The Maryland-National Capital Park and Planning Commission
Office of the Inspector General

Kronos UKG Migration
Audit No. CW-002-2025
May 30, 2025

Distribution:

Audit Committee
Dorothy Bailey
Mitra Pedoeem
Erin White
Benjamin Williams

Maryland-National Capital Park and Planning Commission
L. Todd Allen
Chip Bennett
Joe Bistany
Debra Borden
Mazen Chilet
Gavin Cohen
Artie Harris
Tracey Harris
Joyce Kesselring
Jason Lawrence
Peter Shapiro
Bill Spencer
Tracey Harvin
Brian Coburn
John Kim-Norris

Office of the Inspector General
Renee Kenney
Modupe Ogunduyile
Irith Dror

Kronos UKG Migration

Table of Contents

I. EXECUTIVE SUMMARY

A. Overall Perspective

The Maryland-National Capital Park and Planning Commission (M-NCPPC or Commission) was using the UKG Workforce Central Timekeeper product (formerly Kronos Timekeeper) as its electronic timekeeping system, hosted on the Kronos Private Cloud (KPC). The vendor announced plans to retire the UKG Workforce Central Timekeeper product and its hosting option by the end of December 2025. As a result, the Commission would lose access to its cloud-hosted timekeeping system on the retirement date. The electronic timekeeping system is an integral part of the Commission's payroll operations. If not available, it would impact the Commission's ability to efficiently and accurately process payroll data and pay its employees. To mitigate these risks, a project was approved and implemented to migrate the program and data to a current modern UKG cloud solution.

Per the Project Management Office (PMO), within the Office of the Chief Information Officer (OCIO), the project includes the following goals:

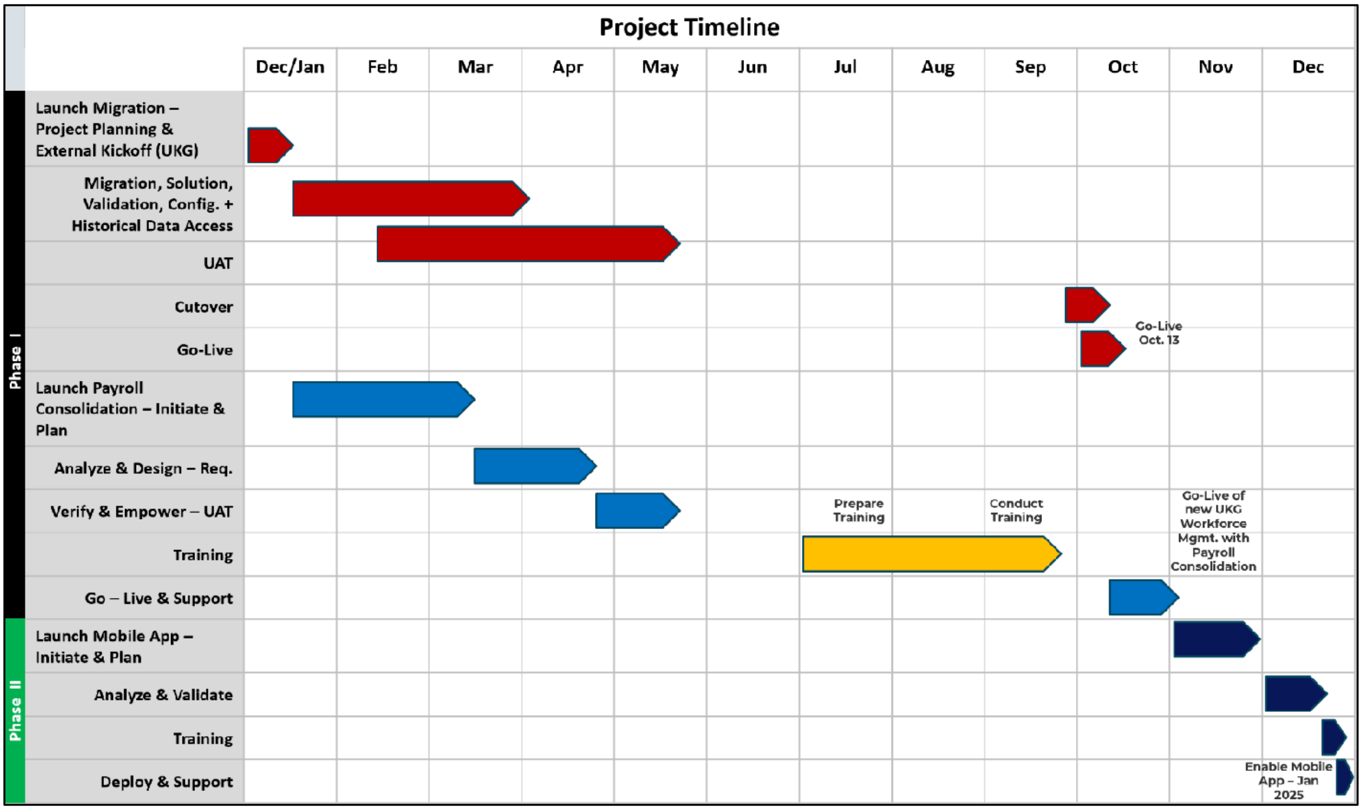
Goal 1 - Migration from UKG Workforce Central Timekeeper to the UKG Pro Workforce Management solution.

