Public Records Request Application: Better support is needed to help the application sponsor address identity and access management controls

April 2026

Kristine Adams-Wannberg, CIA, CGAP, CFE

Washington County Auditor

You can obtain copies of this report by contacting us at:

Washington County Auditor's Office
221 S. First Ave, MS 31
Hillsboro, OR 97123-3901
(503) 846-8798
countyauditor@washingtoncountyor.gov

OR download and view an electronic copy at:
https://www.washingtoncountyor.gov/auditor

Do you have feedback on this audit report? Do you have ideas for how Washington County can better serve you and your community?

Please visit our feedback form below to submit your ideas on this report or topics you would like to see audited!

https://forms.co.washington.or.us/form/contact-the-auditor

Cover photo and icon images in the report are from Microsoft 365, unless otherwise noted.

Kristine Adams-Wannberg
Washington County Auditor

April 23, 2026

Dear Washington County Community Members:

This report contains the results of our audit of the County's public records application, focusing specifically on the identity and access management of the application. Identity and access management controls make sure the right people and devices have the right level of access for their job responsibility.

We examined how well the County manages the processes of who has access to that application, the users' abilities, and what happens when changes need to occur. These processes protect information against unauthorized access and abuse.

We found there were gaps in controls, and overall, the County's application sponsor needs more support to set up reasonable, appropriate controls. For example, roles and responsibilities are often unclear in the management of the application. Department user account management needs improvement, and authentication mechanisms need to align with regulations and strong industry practices.

We provide several recommendations to improve management of the application.

We appreciate the cooperation of the County Administrator's Office, the Information Technology Department, and the Sheriff's Office throughout the audit. We also want to express our appreciation to Mary Harshorn, Management Analyst II, in the County Administrator's Office for her collaborative work with our staff and great dedication to continuous improvement.

Thank you,

Kristine Adams-Wannberg, CIA, CGAP, CFE
Washington County Auditor

Office of the County Auditor
221S First Avenue, MS 31 · Hillsboro, OR 97123-3901
phone: (503) 846-8798 · e-mail: countyauditor@washingtoncountyor.gov
web: https://www.washingtoncountyor.gov/auditor

Report Highlights

Why this Audit is Important

The County has many cloud applications it uses to conduct its business. These applications can have information about County work as well as recipients of services.

Identity and access management controls make sure the right people and devices have the right level of access for their job responsibility.

As more cloud-based applications are used, strong identity and access management becomes critical for keeping County information safe.

What We Found

The County's public records application needs better support to help the application sponsor address identity and access management controls.

- Identity and access management roles, responsibilities, and processes are unclear and inconsistently performed.
- Department processes and user account management documentation need improvement.
- Application user roles and permissions are not well defined and assigned for job responsibilities.
- Authentication mechanisms are in place. Additional controls are needed to align with regulations and stronger industry practices.

What We Recommend

We make the following recommendations:

Access Controls

- Update Administrative Policy 203 and Procedures 203A.
- Update job descriptions.
- Update the Security Risk Acknowledgement form.
- When updated, sign the ITS Security Risk Acknowledgement form.
- Define who does what identity and access management responsibilities.

Identity Management	• Define identity management responsibilities. • Standardize identity management processes. • Improve visibility of user accounts. • Implement periodic account review. • Improve communication on employee changes.
Authorization Controls	• Define and document roles and permissions. • Establish role assignment criteria. • Restrict and justify privileged access. • Implement periodic role authorization reviews. • Document authorization change.
Authentication Controls	• Implement multi-factor authentication. • Update policies and procedures for password and multi-factor authentication requirements.

Table of Contents

Report Highlights 1

Background 5
- The County is the custodian of sensitive data 6
- The County is a customer of the cloud application, with responsibilities for identity and access management 6
- The identity and access management framework has several components 7
- The public records application touches many County departments 8

Finding 1: Identity and access management roles, responsibilities, and processes are unclear and inconsistently performed 9
- Management of the application is split between many departments 9
- Application sponsor security guidance is confusing 11
- Recommendations for Finding 1 13

Finding 2: Identity management processes and account management documentation need improvement 15
- Public records application user account management is largely decentralized and has limited documentation 15
- Public records application user accounts are often not managed 16
  - Many user accounts are old and unused 16
  - Most users surveyed did not know their role in the application and many were not aware they had access 17
  - Less than half of survey respondents reported receiving relevant training 18
- Lack of standard procedures causes inconsistent updates 19
- Recommendations for Finding 2 19

Finding 3: Application user roles and permissions are not well defined and consistently assigned based on job responsibilities 21
- Documentation of application roles and permissions is incomplete and inconsistent 22
- Some users have application powers beyond what they need for their jobs 23
- Role definitions were developed informally 24
- Recommendations for Finding 3 25

Finding 4: Authentication mechanisms are in place; additional controls are needed to align with regulations and stronger industry practices 26
- The basics are in place and should be made stronger 26
- Best practices have evolved, and the County should catch up 27
- Recommendations for Finding 4 28

Summary of Audit Recommendations and Assessment of Risk 29

Audit Objectives, Scope, and Methodology 34

Compliance with Audit Standards 37

Management Response to Audit Recommendations 38

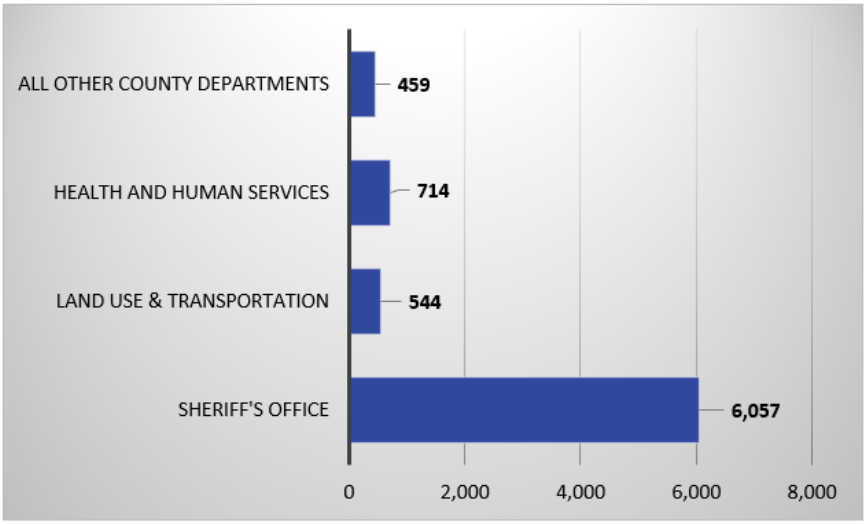
About the Washington County Auditor's Office 57

Background

The County has many computer applications it uses to conduct its business. These applications can have critical information about the County's work as well as recipients of services. It is important to determine how well the County manages who has access to those applications, users' abilities with those programs, and what happens when changes need to occur. Good controls protect information against unauthorized access and abuse.

The Auditor's Office reviewed identity and access management over the County's public records request application. This program manages intake of records requests, gathering and review of information, redaction (if needed), release of information to the requestor, and billing and payments. Over Fiscal Year (FY) 2024, the County opened and processed 7,774 public requests.

Figure 1: Total number of FY 2024 County public records requests by department



Source: County Administrative Office

The County is the custodian of sensitive data

The data stored in Washington County's public records applications contains sensitive information. This storage is regulated under various federal and state laws, such as:

- Criminal Justice Information
- Electronic Protected Health Information
- Federal Taxpayer Information

The County must design and implement effective safeguards to prevent unauthorized access. Failures in this area could result in serious consequences, including penalties, terminations of services, and criminal charges.

To navigate the complexities of Oregon and federal laws and ensure proper handling of records requests, the County developed, documented, and implemented the Public Records Requests Administrative Policy 203 and Procedures 203A. These help County employees in maintaining compliance and promoting transparency of public records requests while ensuring the protection of confidential information.

