Recommendations

13

Custom-Developed Software: Unifying governance will increase consistency.

The Office of County Internal Audit:
Elizabeth Pape, CIA, CFE – County Internal Auditor
Aaron Kay – Performance Auditor

Take survey by clicking here

To request this information in an alternate format, please call (541) 330-4674 or send email to internal.audit@Deschutes.org

Table of Contents:

Highlights:

Why this audit was performed:

The 2022 cybersecurity audit provided a high-level assessment of software security but didn't specifically assess custom-developed software. The County's sole responsibility for custom-developed software security, maintenance, and accuracy heightens the risk over commercially available alternatives.

We recommended that Central Information Technology:

Develop and implement policies encompassing the entire software development life cycle.

Establish an advisory body to develop a software selection process.

Continue efforts to provide data to decision makers on cost, benefits, and risks.

Custom-Developed Software: Unifying governance will increase consistency.

This audit was conducted to assess the effectiveness of Deschutes County's custom-developed software processes and governance structures. The audit aimed to identify areas of improvement and provide recommendations for enhancing software development, maintenance, and management practices.

What was found:

Deschutes County operates under a decentralized information technology structure that has expanded significantly over the past decade. As a result, more information technology staff are now in other departments and elected offices rather than the County Central Information Technology Department. Some of these non-Central information technology personnel possess software development expertise and have contributed to the creation of important applications.

However, the County's governance structure has not evolved to adequately address the growing diversification of development efforts. As a result, there is limited documentation and oversight of custom-developed software projects.

To address these challenges, Deschutes County must strengthen governance, documentation, and oversight processes for custom-developed software. By doing so, the County can mitigate risks, improve efficiency, and align with industry best practices and standards.

1. Introduction

Audit Authority

The Deschutes County Audit Committee authorized the review of custom-developed software in the Internal Audit Work Plan for 2022-2023. Audit objectives, scope, and methodology can be found in **Appendix A**.

Background on Software Development Processes

The software development lifecycle is a structured framework that guides the process of software development, from creating an idea to retirement. It encompasses distinct stages such as design, creation, testing, deployment, maintenance, and eventual retirement of the software. Each phase plays a crucial role in ensuring the final product meets quality standards, expectations, and aligns with business requirements.

Figure 1

Software Development Lifecycle Phases

Source: Amazon Web Services

The development process can vary significantly depending on the size and complexity of the project. For instance, small-scale applications may require minimal design and testing, allowing for rapid deployment. Conversely, large-scale projects need more extensive design, coding, and testing to ensure alignment with

business processes and user needs.

It's essential to recognize the importance of tailoring the development process to fit the specific requirements of each project. Failure to adapt the process can lead to inefficiencies, quality issues, and, ultimately, project failure. Integrating robust quality assurance measures across the entire life cycle is crucial for mitigating risks and ensuring the final product meets or exceeds expectations.

Background on County Information Technology

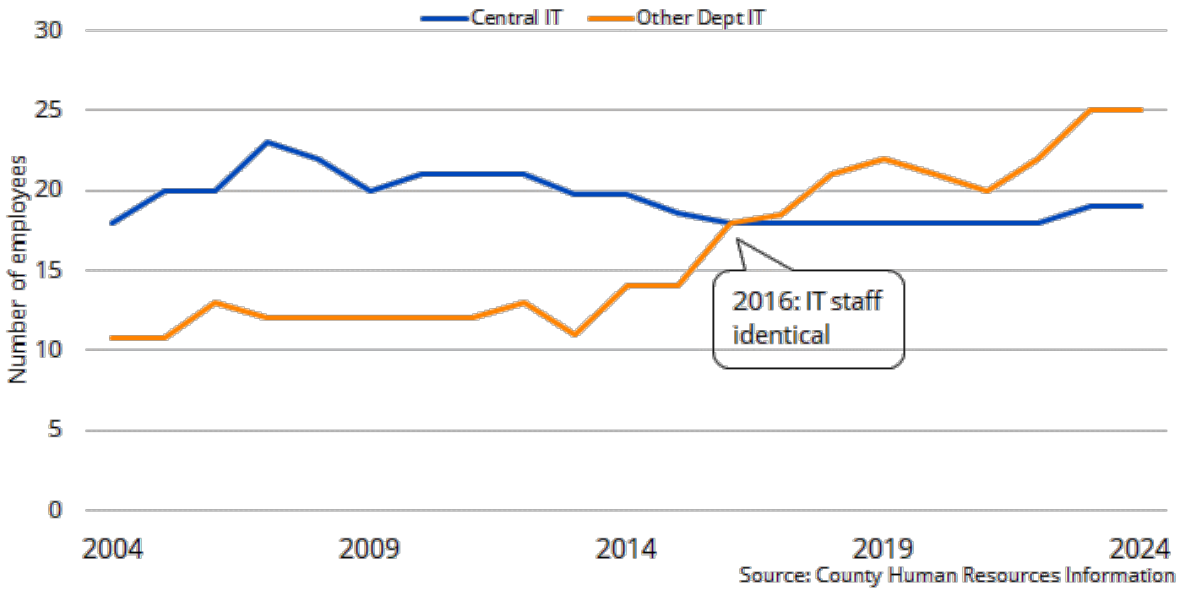
In navigating the landscape of software solutions, the County faces a dual challenge posed by custom-developed software and commercially available alternatives, each presenting distinctive risks. While off-the-shelf software offers expediency in meeting immediate business needs, it often falls short in addressing the distinct requirements of a local government organization. In contrast, custom-developed software holds the promise of alignment with the department or elected office's vision through customization. However, this effort introduces persistent complexities related to maintenance, upgrades, and optimization, particularly impactful for resource-constrained departments like Deschutes County's Central Information Technology Department. Furthermore, custom-developed software may initially appear less expensive than off-the-shelf alternatives, as development and support costs over the software's lifespan might not be factored into cost comparisons but may end up more expensive in the long term.

