



Lavois Campbell, CIA, CISA, CFE, CGA
Chief Audit Executive

January 2023

DeKalb County Government

PLANNING and SUSTAINABILITY

**INFOR PUBLIC SECTOR (HANSEN)
INFORMATION TECHNOLOGY
GENERAL CONTROLS AUDIT**

FINAL REPORT

Audit Report No. IA-2021-015-IT

Page intentionally left blank



HANSEN INFORMATION TECHNOLOGY GENERAL CONTROLS AUDIT
AUDIT REPORT NO. IA-2021-015-IT

FINAL

HIGHLIGHT SUMMARY

Why We Performed the Audit

In accordance with the Office of Independent Internal Audit (OIIA) Annual Audit Plan, we conducted a performance audit of the Information Technology General Control (ITGC) processes within the County's Infor Public Sector (Hansen) Application. The objectives of the audit were to assess the adequacy of the information technology general controls within the Hansen Application in the Planning and Sustainability Department. We assessed whether the controls were sufficient to support the County's business processes and reporting.

The Hansen application is utilized by more than 12 County program areas to support critical public services provided by the County that involve completing several forms and payment of fees. While processing the services, County residents' sensitive and confidential information (e.g., name, address, social security/tax number, email/phone number, insurance details, social media accounts, etc.) is collected. The integrity and security of the information processed on this application are essential to minimize the risks and impact of data breaches that could cost the County financial, operational, and litigation loss.

How We Performed the Audit

The audit focused on the ITGCs related to Hansen Application from January 1, 2021, through the present. Our methodology included, but was not limited to, the following:

- Reviewed relevant policies, procedures, and standards.
- Examined supporting documentation to assess the effectiveness of controls in place.
- Interviewed appropriate County personnel and consultants.
- Conducted walkthrough of processes within the Hansen Application.
- Tested and evaluated the operating effectiveness of ITGC within the Hansen Application.

Background

The Hansen application is a suite of related applications used by several local governments and municipal agencies. Hansen offers three main functions of related modules covering: Infrastructure management; Permitting and licensing, and Utility billing. Dekalb County currently licenses the Permitting and licensing function of the Hansen application. The modules in this function manage different types of permitting and licensing processes, including building and development permits, use permits, business licenses, and trade licenses. It also includes a Code Enforcement module. The Planning and Sustainability Department is the owner of the application data. As with any application, the Hansen IT general controls are expected to be in place to ensure the integrity of the data and processes that the system support.

Dekalb has utilized the Hansen application since 2012.

What We Found

The audit noted that the Hansen application is a fully vendor-hosted Software as a Service (SaaS) application. As a SaaS application, the responsibility for most key ITGCs rests with the vendor (i.e., Change Management, Physical Security, Data Backup and Recovery, and Incident Management) while the County (i.e., the Planning and Sustainability department) is primarily responsible for User Access Management and Contract Performance Monitoring, while there is a shared responsibility among the vendor and the County for change management and incident management.

The audit also identified control gaps between current practices and the documented County policies and information technology better practices and standards.

Audit Results Summary	
Access Control	
1. The Application's password configuration does not align with the County's Password Policy.	
2. Existence of dormant user accounts on the Hansen application.	
3. Unauthorized user access to The Hansen application	
4. User roles and privilege assignments need review.	
5. Superuser user roles' assignment to user accounts needs review.	
Computer/IT Operations	
6. Hansen audit logs' use needs optimization.	
7. Hansen application incident tickets were not resolved timely.	
Application Change Management	
8. Contract management processes need improvement	
9. The Hansen application patch management needs improvement.	
<div style="display: flex; justify-content: space-between;"> <div style="width: 20px; height: 10px; background-color: green; border: 1px solid black;"></div> No exceptions were noted. </div> <div style="display: flex; justify-content: space-between;"> <div style="width: 20px; height: 10px; background-color: yellow; border: 1px solid black;"></div> Exception- Internal control improvements are needed. </div> <div style="display: flex; justify-content: space-between;"> <div style="width: 20px; height: 10px; background-color: red; border: 1px solid black;"></div> Exception - internal control deficiencies/gaps noted. </div>	

What we Recommend

We recommend that Planning and Sustainability work with the vendor and the Department of Innovation and Technology (DoIT) to address the internal control deficiencies and recommended process improvements identified in this report.

How Management Responded: Management agrees with the exceptions noted.