The County is a customer of the cloud application, with responsibilities for identity and access management

The County's public records software is a cloud application. It is hosted by an external provider, who plays a vital role in delivering the service. The arrangement is known as "Software as a Service" (SaaS). In a SaaS arrangement, the County is a customer and enters into contract with a provider. The contract outlines user rights, responsibilities, and compliance requirements of both the provider and the customer.

The provider established initial user roles, role training, and user activity audit logs for the County. However, it is the County's responsibility to ensure effective identity and access management. This involves implementing processes to reduce the risk of unauthorized access and to complying with laws designed to protect confidential data. It also includes the County's application sponsor completing a security risk acknowledgement which involves identifying risks and developing security controls to address these risks.

Mitigating risks is the process of developing and implementing strategies to reduce the potential negative impact or likelihood of threats (risks) down to an acceptable level.

The identity and access management framework has several components

Identity and Access Management (IAM) is a framework that combines policies, processes, and technologies to verify user identities and manage access. Key components of an effective IAM program include the following:

- Governance: Establishing and overseeing policies and processes that align with organizational goals.
- Access Control: Defining what resources users can access based on their needs.
- Identity Management: Keeping track of user accounts and roles to manage access efficiently.
- Authentication Controls: Implementing methods like passwords or biometrics to verify a user's identity.
- Authorization Controls**:** Ensuring users have the appropriate permissions for their roles.

- Monitoring Controls: Tracking user activities to identify any unusual or inappropriate behaviors.

By focusing on these areas, organizations can design and implement processes that protect their data from unauthorized access, ensure compliance with regulations, and protect themselves from security threats.

The public records application touches many County departments

The public records application involves each County department with records requests. Management of the application involves three key departments. The County's Administrative Office (CAO) is the application sponsor and oversees the application and its related policies for all County departments, apart from the Sheriff's Office. The CAO's office is also the primary contact for the platform, providing essential training and support. The Sheriff's Office manages the system specifically for that organization.

The County's Information Technology Services Department (ITS) also plays a critical role. It handles the technical responsibilities for application. This includes managing configurations and providing ongoing support to ensure the system operates effectively and securely. Together, these roles contribute to the smooth functioning and compliance of the application.

Configuration management makes sure an IT system (services, applications, network, etc.) is set up correctly, updates safely, and is tracked throughout its life cycle.

The initial estimates of the number of users the County's public records software would have when the application was initiated was 60 active users. As of March 2025, there were 539 active accounts.

Finding 1

Identity and access management roles, responsibilities, and processes are unclear and inconsistently performed

Information security standards[1] require organizations to establish access controls. This ensures users are granted and retain access only as appropriate for their job responsibilities. Effective access controls include clearly defined responsibilities for who is managing access and documented processes for granting and removing access. This includes periodic review of users and their access levels.

Access Controls is defining what resources users can access based on their needs.

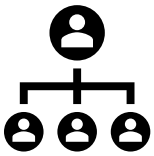
Management of the application is split between many departments

The County has administrative policies and procedures[2] to address records requests processes. These documents, however, do not address management of the records application. The County Administrative Office (CAO) is the application sponsor and is responsible, overall, for the application. The extent of these responsibilities, and the principles used to manage identity and access, are not well documented or consistently enforced by the CAO and the Sheriff's Office. The Information Technology Services (ITS) Department's role and responsibilities are also not clear, and there is some confusion between staff as to which department is responsible for what access management roles.

County departments have access to the records request application and a role in identity and access management for the application, although there is limited direction as to what that includes. The departments responsible for managing user account access developed a few documents. However, these do not establish a clearly defined or consistently

[1] This includes industry recognized information security standard such as the National Institute of Standards and Technology through the U.S. Department of Commerce and the Center for Internet Security (CIS) Critical Security Controls version 8.1 data regulations in federal law.
[2] County Public Records Request Administrative Policy 203 and Procedures 203A were adopted October 18, 2018, and in March 2024, Procedures 203A were reviewed and updated.

enforced access control process for this application. There are no documented requirements that departments periodically review their employee's user access to confirm that users' access remains appropriate, necessary, and authorized. Responsibility for reviewing access is not clearly assigned within departments, and no standardized process exists to verify that user access aligns with an individual's current job responsibilities or a department's business needs.



We found some departments had limited understanding of the different user roles in the records application. This was a result of obtaining a data set from the Department of Human Resources of all employees with an internal change that resulted in a new position or department for the period of March 11, 2024, through March 10, 2025. Using this data set, we joined it to the 539 active public records application user accounts. The results provided us with a list of 207 workforce members with active user accounts. From this, we judgmentally sampled higher risk users with greater access and capabilities to the application. We selected eleven user accounts with an internal position change based on role assignments to assess the following:

1) Application user access after the employment change was appropriate (authorized) based on the user's new job responsibilities.

2) The supervisor understood the user role assigned.

3) The assigned application role was required for the user's job responsibility.

Figure 2: Analysis of records system sample employee of employee job changes from March 11, 2024 to March 10, 2025

Response	1. Authorized Access	2. Supervisor Understands Role	3. Role was required for job responsibility
Yes	6	2	6
No	2	5	2
Unclear*	0	1	0
No Response	3	3	3
Total	11	11	11

* Supervisor response did not answer the question.

Source: Washington County Auditor's Office.

We found access was not consistently removed by the old department after the employee transferred to the new department. While some users may have continued to require access in their new position, many of the supervisors that responded did not understand the assigned roles, and two supervisors indicated familiarity with the user role granted in the records application.

Application sponsor security guidance is confusing

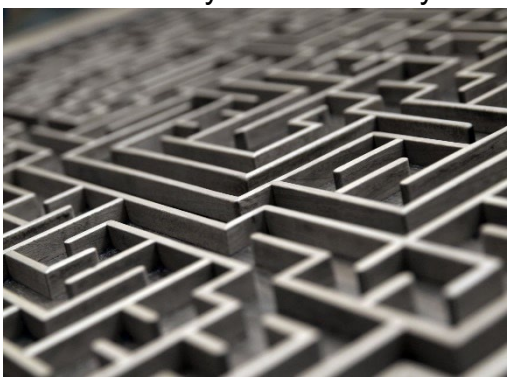
The County provides application sponsors with a Cloud Service Security Risk Acknowledgement form for SaaS applications. The document sets expectations for user management and risk mitigation, but those expectations are confusing, and the document does not include guidance, templates, or support defining how those requirements should be implemented or what access controls are required.

At the time of implementation, ITS had a Security Risk Acknowledgement Form Template. According to ITS, this was not a requirement when the public records application started implementation. Because of this, the security risk acknowledgement for the records application was not provided to the application sponsor and access control expectations were not formally documented.

Staff developed access management tasks for the application informally over time, relying on information passed down from previous employees or self-taught. ITS provides some documentation to address the technical aspects of access controls. It is not enough, however, to understand what is expected so that the tasks align with ITS policy and procedures.

In addition, the job descriptions for staff in the County Administrative Office and the Sheriff's Office do not include access management responsibilities. Staff who manage the application often perform these responsibilities without any training or identity and access management knowledge.

The issues occurred because the County has not clearly defined or consistently enforced who is responsible for managing user access to the records application. County Administrative Policy 203 is outdated and does not establish access control responsibilities for the application sponsor, ITS, or departments. In addition, while the County now requires completion of a security risk acknowledgement for SaaS applications, this was never completed at implementation, and the Security Risk Acknowledgement form lacks implementation guidance.



As a result, the County faces an increased risk that users may be granted or retain access that is not authorized or appropriate for their job responsibilities. Inadequate oversight and inconsistent access management processes can result in gaps in monitoring, delayed removal of access, and noncompliance with County policy and applicable laws and regulations governing public records. These conditions increase the likelihood of unauthorized access, data exposure and audit or regulatory findings which could undermine public trust and expose the County to operational, legal, and reputational risk.

Recommendations for Finding 1

Recommendation 1-1: Update Administrative Policy and Procedure

The County Administrator should update Administrative Policy 203 and Procedure 203A to define the identity and access management responsibilities for the records application sponsor, the Information Technology Services (ITS) Department, and other departments.

