized and appropriate actions.</td>
</tr>
<tr>
<td>Google Cloud SendGrid Twilio</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 environmental 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>Google Cloud SendGrid Twilio</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>Subservice provider(s)</td>
<td>Criteria</td>
<td>Expected subservice organization controls</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Google Cloud</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>SendGrid</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Twilio</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google Cloud</td>
<td>PI1.1, PI1.2,</td>
<td>Controls and policies to address timely and accurate processing of inputs and outputs by the system.</td>
</tr>
<tr>
<td></td>
<td>PI1.3</td>
<td></td>
</tr>
<tr>
<td>Google Cloud</td>
<td>CC6.1, CC6.6,</td>
<td>Data that is uploaded or created in the Google Cloud is encrypted at rest.</td>
</tr>
<tr>
<td></td>
<td>A1.2</td>
<td></td>
</tr>
</tbody>
</table>
User entity responsibilities

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 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, CC6.6, and PI1.3).
- User entities are responsible for reviewing permission levels associated to Functional Access Profiles and Data Access Profiles (CC6.1, CC6.2, CC6.6 and PI1.3).
- User entities are responsible for managing UKG access to their tenants (CC6.1, CC6.2, and CC6.6).
- 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 (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 confirming communication protocol is acceptable to the end-user when transmitting data (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 (CC6.3, C1.1 and C1.2).
- User entities are responsible for reviewing changes to their data to ensure that changes are appropriate and authorized (CC8.1 and C1.1).
- User entities are responsible for reviewing notifications from UKG of changes to the UKG Dimensions 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, confidentiality, or processing integrity 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 determining that the transaction processing functionality within the UKG Dimensions application meets their expectations and notifying UKG timely with any required changes or enhancements (PI1.3 and PI1.4).
• User entities are responsible for the completeness and accuracy of data input to the UKG Dimensions application via either direct data input or API (PI1.2).
• User entities are responsible for reviewing system outputs for completeness and accuracy and notifying UKG of any discrepancies (PI1.4).
• User entities are responsible for monitoring all required scheduled jobs for timeliness and completeness and notifying UKG if support is required (PI1.4).
• 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 (PI1.2, PI1.4 and CC8.1).
• User entities are responsible for ensuring that changes to APIs post go live, including any configurations, are authorized, tested and approved (PI1.1, PI1.3, PI1.4, PI1.5 and CC8.1).
• User entities are responsible for monitoring the completion status of APIs and investigating any integration failures (PI1.1, PI1.2, PI1.3 and PI1.4).
• User entities are responsible for approving the list of users authorized to approve configuration items prior to go-live (CC8.1)