Over the past two decades, the Central Information Technology Department has undergone significant transformation; from a focus on internal software development to strategic operational support. The department downsized its development team by two-thirds from six dedicated developers to two, while the operational team has been as high as eighteen staff. This shift, driven by an increased reliance on technology and economic constraints, led to an increase in distributed information

technology staff across various departments and elected offices.

Figure 2

County Information Technology staffing levels from FY 2004-FY2024



Currently, there are more information technology employees outside of Central Information Technology than within it. This is also known as a decentralized or federated structure. Under this structure, different units within the County maintain varying degrees of autonomy while remaining interconnected. Out of the twenty-five other department employees with specific information technology responsibilities, seven possess the expertise to develop software applications tailored to the objectives of their respective departments or elected offices. They work in Community Development, Assessor's Office, Office of the District Attorney, Sheriff's Office, and the Road Department.

There are positive aspects to the federated model. Each department or elected office with their own information technology staff can create software solutions to their specific needs without having to rely on the Central Information Technology Department. Distributed information technology staff can be more responsive to the diverse needs of their specific work environment, often providing an array of information technology support services in addition to software.

Figure 3

Organizational approaches with unique pros and cons

	IT Structure	
		
	Centralized	Federated
Advantages	Consistency Economies of Scale Efficiciency	Adaptability Responsiveness Proximity
Disadvantages	Rigidity Slowness Bureaucracy	Inequity Unrealized savings Duplication

Source: Auditors interpretation of organizational approach from a distribution of authority chart in the Oregon Secretary of State audit on Department of Administrative Services Workforce Crises.

Conversely, the federated information technology structure can increase cybersecurity risks through:

- coordination and communication gaps, hindering swift response to emerging threats or incidents;
- distribution of authority, hindering the management and utilization of resources to support the goals of the entire organization;
- inconsistent expertise levels and security practices, leading to varying degrees of cybersecurity readiness; and
- inherent differences in priorities and philosophies, potentially resulting in conflicting approaches to cybersecurity.

Therefore, while federated structures offer autonomy and flexibility, each unit must carefully navigate the complexities of inter-organizational collaboration and align their software development strategies to mitigate inherent risks.

2. Findings

The audit objectives were to evaluate Deschutes County's custom-developed software processes and governance structures for effectiveness. It sought to highlight areas for improvement and offer recommendations to enhance software development, maintenance, and management practices. Organizing audit findings according to the phases of the software development lifecycle—planning and analysis, design, implementation, testing and integration, deployment, and maintenance— is intended to provide a structured approach for assessment and action planning.

Deschutes County's information technology structure differs significantly from other like-size counties in Oregon, such as Lane, Marion, Clackamas, and Jackson Counties, which use centralized information technology functions. Though Deschutes County's federated system has improved department-level support for efficient operations and service delivery, administrative decentralization has led to inconsistent management strategies, particularly in the governance of software development.

Without established policies around software development in departments and elected offices there is a governance gap within the County's information technology federated structure. As a result, the County faces potential risks in custom-software development related to duplicated efforts, security breaches, interoperability issues, and limited strategic alignment and innovation.

To address these risks, it is imperative for Deschutes County to prioritize the development of robust information technology governance policies for software development across its decentralized structure. This may involve creating an advisory body to foster collaboration between departments, implementing standardized procedures, and leveraging information collection efforts to plan for, invest, maintain, and secure custom-developed software products. These proposed strategies and recommendations for custom-developed software can also apply

to commercial software purchases for both Countywide and departmental specific needs. Recommendations made in this report are directed towards the Central Information Technology Department not as a call for centralization, but rather because they possess the necessary expertise and understanding to effectively address the findings. This approach acknowledges the department's specialized knowledge without implying a broader centralization of decision-making or control.

Custom-developed software planning is not coordinated.

In the past, custom-developed software planning was typically conducted separately by different departments, except for the largest projects. Though recent efforts by the Central Information Technology Director have aimed to improve coordination and communication of development projects, the absence of formal selection processes remains a significant challenge in software planning.

Central Information Technology has implemented a preliminary process to evaluate other departmental proposals based on identified needs. However, the process is missing several critical components necessary for a comprehensive assessment, including a documented evaluation of the risks, project costs, and the availability of alternative commercial products. Complicating matters further is the federated information technology structure, where departments and elected offices with their own development staff can bypass Central Information Technology's evaluation process, making decisions independently within their divisions.

The National Institute of Standards and Technology has defined industry best practices which emphasize proper planning to ensure systems provide a security level commensurate with operational risks, enhance productivity and performance, and enable innovative management and organization methods.

Custom-developed software projects entail various risks, spanning from poor user experience and performance issues to security vulnerabilities and maintenance challenges. Currently, individual departments and developers are assessing the risks within their respective projects, but they have never taken the step to document or implement a formal risk assessment that identifies the likelihood and impact of threats. This critical process omission underscores the pressing need for a comprehensive risk assessment approach that incorporates the County's overarching information technology risk management strategy.

To fully grasp the resources necessary for completing a project and making the most of investments in custom-developed software projects, it's crucial to conduct a cost-benefit analysis. That analysis faces obstacles because of the limited information of completed projects and their associated costs. Staff are not tracking the costs of custom-developed software, preventing comparison with commercially available options, and contributing to a perception that custom-developed software services are free.

The County’s decentralized approach not only undermines

centralized oversight, but also exacerbates inconsistencies and inefficiencies across software planning efforts. Consensus among County staff, both within and outside the Central Information Technology Department, affirms that Deschutes County's approach to custom-developed software investments is predominantly characterized by its lack of structure and predictability. This assessment underscores the critical need for conducting thorough project cost-benefit analyses and robust risk assessments, providing essential documentation to guide informed decision-making processes.