Recommendation 1-2: When updated, sign the ITS Security Risk Acknowledgement form

The County Administrator should sign and return the ITS Security Risk Acknowledgement form once it has been updated by ITS.

Recommendation 1-3: Update job descriptions

The County Administrator should request that the appropriate managers in the County Administrative Office and Sheriff's Office review and revise job descriptions for employees under their supervision to reflect any identity and access management responsibilities they might have within the organization's public records request cloud-based application. This should be done in coordination with the Human Resources Department's process for updating job descriptions.

Recommendation 1-4: Update the Security Risk Acknowledgement form

The County Administrator, through Information Technology Services, should update the Information Security Risk Acknowledgement form to require acknowledgment from the SaaS application sponsors and provide sufficient support, templates, and guidance for the sponsor.

Recommendation 1-5: Define who does what identity and access management responsibilities

The County Administrator, through Information Technology Services, should work with the County Administrative Office and Sheriff's Office to develop an agreed-upon role matrix

that clearly establishes accountability for different identity and access management responsibilities of the records application. This would include what aspects departments are responsible for managing.

Finding 2:

Identity management processes and account management documentation need improvement

Identity management controls help ensure user accounts are created, maintained, and removed in a timely and accurate manner throughout the user's employment with an organization. Identity and access management security controls require organizations to establish processes for managing user identities so that access is limited to current, authorized users and reflects changes in user employment status or job responsibilities. Effective identity management includes processes for onboarding users, updating access when roles change, and promptly removing access when it is no longer needed.

Public records application user account management is largely decentralized and has limited documentation

While the County Administrative Office (CAO) is the application sponsor, each department also has a role in managing their own public records application users. For example, when employees onboard, transfer between departments, or leave County employment, each department is responsible for the notifying Information Technology Services (ITS) Department using standard forms. There is no requirement, however, that user account access changes to the public records application are documented on the form and communicated to the CAO who is responsible for managing user accounts. There is an assumption in the County that departments are responsible for user access to applications, but there is no formal, documented requirement. As a result, changes in employment status are not consistently communicated and access removed.

Identity management is keeping track of user accounts and roles to manage access efficiently**.**

The County's ITS department processes employee terminations and transfers for County network and system access. The CAO, responsible for the majority of departments, rarely gets these updates. ITS considers its role limited to technical support and sees managing user accounts for the public records application as the responsibility of individual departments and the application sponsor.

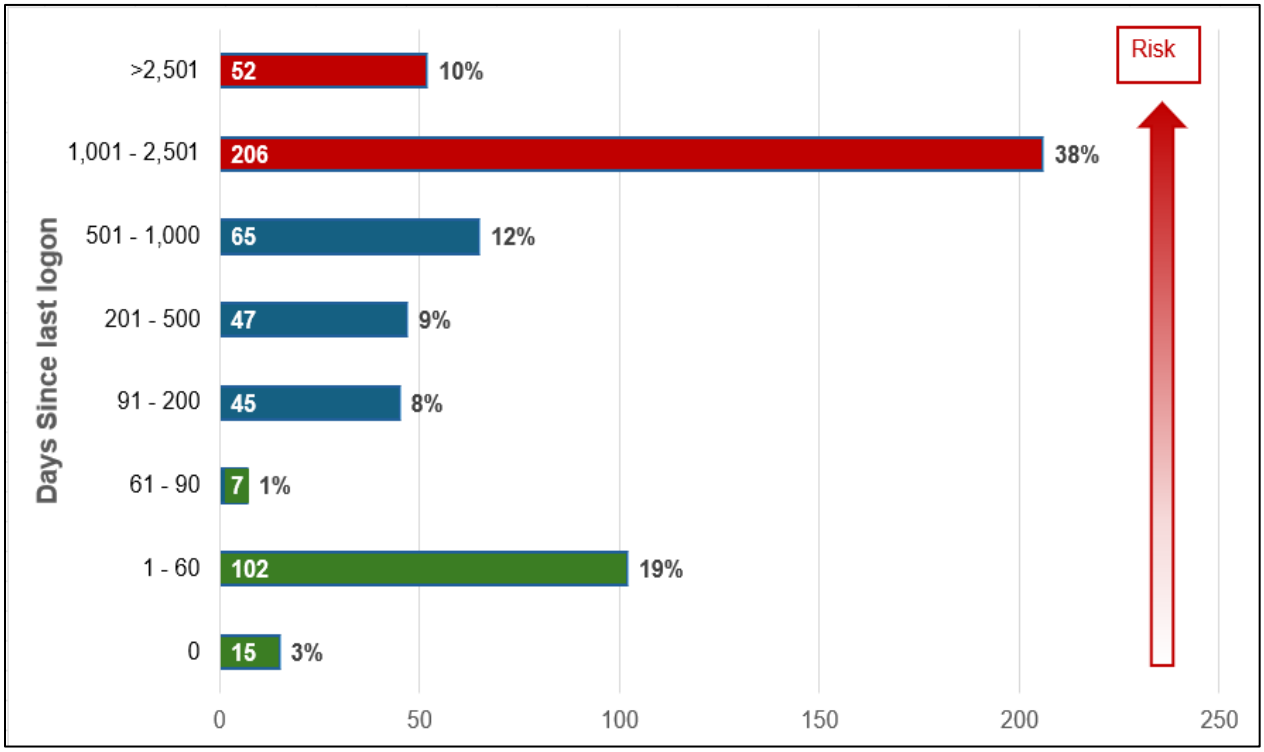
Public records application user accounts are often not managed

Many user accounts are old and unused

As part of the audit, we reviewed the 539 active user accounts in the application to determine whether user access was removed or disabled when it was no longer required. We performed this analysis to evaluate whether the accounts reflect current County employees and ongoing business needs.

We found a significant number of accounts were not adequately maintained. Of the 539 total accounts in the application, 52 accounts (10 percent) showed inactivity exceeding 2,501 days (almost 7 years). 258 accounts of the 539 total (48 percent) exceeded 1,001 days of inactivity. 415 accounts of the total 539 (77 percent) had not accessed the application for more than 90 days. These all surpass both the County 90-day and Center for Internet Security (CIS) 45-day recommended period of inactivity timeframes.

Figure 3: Analysis of dormant user accounts in public records application



Source: Washington County Auditor's Office

The CAO staff recently started limited account reviews.

Most users surveyed did not know their role in the application and many were not aware they had access

We surveyed 512 active public records application users using an updated data set as of July 10, 2025. Our goal was to assess whether users had equitable access to training[3] offered by the two departments assigned responsibility for managing training. It is important to note that County Administrative Office and Sheriff's Office each create their own training materials and platform for the application. Our audit

[3] Equitable Opportunity to train was defined for staff as having an opportunity to complete the training regardless of position, background, or work location. This includes having sufficient opportunity to access resources, sufficient time to train, support, and guidance.

did not include an evaluation of the training processes or documentation.

We gathered anonymous responses to eight questions from 220 users representing 21 County departments. We had a 43 percent response rate on the survey. The survey highlights gaps in user knowledge of their role, specifically:

- 74 percent of respondents did not know of their assigned user roles.
- 32 percent of respondents were unaware they were users of the records application.
- 60 percent of respondents reported receiving no training for their current user roles.

These results suggest a lack of communication and clarity to the user about their assigned role. This can lead to misinformation about their permissions and responsibilities, potentially resulting in errors and quality problems.

Less than half of survey respondents reported receiving relevant training

Of the 40 percent of respondents who reported receiving training we found:

- 57 percent felt they had equitable training opportunities.
- 67 percent found it relevant to their roles.
- 62 percent felt it helped them understand necessary laws and policies.
- 48 percent expressed satisfaction with the training and 43 percent remained neutral as to their satisfaction.

These results indicate gaps in training availability and opportunities which highlight the need for improvement

to ensure all users have equitable access to relevant role training.

Lack of standard procedures causes inconsistent updates

The County has limited assurance user accounts for the public records application reflect current need for access to the application and job responsibilities. As a result, accounts may remain active longer than necessary or may not be updated promptly. These conditions increase the risk of inappropriate access to public records information and make it more difficult for the County to demonstrate effective oversight of user access. Inconsistent identity management practices reduce operational efficiency and increase reliance on manual controls.

