Risk Management

Adopting Enterprise Risk Management will help the County better manage its risks

April 2019

Multnomah County Auditor's Office

Jennifer McGuirk, Multnomah County Auditor

Jennifer McGuirk
Multnomah County Auditor

Fran Davison
Nicole Dewees
Mandi Hood
Craig Hunt
Annamarie McNiel
Marc Rose
Mark Ulanowicz
Caroline Zavitkovski

March 21, 2019

Dear Multnomah County community members,

I am pleased to issue this audit report on County risk management. This audit was largely overseen by the prior County Auditor, Steve March, working with Craig Hunt, CPA, and Marc Rose, CFE. Through many hours of research, interviews, and data analysis, we arrived at a set of important recommendations to help the County improve its approach to managing risk.

A focus of our report is on the need to establish an enterprise risk management (ERM) system at the County. We are well positioned to start that process. The County has done a good job managing what we traditionally think of as risk, such as a focus on hazards and on managing financial risk with tools like insurance. And importantly, the Chief Operating Officer has made risk discussions a regular part of the Countywide governance groups that she oversees. These efforts mean that the County has a solid foundation on which to build an effective ERM system that is woven into County operations at every level, and that has clearly articulated processes for risk identification, assessment, and mitigation.

While our departments have different business lines, there are commonalities in the communities they serve and the tight resource environment we all face. An ERM system that meets best practices will help the County take advantage of opportunities to better serve our vulnerable community members, both by individual departments and across departments, as well as help the County avoid loss of the resources and sensitive data entrusted to us.

Sincerely,

Jennifer McGuirk, MPA, CIA,
Multnomah County Auditor

Table of Contents

Report Highlights

What We Found

We found the County is not employing the most effective approach to overall risk management. While other organizations turn toward Enterprise Risk Management (ERM) – a modern risk management approach – the County's approach to risk management is traditional, focused primarily on managing losses through insurance coverage and attention to workplace safety. We reviewed the administration of these traditional functions and were encouraged by what we found – consistent, professional monitoring and management, which ultimately protects employees and the public, and saves the County money. But implementing ERM would benefit the County by focusing management's attention on the organization's most significant risks, greatly improving its ability to meet its mission, goals and objectives, and supporting more effective use of taxpayer dollars.

In addition, we found that the County lacks a risk committee; monetary settlement administrative processes limit efficiency and transparency; and administrative leave pay is on the rise, signaling increasing underlying issues. Our audit included a look at County employee perceptions of workplace safety. Generally, employees perceive workplace safety as a top priority, though the County has seen some significant accidents and near-miss incidents, and employees in the Sheriff's Office and Department of Community Justice perceive the County's prioritization of safety more skeptically.

Why We Did This Audit

About $125 million flows through the risk fund each fiscal year: for employee benefits, to pay for worker's compensation expenses, insurance, liabilities, and the administrative costs of Risk Management and the County Attorney. In this audit, we wanted to make sure that the County is managing its risks effectively and following risk management best practices.

What We Recommend

By making changes, the County can be more prepared for risks to its services and reputation, capitalize on opportunities, and potentially reduce expenses. We recommend:

- The County should implement an ERM approach to risk management.
- The Chief Operating Officer (COO) should form a high-level risk management committee, or formally add a risk management function to an existing committee that reaches all departments and offices, and includes the Risk Manager.
- The COO, Risk Management, and County Attorney's Office should clarify some key administrative functions.
- Select departments should conduct research to understand employee perceptions of County safety culture.

Results

The County should move to Enterprise Risk Management

Multnomah County employs a *traditional* approach to risk management. Multnomah County's Risk Management function primarily deals with hazards in three main areas:

- The Property and Liability section focuses on countywide risk exposures, liability and property claims, purchasing insurance, and loss control/prevention.
- The Workers' Compensation section administers work-related employee injury and illness processes and assists employees in returning to their jobs.
- The Safety and Health section oversees loss prevention efforts by assisting departments to meet the loss prevention requirements of a workers' compensation self-insured employer.

Best practice calls for a much broader and more significant role for managing risks called enterprise risk management or ERM. Risk management activities the County currently performs remain essential but become a part of the County's overall risk profile. The chart below shows the differences between traditional and enterprise risk management.

ERM is a structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives.

Traditional Risk Management	**Enterprise Risk Management**
Focuses on hazards	Strategically focused to align with mission and values
Silo approach	Holistic approach
Tends to focus on reactive analysis	Proactive
As needed, ad hoc or compliance driven	Ongoing, continuous
Manages risks that can be transferred	Manages risk to mission and strategy
Risk viewed as bad	In addition mitigating risks, ERM recognizes opportunities to pursue.
Risk experts responsible for insurance and prevention. Risk Manager is insurance buyer.	Risk owners manage risk. Risk Manager is the risk facilitator and leader.
Transfer risk to, for example, an insurance provider	Optimize risk to increase value and achieve goals

Source: Auditor's Office summary of ERM literature

Traditional risk management would not take into account potential decreases in federal funding that could negatively affect a variety of County services to its vulnerable community members.