TABLE OF CONTENTS

HIGHLIGHT SUMMARY -----	2
BACKGROUND AND INTRODUCTION -----	4
AUDIT RESULTS -----	7
FINDING 1: THE APPLICATION'S PASSWORD CONFIGURATION DOES NOT ALIGN WITH THE COUNTY'S PASSWORD POLICY. -----	8
FINDING 2: EXISTENCE OF DORMANT USER ACCOUNTS ON THE HANSEN APPLICATION -----	9
FINDING 3: UNAUTHORIZED USER ACCESS TO THE HANSEN APPLICATION -----	10
FINDING 4: USERS ROLES AND PRIVILEGE ASSIGNMENTS NEED REVIEW -----	11
FINDING 5: SUPERUSER ROLE ASSIGNMENT NEEDS REVIEW -----	12
FINDING 6: HANSEN AUDIT LOGS' USE NEEDS OPTIMIZATION -----	14
FINDING 7: HANSEN INCIDENT TICKETS WERE NOT RESOLVED TIMELY. -----	14
FINDING 8: CONTRACT MANAGEMENT PROCESSES NEED IMPROVEMENT. -----	16
FINDING 9: THE HANSEN APPLICATION PATCH MANAGEMENT NEEDS IMPROVEMENT. -----	17
APPENDICES -----	19
Appendix I – Purpose, Scope, and Methodology -----	19
Appendix II – Management Response -----	20
Appendix III – Definitions and Abbreviations -----	21
Appendix IV – Application Roles -----	22
DISTRIBUTION -----	23
PROJECT TEAM -----	24
STATEMENT OF ACCORDANCE -----	25



BACKGROUND AND INTRODUCTION

The Infor Public Sector (formally “Hansen”) application is a suite of related applications used by several local governments and municipal agencies. Hansen offers three main functions/ groups of related modules covering: Infrastructure management; Permitting and licensing, and Utility billing. DeKalb County currently licenses the permitting and licensing function of the application. The modules in this function manage different types of permitting and licensing processes, including building and development permits, use permits, business licenses, and trade licenses. It also includes a code enforcement module because code enforcement follows the same general process as permitting and licensing.

The modules are structured around a core application record that makes sure all requirements are met and sees the process through to its completion. Associated with the application are supporting records such as reviews, inspections, hearings, conditions, and fees. The application processing is structured around application workflows, which specify which requirements must be completed and in what order.¹

DeKalb has utilized the Hansen application since 2012. Hansen became a vendor-hosted Software as a Service (SaaS) application in October 2015. On December 15, 2020, the Board of County Commissioners (BOC) approved an extension of the existing vendor contract to December 31, 2023.

Why this Audit was Performed

The Hansen application is utilized by several program areas to support **major business functions and critical public services** provided by the County as indicated below. The Planning and Sustainability Department is the owner of the application data and approves user access to application data by other County departments.

Hansen application users include:

- Planning and Sustainability
 - Permits
 - Business and Alcohol License
 - Plan Review
 - Land Development
 - Long Range Planning
 - Inspections
 - Current Planning/Zoning
- Code Enforcement
- Geographic information system Department (GIS)
- Fire department
- Sanitation Division

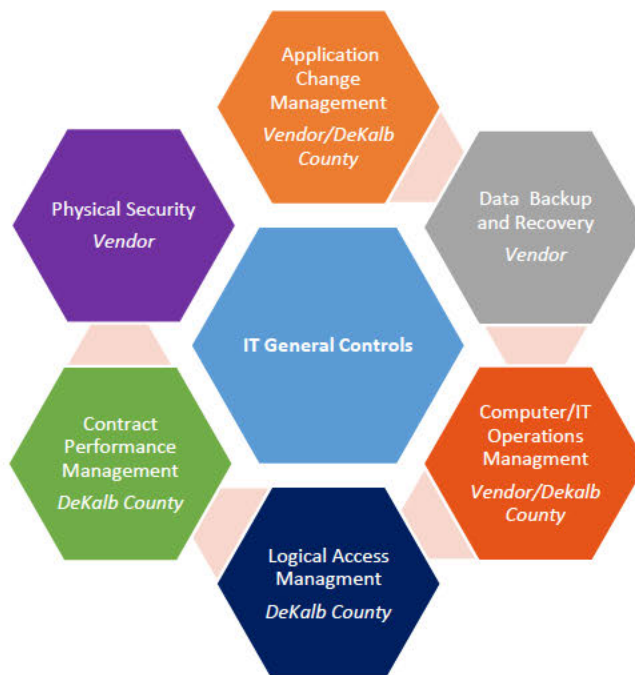
The provision of some of these services involves the collection, processing, and storage of sensitive Personal Identifiable Information (PII) such as Name, address, social security/tax number, email/phone number, insurance details, social media accounts, etc.

¹ [Infor Public Sector overview](#)



As with any application, there are Information Technology General Controls (ITGC) that are expected to be in place to ensure the integrity of the data and processes that the systems support. As a SaaS application, the primary responsibility for key ITGCs rests with the vendor (i.e., Change Management, Physical Security, Data Backup and Recovery, and Incident Management) while the County (i.e., the Planning and Sustainability department) is primarily responsible for User Access Management and Contract Performance Monitoring, while there is a shared responsibility among the vendor and the County for change management and incident management.

Figure 1: Hansen ITGC Responsibilities



This audit focused on the following ITGC components that the County has some responsibility to perform.

Logical access controls - The policies, procedures, organizational structure, and electronic access controls that are designed to restrict access to computer software and data files. The County has the sole responsibility of user access administration (i.e., granting, modifying, and disabling system access).