Following industry best practices empowers decision makers with critical insights, enabling them to make cost-effective, risk-based decisions essential for delivering the County's core services.

Recommendation #1

Central Information Technology should establish an advisory body comprising diverse County stakeholders to drive a project-centric investment process to support executive decision making.

Key aspects could include:

- *evaluating business needs for each project*
- *identifying ownership and responsibilities for each project;*
- *developing a project-centric investment selection process;*
- *collecting and disseminating project-centric investment information such as costs, benefits, schedule, risk assessment, and performance metrics; and*
- *planning for the succession of products and development resources.*

Recommendation #2

Central Information Technology should develop and implement a policy for custom-software development, outlining a standardized methodology for determining costs associated with projects throughout the County.

While planning is most often thought of as the beginning of the process, in terms of the software development lifecycle, it is also the end. Planning for succession of custom-developed software products and the developers that created them are just as important as planning for a new product. As decentralized staff leave the County, they carry away valuable knowledge and support for their developed applications. Often, Central Information Technology inherits the responsibility for maintaining applications they were not involved in developing.

Central Information Technology has a good understanding of its own existing products that may be approaching end-of-life status. However, the absence of a complete portfolio of custom-developed software for the entire organization hampers the County's ability to establish efficient transition processes, raising the risk of software vulnerabilities and potential data breaches on the County's network environment.

Recommendation #3

Central Information Technology should develop and implement a policy requiring annual reporting of all software applications used by each department and elected office to ensure an updated inventory is maintained.

2. Design
Create a design specification. This should answer the question, "How will we build this?".

County developers are not documenting custom-developed software design specifications.

There is no formal documentation of architecture for each software development project. Despite the presence of some documentation within software profiles that identifies servers, endpoints, and dependencies, developers inconsistently record this information across projects, resulting in gaps in understanding and documentation of the software architecture. Formal documentation of architecture provides clarity and transparency in understanding of the design structure, components, and data flows. This understanding is essential for identifying security and privacy requirements specific to each software application.

The County relies heavily on security and privacy controls inherited through the use of Microsoft as the primary software development framework. The County has not formalized security and privacy policies that apply to the design phase of the software development lifecycle. These policies are applied uniformly throughout the lifecycle. To protect a system from risk

and implement the most cost-effective security measures, system owners, managers, and users need to know and understand the vulnerabilities of the system.

The National Institute of Standards and Technology highlights that it is important to establish security and privacy policies tailored to the design phase of the lifecycle. This ensures security considerations are integrated from the outset, reducing the risk of vulnerabilities and unauthorized access.

Existing County policies related to information technology do not establish Countywide security standards or provide guidance about documentation for custom-software development projects. The policies also have not been kept up to date. Three key areas outline the County's governance policies regarding software:

- Computer, E-mail, and Mobile Computing Device Use,
- Consumer Identity Theft Protection, and
- Web-based Property Related Applications.

Although the Identity Theft Protection policy was updated this year after 15 years without revision, the Device Use policy has remained unchanged since its approval in 2006. The Web-based Application policy pertains specifically to DIAL, the largest and most complex County custom-developed software product. While this policy addresses data privacy for DIAL, it does not include provisions for security standards in maintaining or evolving the application.

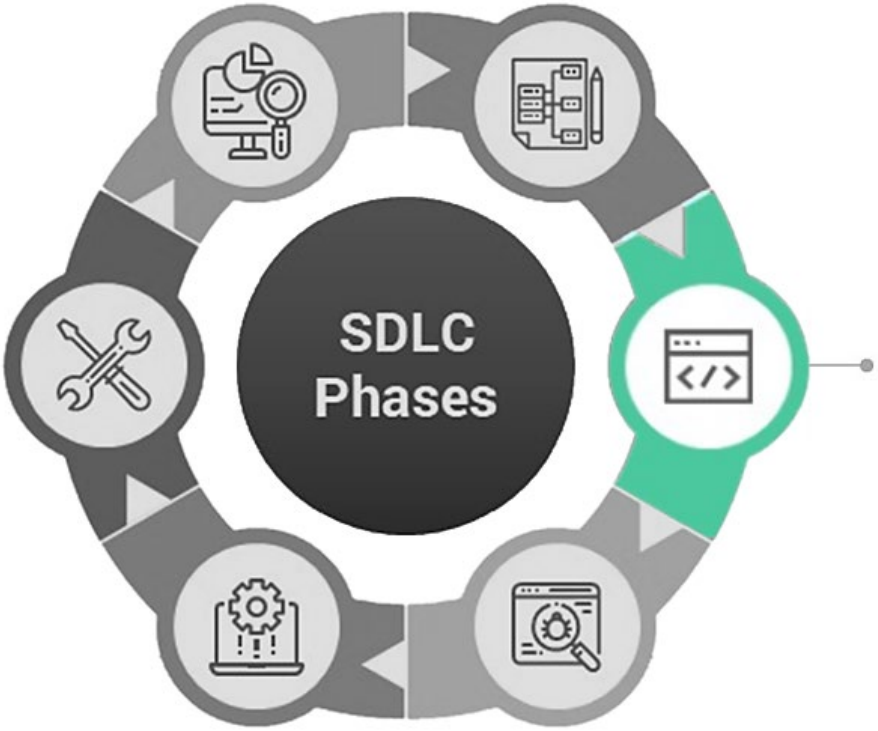
Without comprehensive County policies, responsibility for security and privacy implementation shift to departments and elected offices with information technology development staff, who may not have the necessary expertise to enact comprehensive security practices. Information technology policies and procedures for custom-software development are largely absent, even at the department level, increasing the risks associated with projects not adhering to best practices.