Goal 2 - Consolidation of the M-NCPPC's payroll cycles (B2 and B1) into a single pay schedule by eliminating the B2 pay schedule and related processes.

Goal 3 - Providing historical data access to attendance data, on premise.

Goal 4 - Deployment of the UKG Pro Workforce Management mobile solution with single sign-on (SSO).

The project was planned for deployment in two phases, with the migration, payroll schedule change, and historical data solution going live in Q4 2024, and the mobile solution planned for Q2 2025 see next page:


Project Timeline
Dec/Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Phase I
Launch Migration – Project Planning & External Kickoff (UKG)
Migration, Solution, Validation, Config. + Historical Data Access
UAT
Cutover
Go-Live
Launch Payroll Consolidation – Initiate & Plan
Analyze & Design – Req.
Verify & Empower – UAT
Training
Go – Live & Support
Phase II
Launch Mobile App – Initiate & Plan
Analyze & Validate
Training
Deploy & Support
Go-Live Oct. 13
Prepare Training
Conduct Training
Go-Live of new UKG Workforce Mgmt. with Payroll Consolidation
Enable Mobile App – Jan 2025

B. Audit Objective, Scope, and Methodology

Objective

Based on the four defined project goals, this audit is focused on the risks and controls for the following processes:

1. Cloud-to-cloud data migration implementation
2. New payroll schedule implementation
3. Cloud to on-prem data conversion implementation

The primary objectives of this audit were to ensure:

- The correctness, completeness, reliability and integrity of the migrated data,
- The viability of the new system's operating effectiveness, and
- The security of logical access to the migrated data, and of physical access to the on prem facility.

Scope

Through stakeholder interviews and the review of project documentation, the Office of the Inspector General (OIG) reviewed the following process and control objectives:

- **Project planning** - The project plan is documented and regularly updated, with management approvals obtained at each stage for the corresponding deliverables.

- **Application Functionality** - Application functionality is subject to an assurance review.

- **Acceptance Testing** - The planning and outcomes of acceptance testing are documented, issues are resolved, and management approval is obtained upon completion. Testing is conducted in a dedicated test environment.

- **Post-implementation review** - A post-implementation review that includes evaluating project outcomes against objectives, identifying and documenting any issues, and implementing corrective actions, is performed and documented. Management approval of the review results, to confirm all issues are resolved, is obtained.

- **Backup Data Security** - Data backups are encrypted, stored safely, and available as needed.

- **Data Center Operations** - Physical and logical security controls are implemented within the data center, including access controls, surveillance systems, regular security audits, and intrusion detection mechanisms. Security measures are documented, regularly reviewed, and approved by management.

- **Identity and Access Management** - Responsibility for user authentication remains with the customer. Single sign on and authentication is used to access the cloud instance. Identity processes ensure only authorized users have access to data and resources, User activities can be audited and analyzed, and the customer has control over access management.

- **Data Security** - Data in transit are encrypted over networks with private keys known only to the customer. Data stored on the cloud in live production are encrypted and knowledge of the decryption keys is limited to the customer. Test data do not contain, and are prohibited from using, copies of any current or historical production data containing sensitive/confidential information.

- **Interfaces/Integration** - An integration strategy has been developed that includes detailed planning, compatibility assessments, and testing procedures. Interface testing in a controlled environment is conducted to identify and resolve compatibility issues and resolve them before the Go-Live.

In addition, the audit scope was designed to identify possible fraud, waste, or abuse within the process(es) being audited.

The audit covered the period from January 1, 2024, through January 31, 2025.