Application change management controls - The process that management uses to identify, document, and authorize changes to the Hansen Application. This control also involves the patch management process that considers identifying, testing, and applying code changes to fix bugs and close security vulnerabilities/gaps. The County is responsible for capturing and securing approvals for change requests, and testing



proposed changes prior to implementation, while the vendor is responsible for implementing authorized changes.

Computer/IT operation controls - Computer operation controls consist of various subcategories of controls that relate to the operation of IT systems. These controls check whether IT systems continue to operate as expected, such as log and Incident, and third-party service management. The County is responsible for reporting and tracking the application's operational incidents under the incident management process while the vendor is responsible for the timely resolution of reported incidents.

Contract Performance Management – The County relies on the third-party vendor to help keep the Hansen application operating effectively. The County is responsible for managing all interactions with the vendor to ensure that the vendor and County roles and responsibilities are defined and that the vendor is meeting performance expectations.

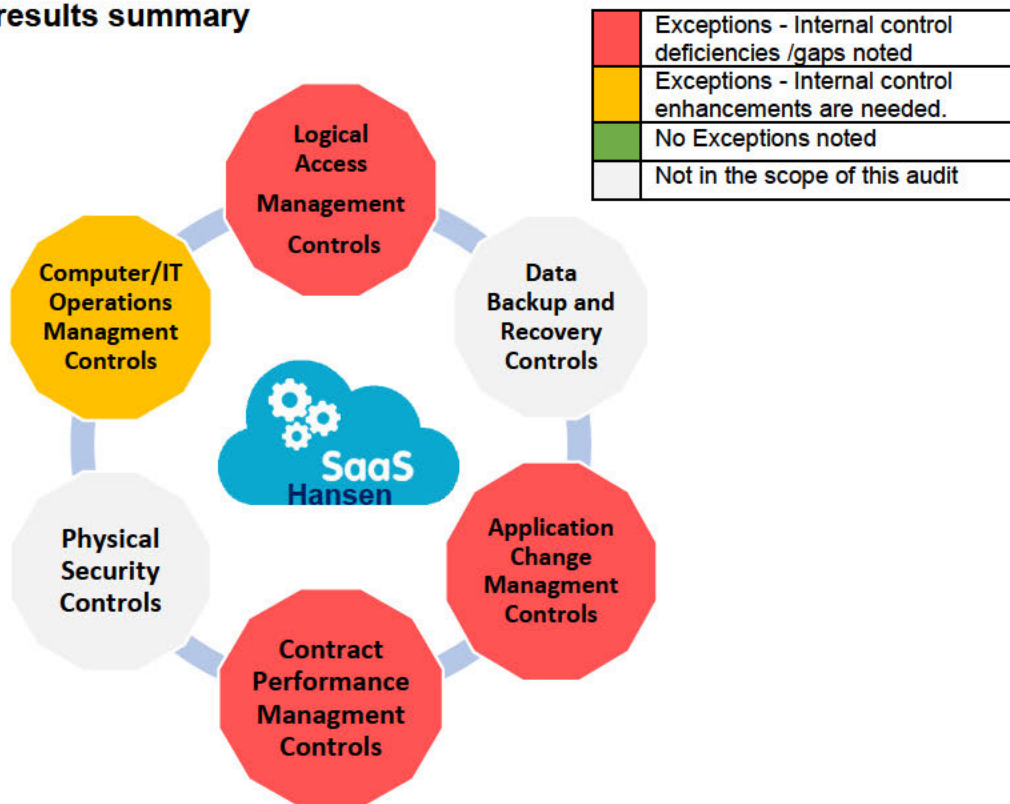
The other ITGC components, Data Backup, and Physical Security were excluded from the scope of this audit because the vendor has the responsibility to ensure the controls are designed and operate effectively and these controls were recently assessed by an independent auditor.



AUDIT RESULTS

As a Software as a Service (SaaS) application, the responsibility for most key ITGCs rests with the vendor (i.e. Change Management, Physical Security, Data Backup and Recovery, and Incident Management) while the County (i.e. the Planning and Sustainability department) is primarily responsible for User Access Management and Contract Performance Monitoring. The audit also identified control gaps between current practices and the documented County policies and information technology better practices and standards.

Figure 3: Audit results summary



Logical Access Management – Findings 1 - 5

Access management controls are primary controls that apply constraints on who (or what) can perform actions or access/view resources and data. They help minimize the security risk of unauthorized access to the application’s capabilities/functionalities and data. Typically, access controls have two key aspects, authentication, and authorization. Authentication verifies that a user confirms whom they say they are at the time access is requested while authorization determines if a particular user has the appropriate permissions to access or alter the data.



Effective access controls will also consider password procedures, such as password expiration, complexity, and role-based access, and have effective monitoring to help identify and correct inappropriate access on the Hansen application. Access requests should be reviewed and approved by the owners of the data (the Planning and Sustainability Department). Ineffective logical access controls expose the County to unauthorized access to data or computer networks, which can cause damage to the County in a number of ways. The unauthorized user may directly steal files, data, and sensitive information, or interrupt operations. This audit identified the following opportunities for strengthening logical access management controls.