ERM significantly expands upon traditional risk management duties to manage organization-wide risks to mission and strategy. For example, traditional risk management would not take into account potential decreases in federal funding throughout the County that could negatively affect a variety of services performed by multiple programs to its vulnerable community members. In addition to mitigating risks, ERM recognizes opportunities for the County to pursue. For example, ongoing advances in technology create numerous opportunities that improve efficiency and communication. ERM considers *all* types of risks an organization encounters and provides a means to transparently decide on what path is appropriate. For example:

- Strategic—With demographic shifts, the County may need to relocate or expand services.
- Financial—Legislative changes to PERS could help or harm the County.
- Compliance—Failure to comply with federal grant regulations could endanger funding of vital public services.
- Operational— Loss of key personnel and institutional knowledge through retirement or competition.
- Hazard—Injury to the public on County-owned premises or from a County-operated vehicle.
- Reputational— Data breach of sensitive information due to electronic security lapses.

ERM embeds risk awareness into an organization, seeking to enhance its transparency and accountability. ERM's success requires sustained attention from the top of the organization. As such, we believe it should be under the supervision of the Chief Operating Officer with the more traditional functions remaining under the Chief Financial Officer. This is an opportunity for the COO to build on the good work she has already done to bring a risk focus into the County.

Definitions from Playbook: Enterprise Risk Management for the U.S. Federal Government

Risk: The effect of uncertainty on achievement of objectives. An effect is a deviation from the desired outcome – which may present positive or negative results.

Risk Management: A coordinated activity to direct and control challenges or threats to achieving an organization's goals and objectives.

Risk Assessment: The identification and analysis of risks to the achievement of business objectives. Risk assessment involves evaluating the significance and likelihood of a risk, as well as any controls or other measures that mitigate or eliminate that risk.

Risk Profile: A prioritized inventory of an organization's most significant risks.

Risk Tolerance: The acceptable level of variance in performance relative to the achievement of objectives.

Risk Appetite: The articulation of the amount of risk (on a broad/macro level) an organization is willing to accept in pursuit of strategic objectives and value to the enterprise.

There are many benefits to ERM

ERM's goal is to focus management's attention on the organization's most significant risks and improve its ability to meet its mission, goals, and objectives. The organization seeks to align the amount of risk it is willing to accept with strategic objectives and use a consistent approach to assess risks. ERM significantly lowered the University of California's total cost of risk from $18.46 per $1,000 in fiscal 2003 to $13.31 per $1,000 of the operating budget in fiscal 2010. In FY2010 alone, the university reduced its overall cost of risk by approximately $80 million.

As a silo buster, ERM creates forums where managers work together to identify and manage cross-enterprise risks and to draw upon the expertise of all managers involved. As a result, the quality and availability of information should improve and strengthen senior leadership decision-making for a more efficient and effective means of managing risk. ERM prioritizes significant risks so that an organization can allocate scarce resources to address those risks that best contribute to overall value.

ERM implementation needs a high-level champion and will take time to build

In order for the County to realize the benefits of ERM, it must have strong support from the top of the organization. In fact, a high-level champion might be the most important factor for establishing, building, and sustaining a successful ERM program. ERM is not an isolated activity. For ERM to work, risk information must flow freely throughout the organization. The County should fully integrate ERM into its day-to-day management and steadily into its culture. The County should start moving towards ERM, but we recognize that it will take some time to integrate ERM into decision-making processes.

We have learned that the County's Chief Operating Officer guides Countywide governance groups, such as the Corporate Council and Director's Council, which include discussion of short- and long-term risk identification and mitigation. It is positive that these discussions are happening at the top of the organization because they suggest that the County is in a good position to transition to a working ERM program. In a well-functioning ERM system, risk assessments start at the unit level and work up; ERM takes place at each level of the organization, not just at the top.

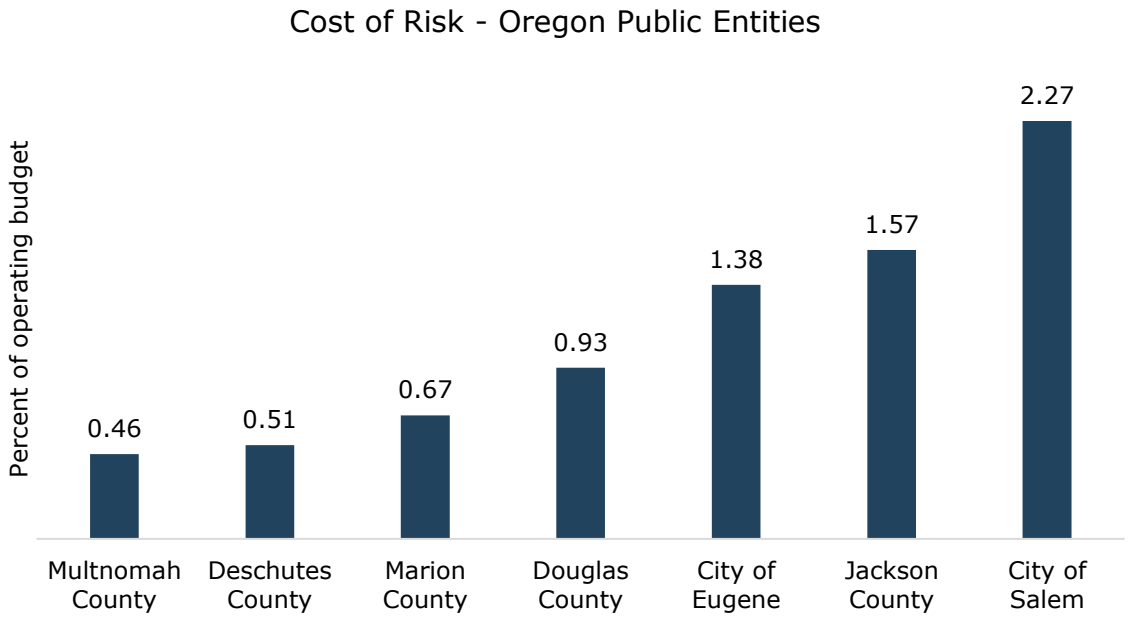
Appendix A answers frequently asked questions about ERM and how it would benefit the County.