Recommendation #4

Central Information Technology should develop and implement a policy for custom-software development identifying security and privacy requirements for all projects throughout the County.

Recommendation #5

Central Information Technology should develop and implement a policy for custom-software development incorporating formal documentation of system architecture for all projects throughout the County.



Limited coding standards exist for custom-developed software.

Among the nine development-capable staff employed by the County, only one has documented coding standards. While

developers generally adhere to basic industry coding standards, there is a notable absence of a unified and consistent approach to software implementation and coding practices. Although most developers use the endorsed programming language, not all do, leading to inconsistencies in the development approach.

Standard use of approved programming languages ensure consistency in source code, making it easier for developers to understand and maintain each other's code. When everyone uses the same language, developers can quickly adapt to new projects or contribute to existing ones with no need to learn different syntaxes or models.

As previously noted, County information technology policies are outdated and do not provide guidance for custom-software development. They do not include unified coding standards. The absence of a documented process increases the risk of inefficiencies and inconsistencies in software implementation practices, potentially leading to delays, errors, and increased costs. There are also potential maintenance challenges from inconsistency in coding, impeding the agility and responsiveness of addressing software issues if they arise.

Recommendation #6

Central Information Technology should develop and implement a policy for custom-software development, defining unified coding standards for all developers throughout the County.

Limited oversight over software developer testing poses a risk to data security.

Although County software developers demonstrate strengths in certain aspects during the testing phase, such as source code protection and utilization of test environments, other areas could be improved. Currently, there are no documented conditions for when to use independent developer code reviews or alternative application testing methods, resulting in assessments being based solely on individual developer judgment. This not only fosters departmental and developer siloing but also heightens the risk of software flaws. It's notable that twenty-seven out of the thirty-five applications reviewed (78%) had no independent review process built in because only one developer contributed to coding or maintenance. Staff reported that some code review occurs but is not documented or formalized.

A secure repository ensures the protection of source code utilizing a version control system during testing. Version control not only tracks modifications made to the code but also provides

the ability to revert to previous versions if needed, thereby protecting against accidental or malicious changes during testing. However, the utilization of the secure repository is limited to Central Information Technology, with inconsistent availability across other departments housing information technology personnel. This inconsistency results in the reliance on local storage methods to safeguard source code. Surprisingly, even Central Information Technology fails to consistently utilize the secure repository for housing application source code, as evidenced by the discovery of four missing applications during the audit. Those four applications were safeguarded locally. While certain applications may not necessitate placement in a secure repository based on varying privacy and security risks, the absence of a standardized process creates discrepancies in access and control. Consequently, this disparity poses potential threats to the security and integrity of the source code.

In the reviewed applications, test environments were used appropriately, but individual developers frequently made decisions about their use. It is essential to document decisions regarding testing environments, establish approval processes, and implement control mechanisms, thus ensuring consistency and reliability throughout the testing phase.

As in other areas, County information technology policies do not address testing for custom-developed software. This introduces significant risks for the County. Without established guidelines, there's a heightened potential for inconsistent testing practices, leading to project delays or errors, which may affect the overall quality of software products delivered.

Recommendation #7

Central Information Technology should develop and implement a policy for custom-software development, defining standardized testing conditions and criteria for all projects throughout the County.

Recommendation #8

Central Information Technology should provide access to the secure repository for all County developers.

Critical information for custom-developed software remains undocumented.

Once software development projects reach the deployment phase, they become applications. Documentation of the system for administrators and users is missing for most applications, posing a substantial risk to effective management, and understanding of the software. Comprehensive documentation is crucial for ensuring proper maintenance, troubleshooting, and future development of the software.

Developers and software stakeholders also have not implemented formal documentation addressing the purpose, scope, roles, responsibilities, management commitment, or coordination between departments and elected offices for

deployed custom-developed software. Documentation could come in the form of service level agreements for each application. Service level agreements outline the agreed-upon performance and responsibilities between the service provider (such as the development-capable staff or Central Information Technology Department) and the customer (internal stakeholders, end-users, or external clients).

One example would be the County's Record of Client Services desktop application. The Central Information Technology Department developed the application for Health Services to track and coordinate services for individuals enrolled in the Intellectual/Developmental Disabilities Program. Central Information Technology is informally responsible for maintaining the application, while Health Services controls access and updates internal users. They did not create a service level agreement when they deployed this application in 2017 defining this relationship.