Recommendations for Finding 2

2-1 Define identity management responsibilities

The County Administrator should clearly define and document responsibilities for managing application user accounts, including account creation, modification, and removal.

2-2 Standardize identity management processes

The County Administrator should develop and implement standardized procedures for onboarding users, updating access when roles change, and removing access when it is no longer required.

2-3 Improve visibility of user accounts

The County Administrator should establish a method to maintain a complete and current record of application user accounts to support oversight and review.

2-4 Implement periodic account review

The County Administrator should establish and complete periodic reviews of user accounts to confirm all user accounts remain necessary and appropriate.

2-5 Improve communication on employee changes

The County Administrator, through Information Technology Services, should change the employee termination, onboarding, and transfers (user access change) forms to clearly notify departments of their responsibility to communicate user application access changes to the staff responsible for managing applications.

Finding 3:

Application user roles and permissions are not well defined and consistently assigned based on job responsibilities

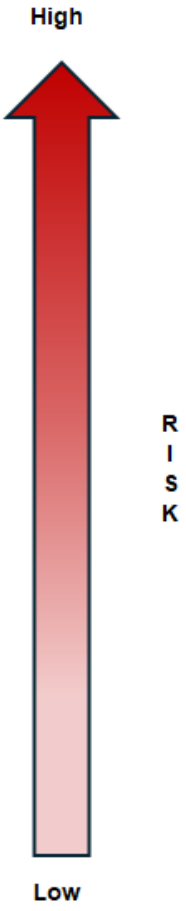
Authorization controls require that user role and permissions are granted based on their job responsibilities and the organization's business needs. The controls are based on the principle of "least privilege". This is the idea that each user should only have access to what they absolutely need in order to perform their job responsibilities, and no more. Federal information security standards require organizations to define and document application roles and associated permissions, restrict privileged access, and periodically review user authorizations to ensure that access remains appropriate. Effective authorization controls also require consistency in how roles and permissions are assigned and managed.

The County's public records application includes eight user roles with varying levels of access, including administrative and other highly privileged roles. These roles are designed based on the user's job responsibility and data they need to do their tasks. Some are described in the table below:

An **authorization control** is like having a security guard at the door who checks if you have the right permission to enter and do certain things inside.

Figure 4: Examples of some typical application roles, permissions, and access

User Role	Capabilities or Permissions	Access and Restrictions
System Administrator (Keys to the Kingdom)	**Permissions:** Manage all users, delete data, system configuration, audit logs, access control, data backup, security, training and support, reporting tools, etc.	**Access:** Full unrestricted access/control of the entire application. **Restrictions**: Few, if any restrictions.
Privileged* (Superuser-Manager)	**Permissions:** More than a power user. Sensitive data: access, modify, delete, export. Manage users: create, delete, modify, assign roles, etc. * often confused with system administrator	**Access**: Manage settings, data, or users within one specific module or application area. Access just enough for job without full system control. **Restrictions**: Limited to their designated function. Cannot change system wide settings.
Power (Gate Keeper)	**Permissions**: Review and approve end user work, access broader data or records, advanced reporting, assign and manage work.	**Access:** Basic access + elevated for job responsibilities. **Restrictions:** Cannot create, delete, or modify user accounts. No access to application settings.
End (Basic Access)	**Permissions:** View, create, edit their own data, enter data, process requests, and generate reports.	**Access:** Limited to day-to-day work within their permissions. Limited access to sensitive data. **Restrictions**: Cannot delete public records requests, change system settings, or access other user's data.



Source: Washington County Auditor's Office

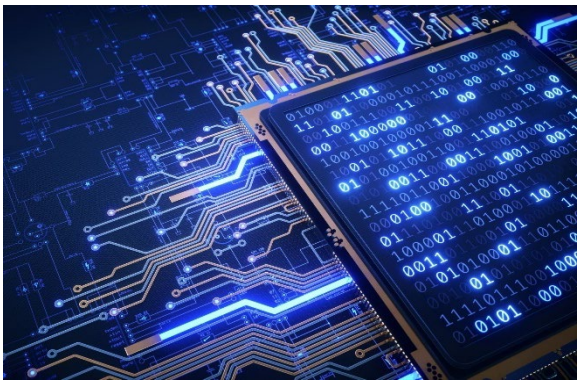
Documentation of application roles and permissions is incomplete and inconsistent

Documentation describing the different application roles and permissions is incomplete and inconsistent across managing departments. Existing documentation does not clearly describe what permissions are granted by each role, which roles are considered privileged or system administrators, and which job functions require specific roles.

Some users have application powers beyond what they need for their jobs

The County has not established clear or consistent authorization controls to ensure that roles and permissions assigned to users align with their job responsibilities. During the audit, we found some users were assigned roles that provided access beyond what was necessary for their job responsibilities. In some cases, users were assigned conflicting or overlapping permissions. There was also no evidence that authorization decisions were reviewed to confirm that assigned roles and permissions were appropriate and necessary.

We obtained a complete list of application users and found 539 active user accounts. Each user was assigned to one of the eight application roles. Three of the eight roles are designated as a different type of system administrator. We reviewed those roles because they are the highest risk to the County.



Administrative roles should be limited because they have a lot of power to change aspects of the application and the powers of the users that have access. We found eleven of the 539 active accounts, including the vendor, assigned to an administrator role.

Our review of the eleven system administrative users focused on whether the assigned role and permissions aligned to County documentation and job responsibilities. We found the majority of County users assigned the role of system administrator was excessive. Their job responsibilities did not require the level of access granted to them. They had conflicting permissions, nearly full access to the application, including full access to billing functions and aside from a restriction of bulk delete, full access to payment processes. This includes the ability to create, edit, and delete records. One of these system administrators had not logged onto their account in almost 600 days.

Figure 5: System administrator user review shows too many administrators

Role Review Results	Users
User job requires some level of elevated access, but not System Administrator role	2
System Administrator role is not appropriate and should be removed	6
User role is appropriate	3

Source: Washington County Auditor's Office

Role definitions were developed informally

The County has not formally defined or put in place authorization control standards. Responsibilities for defining roles in the application and assigning permissions, as well as reviewing role authorizations, were not clearly documented or enforced following system implementation. Knowledge of the application's authorization capabilities was limited to a small number of individuals. These were based on staff understanding, historical practices, or vendor interactions during implementation rather than documented system capabilities. Some staff left the County over time, and their role management responsibilities were transferred without sufficient documentation, training, or oversight for the next staff member.

As a result, the County cannot ensure that users consistently have access limited to what is necessary to perform their job responsibilities. Inconsistent or excessive permissions increase the risk of unauthorized access, inappropriate modification or disclosure of public records, and errors affecting data integrity. These conditions increase the risk of noncompliance with County policy and applicable laws and regulations and reduce the County's ability to detect or prevent misuse of system privileges.

Recommendations for Finding 3

Recommendation 3-1: Define and document roles and permissions

The County Administrator should develop and maintain clear documentation that defines public records application roles, associated permissions, and identifies which roles are considered privileged.

Recommendation 3-2: Establish role assignment criteria

The County Administrator should define criteria for assigning roles based on job function and business need to ensure permissions align with the principle of least privilege.

Recommendation 3-3: Restrict and justify privileged access

The County Administrator should limit assignment of administrative and highly privileged roles to users with a documented business justification.

Recommendation 3-4: Implement periodic role authorization reviews

The County Administrator should establish a documented process for periodically reviewing user roles and permissions to confirm continued appropriateness.

Recommendation 3-5: Document authorization changes

The County Administrator should require documentation of changes to user role descriptions, associated permissions, and role assignments.

Finding 4:

Authentication mechanisms are in place; additional controls are needed to align with regulations and stronger industry practices

Authentication controls verify the identity of users accessing systems and data. Information security standards and regulatory requirements require organizations to implement authentication mechanisms that align with the sensitivity of the data accessed. Confidential or regulated data need stronger authentication. Effective controls include strong password requirements, centralized authentication where feasible, and multi-factor authentication (MFA) for access to sensitive data or systems.