FINDING 1: THE APPLICATION'S PASSWORD CONFIGURATION DOES NOT ALIGN WITH THE COUNTY'S PASSWORD POLICY.

During the audit, we reviewed the County Password Security Policy and determined that the password [REDACTED] on the Hansen application were not as required by the policy:

[REDACTED]

Inadequate password controls can expose the County to unauthorized access of data, fraud, or the interruption of services. [REDACTED]

[REDACTED]

Recommendation:

We recommend that Planning and Sustainability management coordinate with the application vendor to implement password parameters for the Hansen application that aligns with the County's "Password Security Policy" as it relates to password [REDACTED].

Management Response (Director, Planning and Sustainability):

<i>Management Agreement</i>	<i>Description of Management's Action Plan to Address Finding</i>	<i>Estimated Timeline to implement Action Plan</i>
<input checked="" type="checkbox"/> Agree <input type="checkbox"/> Disagree	Planning IT met with DeKalb IT and received the county password parameters, and those changes were incorporated into our test environment and it worked for new users. [REDACTED]	This should be completed by the 1 st quarter of 2023.
<p><i>Reason For Disagreement:</i></p>		



FINDING 2: EXISTENCE OF DORMANT USER ACCOUNTS ON THE HANSEN APPLICATION

During the audit, we reviewed enabled user accounts on the Hansen application and identified the existence of dormant accounts. We noted that some user accounts have not been used to log on to the Hansen application for as much as 212 months at the time of the audit. The details are:

■ [REDACTED]

Dormant accounts increase the risk of account takeover by unauthorized users and exploitation of the County’s information due to a data breach.

Recommendation:

We recommend that Planning and Sustainability management work with the DoIT management to:

- Establish a documented procedure for the determination and management of dormant accounts. The procedure should require the timely removal of accounts that have been deemed to be dormant (for 90 days or less).
- **Review the ■ dormant accounts identified by this audit and take immediate remedial action as necessary, ■**

Management Response (Director, Planning and Sustainability):

<i>Management Agreement</i>	<i>Description of Management’s Action Plan to Address Finding</i>	<i>Estimated Timeline to implement Action Plan</i>
<input checked="" type="checkbox"/> Agree <input type="checkbox"/> Disagree	Of the ■ records identified, ■ ■ ■ ■	We anticipate the end of January 2023 to clean up the remaining ■ accounts after reaching out to the different agencies. For the ■ accounts which are dormant because there are no licenses tied to these accounts and they can no longer access the system, we anticipate the end of the 2 nd quarter of 2023 to finish that cleanup, we have deemed these accounts lower priority as they cannot access the system. ■ ■ ■ ■ ■
<p><i>Reason For Disagreement:</i></p>		



FINDING 3: UNAUTHORIZED USER ACCESS TO THE HANSEN APPLICATION

During the audit, we reviewed the procedure for granting users access to the Hansen application. We also reviewed a sample of active user accounts and noted the following instances of unauthorized user accounts:

- Documented procedures for granting access to the application do not exist.
- For 8 of 8, 100% sample of new user accounts created during our period of January 2021 to December 2021, no documented evidence of user access request and authorization was provided.

We further reviewed the population of active application user accounts to determine if they were County employees. We determined that:

- 22 active user accounts **did not** belong to DeKalb County employees. The user account details were not found on both the list of all former County employees, or the list of active County employees provided by the Human Resources Department for the audit period.
 - 17 of these user accounts have application access privileges that enable them to add or modify records (i.e., business license roles).
 - 13 of these user accounts have been used to access the Hansen application. We were unable to determine what operations were executed under these user accounts.

Recommendation:

We recommend that Planning and Sustainability management:

- Establish a standard procedure for requesting access, authorizing access, and modifying user access to the Hansen application. The document should include but not be limited to procedures for the review/approval of user access requests based on job responsibilities, the frequency of ongoing user access reviews, key roles and responsibilities for application administrators and users, and should be consistent with applicable County standards and guidelines.
- **Review and disable the 22 user accounts for non-County employees that were identified during this audit.**
- Work with the application vendor and the DoIT to implement a process for authenticating application users against the County active network directory, to help ensure they are valid County employees.

Management Response (Director, Planning and Sustainability):

<i>Management Agreement</i>	<i>Description of Management's Action Plan to Address Finding</i>	<i>Estimated Timeline to implement Action Plan</i>
<input checked="" type="checkbox"/> Agree <input type="checkbox"/> Disagree	17 user accounts of the 22 listed were removed from the system. 8 of the accounts were for the Board of Health Division. Planning IT will be working with the DeKalb IT to come up with standard procedures for access and modification of access for users of the Hansen application. We plan to use our internal [REDACTED] system to help in that process as well.	1 st Quarter 2023 Jan-Feb timeline to document standard procedures for access.
<p><i>Reason For Disagreement:</i></p>		