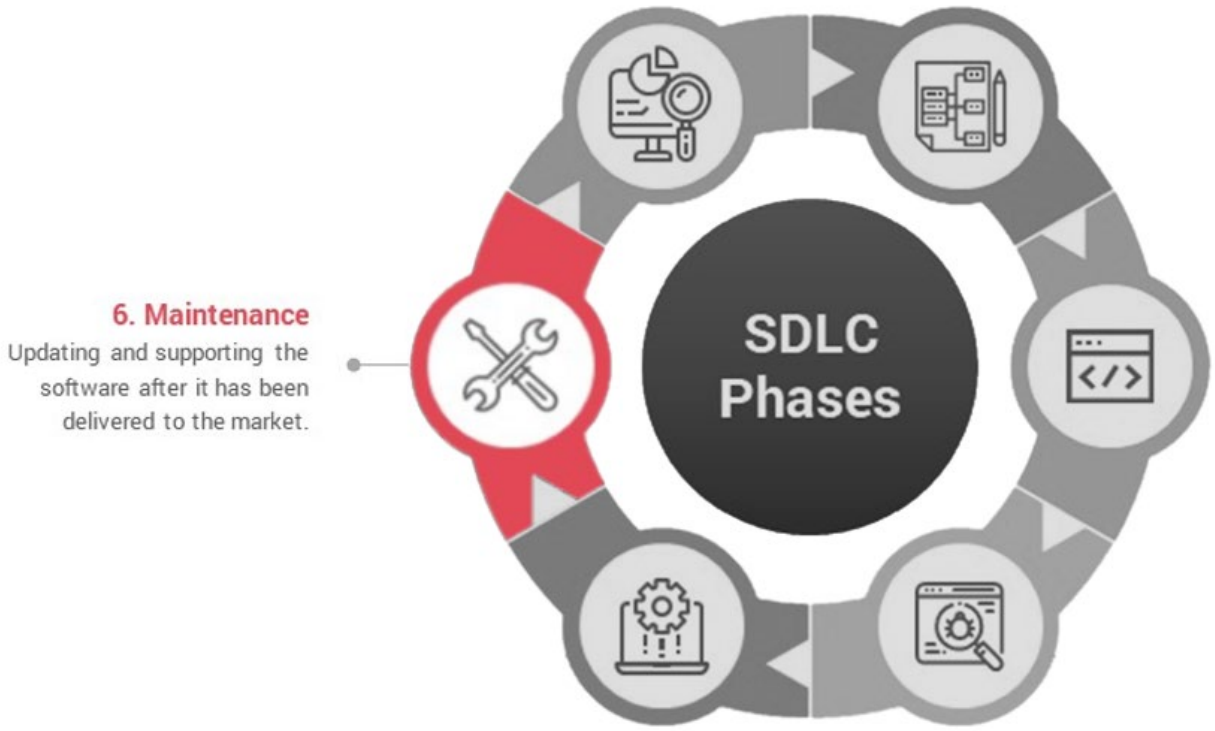
Again, County information technology policies do not address deployment practices for custom-developed software. The absence of system and user documentation undermines the overall integrity and security of the deployed software. Without clear agreements in place, there is a heightened risk of inconsistencies, misunderstandings, and mismanagement of software deployment processes, leading to potential security vulnerabilities and operational inefficiencies.

Recommendation #9

Central Information Technology should develop and implement a policy for custom-software development, requiring comprehensive system and user documentation for software applications throughout the County.

Recommendation #10

Central Information Technology should establish internal agreements with departments requesting developed software or when inheriting maintenance responsibilities of previously deployed applications.



County developers maintain custom-developed software as needed but do not track cost and performance.

Software maintenance tasks encompass a range of activities aimed at ensuring the ongoing functionality, reliability, compliance adaptation, and security fortification of software systems. These tasks typically include identifying and fixing bugs or errors, implementing updates or patches to address vulnerabilities, optimizing performance, and accommodating changes in requirements or technological environments.

County developers do a good job maintaining deployed software. For the applications reviewed, developers appropriately

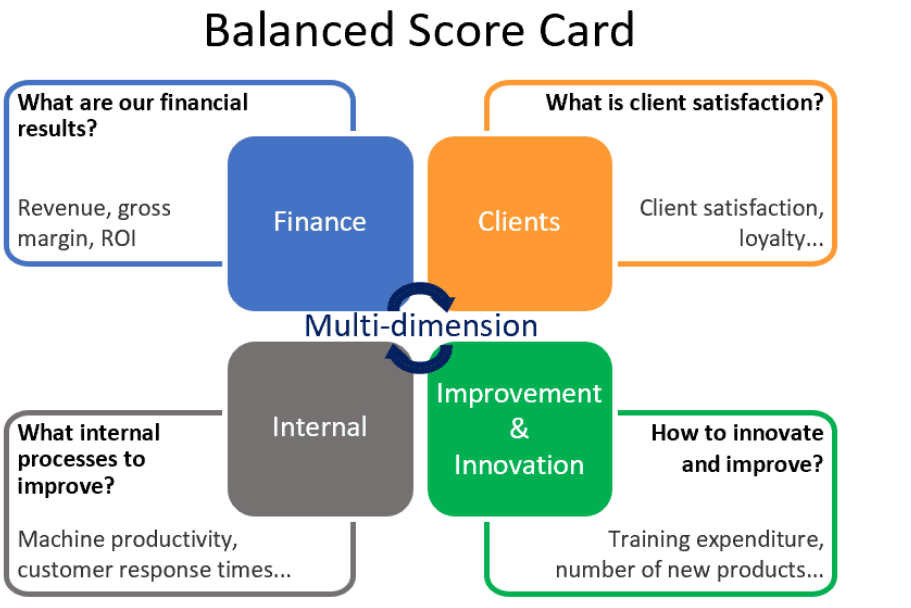
controlled user access based on the business use of the application. The County's network monitoring software records any network or system events, and the County regularly backs up data through established processes or third-party tasks.

Despite efforts to maintain custom-developed software, staff did not track maintenance costs or time spent. Central Information Technology is currently establishing a service desk model with the aim of capturing and tracking data on how much time they spend on software maintenance to calculate costs. Federated information technology staff should also contribute to the service desk model to ensure accurate reporting.

The United States General Accounting Office's maturity model calls for the development and evaluation of key measures and methods to assess software performance. One example would be a balanced scorecard approach seen in **Figure 4**. This information would then be used in the continuation of the software lifecycle at the planning and analysis phase to provide decision-makers with the measured success of each application.

Figure 4

Balanced Score Card performance measurement approach



Source: Wevalgo consultant group

Recommendation #11

Central Information Technology should develop and implement a policy for custom-software development maintenance protocols throughout the County.

Recommendation #12

Central Information Technology should continue efforts to capture data for maintaining custom-developed software and make those tools available to other information technology personnel.

Recommendation #13

Central Information Technology should use collected data to create performance measures for custom-developed software.

3. Conclusion

In summary, Deschutes County's federated approach to developing custom software presents both advantages and challenges. Though the decentralized structure allows departments to tailor solutions to their needs, it also brings challenges to coordination, governance issues, and heightened risks to County systems.