The basics are in place and should be made stronger

The County has implemented basic authentication mechanisms for the public records application, for example usernames and passwords and single sign-on (SSO).[4] These controls alone do not fully align with current regulatory requirements and stronger industry standards for systems that process sensitive public records data.

Authentication Controls are about implementing methods like passwords or biometrics to verify a user's identity.

Multi-factor authentication is not consistently enforced for application users. This includes users with elevated or administrative access and users accessing sensitive or restricted data. County password requirements also do not align with the County's adopted standards and evolving industry standards.

Multi-factor authentication is a security feature that adds an extra layer of protection by requiring two different forms of verification when logging into an account.

[4] Single Sign-On is an authentication mechanism that allows users to access multiple applications and websites using a single set of login credentials, such as a username and password.

The County has taken some steps to improve authentication controls in response to prior audit findings. However, changes to regulatory requirements, such as updates to the Criminal Justice Information Services security policy, were not fully incorporated into records application authentication requirements. As a result, the authentication controls for the application have not been updated to reflect current regulatory expectations.

Best practices have evolved, and the County should catch up

The issues identified occurred because authentication requirements for the application have not been formally reassessed as standards and best practices evolved. Information Technology Services policies governing multi-factor authentication (MFA) are inconsistent and the procedures are weak, lacking the clarity needed to enforce stronger controls on systems holding sensitive or regulated data. Despite procedures requiring stronger controls, such as MFA, it was never implemented. In addition, the County did not monitor regulatory changes which left authentication requirements for the records request application outdated.

Without appropriate authentication controls and consistent enforcement of stronger mechanisms, including MFA, the likelihood of unauthorized access, data exposure, and misuse of public records data increases. These conditions also increase the risk of noncompliance with applicable regulatory requirements, which could result in audit findings, sanctions, or reputational harm.

Recommendations for Finding 4

Recommendation 4-1: Implement multi-factor authentication

The County Administrator, through Information Technology Services, should require multi-factor authentication for all records request application users with access to regulated sensitive or restricted data.

Recommendation 4-2: Update policies and procedures for password and multi-factor authentication requirements

The County Administrator, through Information Technology Services, should update policies and procedures for passwords and multi-factor authentication to align with industry standards.

Summary of Audit Recommendations and Assessment of Risk

Based on our findings we make the following recommendations, and provide risk ratings based on our professional judgement:

Risk Rating	Description
Critical	Unacceptable Risk - Immediate Action required. Failure to implement this recommendation creates a high likelihood of unauthorized access to sensitive systems or data
High	Immediate Risk – Prompt Action Recommended. Failure increases the likelihood of inappropriate access, but may require an additional failure or misuse to result in material impact.
Medium	Process Improvement – Not Immediate Threat. Failure does not directly result in unauthorized access, but weakens the control environment.
Low	Efficiency / Administrative Improvement. Failure to implement has minimal impact on actual risk.

Recommendation 1-1: Update Administrative Policy and Procedure

Risk Rating	***Medium***

The County Administrator should update Administrative Policy 203 and Procedure 203A to define the identity and access management responsibilities for the records application sponsor, the Information Technology Services (ITS) Department, and other departments.

Recommendation 1-2: When updated, sign the Information Technology Services Security Risk Acknowledgement form

Risk Rating	***Low***

The County Administrator should sign and return ITS Security Risk Acknowledgement form once it has been updated by ITS.

Recommendation 1-3: Update job descriptions

Risk Rating	***Low***

The County Administrator should request that the appropriate managers in the County Administrative Office and Sheriff's Office review and revise job descriptions for employees under their supervision to reflect any identity and access management responsibilities they might have within the organization's public records request cloud-based application. This should be done in coordination with the Human Resources Department's process for updating job descriptions.

Recommendation 1-4: Update the Security Risk Acknowledgement form

Risk Rating	***Medium***

The County Administrator, through Information Technology Services, should update the Information Security Risk Acknowledgement form to require acknowledgment from the SaaS application sponsors and provide sufficient support, templates, and guidance for the application sponsor.

Recommendation 1-5: Define who does what identity and access management responsibilities

Risk Rating	***Medium***

The County Administrator, through Information Technology Services, should work with the County Administrative Office and Sheriff's Office to develop an agreed-upon role matrix that clearly establishes accountability for different identity and access management responsibilities of the records application. This would include what aspects departments are responsible for managing.

Recommendation 2-1: Define identity management responsibilities

Risk Rating	***Medium***

The County Administrator should clearly define and document responsibilities for managing the public records application user accounts, including account creation, modification, and removal.

Recommendation 2-2: Standardize identity management processes

Risk Rating	***High***

The County Administrator should develop and implement standardized procedures for onboarding users, updating access when roles change, and removing access when it is no longer required.

Recommendation 2-3: Improve visibility of user accounts

Risk Rating	High

The County Administrator should establish a method to maintain a complete and current record of application user accounts to support oversight and review.

Recommendation 2-4: Implement periodic account review

Risk Rating	Critical

The County Administrator should establish periodic reviews of user accounts to confirm accounts remain necessary and appropriate.

Recommendation 2-5: Improve communication on employee changes

Risk Rating	High

The County Administrator, through Information Technology Services, should change the ITS employee termination, onboarding, and transfers (user access change) forms to clearly notify departments of their responsibility to communicate user application access changes to the staff responsible for managing applications.

Recommendation 3-1: Define and document roles and permissions

Risk Rating	Medium

The County Administrator should develop and maintain clear documentation that defines public records application roles, associated permissions, and identifies which roles are considered privileged.

Recommendation 3-2: Establish role assignment criteria

Risk Rating	Medium

The County Administrator should define criteria for assigning roles based on job function and business need to ensure permissions align with the principle of least privilege.

Recommendation 3-3: Restrict and justify privileged access

Risk Rating	*Critical*

The County Administrator should limit assignment of administrative and highly privileged roles to users with a documented business justification.

Recommendation 3-4: Implement periodic role authorization reviews

Risk Rating	*High*

The County Administrator should establish a documented process for periodically reviewing user roles and permissions to confirm continued appropriateness.

Recommendation 3-5: Document authorization changes

Risk Rating	*High*

The County Administrator should require documentation of changes to user role descriptions, associated permissions, and role assignments.

Recommendation 4-1: Implement multi-factor authentication

Risk Rating	*Critical*

The County Administrator, though ITS, should require multi-factor authentication for all records request application users with access to regulated sensitive or restricted data.

Recommendation 4-2: Update policies and procedures for password and multi-factor authentication requirements

Risk Rating	*High*

The County Administrator, though ITS, should update policies and procedures for passwords and multi-factor authentication to align with industry standards.

Management’s response to these recommendations is included in a letter on page 38 of this document.

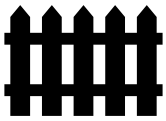
Audit Objectives, Scope, and Methodology

Objectives are the goals of the audit.

Objectives:

To evaluate the design and operating effectiveness of Washington County's public records application identity and access management controls.

Scope and Limitations:



Scope identifies the audit's boundaries.

Our review of identity and access management for the public records application focused on the County Administrative Office, Sheriff's Office, and the Information Technology Services Department. Specifically, we focused on policy and procedure governance, identity management, authentication mechanisms, authorization controls, and access controls for the period of March 11, 2024, through March 10, 2025. Data included all user accounts and various fields from the application under audit, human resources records, and the County's directory system. This audit did not include monitoring control which includes logging, log reviews, and incident handling.

Audit procedures included surveying users and their equitable access to training and awareness of their role in the public records application. The audit did not evaluate the content, completeness, or effectiveness of system training materials.

Methodology describes the work we did to achieve the audit objectives.