Traditional risk management is functioning well although some improvements are needed

The County's approach to risk management is traditional, focused primarily on managing losses through insurance coverage and attention to workplace safety. We reviewed the administration of these traditional functions and were encouraged by what we found – consistent, professional monitoring and management, which ultimately protects employees and the public, and saves the County money. But department managers have not always been responsive to Risk Management's concerns and recommendations, and Risk Management employees do not have enforcement authority with regard to safety measures. To help ensure traditional functions continue to operate well, and looking toward an ERM implementation, County managers should follow through on Risk Management's safety recommendations.

The County's cost of risk compares favorably to other jurisdictions

Cost of risk is a key performance indicator used by the County that compares its risk management costs to other jurisdictions.



Source: Multnomah County's insurance broker who indicated that Multnomah County's cost of risk data combining liability and worker's compensation insurance costs is from 2017, and data from other organizations in the chart is from several years earlier.

While some significant near-miss incidents and accidents have occurred, employees perceive workplace safety as top priority at the County

Workplace safety is a primary function of Risk Management, and should be a top priority at the County. Safety lapses and accidents in the workplace can lead to injuries or death, and can result in lawsuits and fines. While safety specialists in Risk Management act as consultants regarding workplace safety, Oregon and federal laws assign responsibility regarding workplace safety to organization management – department managers, in the case of the County.

Some serious near-miss incidents and accidents have occurred, and department management needs to be responsive to Risk Management's concerns

Risk Management employees noted that the County has had some close calls – dangerous near-miss incidents. In one case at a County facility, a worker placed his hand within six inches of an energized 480-volt power wire. Fortunately, a Risk Management employee happened to be in the building and stepped in. The same facility had to be cleared of employees when workers began cutting concrete –which contains silica dust – without notice. In another County facility, employees were using breakers to turn on the lights, because areas of the building lacked switches.

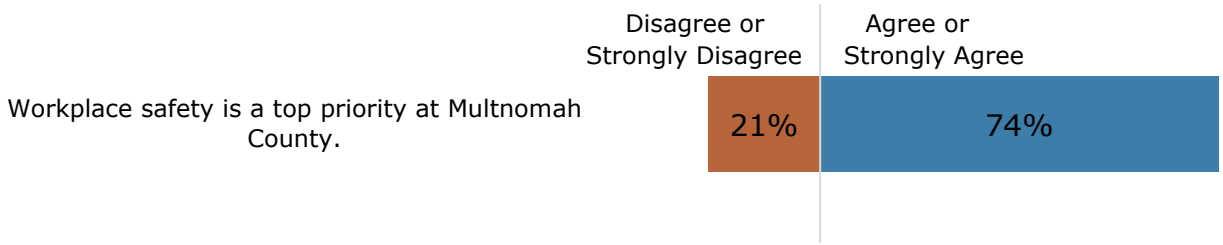
Management has not always been responsive to Risk Management's concerns and recommendations, and Risk Management employees do not have enforcement authority. In one situation, a County building had large drop-offs where vehicles entered, with large grassy areas the public could access. Requests of management to fix the situation went nowhere, and it took two years to be permanently fixed. Proactive risk management practices can help prevent accidents, but it is essential that management take responsibility for safety issues and is responsive to the concerns of Risk Management employees, who generally act as consultants.

To get a better sense of the safety culture at the County, we looked to the views of County employees, about how highly the County values workplace safety.

Employees generally perceive workplace safety as a top priority

As part of the Auditor's 2018 Countywide Ethical Culture survey, we asked employees their perceptions of the County's safety culture. About three quarters of employees indicated that they believed workplace safety was a top priority at the County.

About three-quarters of employees perceive workplace safety as a top priority at Multnomah County