To address these challenges, it's crucial for the County to establish clear guidelines and standards for software development. Key recommendations include establishing an advisory body to drive investment decisions, developing standardized procedures for project evaluation and cost estimation, and implementing policies across the entire software development lifecycle.

By aligning with industry standards and best practices, Deschutes County can enhance the quality of its software, mitigate risks, and better serve its communities. This involves focusing on practical steps to improve the current environment and ensure that

custom-developed software continues to meet the needs of both users and the organization as a whole.

4. Management Response

IT DEPARTMENT

To: Elizabeth Pape, County Internal Auditor
From: Tania Mahood, IT Director/CTO
Date: May 10, 2024
Subject: Management's response to Audit report

Elizabeth,

Central IT agrees with the Audit findings and recommendations in the report. Implementing these suggestions will demand substantial resources to execute the tasks, and the projected completion dates are indicative of Central IT's constrained resources and addressing existing technical debt. The responses below are in chronological order of estimated completion date.

Recommendation #4 and #6 – completion by September 2024
The following two recommendations, #4 and #6, are prioritized as the highest importance for Central IT to protect and maintain our assets. Central IT believes these two recommendations can be completed in a timely fashion and can serve as the initial foundational policy for custom development. All other policy recommendations in this audit will be proposed as additions to the custom development policy at a future date due to limited resources within IT and the complexity of the policy recommendations. Central IT can draft and implement the foundational policy by September 2024 that includes recommendation #4 and #6.

The IT Management team embraces the Audit findings and *recommendation #4 Central Information Technology should develop and implement a policy for custom-software development identifying security and privacy requirements for all projects throughout the County.* In today's rapidly evolving information security landscape, where threats continue to escalate, it's imperative that we take proactive measures to safeguard data and protect privacy across all County projects.

This ever-changing landscape means our past experiences may not inform the future, underscoring the importance of a cautious approach and risk-based analysis in our software development endeavors. In an interconnected world operating 24x7, the potential impact of data exposures is significantly amplified. We cannot afford to underestimate the consequences of security incidents, as any self-inflicted incident could have severe financial and reputational repercussions for the County as a whole. By prioritizing security and privacy requirements in our custom-software development policy, we demonstrate our commitment to responsible stewardship of resources and protecting the interests of our community.

The IT management team concurs with the Audit report findings and recommendation *#6 Central Information Technology should develop and implement a policy for custom-software development, defining unified coding standards for all developers throughout the County.* This is a proactive step towards fostering consistency, transparency, and organizational flexibility in our development processes. By defining and adhering to unified coding standards, we ensure that all developers operate from the same playbook, promoting coherence and efficiency in our coding practices. It creates a foundation for effective collaboration, both internally and with external partners, while also promoting transparency and accountability in our development processes.

Recommendation #12 – completion by June 2025*

The IT management team concurs with the Audit report findings and recommendation *#12 Central Information Technology should continue efforts to capture data for maintaining custom-developed software and make those tools available to other information technology personnel.* to continue efforts to capture data for maintaining custom-developed software and make those tools available to other IT personnel. This is important for enhancing transparency, efficiency, and informed decision-making across our IT operations.

Implementation of an IT Service Management (ITSM) tool is an effort that has already been identified as a need for the organization. Implementing an ITSM tool enables IT to capture maintenance time to calculate costs accurately but also provides valuable insights into software performance. By offering this tool to departments and offices we promote collaboration and consistency in data collection and analysis, ensuring that all IT personnel have access to critical information for their decision-making processes.

This collected data feeds back into the planning and analysis phase of the software development lifecycle, enabling us to make informed decisions about the continued use of software or the exploration of alternative solutions. By leveraging real-time data on maintenance efforts and software performance, we can identify areas for improvement, optimize resource allocation, and mitigate risks associated with outdated or underperforming software.

Furthermore, ongoing performance data captured through the ITSM tool provides valuable feedback on the effectiveness of our software solutions. This allows us to identify trends, address emerging issues proactively, and continuously improve the quality and reliability of our custom-developed software.

Central IT has budgeted $30K/year for an ITSM tool for Central IT employees only. This is a large project and requires significant time and labor to roll out and configure. With limited resources and competing projects, the earliest estimated date for implementing this tool is June 2025.

*This costing and budget doesn't include distributed IT units. The completion of having access for all IT units across the organization will be dependent on the department/office budgets. Cost for IT employees in these departments/offices is unknown at this time.

Recommendation #8 – completion by September 2025*
The IT management team concurs with the Audit report findings and recommendation *#8 Central Information Technology should provide access to the secure repository for all County developers.* This is not only practical but aligns with our commitment to efficiency, security, and transparency in our IT operations. Our current practice of utilizing a centralized code location has proven to be a tried-and-true best practice, offering a secure and scalable solution for managing code repositories. This can facilitate collaboration by centralizing our code management process and enable thorough review of code, promoting quality and reliability in our development efforts.

The availability of the current centralized code solution will need to be configured and scaled to add other developers throughout the County. There is an estimated additional cost of $1,800 with implementing this enterprise solution that Central IT does not currently have budgeted funds for. Therefore, funds will need to be requested and budgeted for in FY26.

*Central IT can implement the solution, create a process to add/remove users, and provide costing to other departments/offices by September 2025. The completion of having access for all developers across the organization will be dependent on the budget of those departments/offices that have developers. For other departments/offices the estimated cost per developer is approximately $200/person/month.

Recommendation #1 – completion by December 2026
The IT management team concurs with the Audit report findings and *recommendation #1 Central Information Technology should establish an advisory body comprising diverse County stakeholders to drive a project-centric investment process to support executive decision making.* Establishing an advisory body is a great step towards enhancing our technology investment process. Involving representatives both within and outside of IT will ensure we are investing in tools that add value to the business while being secure, supportable, and sustainable. This body can also help with prioritizing competing projects across the organization which will effectively allocate resources. By aligning investments with business objectives and ensuring a sufficient return, we can establish a foundation for sustainable growth and success.