Scope Limitation

The audit did not include a review of Goal 4 - the mobile solution deployment.

Methodology

During the audit, inquiry, observation, and analysis were performed. The auditor-in-charge conducted interviews with personnel responsible for the Kronos/UKG migration project planning and implementation in the OCIO, PMO, Department of Finance, and the Department of Human Resources and Management.

In addition, the auditor-in-charge reviewed and analyzed project implementation documentation and deliverables for Goal 1 (Cloud migration) and Goal 3 (On prem historical data conversion). For Goal 2 (Consolidation of the B2 and B1 payroll cycles) analysis and reviews were performed based on the B2 to B1 process checklists implementations, and the validation performed on the consolidated B1 data.

The audit was conducted in accordance with the *U.S. Generally Accepted Government Auditing Standards*. Those standards require that the audit be planned, and fieldwork performed to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the established audit objectives.

C. Frameworks and Risk Mitigation

Frameworks

There are several Information Technology (IT) frameworks that describe risks and controls and provide guidelines for the assurance of IT projects using cloud computing. This audit is based on the following frameworks:

- ISACA's (Information Systems Audit and Control Association) COBIT 2019 (Control Objectives for Information and Related Technologies)
- ISACA's IS (Information Systems) Audit/Assurance Program for Cloud Computing
- CSA (Cloud Security Alliance) Cloud Controls Matrix (CCM) which maps to NIST's (National Institute of Standards and Technology) Cybersecurity Framework v1.1

Risk Mitigation

Effective management of migration and implementation processes is crucial to mitigating the risks associated with software projects, particularly those involving critical business operations and sensitive data.

When safeguards are ineffectively implemented, the following risks are either partially or fully unmitigated, increasing the risk of fraud, abuse, or data breach, with the potential to cause considerable harm to the Commission:

- Inadequate planning for the project may lead to delays, cost overruns, and compromised project quality. It can also result in an incomplete or inaccurate migration potentially affecting stakeholder satisfaction and operational efficiency.
- The outsourced cloud application may lack the necessary functionality and processing controls required to comply with the customer's control policies, potentially leading to non-compliance, data integrity issues, security vulnerabilities, and operational inefficiencies.
- Inadequate planning and execution of acceptance testing may lead to issues with product quality and functionality.
- Inadequate post-implementation review may result in undetected issues remaining unresolved.
- Misplacement or theft of backup information may lead to data loss, unauthorized access, and potential breaches of confidentiality,

compromising business continuity, data integrity, and regulatory compliance.

- Failure to implement physical and logical security controls in the data center may expose critical systems and data to unauthorized access, theft, damage, or cyber-attacks, leading to operational disruptions, data breaches, and potential legal and financial consequences.

- Inadequate identity management processes may lead to unauthorized access, data breaches, misuse/modification of data and compromised system integrity, potentially causing operational, legal, and financial impacts.

- Insufficient identification and protection of sensitive data, whether in transit or stored in the cloud, and inadequate measures to prevent data leakage, could lead to unauthorized access, data breaches, and exposure of confidential information, resulting in legal, financial, and reputational damage.

- Inadequate integration and interfacing of new systems/applications with existing systems or environments may result in compatibility issues, increased complexity, extended implementation timelines, and higher costs, potentially disrupting business operations and reducing overall system efficiency.

D. Major Audit Concerns

The results of our audit indicated the following major audit concern:

Failure to Take Action on Identified High Security Risk

During audit fieldwork completed in December 2024, the OIG identified a significant internal control weakness involving access to the Commission's server room located in the Executive Office Building. At the time **69** employees had access to the server room. Access should only be granted to employees who require access to manage and maintain the servers and network equipment. The OIG immediately issued a memorandum to key stakeholders in the OCIO, DHRM, and Park Police of our discoveries. **Exhibit A** contains a copy of the memorandum. The memo discusses the inherent risks and recommendations for mitigation

On April 11, 2025, the OIG obtained a report(s) from Park Police to ensure appropriate action was taken to address the security concern. The new reports identified **73** employees with access. No action was taken by management upon receipt of OIG's memorandum.

E. Overall Conclusions

The results of our audit indicate deficiencies in the internal controls around access security of the Central Administrative Services (CAS) Information Technology (IT) Data Center, see definitions below.

We believe all weaknesses identified and communicated are correctable

We wish to express our appreciation to management and staff of the OCIO, PMO, Department of Finance, and DHRM for the cooperation and courtesies extended during the course of our review.