FINDING 4: USERS ROLES AND PRIVILEGE ASSIGNMENTS NEED REVIEW

During the audit, we inquired from Planning and Sustainability and DoIT management about the application permissions assigned to each available role assigned to users of the Hansen application. We noted that there was no documentation or report to help determine if the available 38 application roles (See Appendix IV) were set up correctly to enhance the segregation of duty controls on the application access and usage. Additionally, we reviewed the application's active user accounts and found that some user accounts had all the user roles for specific application modules assigned to them, which increases the risk that conflicting roles are not adequately segregated. We noted the following:

- 24 out of 137 persons with access to the Planning (PLN) module were assigned **all** 5 roles available for that module, introducing the risk of these users starting and concluding a task without approval.
- 14 out of 28 persons were assigned to **all** 4 roles of the Fire Marshal (FM) module, which allows them to start and conclude a task.
- 39 out of 62 persons were assigned to **all** the 3 roles of the Cashier module, which allows them to start and conclude a transaction.
- 33 out of 134 persons were assigned **all** 8 roles under the Code Enforcement (CE) module, giving them the privilege to start and conclude a task without an independent review/approval.
- 38 persons with different job titles such as (customer care representative, crew worker, etc.) have a “Confidential” role that does not align with their job responsibilities. A role that can be used to review sensitive (PII) information of customers.

We also identified 12 active generic accounts and [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

A “generic account” ([REDACTED]) is any user account not tied to a specific employee by name, an account that is not enabled and disabled at the beginning and end of a specific user’s employment. Even in the absence of any malicious intent on the part of a former employee, there is the possibility of any generic login credentials getting leaked out the door of an organization. The risk of using a generic account across multiple users is that they lack the visibility, certainty, and accuracy about a particular session that singularly owned accounts have. Additionally, when users have permissions that are more than what they require to perform their job responsibility, they acquire unauthorized access to read or modify information without independent approval.

Recommendation:

We recommend the Planning and Sustainability management work with the vendor and the DoIT to do the following:



- Develop a procedure to periodically review and assign roles to help ensure user accounts roles are based on the employee’s assigned job responsibilities.
- Establish a formal user access matrix for guidance during user access grants and changes.
- Review and remove the generic accounts that are no longer required.

Management Response (Director, Planning and Sustainability):

<i>Management Agreement</i>	<i>Description of Management’s Action Plan to Address Finding</i>	<i>Estimated Timeline to implement Action Plan</i>
<input checked="" type="checkbox"/> Agree <input type="checkbox"/> Disagree	<p>Planning IT has discussed this with DeKalb IT and they will be working together to come up with a matrix for the Hansen users and do a cross-check against existing internal users to maintain appropriate levels of access.</p> <p>We are developing policies and procedures to include Manager’s approval.</p> <p>We looked at the provided list of 12 generic accounts and the following are system accounts:</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	Jan – Feb 2023
<p><i>Reason For Disagreement:</i></p>		

FINDING 5: SUPERUSER ROLE ASSIGNMENT NEEDS REVIEW

During the audit, we reviewed users with access to “superuser” roles in Hansen to ensure that access was appropriate per department and job title. A superuser role is a role that has more privileges than ordinary functional roles. The roles have access to elevated functionalities and might, for example, be able to modify application configurations or data/transaction logic, thereby enabling a user with a such role to start and conclude a transaction. There was a total of **17 users with the “superuser”** role and our review found the following:

- Four DoIT personnel had access to functional superuser roles built for the business process owners.



- Six persons' superuser roles did not align with their job responsibilities based on their job titles, an example of the job titles are zoning officers (3 employees), office assistant (1 employee), Permit technician (1 employee), Building and fire plans examiner (1 employee).


Recommendation:

We recommend that the Planning and Sustainability management collaborates with the vendor and DoIT to:

Establish a standard operating procedure for the review of users' access and Superuser role on the Hansen application modules. The procedure should outline the frequency, duration of the reviews, required information/report, criteria for review, the follow-up process, and the responsibilities of the various stakeholders.

Management Response (Director, Planning and Sustainability):

<i>Management Agreement</i>	<i>Description of Management's Action Plan to Address Finding</i>	<i>Estimated Timeline to implement Action Plan</i>
<input checked="" type="checkbox"/> Agree <input type="checkbox"/> Disagree	Planning took a look at the user's assigned Superuser access control and reduced that number from 17 to 6 users. In addition, Planning is working with DeKalb IT on SOP for the review of users with Superuser access	COMPLETED.
<i>Reason For Disagreement:</i>		

 **Computer/IT Operations: Logs and Incident.**

Computer/IT Operations controls include administrative monitoring procedures that help support optimal performance and security of applications. These include the periodic review of application activity logs and the effective management of application incidents.

Activity logs are a key monitoring control that involves a record of events and changes, typically regarding a sequence of activities or a specific activity. Most IT devices generate logs based on events. They capture events by recording who performed an activity, what was performed, and how the system responded. They are valuable to both the IT teams and the data owners in supporting oversight and verification of compliance with regulations. In addition, they support the monitoring of data and systems for the timely identification of security breaches or vulnerabilities and for rooting out internal data misuse.