This formalized process will enable us to uncover and mitigate risks associated with projects, empowering us to make informed decisions. Additionally, this body will uphold the quality of

projects and their outcomes, fostering transparency and accountability throughout the organization. This transparent decision-making not only enhances trust but paves the way for more successful future technology initiatives.

Recognizing the importance of this recommendation and the limited resources available in the Central IT Department to spearhead the effort, it will take significant time to solicit, organize, and formalize this body. The effort estimated from Central IT is over 240 hours of work resulting in an estimated timing for completion of December 2026. This doesn't account for the significant time requirements from other individuals across the organization to dedicate themselves to this effort that Central IT cannot commit on their behalf.

Recommendation #13 – completion by June 2027
The IT management team concurs with the Audit report findings and recommendation *#13 Central Information Technology should use collected data to create performance measures for custom-developed software.* This is important for assessing the effectiveness, value, impact, and retirement of our IT projects.

Defining performance measures enables us to answer fundamental questions about the success of our custom-developed software. By establishing clear metrics, we gain insight into whether the investments made in these projects have delivered the expected value and efficiencies needed. This not only allows us to evaluate whether the effort justified the results but also provides a consistent framework for assessing the outcomes of our IT initiatives.

Measuring performance also helps us ensure that our software solutions continue to meet the evolving needs of our customers. By monitoring key metrics such as user satisfaction, system reliability, system use, and efficiency gains, we can identify areas for improvement or modifications and make data-driven decisions to optimize the value delivered by our custom-developed software.

Measuring performance may also uncover the need for retirement if software no longer meets County standards or adapts to the evolving needs of the County. These actions not only safeguard the reputation for IT delivering high-quality solutions but also ensure that resources are allocated towards initiatives that yield the greatest value for the County.

Furthermore, having a consistent way to measure the value of projects enables us to weigh their benefits against the total cost of ownership. This holistic approach to performance measurement ensures that we are not only achieving our objectives but also maximizing the return on investment for County resources.

Once recommendation #12 and #1 are complete, Central IT can collect the appropriate data for the organization with an estimated date of June 2027.

Recommendation #2, #3, #5, #7, #9, and #11 – completion by June 2027
Once the advisory group from recommendation #1 is formalized the expectation is for them to assist with the build out the policy from recommendations #4 and #6 to include the recommendations below (#2, #3*, #5, #7, #9, #11). These policy recommendations can be completed by June 2027.

Recommendation #2
The IT management team concurs with the Audit report findings and recommendation *#2 Central Information Technology should develop and implement a policy for custom-software development, outlining a standardized methodology for determining costs associated with projects throughout the County.* This framework will ensure transparency and accountability in our investment decisions. We believe that involving the advisory body in the creation of this policy will be beneficial as their perspectives can view this from not only a technical standpoint, but from a business perspective too. With thorough requirements gathering and data analysis it can shed light on factors such as ongoing support and maintenance. This process can help make informed decisions regarding the total cost of ownership. Creating robust cost controls will enable us to deliver greater value to Deschutes County by ensuring responsible stewardship of resources while driving impactful technology initiatives.

Recommendation #3
The IT management team supports the Audit report findings and recommendation *#3 Central Information Technology should develop and implement a policy requiring annual reporting of all software applications used by each department and elected office to ensure an updated inventory is maintained.* Currently, we lack consistent and comprehensive processes. This hinders our ability to effectively understand the ripple effects of changes, costs, relevancy, or obsolescence. The absence of a formalized review period and standardized procedures for maintenance and retirement further exacerbates these issues, leading to varied lifecycle management practices. Therefore, by identifying assets, it will lay the foundation for the creation of best practices in lifecycle management. Furthermore, this initiative will help provide essential visibility for risk management, compliance, security, and resource allocation. It will ensure accountability and facilitate informed decision-making.

*This recommendation completion is dependent on participation from other departments/offices.

Recommendation #5
The IT management team concurs with the Audit report findings and recommendation *#5 Central Information Technology should develop and implement a policy for custom-software development incorporating formal documentation of system architecture for all projects throughout the County.* This is not just timely but essential in today's dynamic technological landscape. Relying solely on individual employees to hold institutional knowledge is a risk and no longer a sustainable practice. Instead, we must prioritize transparency and collaboration, fostering a culture where knowledge is shared collectively. This shift towards teamwork and cross-training necessitates the need for documentation, ensuring that critical information is readily available and comprehensible to all stakeholders. This will help mitigate the risk of knowledge loss but also enhance the efficiency and effectiveness of our development processes.

Recommendation #7
The IT management team concurs with the Audit report findings and *recommendation #7 Central Information Technology should develop and implement a policy for custom-software development, defining standardized testing conditions and criteria for all projects throughout the County.* This is important in enhancing transparency and collaboration within our IT ecosystem and allowing agility in our IT ecosystem.
By implementing standardized testing conditions and criteria, we not only streamline our testing processes but also create opportunities for mutual support and collaboration. Testing across units allows us to leverage collective expertise and resources, breaking down silos and fostering a culture of cooperation and knowledge sharing. While individual teams may face resource constraints, pooling resources and expertise enables us to achieve better outcomes collectively. Together, we can overcome challenges and deliver high-quality software solutions that meet the needs of our County.

Recommendation #9
The IT management team concurs with the Audit report findings and recommendation *#9 Central Information Technology should develop and implement a policy for custom-software development, requiring comprehensive system and user documentation for software applications throughout the County.* This is a proactive step towards enhancing efficiency and support for both developers and end-users alike.

While we may already be documenting aspects of our software applications, providing standardized templates will streamline the process and ensure consistency across all projects. This standardization not only makes documentation more accessible but also facilitates faster and more efficient documentation efforts for developers.