Methodology:

To accomplish our objectives, we:

- We identified criteria for the audit using Center for Internet Security (CIS) Critical Security Controls Version 8.1, August 2024 Safeguards 5 Account Management, Safeguard 6 Access Control, and limited Safeguard 3.3 Configure Data Access Control Lists. We used the CIS Password Policy Guide, December 2021, and the National Institute of Standards and Technology (NIST) Internal Report 8523, September 2025. We used Multi-Factor Authentication for Criminal Justice Information Systems Implementation Considerations for Protecting

Criminal Justice Information, and Criminal Justice Information Services (CJIS) Security Policy version 5.9.4 12/20/2023. Government Accountability Office (GAO) Standards for Internal Control in the Federal Government, September 2014 (Principle 11 Design Activities for the Information System) and the Government Auditing Standards 2018 Revision with Technical Update April 2021.

- Where the CIS Critical Security Controls Version 8.1 did not align for an application, we used; NIST Special Publication 800-53 revision 5, 12-10-2020 and GAO's Federal Information Systems Controls Audit Manual 2024 (FISCAM). For example, privileged accounts for the application would fall under FISCAM AC.02.04.01. The use of privileged accounts is restricted to individuals or processes with a legitimate need.

- We reviewed other audit identity and access management audits, memorandums, studies from federal, state, and local government, such as from GAO, the U.S. Office of Management and Budget, the Oregon Secretary of State, and the Metro Auditor's Office.

- We reviewed the legal requirements for County Public Records Requests as they relate to identity and access management. This review is included:
    - Oregon Revised Statutes 192 – Records, Public Reports and Meetings 2023 Edition and 2024 Session Law updates, and State of Oregon Department of Justice Attorney General's Public Records and Meetings Manual 2024.
    - County Administrative 203 Public Records Request Policy and 203A Administrative Procedure, department policies, procedures, guidance, trainings, and ITS knowledge base articles.
    - Public records application 2018 and 2022 contracts.

- We interviewed several Washington County staff from the County Administrative Office, Sheriff's Office, Information

Technology Services Department, and the Human Resources Department.

- We contacted multiple county department supervisors, managers, and in some cases application users to review and verify user information.

- We reviewed the vendor's application documentation and contacted the vendor for clarification on accounts, account processes, and best practices.

- We obtained and examined active user account data from the public records application, Human Resources' terminations, and change records, and ITS system of record user accounts.

- We reviewed Washington County's internal controls over identity and access management and identified the results of these controls in the audit. These controls focused on the control environment, control activities, monitoring, and information and communication.

- We surveyed all enabled application users using the County-approved Qualtrics application to assess whether the training for users was designed and implemented to ensure equitable training for all while complying with applicable laws and policies.

- Due to the sensitive nature of security and in accordance to ORS 192.345 (23) and Generally Accepted Government Auditing Standards, we wrote this report at a high level which prevents any possibility of disclosure of any sensitive or confidential information. Additionally, we communicated the extent of the security weaknesses verbally to agency management to ensure that no critical security information is publicly disclosed.

Compliance with Audit Standards

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.

April 20, 2026

Kristne Adams-Wannberg, County Auditor
Washington County Auditor's Office
221 S First Avenue
Hillsboro, OR 97123-
3901

Re: Public Records Request Application

Dear Ms. Adams-Wannberg,

This letter serves as the management response to the County Auditor's final draft audit report titled "Public Records Request Application: Beter support is needed to help the application sponsor address identity and access management controls." Although we don't agree with all of the audit's findings and recommendations, we appreciate that the intent of the audit report is to make the County's use of the cloud-based system better.

I would like to show appreciation for the staff in the County Administrative Office, Information Technology Services and Sheriff's Office who have worked with the Auditor's Office over the last several months gathering information, explaining process flows, hosting demonstrations and answering questions. The work of these employees allows Washington County to maintain compliance with Oregon public records laws in a secure manner and support the value the organization places on transparency and maintaining public trust. I would also like to acknowledge the work of the Washington County Auditor's Office in learning about the County's obligations under Oregon public records law, the employees who help facilitate thousands of responses to public records requests each year and the intricacies of the web-based system that makes the process run more smoothly.

There are some good suggestions for improving the secure use of data and the roles of those operating the system, however the audit does not provide the full context nor express a meaningful understanding of the primary purpose of this particular cloud-based tool. Unlike many technological solutions that aid Washington County in *protecting* information from release, the public records request system that is the subject of this audit is designed to securely *release* information requested by the public in compliance with state law. Prior to the implementation of the current cloud-based system, public records requests were made by sending email or using forms that were often completed by hand. Documenting requests, cost estimation, invoicing, records gathering and the transmission of responsive records were all steps in a statutorily driven process that the County handled without a centralized tool. The advent of technology has accelerated the County's efficiency and effectiveness in an era when online access is preferred by the public. Washington County's safe use of the current web-based tool is a vast improvement over our approach in the past.

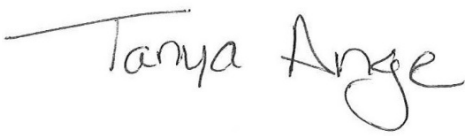
It is also important to note that Oregon's public records laws, while allowing an important view into the workings of local government, are also an underfunded state mandate. Despite cloud-based tools that assist in the process and the ability to seek cost reimbursement from requesters, significant costs in responding to public records requests are unreimbursed and therefore borne by the taxpayer-funded County government. What's more, most employees handling records requests do so *in addition* to other duties and tasks required of them in service to the public. Any additional requirements made of employees, including those recommended by this audit, should be viewed through such a lens.

Finally, I'd like to acknowledge the support of the Board of County Commissioners in recognizing this context, especially as it relates to the use of scarce public resources, the environment of increasing state and federal requirements on local governments and the substantial workload of County employees.

The remainder of this letter includes more detailed staff responses to each of the findings and recommendations contained in the audit report.

Please contact me or Assistant County Administrator Ann Ober at 503-846-8586 with any questions.

Sincerely,



Tanya Ange, ICMA-CM
County Administrator

Finding 1: Identity and access management roles, responsibilities, and processes are unclear and inconsistently performed	
Narrative response: Administrative Policy 203 and Procedure 203A provide the County with a basic approach for complying with Oregon law for responding to records requests as mandated under ORS Chapter 192. The law and this policy framework govern the County's response, regardless of what tools are used. Indeed, the law does not require that requesters use any system or application to make records requests, only that they be made to a local government in writing (ORS 192.324(1)).	
Finding 1 Recommendations	**Management Response**
Recommendation 1-1: Update Administrative Policy and Procedure The County Administrator should update Administrative Policy 203 and Procedure 203A to define the identity and access management responsibilities for the records application sponsor, the Information Technology Services (ITS) Department, and other departments.	**Agree/disagree; management approach described below:** Agree and disagree Management agrees that Administrative Policy 203 and Procedure 203A should be reviewed and updated periodically to maintain compliance with the legal framework for responding to public records requests. Nonetheless, the heart of this recommendation seeks to "define the identity and access management responsibilities for the records application sponsor." This goal can be best achieved without making explicit references to a specific application, but instead by developing and updating user manuals and training that directly refer to the County's current application. Such an approach would allow for the unique use cases experienced by the Sheriff's Office versus the remaining parts of the County organization. Notably, ITS has already updated Administrative Policy 606 Cloud Service and Administrative Policy 609 Data Governance to clarify roles and responsibilities as recommended. Management intends to continue pursuing

	this approach so long as resources are available to support it. **Target timeline to complete management-identified implementation activities:** Within 18 months, assuming available resources **Additional comments:** **Contact:** Destiny Fogarty-Olivas, Information Security Officer, ITS for ITS Policy Update status
Recommendation 1-2: When updated, sign the ITS Security Risk Acknowledgment form The County Administrator should sign and return the ITS Security Risk Acknowledgment form once it has been updated by ITS.	**Agree/disagree; management approach described below:** Agree ITS is in the process of updating the cloud service sponsors and data owners for all cloud-based services that are known to be used by the County. This updated Cloud Service Sponsor Acknowledgment form will be sent to all sponsors and data owners for approval. Since the application that is the subject of this audit is a cloud service known to ITS, the revised acknowledgment will be part of this effort. **Target timeline to complete management-identified implementation activities:** Within eight months, assuming available resources **Additional comments:** **Contact:** Destiny Fogarty-Olivas, Information Security Officer, ITS