An incident is an unplanned interruption to or quality reduction of an IT service. While **incident management** is the practice established to analyze, identify, and correct



application problems while taking actions that can prevent the future negative impact of incidents. Effective incident management involves understanding why issues happen through analysis, discerning roles, and responsibilities, developing a knowledge base, and gaining insights that can lead to better operations, fewer incidents, and faster resolutions. Currently, the County manages Hansen incidents on the DoIT helpdesk application.

Inadequate activity logging can result in unauthorized activities and breaches going undetected. Ineffective incident management can result in the untimely resolution of incidents which can impact the service operation.

FINDING 6: HANSEN AUDIT LOGS’ USE NEEDS OPTIMIZATION

During the audit, we determined that the application-level logs that are maintained captured only high-level events, [REDACTED]

[REDACTED] Additionally, the application-level logs are not periodically reviewed by Planning and Sustainability management to identify trends and insights that might indicate abnormal access and breaches.

Recommendation:

We recommend the Planning and Sustainability management work with the vendor and DoIT to:

- Establish guidelines to generate the logs of activities performed using privileged accounts ([REDACTED]) on the Hansen application.
- Establish a procedure and measure to ensure the logs are protected from unauthorized modification and periodically reviewed for insights.

Management Response (Director, Planning and Sustainability):

<i>Management Agreement</i>	<i>Description of Management’s Action Plan to Address Finding</i>	<i>Estimated Timeline to implement Action Plan</i>
<input checked="" type="checkbox"/> Agree <input type="checkbox"/> Disagree	[REDACTED]	We are looking into having this addressed or a plan in place by end of 1 st quarter of 2023. Infor resources will be engaged in quarter 2023.
<i>Reason For Disagreement:</i>		

FINDING 7: HANSEN INCIDENT TICKETS WERE NOT RESOLVED TIMELY.

During the audit, we reviewed the 47 open, on-hold, or in-progress incident tickets captured on the County DoIT Helpdesk application during the audit period. We determined



that the incidents on the DoIT Helpdesk application were not resolved timely. Details of our observations are:

- 5 of the 47 incident tickets reviewed, were incorrectly classified as Hansen tickets (i.e., they were not related to the Hansen application).
- For the remaining 42 Hansen-related incident tickets:
 - 35 of 42 incidents were either in "In-Progress", "On-hold" or "Open" status and were over the due date by 7 months and more as at the time of the audit.
 - 6 of 42 have not considered overdue because they were on-hold waiting for the requester's response.

Recommendation:

We recommend that the management of Planning and Sustainability:

- Collaborate with the DoIT management to establish a documented incident management process to help ensure Hansen tickets are resolved/closed timely based on established timelines, priorities, and severity/impact analysis.
- **Review the unresolved tickets identified during this audit and ensure they are resolved and closed out as necessary.**

Management Response (Director, Planning and Sustainability):

<i>Management Agreement</i>	<i>Description of Management's Action Plan to Address Finding</i>	<i>Estimated Timeline to implement Action Plan</i>
<input checked="" type="checkbox"/> Agree <input type="checkbox"/> Disagree	The DOIT tickets and Infor tickets were identified, and the majority were deemed to be items that could be closed out. We are working with DeKalb IT to be proactive to these requests when they come in and address them as needed.	COMPLETED
<i>Reason For Disagreement:</i>		

Contract Performance Management

Contract or third-party management is the process whereby entities, like the County, monitor and manage interactions with all external parties with which it has a relationship. The County relies on a third-party vendor to provide the Hansen software service and to help ensure the Hansen application operates effectively. If the vendor does not deliver on expectations, there can be devastating and long-lasting impacts on the County operations. The County also becomes vulnerable to risks as a result of sharing confidential, sensitive personal and business information with vendors. Thereby introducing cybersecurity, business continuity, privacy, geopolitical, reputational, and compliance risks to the organization. A robust third-party management that involves effective contract



management that clearly defines and establishes the terms and parameters of the services provided is required.

FINDING 8: CONTRACT MANAGEMENT PROCESSES NEED IMPROVEMENT.

Based on our review of the contract and service level agreement (SLA) and discussions with the County management, we determined that contract management responsibility was not defined, and key processes could be strengthened in the following areas:

Contract monitoring:- The County has not regularly requested and reviewed key contract monitoring information such as performance and availability (uptime) reports and Service Organization Control (SOC) 2 Independent Auditor's reports, which provide assurance about the suitability and effectiveness of the service provider's controls that are relevant to security, availability, processing integrity, confidentiality and/or privacy.

Contract renewal:- The contract renewal was completed at least 6 months after the expiration of the previous contract which expired in December 2020.

Contract Formation:- The following best practice provisions were not defined in the Service Level Agreement:

- Right to audit clause.
- Incident response time and incident prioritization level criteria.
- A requirement that Recovery Point Objective (RPO - The point in time to which data must be recovered after an outage) and Recovery Time Objective (RTO -): The maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources) aligns with the County's business objectives.
- A requirement that the data retention period aligned with applicable County retention schedules.
- Guarantees for protection and privacy of data processed or stored by service provider's subcontractors, such as Amazon Web Services, and data backup monitoring by vendors in India and the Philippines.