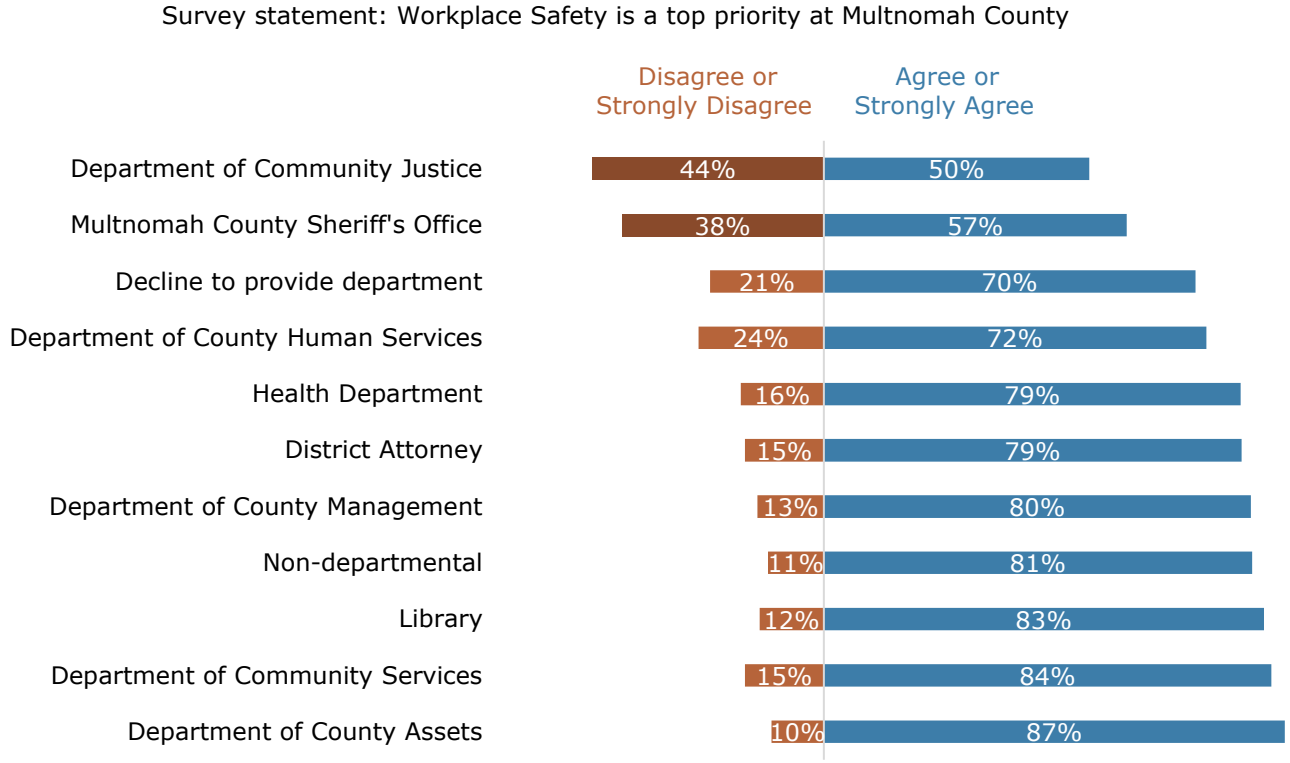


Source: Auditor's Office Survey

Fewer employees in the Department of Community Justice (DCJ) and the Sheriff's Office perceive safety as a top priority

Two departments, DCJ and the Sheriff's Office, deviated from others in terms of the way employees perceive the County's safety priorities, with larger proportions of employees indicating that safety is not a top priority at the County. We advise these two organizations do additional follow-up to learn more about these perceptions.

Employees in the Department of Community Justice and Sheriff's Office perceive safety as a lower priority



Source: Auditor's Office Survey

Through the survey, we received a number of comments regarding workplace safety. The most common concerns were about employee safety around downtown County buildings and employee safety for those employees out in the field or working directly with the public. These comments signal the need for County management to learn more from employees about specific workplace safety concerns.

Clarifying and updating County code, rules, and internal controls processes is needed to make claims administration more efficient

Within the County's traditional risk management approach, we identified a few items that could help the County favorably manage its cost of risk.

The third party administrator (TPA) settlement limit could increase to more quickly resolve smaller claims and decrease County workload

Risk Management is responsible for the administration and oversight of the claims process for the County's self-insured exposures and the Worker's Compensation program through a contract with a TPA.

The County's TPA provides detailed reports on claims to the County and currently has settlement authority of $2,500 for general liability claims. Risk Management informed us that the $2,500 settlement authority has been in place for many years. Because costs have increased over the years, the TPA currently has strong internal controls in place, and the County's threshold is relatively low compared to other jurisdictions, the recommended Risk Management Committee should increase the settlement authority amount. Doing so will allow a more expeditious resolution of smaller claims and decrease County workload. The County must keep monitoring the TPA to ensure it continues to have strong internal controls.

Compared to other jurisdictions, the County's settlement authority limits are relatively low

Jurisdiction	TPA or Self-Administered	Position	Settlement Authority Limit
Multnomah County	TPA	TPA Risk Manager (Worker's Comp) County Attorney County Board of Commissioners	$2,500 $25,000 $25,000 $25,001 or more
Clackamas County	TPA	TPA Risk Manager County Council County Executive Board	$5,000 $80,000 (note 1) $80,000 (note 1) $99,999 (note 1) $100,000 or more
City of Eugene	Self-Administered	Claims Analyst Risk Manager City Attorney City Manager	$5,000 $25,000 $99,999 $100,000 or more
Washington County	Self-Administered	Risk Manager County Council Risk Management Committee Board	$10,000 before litigation filed $10,000 after litigation filed $25,000 $25,001 and above
City of Salem	Self-Administered	Risk Manager City Manager Board	Up to $25,000 Up to $50,000 $50,001 or more
Marion County	Self-Administered	Risk Manager Risk Manager Legal Council Chief Administrator Board	$50,000 property damages $25,000 non-property damages $50,000 after litigation filed $100,000 $100,001 or more

Sources: Multnomah County Risk Management and Auditor analysis.
Note 1: The Risk Manager and County Council must agree for the $80,000 limit. The County Executive must agree with the Risk Manager and County Council for the $99,999 limit.

The County Attorney has settlement authority for claims up to $25,000. For settlements exceeding $25,000, approval by the Board of County Commissioners (BOCC) at a public meeting is required. Since 2014, about half of the employment settlements were paid using administrative leave pay exclusively or in combination with cash. The monetary impact of administrative leave is not considered as a component of reaching the $25,000 threshold, and therefore such settlements are not elevated to the BOCC for approval at a public meeting. One effect of this practice is less public transparency of employment settlements.