Comprehensive and standardized documentation benefits end-users by providing them with the information they need to navigate and utilize software applications effectively. With this documentation in place, end-users can find answers to their questions more quickly. It can also reduce the burden on tier 1 support teams by empowering end-users to troubleshoot and resolve issues independently. This not only saves time and resources but also fosters a sense of empowerment and ownership among end-users.

Recommendation #11
The IT management team concurs with the Audit report findings and recommendation *#11 Central Information Technology should develop and implement a policy for custom-software development maintenance protocols throughout the County.* This is essential in ensuring the reliability, security, and longevity of our software solutions.

By establishing clear maintenance protocols, we can set expectations regarding when maintenance activities will occur, ensuring that critical updates, patches, and fixes are implemented in a timely manner. The combination of creating standardized maintenance efforts and the IT change management process not only promotes employee satisfaction by

minimizing disruptions but secures our assets and reduces our technical debt accumulation.

Security issues are a significant concern in today's digital landscape, and regular maintenance is essential for mitigating these risks. By proactively addressing security vulnerabilities and implementing patches and updates in a timely manner, we can minimize the likelihood of security breaches and protect sensitive data from unauthorized access.

Furthermore, addressing technical debt through systematic maintenance protocols is critical for ensuring the long-term viability and sustainability of our software solutions. By regularly reviewing and addressing technical debt, we can prevent the accumulation of outdated code and infrastructure, reducing maintenance costs and improving overall system performance.

Recommendation #10 – completion by December 2027
The IT management team concurs with the Audit report findings and recommendation *#10 Central Information Technology should establish internal agreements with departments requesting developed software or when inheriting maintenance responsibilities of previously deployed applications.* This is essential for ensuring clarity, accountability, and effective resource allocation within our IT ecosystem.

By implementing agreements, we can clearly define roles and responsibilities, setting expectations for both Central Information Technology and the requesting departments/offices. These agreements outline what services we are committing to provide, including maintenance, support, and updates, as well as the corresponding benchmarks and tracking mechanisms to monitor performance and ensure compliance.

Without these agreements in place, we risk operating in a state of ambiguity, where expectations are unclear, and resources may be inadequately allocated. By formalizing agreements, we can establish benchmarks for service levels, track performance against these benchmarks, and ensure that resources are allocated appropriately to meet the needs of our stakeholders.

Additionally, understanding the business requirements of the requesting departments is essential for delivering software solutions that truly meet their needs. These agreements provide an opportunity to align IT initiatives with departmental objectives, fostering collaboration and ensuring that our technology investments deliver value to the County as a whole.

This will take significant work to accomplish for every department/office that Central IT has built solutions for at the County. Other items should be included in these agreements outside of just software development which will take additional time to create and implement. Estimated date for the completion of this recommendation is December 2027.

5. Appendix A: Objective, Scope, and Methodology

The County Internal Auditor was created by the Deschutes County Code as an independent office conducting performance audits to provide information and recommendations for improvement.

The audit included limited procedures to understand the systems of internal control around custom-developed software. Audit findings result from departures from prudent operation. The findings are, by nature, subjective. The audit disclosed certain policies, procedures and practices that could be improved. The audit was neither designed nor intended to be a detailed study of every relevant system, procedure, or transaction. Accordingly, the opportunities for improvement presented in the report may not be all-inclusive of areas where improvement may be needed and does not replace efforts needed to design an effective system of internal control.

Management has responsibility for the system of internal controls, including monitoring internal controls on an ongoing basis to ensure that any weaknesses or non-compliance are promptly identified and corrected. Internal controls provide reasonable but not absolute assurance that an organization's goals and objectives will be achieved.

"Audit objectives" define the goals of the audit.

Objectives and Scope

Objectives included:

1. Is the County following consistent quality and standards in custom-software development?
2. Do the existing controls provide robust and comprehensive management of information security throughout the entire lifecycle of custom-developed software?

Scope and timing:

The audit occurred between December 2023 and March 2024 and included all custom-developed software deployed or in development at Deschutes County as of January 2024. The scope

did not include all aspects of internal controls over custom-developed software. Custom-developed software, as defined for this audit, includes applications developed and deployed by County developers, including contracted development resulting in compiled products. However, it excludes any customization of commercially purchased software. The audit did not evaluate software development aimed at enhancing commercially purchased products' efficiencies, reporting, or integration. Additionally, minor scripting for routine business process improvement was not within the scope of the audit. Any assessment of general entity-wide information security controls was limited to meeting the specific objectives of the audit.

Methodology

Audit procedures included:

Audit procedures are created to address the audit objectives.

- Reviewing consistency in the use of coding standards, version control, testing procedures, and documentation across the County's deployed custom-developed software.
- Reviewing the relevant security and privacy controls in place for selected custom-developed software throughout the entire software lifecycle using a random sampling of the software active at the time of the audit. The sample, comprising 12% of the total population, is sufficiently representative to allow for confident projections of findings to the entire population.
- Interviewing selected departmental management and staff.
- Analysis of data to evidence application testing, configuration management, and security practices within the secure repository used for custom-developed software.
- Benchmarked Deschutes County to other like-size counties using publicly available information or direct communication with management.
- Assessed the maturity level of the County's Information Technology investment process related to custom-

developed software using the United States General Accounting Office Executive Guide on Information Technology Investment Management Version 1.1.

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.

(2018 Revision of Government Auditing Standards, issued by the Comptroller General of the United States.)

Please take a survey on this report by clicking this link:
https://forms.office.com/g/pPxCHuRHbq

Or use this QR Code:

If you would like to receive future reports and information from Internal Audit or know someone else who might like to receive our updates, sign up at http://bit.ly/DCInternalAudit.