Recommendation:

We recommend that the Planning and Sustainability management should work with the:

- Purchasing and Contracting Department and Law Department to implement processes for effective management of the contract and ensure the contract addressed the gaps identified above.
- DoIT management to obtain and review the application performance availability reports for performance trend analysis and possible credit points.
- Vendor representative to ensure Planning and Sustainability obtains and reviews the periodic SOC2 Independent Auditor's reports in a timely manner.



Management Response (Director, Planning and Sustainability):

<i>Management Agreement</i>	<i>Description of Management's Action Plan to Address Finding</i>	<i>Estimated Timeline to implement Action Plan</i>
<input checked="" type="checkbox"/> Agree <input type="checkbox"/> Disagree	Planning and Sustainability will work with DeKalb IT, Purchasing, and Law to address the items identified in this audit.	End of January 2023
<i>Reason For Disagreement:</i>		



Application Change Management

The Information Technology (IT) landscape changes over time. Obsolete systems need to be replaced, while existing solutions require upgrades to address demanding business requests and requirements. IT needs to roll out new solutions to meet regulations. Application change management is a process designed to understand and minimize risks while making IT changes. Risks such as customer/supplier dissatisfaction, budget overruns, and loss of business hours. Application change management extends to patch management which involves identifying, testing, and applying code changes to fix bugs and close security vulnerabilities/gaps. The County's DoIT supports the Planning and Sustainability department in the change control process around the Hansen application with respect to identifying required change, capturing, and securing change request approvals while the vendor has the responsibility of analyzing and implementing the approved changes.

FINDING 9: THE HANSEN APPLICATION PATCH MANAGEMENT NEEDS IMPROVEMENT.

As of the time of the audit, we noted that the Hansen application has not been patched since April 2021. The vendor releases patches (bug fixes and new features) for the Hansen application every quarter, however, the latest installed patch on the application was the January 2021 patch. We determined the application was missing 5 (defect fixes, improvements, and new features) patches. Additionally, we noted that the vendor did not coordinate and notify the County of critical server security patches that need to be applied hence, the County Hansen administrators were unaware of the last time the critical server security patches were applied. Currently, the required patches have been applied as needed.

We also observed that the distribution list of personnel that receives email notifications about application patches and upgrades included unauthorized persons.

Recommendation:

We recommend the Planning and Sustainability management work with the vendor and DoIT to:



- **Remove invalid contact information identified by this audit from the current email distribution list for upgrade and patch information.**
- Establish a procedure for routine validation of the County contact list with the vendor.
- Establish agreements and procedures with the vendor of the Hansen application for the timely notification of required system patches based on the severity of a potential vulnerability if the flaw is publicly known and can be exploited.
- Develop benchmarks for the implementation of the patches within the County's time period of the release of the patches. The time period for updates should be based on factors that include the security category of the system, the criticality of the update (i.e., the severity of the vulnerability related to the discovered flaw), the County risk tolerance, or the prevalent threat environment.

Management Response (Director, Planning and Sustainability):

<i>Management Agreement</i>	<i>Description of Management's Action Plan to Address Finding</i>	<i>Estimated Timeline to implement Action Plan</i>
<input checked="" type="checkbox"/> Agree <input type="checkbox"/> Disagree	Engaging Infor Support to develop a patch and release management plan. We created a ticket with Infor Concierge for this request, awaiting a point of contact.	End of January 2023. DeKalb IT has disabled Portal access for the names identified and disabled notification of the names not apart of DeKalb or no longer active.
<i>Reason For Disagreement:</i>		



APPENDICES

Appendix I – Purpose, Scope, and Methodology

Purpose

The purpose of the audit was to evaluate the Information Technology General Controls related to the Infor Public Sector (Hansen) application and processes. Our focus was on current processes and IT general controls in place, including but not limited to application change management, logical Access, and vendor contract management.

Scope and Methodology:

The scope of our audit focused on the performance of Information Technology General Controls (ITGC) around the Infor (Hansen) application from January 1, 2021, through the present.

Our methodology included but was not limited to:

- Interview appropriate County personnel and external parties
- Research related best practices
- Select a sample for transactions for testing.
- Reviewing supporting documentation.



Appendix II – Management Response



404.371.2155 (o)
404.371.4556 (f)
DeKalbCountyGa.gov

178 Sams Street
Decatur, GA 30030

Chief Executive Officer
Michael Thurmond

DEPARTMENT OF PLANNING & SUSTAINABILITY

Interim Director
Cedric Hudson

January 12, 2023

Lavois Campbell
Chief Audit Executive
Office of Independent Internal Audit
1300 Commerce Drive, Suite 300
Decatur, Georgia 30030

RE: Management Response to “Hansen Information Technology General Control” Audit Report

Dear Mr. Campbell:

In accordance with DeKalb County, Georgia – Code of Ordinances / Organizational Act Section 10A- Independent Internal Audit, this is our response to the audit named above provided in this document. As required by the ordinance, our response includes 1) a statement regarding our agreement or disagreement along with reasons for any disagreement, 2) our plans for implementing solutions to issues identified, and 3) the timetable to complete such plans.