The settlement threshold comes into play in another way, as well. We learned about a settlement stemming from an auto accident, where the cumulative value to multiple parties exceeded $25,000, and the County Attorney's Office approved the settlement rather than the BOCC. Clarification of the resolution language regarding the $25,000 threshold would provide guidance about whether such settlements should be approved at the BOCC level. The County Attorney's settlement authority threshold, like the TPA's authority, hasn't changed in years and may benefit from review by the recommended Risk Management Committee for possible increase or alteration

Additional changes could streamline operations and identify new risks

We identified some additional trends and issues with regard to administrative processes:

- Over the past three years, administrative leave paid to employees placed on administrative leave totaled over $1 million, and the expenses are trending up. In FY2016, these expenses were around $230,000, but in FY2018, reached about $550,000. Administrative leave expense may be an indicator of underlying personnel issues. Central Human Resources should track these expenses to help identify issues that need addressing to prevent increasing expenses.

Paid administrative leave is on the rise, signaling an increase in employee investigations and settlements

Source: Auditor's Office analysis of SAP data. Amounts reflect administrative leave pay for those employees on administrative leave, and does not include leave pay for events like snow closures, etc.

- Multnomah County Code generally prescribes the administrative functions and operations of County government. In some cases, the code as written does not reflect current practice. The County should improve this. See Appendix C for detail.
- We strongly suggest that the County form a high level Risk Management Committee to elevate and better communicate larger, organization-wide risk issues, refine approval authorities, and define how much as well as what types of risk it is willing to accept or pursue. Members could include the Risk Manager, County Attorney or designee, and COO or designee.

Recommendations

1. The County under the Chief Operating Officer's direction should begin moving to implement ERM. Appendix A describes what the County should do to implement ERM.
2. Until the governance structure of ERM is firmly in place, the COO will still need to establish a Risk Management Committee. Members of the Committee could include the Risk Manager, County Attorney, CFO and COO or their designees.
3. The recommended Risk Management Committee, should increase the settlement authority amount for the third-party administrator, and clarify settlement amounts for the Risk Manager, County Attorney's Office, Risk Management Committee, and the Board of County Commissioners. The Risk Management Committee should periodically revisit these amounts especially if conditions change.
4. Central Human Resources should track and monitor the use of administrative leave.
5. The recommended Risk Management Committee should update the County Code for better clarity. See Appendix C for specific recommendations.
6. The Sheriff's Office and Department of Community Justice should carry out additional work – possibly a survey – to develop a better understanding of employee perceptions about workplace safety.

Objectives, Scope, & Methodology

The objectives of this audit were to:

- Discuss the benefits of an Enterprise Risk Management (ERM) approach to managing County risks/opportunities as well as the challenges associated with implementing and sustaining it.
- Develop a profile of the County's attitude/opinions towards risk and safety issues by conducting a survey.
- Investigate and seek clarity on various traditional risk management issues.

To accomplish these objectives we:

- Analyzed budgets and other financial information. Reviewed the third party administrator's (TPA) liability account in the County's financial records. We also studied administrative leave associated with employee terminations.
- Interviewed Risk Management personnel, the Chief Financial Officer, the County Attorney and personnel from the County Attorney's Office, and managers in the Sheriff's Office, Department of Community Service, and the Library.
- Contacted and received information from other counties that use ERM.
- Reviewed other jurisdiction's traditional risk management and ERM policies and procedures, audits, governance structures, maturity models, and risk registers.
- Conducted an extensive review of ERM literature.
- Analyzed whether the proper approvals were observed for settlements.
- Included safety questions on the Auditor's Office bi-annual, County-wide survey.
- Reviewed a variety of management reports including audits of the TPA, claims and incidents for FY2016-2018, Risk Management's most recent annual reports, the Insurance Summary Report for FY2018, as well as cost of risk data from the County's insurance broker.
- Explored Risk Management's new claims and incident tracking software.
- Examined the County's risk management code and administrative procedures.
- Reviewed Risk Management's written claim management internal control procedures and job descriptions.

We analyzed Risk Fund financial data for fiscal years 2014 through 2018 from SAP, the County's enterprise resource planning system. Based on the annual review of SAP datasets by the County's external auditor, our office has determined that the data were sufficiently reliable for the purposes of this report.

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.

Audit Staff

Craig Hunt, CPA, Principal Auditor
Marc Rose, MBA, CFE, Principal Auditor

Appendix

Appendix A: ERM Frequently Asked Questions

What is risk?
Risk is the effect of uncertainty on objectives.

What is Enterprise Risk Management (ERM)?
ERM ties risk management to what is most important to the organization. According to the Institute for Internal Auditors, ERM is a "structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives."

ERM addresses the need for information about major risks to flow both up and down the organization and across its organizational structures to improve the quality of decision-making. Through ERM, governments increase both their value to taxpayers and their chances of achieving their objectives.

How long has ERM been around?
ERM has been in practice in the United States for roughly 15 years. The Committee of Sponsoring Organizations (COSO) established the first framework for ERM in 2004, and updated it 10 years later in 2014. The International Standards Organization (ISO) established a framework for ERM in 2009 and updated it in 2018. ERM is best practice and is here to stay.

In July 2016, the federal government issued OMB Circular A-123 that required all federal agencies to implement ERM. U.S. state and local government have lagged behind the private sector but are slowly beginning to realize ERM benefits. Washington, Tennessee and Texas are examples of states that have adopted ERM. Several counties, cities, universities and other local entities such as King County, WA; Yuma County, AZ; Oregon City, OR; University of California, CA; and the Tualatin Valley Water District in Oregon implemented ERM. The use of ERM in other countries is more widespread than the United States.