Recommendation 1-3: Update job descriptions The County Administrator should request that the appropriate managers in the County Administrative Office and Sheriff's Office review and revise job descriptions for employees under their supervision to reflect any identity and access management responsibilities they might have within the organization's public records request cloud-based application. This should be done in coordination with the Human Resources Department's process for updating job descriptions.	**Agree/disagree; management approach described below** Agree This process, led by the Human Resources Department, places responsibility on managers and supervisors to produce accurate job descriptions for submission to HR. The effort began in 2024-25, in alignment with the County's launch of the Workday enterprise resource planning tool. These job descriptions have not yet been officially approved by the County, however. Additional work will be required in alignment with HR's Classification and Compensation project. Management intends to implement this recommendation in a manner that is consistent with the organization-wide Classification and Compensation project. As management understands this recommendation, the review would involve fewer than a dozen employees, some of whom already have a reference to public records requests in their job descriptions. Job descriptions should not be the sole basis for access management. **Target timeline to complete management-identified implementation activities:** Within 24 months, assuming available resources **Additional comments:** **Contact:** Philip Bransford, Communications Officer, County Administrative Office
Recommendation 1-4: Update the Security Risk Acknowledgment form	**Agree/disagree; management approach described below:**

The County Administrator, through Information Technology Services, should update the Information Security Risk Acknowledgment form to require acknowledgment from the SaaS application sponsors and provide sufficient support, templates, and guidance for the sponsor.	Agree The Information Security Risk Acknowledgment form should be updated to align with the roles and responsibilities described in Administrative Policy 606, Cloud Service, and Administrative Policy 609, Data Governance, and the accompanying procedures. The updated form would provide a less technical description of the roles and responsibilities of a Cloud Service Owner. **Target timeline to complete management-identified implementation activities:** Within 12 months, assuming available resources **Additional comments:** **Contact:** Destiny Fogarty-Olivas, Information Security Officer, ITS
Recommendation 1-5: Define who does what identity and access management responsibilities The County Administrator, through Information Technology Services, should work with the County Administrative Office and Sheriff's Office to develop an agreed-upon role matrix that clearly establishes accountability for different identity and access management responsibilities of the records application. This would include what aspects departments are responsible for managing.	**Agree/disagree; management approach described below:** Agree Administrative Policy 606 Cloud Service and Administrative Policy 609 Data Governance and accompanying procedures describe roles and responsibilities for Cloud Service Sponsors/Data Owners. Should the roles described in these policies differ from those for maintaining a cloud-based application, such as the one that is the subject of this audit, a responsibility matrix should be drafted so that all parties are clear on their responsibilities. Such a matrix should be included in an updated application manual supported by additional training. This

	approach would require sufficient resources and ime to implement. **Target timeline to complete management-identified implementation activities:** Within 18 months, assuming available resources **Additional comments:** **Contacts:** Philip Bransford, Communications Officer, County Administrative Office Cassaundra Sorensen, Records and Evidence Manager, Washington County Sheriff's Office

Finding 2: Identity management processes and account management documentation need improvement
Narrative response: A larger context is needed to fully understand the County's use of its public records request application. First, the records generated by any County employee are potentially subject to release through a public records request under Oregon law (ORS Chapter 192, among other provisions). In addition, Oregon public records law allows local governments to seek reimbursement from requesters for the "actual cost of making public records available, including costs for summarizing, compiling or tailoring the public records, either in organization or media, to meet the request" (ORS 192.324(4)(a)). Indeed, Oregon records law *requires* that the County seek the permission of requesters to proceed with gathering responsive records if the estimated costs of doing so would exceed $25 (ORS 192.324(4)(c)). Within this legal framework, Washington County seeks to balance transparency with minimizing "impact on County workload and resources" when responding to requests (Washington County Administrative Policy 203: Public Records Request). Complying with this combination of legal and policy requirements is challenging no mater how a local government approaches it, but doing so without a centralized, widely accessible

application would make compliance even more difficult. Such a tool would ideally have features such as:

1. Allowing access by *every employee in the entire organization* should their records be subject to a request;
2. Providing a method for calculating cost estimates for reimbursement of *any* employee's time gathering and preparing responsive records; and
3. Creating an interface with requesters whereby they can easily make requests, approve or reject cost estimates and ultimately receive the records they are seeking from their local government.

Washington County's application supports all three of these critical features in a secure environment for both employees and members of the public. It does so by allowing every employee to become a user, both to upload responsive records and to estimate their labor time based on the scope of each request.

Finally, management considers the risk environment for using this application to be low as a matter of course because:

1. Only current employees may access the system through their existing, secured and active network accounts;
2. Employees tasked with organizing responses to records requests are trained in their responsibilities within the system and tend to be the most knowledgeable people in the organization regarding the protected nature of data within their specific service areas; and
3. The data moving through the application is, by design, destined for release to members of the public, overwhelmingly without need for redaction.

Although the intent behind this audit finding is well taken, the emphasis on data security risks seems exaggerated, and the remedies called for are burdensome for staff already tasked with other priorities beyond public records requests.

Finding 2 Recommendations	**Management Response**
2-1 Define identity management responsibilities The County Administrator should clearly define and document responsibilities for managing application user accounts,	**Agree/disagree; management approach described below:** Agree Management intends to implement this recommendation through an updated

including account creation, modification, and removal.	application manual, additional training and improved communication between CAO and departments. This approach would require sufficient resources and time to implement. **Target timeline to complete management-identified implementation activities:** Within 18 months, assuming available resources **Additional comments:** **Contacts:** Philip Bransford, Communications Officer, County Administrative Office Cassaundra Sorensen, Records and Evidence Manager, Washington County Sheriff's Office
2-2 Standardize identity management processes The County Administrator should develop and implement standardized procedures for onboarding users, updating access when roles change, and removing access when it is no longer required.	**Agree/disagree; management approach described below:** Agree and disagree As mentioned in response to the prior recommendation, management intends to implement this recommendation through an updated application manual, additional training and improved communication between CAO and departments. In addition, ITS will begin issuing a weekly notification email to system administrators, including those supporting the application that is the subject of this audit, that lists terminated employees and employees who appear to have changed departments or divisions in the last 10 days. This approach would require sufficient resources and time to implement.

	As outlined in the response to recommendation 2-5 below, we respectfully disagree with the audit's characterization of risk as being "high." **Target timeline to complete management-identified implementation activities:** Weekly emails from ITS to system administrators will begin immediately. Updated user manual and additional training will be implemented within 18 months, assuming available resources. **Additional comments:** **Contacts:** Philip Bransford, Communications Officer, County Administrative Office Cassaundra Sorensen, Records and Evidence Manager, Washington County Sheriff's Office
2-3 Improve visibility of user accounts The County Administrator should establish a method to maintain a complete and current record of application user accounts to support oversight and review.	**Agree/disagree; management approach described below:** Agree and disagree As mentioned in response to prior recommendations, this recommendation can be implemented with improved user guidance, training and the weekly communication about employee status from ITS to system administrators. As outlined in the response to recommendation 2-5 below, we respectfully

	disagree with the audit's characterization of risk as being "high." **Target timeline to complete management-identified implementation activities:** Weekly emails from ITS to system administrators will begin immediately. Updated user manual and additional training will be implemented within 18 months, assuming available resources. **Additional comments:** **Contacts:** Philip Bransford, Communications Officer, County Administrative Office Cassaundra Sorensen, Records and Evidence Manager, Washington County Sheriff's Office
2-4 Implement periodic account review The County Administrator should establish and complete periodic reviews of user accounts to confirm all user accounts remain necessary and appropriate.	**Agree/disagree; management approach described below:** Agree and disagree As mentioned in response to the prior recommendations, this recommendation can be implemented with improved user guidance, training and the weekly communication about employee status from ITS to system administrators. As outlined in the response to recommendation 2-5 below, we respectfully disagree with the audit's characterization of risk as being "critical." **Target timeline to complete management-identified implementation activities:**