If you have any questions about this response, please contact Cedric Hudson, Interim Director Planning and Sustainability.

Sincerely,

Cedric Hudson _____

Cedric Hudson, Interim Director, Planning and Sustainability



Appendix III – Definitions and Abbreviations

Acronyms and Abbreviation

OIIA: Office of Independent Internal Audit

DoIT: Department of Innovation and Technology

ITGC: Information Technology General Controls

SaaS: Software as a Service

Key Definitions

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.

Authorization: Access privileges granted to a user, program, or process or the act of granting those privileges.

Logical Access Control System: An automated system that controls an individual's ability to access one or more computer system resources, such as a workstation, network, application, or database. A logical access control system requires the validation of an individual's identity through some mechanism, such as a PIN, card, biometric, or other tokens. It can assign different access privileges to different individuals depending on their roles and responsibilities in an organization.

Privileged User/Account: A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Security Control: The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.

Recovery Point Objective (RPO): The point in time to which data must be recovered after an outage.

Recovery Time Objective (RTO): The maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the maximum tolerable downtime.

Software as a Service (SaaS): is a software distribution model in which applications are delivered over the Internet—as a service or licensed on a subscription basis

and are centrally hosted. Instead of installing and maintaining software, you simply access it via the Internet, freeing yourself from complex software and hardware management.



Appendix IV – Application Roles

#	Role Name		
1	Ad Hoc Reports	19	CE Hearing
2	Admin	20	CE Inspector
3	BL Inspector	21	CE Reviewer
4	BL Reviewer	22	CE Supervisor
5	BL Supervisor	23	CE System Enquiry
6	BL Technician	24	Confidential
7	BLD Inspector	25	Customer Service
8	BLD Inspector Sup	26	FM Inspector
9	BLD Permit Tech	27	FM Intake
10	BLD Permit Tech Sup	28	FM Reviewer
11	BLD Reviewer	29	FM Supervisor
12	BLD Reviewer Sup	30	Land Develop Intake
13	Cashier	31	PLN Hearing
14	Cashier Manager	32	PLN Inspector
15	Cashier Supervisor	33	PLN Planning Intake
16	CE Building Case	34	PLN Reviewer
17	CE Case	35	PLN Supervisor
18	CE Customer Service	36	Report Development
		37	Super User
		38	System Inquiry



DISTRIBUTION

Action Official Distribution:

Cedric Hudson, Interim Director of Planning and Sustainability

Statutory Distribution:

Michael L. Thurmond, Chief Executive Officer

Zachary L. Williams, Chief Operating Officer/ Executive Assistant

Robert Patrick, Board of Commissioners District 1

Michelle Long Spears, Board of Commissioners District 2

Larry Johnson, Board of Commissioners District 3

Steve Bradshaw, Board of Commissioners District 4

Mereda Davis Johnson, Board of Commissioners District 5

Ted Terry, Board of Commissioners District 6

Lorraine Cochran-Johnson, Board of Commissioners District 7

Lisa Earls - Chairperson, Audit Oversight Committee

Gloria G. Gray , Vice-Chairperson, Audit Oversight Committee

Tanja Christine Boyd-Witherspoon, Pro-Tem, Audit Oversight Committee

Adrienne T. McMillion, Audit Oversight Committee

Harold Smith, Jr., Audit Oversight Committee

Information Distribution:

Zachary L. Williams, Chief Operating Officer/ Executive Assistant

Vivian Ernstes, County Attorney

La'Keitha D. Carlos, CEO's Chief of Staff

Kwasi K. Obeng, Chief of Staff, Board of Commissioners



PROJECT TEAM

This report was submitted by:

Rubby A. Ibe-Ikechi

Rubby A. Ibe-Ikechi, CISA, ISO/IEC 27001 LA
IT Audit Manager,
Office of Independent Internal Audit

01/25/2023

Date

This report was reviewed and approved by:

Lavois Campbell

Lavois Campbell, CISA, CIA, CFE, CGA-CPA
Chief Audit Executive
Office of Independent Internal Audit

1.25.2023

Date



STATEMENT OF ACCORDANCE

Statement of Accordance

The mission of DeKalb County is to make the priorities of the citizens of DeKalb County; the priorities of County government - by achieving a safer DeKalb, building stronger neighborhoods, creating a fiscally accountable and more efficient county government, and uniting the citizens of DeKalb County.

The mission of the Office of Independent Internal Audit is to provide independent, objective, insightful, nonpartisan assessment of the stewardship or performance of policies, programs, and operations in promoting efficiency, effectiveness, and integrity in DeKalb County.

This performance audit was prepared pursuant to DeKalb County, Georgia – Code Ordinances/Organizational Act Section 10A- Independent Internal Audit. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

This report is intended for the use of the agency to which it was disseminated and may contain information that is exempt from disclosure under applicable law. Do not release without prior coordination with the Office of Independent Internal Audit.

Please address inquiries regarding this report to the Office of Independent Internal Audit at 404-371-2765.