Irith Dror, CISA, CGEIT
Senior IT Auditor

Modupe Ogunduyile, CIG
Deputy Inspector General

Renee M. Kenney, CIG, CPA, CIA, CISA
Inspector General

May 30, 2025

Conclusion Definitions

Satisfactory	No major weaknesses were identified in the design or operation of internal control procedures.
Deficiency	A deficiency in the design or operation of an internal control procedure(s) that could adversely affect an operating unit's ability to safeguard assets, comply with laws and regulations, and ensure transactions are properly executed and recorded on a timely basis.
Significant Deficiency	A deficiency in the design or operation of an internal control procedure(s) which adversely affects an operating unit's ability to safeguard assets, comply with laws and regulations, and ensure transactions are properly executed and reported. This deficiency is less severe than a material weakness, yet important enough to merit attention by management.
Material Weakness	A deficiency in the design or operation of an internal control procedure(s) which may result in a material misstatement of the Commission's financial statements or material impact to the Commission.

II. DETAILED COMMENTARY AND RECOMMENDATIONS

1. Implement CAS IT Review and Monitoring Controls Over Physical Access to the CAS IT Server Room

Issue: The migration of the UKG Kronos timekeeping system to the new UKG Pro Workforce Management solution includes the establishment of a historical attendance database, to be hosted on premise within the CAS IT Server room. As of December 2024, there were **69 employees** who could access the server room[1]. Most of them did not have assigned responsibilities that require access to manage and maintain the servers and network equipment. As of April 11, 2025, there are **73** employees with access to the server room.

In addition, monitoring by CAS Enterprise IT (EIT) is not being performed. For example:

- a list/report of employees with access to the server room is not reviewed periodically; and
- a list/report of who actually entered the server room is also not being reviewed periodically.

Note: The CAS IT server room access is controlled through badge security attributes, managed by the Maryland-National Capital Park Police, Prince George's County Division, Security & Public Safety Systems Office (Park Police).There are no formal guidelines or procedures to guide Park Police when assigning employees to various Commission locations. Recommendations to strengthen this process will be included in a complimentary audit currently being completed by the OIG[2].

Criteria: NIST Industry security best practices state access to a server room should be limited to authorized IT personnel, typically including system administrators, network engineers, and dedicated server technicians, who require access to manage and maintain the servers and network equipment. Generally, individuals outside of IT, like cleaning staff, security personnel, or general office employees, should not have access unless specifically authorized for a controlled situation.

Cause: EIT management has not prioritized monitoring and reviewing of the CAS IT Server room.

Risk: NIST Industry security best practices dictate that access to a server room should be limited. **Exhibit B** contains a list of typical risks of excessive access to a server room.

[1] **SEE MAJOR AUDIT CONCERN ON PAGE 7.** CAS EIT management was notified by OIG of the excess access on December 4, 2024. The OIG provided management with recommendations on least privilege access assignments. No action was taken to mitigate the identified risk.

[2] Employee Building Access Controls, CW-007-2025

Recommendation: Management should take immediate action to reduce access privileges to the IT server room in the Executive Office Building.

In addition, we recommend that IT management implement two review and monitoring controls:

- **Conduct regular reviews to ensure continued appropriate access** to the CAS IT Server room, and revise access as necessary (currently based on lists provided by PGC Park Police Security & Public Safety Systems office).

- **Conduct regular reviews of employees who have physically entered the server room** (e.g. based on paper or electronic records that detail who and when someone enters and exits the room and generate logs accordingly).

Issue Risk: High

Management Response:

Swift action: Immediate action has been taken to immediately reduce access privileges to the IT server room in the Executive Office Building. We have communicated with the PGC Park Police Security and Public Safety Systems office to revoke server room access for everyone except for 11 employees: nine IT staff members and two facility management employees. This change has been confirmed.

Regular reviews of employees who have physically entered the server room: We requested that PGC Park Police Security & Public Safety send real-time notifications to the Chief Information Officer, Enterprise IT and the IT group. The real-time notification took effect on 5/19/2025.

Regular reviews to ensure continued appropriate access: The current Lenel system cannot generate automated reports. The system will be upgraded to a new software version within the next six months, which will enable automated reporting capabilities. After the upgrade, I will request a semi-annual access list report.