What are some of the distinguishing features of ERM?
The Risk and Insurance Management Society (RIMS) identified several critical features of ERM:

- ERM includes all areas of an organization's exposure to risk whether it be financial, compliance, operational, strategic, hazard, reputational or other. Organizations prioritize and manage risks as an interrelated risk portfolio.

- Organizations evaluate the risk portfolio in the context of all significant internal and external environments, systems, circumstances and stakeholders. ERM understands that risks in different departments or units can be interrelated and may create a combined exposure that differs from the sum of the individual risks.
- ERM seeks to embed risk management as a component in all critical decisions throughout the organization.

How is ERM different from what the County does now?
The County currently operates in a traditional risk management mode. The chart below compares traditional risk management to ERM.

Traditional Risk Management	Enterprise Risk Management
Focuses on hazards	Strategically focused to align with mission and values
Silo approach	Holistic approach
Tends to focus on reactive analysis	Proactive
Ad hoc and compliance driven	Continuous
Manages risks that can be transferred	Manages risk to mission and strategy
Risk viewed as bad	In addition mitigating risks, ERM recognizes opportunities to pursue.
Risk experts responsible for insurance and prevention. Risk Manager is insurance buyer.	Risk owners manage risk. Risk Manager is the risk facilitator and leader.

Source: Auditor's Office summary of ERM literature

ERM does not replace traditional risk management, which focuses on mitigating losses. Risk management activities the County is currently performing remain a very important function. The County will still have to help keep people safe and respond to claims and lawsuits. As shown in the chart above, traditional risk management is associated with some type of insurance product such as property or general liability for hazards. There may be times when one of these 'traditional' areas will need more attention and could become a new organizational goal for the ERM process.

By using a traditional risk management system, the County has gaps in risk identification, assessment, and treatment between departments or programs that can remain undiscovered. ERM is an effective silo buster that elevates important risks above the department or program level where risks can fall through the cracks and remain unnoticed until it is too late and an adverse event occurs. ERM addresses the full range of an organization's risk portfolio opening the door to a wider variety of choices through organization-wide alternatives.

Although not formally, departments and programs work to manage their risks, but without clear information about any shared risks from other areas of the organization. Traditional risk management results in inefficiencies because it does not manage these shared risks very well. Management's actions taken to deal with risk in one section of an organization may be at odds with those taken in another part of the organization. Different parts of an organization working on the same risks is duplicative and may handle risks inconsistently due to dissimilar approaches to risk management.

What are the benefits of ERM?

There are many benefits to ERM. The value of ERM is difficult to quantify because no monetary loss occurs when an organization identifies and takes action to avoid a harmful risk. That being said, ERM significantly lowered the University of California's total cost of risk from $18.46 per $1,000 in fiscal 2003 to $13.31 per $1,000 of the operating budget in fiscal 2010. In FY2010, alone the university reduced its overall cost of risk by approximately $80 million.

Moody's and Standard & Poor's (S&P) are key rating agencies that affect the cost of borrowing. Both of these agencies now examine organizations' approaches to managing their risks. Because the University of California's ERM approach, it earned a more favorable rating and saved approximately $10 million from 2005 to 2012 by lower borrowing costs through lower interest rates. Yuma County, Arizona's ERM led to better worker's compensation claim management and service, as well as nearly $300,000 in the first year of establishing ERM.

The Electric Power Board (EPB) of Chattanooga is another example of the monetary benefits from implementing ERM. After a large automaker proposed building a plant in the area, the EPB was concerned about how frequent power outages may interfere with the automaker's production. In response to this risk, EPB upgraded their system to reduce the chances of power outages. As additional benefits, when a storm occurred in 2012, these upgrades saved more $1 million in overtime costs. The system upgrade also included automatic meter reading, which provided annual savings of $1.6 million. Without ERM, EPB may not have considered this risk and realized the savings.

ERM focuses management's attention on the organization's most significant risks and greatly improves its ability to meet its mission, goals and objectives. As a silo buster, ERM creates forums where managers work together to identify and manage cross-enterprise risks to draw upon the expertise of all managers involved. As a result, the quality and availability of information improves and strengthens senior leadership decision-making for a more efficient and effective means of managing risk. There are a smaller number of surprises or crises because fewer negative events catch management off guard.

ERM prioritizes significant risks so that an organization can allocate scarce resources to address those risks that best contribute to overall stakeholder value. The organization aligns their risk appetite (risks it desires to pursue) with strategic objectives and uses a consistent approach to evaluate risks. ERM embeds risk into an organization's governance and culture thereby enhancing its transparency and accountability.

How long does it take to establish ERM?

ERM is a continuous process that should mature over time but certainly does not happen overnight. However, with the right setup and high-level support, organizations can begin to realize benefits as ERM develops. Fully implementing ERM may take as long as three to five years. On a cautionary note, ERM development has its own risks according to Price Waterhouse Coopers (PWC). Without firm commitment, PWC observed that ERM programs may build up quickly in response to an event and then atrophy, start and stop every few years or stagnate.

To avoid these difficulties, organizations must try to build an ERM program that can respond well to the inevitable trials it will face. Organizations must strive to create a sustainable, value-adding ERM program that can endure management turnover, shifting priorities and resource challenges. These challenges and others are discussed in more detail below.

Does ERM work for the public sector?

Yes. The benefits of ERM apply to both the public as well as the private sector. The public sector must approach their risks differently than the private sector because the nature of their risks are different. The public sector lacks the profit motive, threat of business failure and must balance their duties of citizen protection and well-being. Public sector entities must continually provide, for example, services for health, social service, and criminal justice programs where a private sector business has the option to discontinue unprofitable services. Private sector risks focus on threats to revenue generation and cost containment. Consequently, the private sector may have a greater risk appetite and higher risk-reward tradeoff.