	Weekly emails from ITS to system administrators will begin immediately. Updated user manual and additional training will be implemented within 18 months, assuming available resources. **Additional comments:** **Contacts:** Philip Bransford, Communications Officer, County Administrative Office Cassaundra Sorensen, Records and Evidence Manager, Washington County Sheriff's Office
2-5 Improve communication on employee changes The County Administrator, through Information Technology Services, should change the employee termination, onboarding, and transfers (user access change) forms to clearly notify departments of their responsibility to communicate user application access changes to the staff responsible for managing applications.	**Agree/disagree; management approach described below:** Agree and disagree As mentioned in response to the prior recommendations, this recommendation can be implemented with improved user guidance, training and the weekly communication about employee status from ITS to system administrators.. Management respectfully disagrees with the audit's characterization of this issue as "high" risk. While there may be brief timing gaps when an employee transfers departments and their Public Records Request access has not yet been updated, the practical impact of this scenario is limited. In such cases, the only potential exposure is that an employee might temporarily view public records requests for a department other than the one to which they have transferred. No broader systems,

	sensitive data, or County resources are placed at risk. In addition, strong compensating controls æ already in place. The onboarding process is fully managed through established ITS procedures, ensuring that network access is disabled upon an employee's separation from the County. Because access to the public records response application requires authentication through Active Directory Federation Services (ADFS), former employees cannot access the application unless they have active County network credentials. This integrated process ensures that onboarded individuals cannot access the application. Together, these controls, ADFS restricting access to active workforce members, ADFS gatekeeping access to the application and ITS' tightly controlled off-boarding process, significantly mitigate the risk and reduce the likelihood of inappropriate access. **Target timeline to complete management-identified implementation activities:** Weekly emails from ITS to system administrators will begin immediately. Updated user manual and additional training will be implemented within 18 months, assuming available resources. **Additional comments:**

	Contacts: Philip Bransford, Communications Officer, County Administrative Office Cassaundra Sorensen, Records and Evidence Manager, Washington County Sheriff's Office

Finding 3: Application user roles and permissions are not well defined and consistently assigned based on job responsibilities	
Narrative response: With the exception of the characterization of "high" and "critical" data security levels, management agrees with this finding in the context of continuous improvement. As mentioned in response to prior findings, it is important to recognize and appreciate the efforts of staff already committed to ensuring role clarity, training and system support.	
Finding 3 Recommendations	**Management Response**
Recommendation 3-1: Define and document roles and permissions The County Administrator should develop and maintain clear documentation that defines public records application roles, associated permissions, and identifies which roles are considered privileged.	**Agree/disagree; management approach described below:** Agree As mentioned in response to the prior recommendation, management intends to implement this recommendation through an updated application manual, additional training and improved communication between CAO and departments. This approach would require sufficient resources and time to implement. **Target timeline to complete management-identified implementation activities:**

	Within 18 months, assuming available resources **Additional comments:** **Contacts:** Philip Bransford, Communications Officer, County Administrative Office Cassaundra Sorensen, Records and Evidence Manager, Washington County Sheriff's Office
Recommendation 3-2: Establish role assignment criteria The County Administrator should define criteria for assigning roles based on job function and business need to ensure permissions align with the principle of least privilege.	**Agree/disagree; management approach described below:** Agree As mentioned in response to the prior recommendation, management intends to implement this recommendation through an updated application manual, additional training and improved communication between CAO and departments. This approach would require sufficient resources and time to implement. **Target timeline to complete management-identified implementation activities:** Within 18 months, assuming available resources **Additional comments:** **Contacts:** Philip Bransford, Communications Officer, County Administrative Office

	Cassaundra Sorensen, Records and Evidence Manager, Washington County Sheriff's Office
Recommendation 3-3: Restrict and justify privileged access The County Administrator should limit assignment of administrative and highly privileged roles to users with a documented business justification.	**Agree/disagree; management approach described below:** Agree and disagree As mentioned in response to the prior recommendation, management intends to implement this recommendation through an updated application manual, additional training and improved communication between CAO and departments. This approach would require sufficient resources and time to implement. We respectfully disagree with the characterization of risk as being "critical." **Target timeline to complete management-identified implementation activities:** Within 18 months, assuming available resources **Additional comments:** **Contacts:** Philip Bransford, Communications Officer, County Administrative Office Cassaundra Sorensen, Records and Evidence Manager, Washington County Sheriff's Office
Recommendation 3-4: Implement periodic role authorization reviews The County Administrator should establish a documented process for periodically	**Agree/disagree; management approach described below:** Agree and disagree Management intends to implement this recommendation through an updated

reviewing user roles and permissions to confirm continued appropriateness.	application manual, additional training and improved communication between CAO and departments. This approach would require sufficient resources and time to implement. We respectfully disagree with the characterization of risk as being "high." **Target timeline to complete management-identified implementation activities:** Within 18 months, assuming available resources **Additional comments:** **Contacts:** Philip Bransford, Communications Officer, County Administrative Office Cassaundra Sorensen, Records and Evidence Manager, Washington County Sheriff's Office
Recommendation 3-5: Document authorization changes The County Administrator should require documentation of changes to user role descriptions, associated permissions, and role assignments.	**Agree/disagree; management approach described below:** Agree As mentioned in response to the prior recommendations, management intends to periodically review user role descriptions, permissions and assignments. This recommendation can be implemented through an updated application manual, additional training and improved communication between CAO and departments. This approach would take training resources on the part of CAO and departments to implement.

	Target timeline to complete management-identified implementation activities: Within 18 months, assuming available resources **Additional comments:** **Contacts:** Philip Bransford, Communications Officer, County Administrative Office Cassaundra Sorensen, Records and Evidence Manager, Washington County Sheriff's Office

Finding 4: Authentication mechanisms are in place; additional controls are needed to align with regulations and stronger industry practices	
Narrative response: Implementation of recommendations under this finding in the audit involves the County's approach to maintaining a secure technology environment. Because of this context, management is applying the exemptions in Oregon's public records laws (ORS 192.345(23)(c) and ORS 192.355(33)(c)) and management's response will be transmitted to the Auditor's Office confidentially.	
Finding 4 Recommendations	**Management Response**
Recommendation 4-1: Implement multi-factor authentication The County Administrator, through Information Technology Services, should require multi-factor authentication for all	**Agree/disagree; management approach described below:** Management's response is exempt under (ORS 192.345(23)(c) and ORS 192.355(33)(c)

records request application users with access to regulated sensitive or restricted data.	**Target timeline to complete management-identified implementation activities**: Within 18 months, assuming available resources **Additional comments:** **Contacts:** Wayne Flynn, Enterprise Systems Division Manager, ITS
Recommendation 4-2: Update policies and procedures for password and multifactor authentication requirements The County Administrator, through Information Technology Services, should update policies and procedures for passwords and multifactor authentication to align with industry standards.	**Agree/disagree; management approach described below:** Management's response is exempt under (ORS 192.345(23)(c) and ORS 192.355(33)(c) **Target timeline to complete management-identified implementation activities:** Within nine months, assuming available resources **Additional comments:** **Contacts:** Destiny Fogarty-Olivas, Information Security Officer, ITS

About the Washington County Auditor's Office

The Washington County Auditor's Office conducts performance audits that provide accountability to the public and improve County programs, services, and operations. In conducting audits, the County Auditor's Office follows professional auditing standards that require a high level of independence, objectivity, sound professional judgment, and regular quality assurance reviews.

The County Auditor is elected countywide and operates independently of the Board of County Commissioners and the County Administrator. The Auditor answers directly to Washington County residents and determines the programs and services to be audited.

Our Mission

To promote better government accountability, public policy, and County services through impactful audits and analysis.

Audit Team

- Kristine Adams-Wannberg, County Auditor, Quality Control Reviewer
- Sherry Kurk, Senior Management Auditor, Auditor-in-Charge
- Fiona Howell Earle, Senior Management Auditor, Quality Control Reviewer