Expected Completion Date: December 2025

Follow-up Date: January 2026

III. EXHIBITS

Exhibit A - Memo to Management

December 4, 2024

To: Mazen Chilet, Chief Information Officer (CIO)

Joe Bistany, Information Technology (IT) Division Chief – Office of the CIO (OCIO)

Ike Onyegbado, Chief Information Security Officer - OCIO

Brian Coburn, Corporate Administrative Services and Performance Management Chief – Department of Human Resources and Management

John Kim-Norris, Program Manager Security & Public Safety Systems – Prince George's County Park Police

From: Renee Kenney, Inspector General Renee Kenney

Re: Access to the Executive Office Building (EOB) Server Room

Background

The Office of the Inspector General (OIG) is engaged in an IT audit of the UKG Kronos timekeeping system migration to the new UKG Pro Workforce Management solution.

The project includes the establishment of a historical attendance database, to be hosted on premise in the EOB IT Server room. Due to the on premise historical database location, one part of the audit involves a physical security evaluation of access to the server room.

This access is controlled through badge security attributes, managed by Prince George's County Park Police Security & Public Safety Systems office. Currently, there are **69** employees who can access the server room. These employees belong to two badge security groups (group numbers are defined in the application used for badge management):

- Group 1: EOB - 24/7 All Readers - less OIG - 38 employees
- Group 3[1]: EOB 3rd - CAS IT Server - 31 employees

I have attached a copy of the access report for your convenience.

[1] Group 2 is a Master Safety Group with no employees.

Industry security best practices dictate that access to a server room should be limited to authorized IT personnel, typically including system administrators, network engineers, and dedicated server technicians, who require access to manage and maintain the servers and network equipment. Generally, individuals outside of IT, like cleaning staff, security personnel, or general office employees, should not have access unless specifically authorized for a controlled situation.

Recommendations to strengthen internal controls over access to the server room will be included in the final audit report. However, given the risk level associated with excess access, the OIG is notifying management of our draft findings and recommendations prior to the issuance of our audit report. Note: Appendix A contains risk examples for excessive access to a server room.

Although it is the responsibility of management to determine who should have access to the server room, we have provided some guidance below.

1. Limit Access and Control
   a. No one from group 1 should have server room access permission, with the exception of four people who should be moved to group 3:

61689	Coburn	Brian	Corporate Policy Mgmt. Services
48222	Williams	Dale	Corporate Policy Mgmt. Operations
48320	Ortiz	Byron	Corporate IT Office
63664	Chilet	Mazen	Chief Information Officer

   b. Only four employees in group 3 should retain server room access:

46843	Bistany	Joseph	IT Division Chief
47296	Laryea	Andrews	Systems Manager
35759	Mendoza	Elvis	IT/Telecom Support Specialist III
26745	Thomas	Steven	IT/Telecom Support Specialist III

   c. Everyone else in group 3 should be removed.

2. Improve process for assigning access including approvals and periodic reviews

   The process for assigning and controlling access typically involves:
   a. Identifying who should get and/or keep access based on roles and responsibilities
   b. Requesting access through a designated system
   c. Obtaining necessary approvals from relevant management
   d. Granting access
   e. Conducting regular reviews to ensure continued access appropriateness

f. Revising access as necessary based on reviews. This process should be documented and enforced with clear guidelines for access permissions, and review frequencies, depending on the sensitivity of data involved.

3. Perform Logging and Monitoring

   This includes maintaining a system that records details of who and when anyone enters and exits the room and generate logs accordingly; and using cameras for visual control and recording.

Exhibit B - Risks of Excessive Access to a Server Room

There are multiple risks when access to a server room is inadequately controlled, all stemming from the ability of an unauthorized person to manipulate or access sensitive equipment and data within the server room. The risks include:

- **Data breaches:** Malicious actors gaining access to the server room could steal sensitive data stored on the servers, leading to privacy violations and significant financial losses.
- **System disruption:** Accidental or intentional tampering with server hardware could cause system outages or malfunctions, disrupting critical business operations.
- **Hardware damage:** Unauthorized individuals might mishandle or damage sensitive equipment within the server room, leading to costly repairs or replacements.
- **Malware installation:** An unauthorized person could potentially install malicious software on servers, compromising system security and potentially leading to data breaches.
- **Unauthorized configuration changes:** Improper access could allow someone to change server settings or configurations without authorization, potentially causing operational issues.
- **Physical theft:** Valuable hardware components like hard drives or network devices could be stolen from the server room if access is not properly controlled.
- **Accidental damage:** Even with good intentions, someone without proper training could accidentally damage equipment while attempting to access or work on servers.