The public sector does not work to maximize shareholder value by selling goods and services to generate profits as the private sector does. Instead, the public sector maximizes stakeholder value providing services to the public by fulfilling the organization's objectives in a cost-efficient way. According to the IBM Center for the Business of Government: "Achieving organizational objectives in the public sector is frequently made more challenging than in the private sector because there is much less unanimity regarding goals and priorities among external stakeholders." Further, public sector avoidance of many of its risks is not an option.

Cyber security is a good example of how the public sector differs from the private sector. Cyber breaches can be devastating to both sectors. Private sector risks focus on losing a competitive advantage through loss off trade secrets or assets. Public sector risks deal more with protecting confidential client information and the reputational risks from not doing so.

Are there ERM standards available?

There are several ERM governance frameworks available to help organizations develop ERM. Organizations should customize the framework to fit their mission, needs, structure, and culture. Practically, there are only two frameworks for the County to consider: COSO and ISO 31000. There are other frameworks such as the United Kingdom's Orange book but the United States appears to use mostly COSO and ISO 31000.

Risk management professionals in the United States know the COSO ERM well. COSO defines ERM as "a process, effected by an entity's board of directors, management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

ISO 31000 states that the purpose of risk management is the creation and protection of value. ISO 31000's purpose is to integrate the management of risk into a strategic and operational management system. ISO 31000 is flexible and applies to any organization, big or small, private or public. ISO 31000 recommends that organizations develop, implement, and continuously improve a framework whose purpose is to integrate the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values, and culture.

In our opinion, ISO 31000 appears more flexible and adaptable to the County's diverse set of programs than COSO. The Public Risk Management Association supports ISO 31000 as does King County, WA and Yuma County, AZ. The language in ISO 31000 is likely more acceptable to the County than COSO's more financial/internal control oriented language.

How is ERM structured?

Managing risk is part of governance and leadership. The effectiveness of risk management will depend on ERM's integration into the governance of the organization, including decision-making. Good governance builds value through ethical behavior, fairness, transparency, fiscal accountability and social responsibility. Governance creates organizational structure, shapes mission and culture, and establishes policies and procedures.

Organizations need to build their governance structure on the understanding that stakeholders can be internal or external to the agency. Communication and consultation practices should identify risks that include the viewpoints of both internal management as well as external stakeholders.

A survey conducted by the Association for Federal Enterprise Risk Management (AFERM) revealed that while ERM programs exist in a variety of contexts and organizational structures, one common theme (83% of respondents) was that ERM programs have dedicated central resources. Some agency governance structures are beginning to include a central Chief Risk Officer (CRO), dedicated to organization-wide efforts to manage risk.

Effective risk governance requires continuing and focused support from the top of the organization. One approach is to create a risk management committee, chaired by the Chief Operating Officer. A high-level committee or committees should oversee the risk management function. For example, Yuma County, developed charters for two committees: the Enterprise Risk Development Team (ERDT) and a higher-level Enterprise Risk Committee (ERC). The ERDT conducts workshops throughout the County to help identify and discuss key risks. Each quarter, ERC meets to discuss the work of the ERDT.

Regardless of the exact structure, risk committees should make sure there are policies and procedures addressing risk management governance and practices. Risk committees should also ensure there are clear processes for reporting risks on an organization-wide basis and monitor risk controls. Risk committees should monitor corrective actions that address any risk management problems.

How does the culture of an organization affect ERM?

The risk culture of an organization is of critical importance to effective implementation of ERM. Changing a new organizational culture takes time. Culture change can only occur if top-level organization leaders champion ERM and encourage the flow of information needed for effective decision-making. Organizations implementing ERM can choose to build cooperation and collaboration into individual performance standards that encourage management to accept feedback about risks.

The organization must have a strong and positive culture of risk awareness. In a positive risk culture, every person in the organization believes that managing risk is part of his or her job. According to federal government standards, organizations should establish an open, transparent culture that encourages employees to communicate information about potential risks with their superiors without fear of retaliation or blame. This open and transparent culture will identify risks as well as potential opportunities earlier.

Organizations can use many tools for building risk awareness into the culture. To start, the organization should develop a common risk vocabulary. The organization can also train employees on ERM, engage employees in ERM efforts and customize the ERM approach to its mission and culture.

What are risk tolerance and risk appetite?

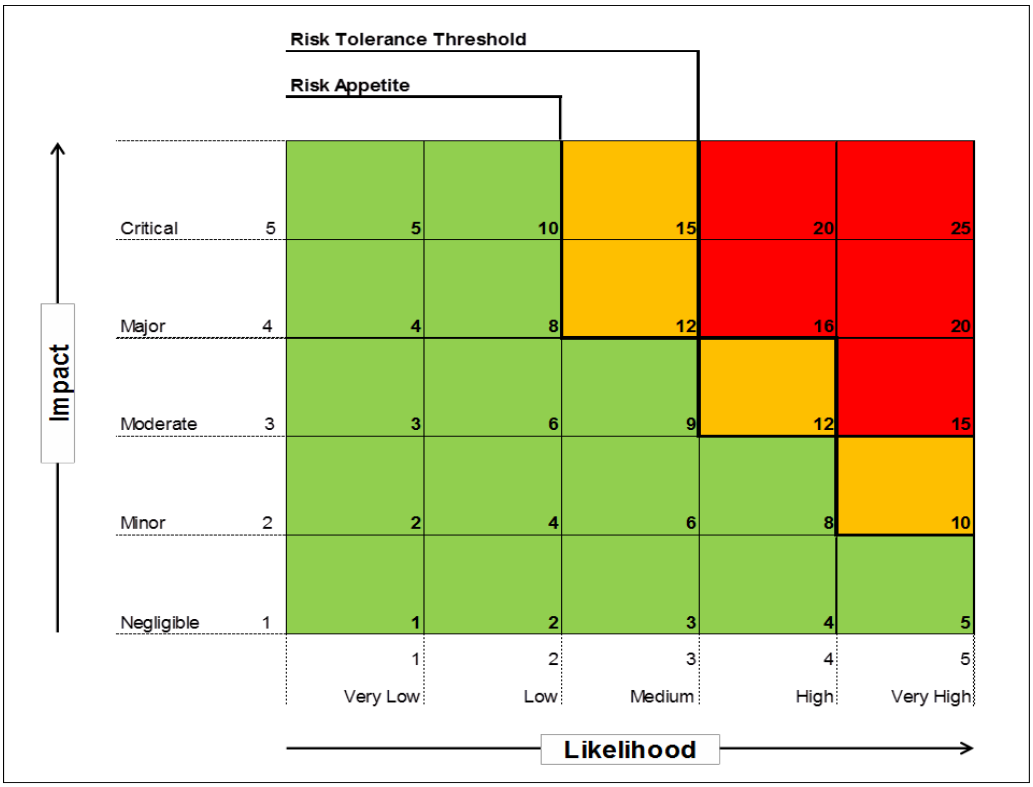
Organizations cannot achieve their objectives without taking risks. Risk tolerance and risk appetite help define how much risk it takes. Accordingly, an effective ERM program is incomplete without determining an organization's risk tolerance and risk appetite.

Risk tolerance is like drawing a risk line in the sand that the organization does not want to cross. Most often quantified and stated in terms of absolutes, organizations often express risk tolerance in terms of unacceptable outcomes. For example, on an organization-wide basis, employee turnover is to be less than x% in any given 90-day period or the percentage of client satisfaction should be above x%.

While risk tolerance is about what management can allow the organization to deal with, risk appetite is the risk an organization wishes to pursue to achieve its objectives. Defining risk appetite is critical to establishing ERM and is needed to formulate risk responses. Defining risk appetite flows down from the Board and up from programs. Each program sets its risk appetite levels that are within the risk appetite boundaries established for the entire organization. Risk appetite will likely be different throughout the organization for different risks and will vary over time.

Risk tolerance and appetite, a product of the risk assessment process described in the next question and illustrated below, reveals the organization's risk profile. The purpose of a risk profile is to provide an analysis of the risks an organization faces toward achieving its strategic objectives arising from its activities and operations.

Heat Map Illustrating Risk Appetite and Risk Tolerance



Source: Risk Management Strategy, West Sussex County Council, United Kingdom, March 2018

What does the risk assessment process entail?

Organizations will first need to identify specific objectives and document them as part of its risk profile. After the organization describes its objectives, the risk assessment process involves risk identification, analysis, evaluation and treatment. According to ISO, the purpose of risk identification is to find, recognize and describe risks that might help or prevent an organization achieving its objectives. Once identified, risks/opportunities can be categorized. For example, ERM addresses all kinds of risks including:

- Strategic—demographic trends, technology innovations
- Financial—credit, liquidity
- Compliance—failure to comply with state or federal regulations
- Operational—cyber security, succession planning, customer service
- Reputational—misuse of resources, contract mismanagement
- Hazard—liability, property, crime, safety

Risk analysis involves a detailed examination of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness. Risk evaluation compares the results of the risk analysis with risk criteria to determine where additional action is required. Criteria for the evaluation of risks includes likelihood and impact as well as time-related factors.

For example, likelihood and impact could be ranked on a 1-5 scale as shown below. Examples of the organization's response to risk include acceptance, avoidance, reduction, sharing or transfer.

Likelihood scale

Likelihood	Definition
1 - Very Low	Risk event **rarely** to occur, or occurs less than once every 10 years.
2- Low	Risk event **unlikely** to occur, or occurs less than once a year, but more than once every 10 years.
3- Medium	Risk event **possible** to occur, **or** occurs between 1-10 times a year.
4. High	Risk event **highly likely** to occur, **or** occurs between 11-50 times a year.
5- Very High	Risk event **almost certain** to occur, **or** occurs > 50 times a year

Source: Playbook: Enterprise Risk Management for the U.S. Federal Government

Impact Scale

Measured Impact	1 - Very Low	2 – Low	3 – Moderate	4 - High	5 - Very High
Reduced quality and performance	Degradation in Activity/Role is negligible	Degradation in Activity/Role is noticeable	Degradation in Activity/Role has Material Impact on Performance of Key Function(s)	Degradation in Activity or Role Requiring Escalation	Degradation of Activity or Role Severely Impacts Key Deliverable or Performance Measure

Source: Playbook: Enterprise Risk Management for the U.S. Federal Government

Management generally has a sense of the risks that their part of the organization faces, but they have no formal risk register and profile to document these risks, risk treatments, and formally track progress.

The risk register and risk profile are two key products of the ERM risk assessment process. To create a risk register managers and staff at all levels of the organization list and describe their major risks. Once completed, the risk register identifies enterprise risks and documents the risk analysis, risk scores, risk treatments, results of risk treatments and status of each risk. The risk profile uses the risk registers to prioritize an inventory of the most significant risks.

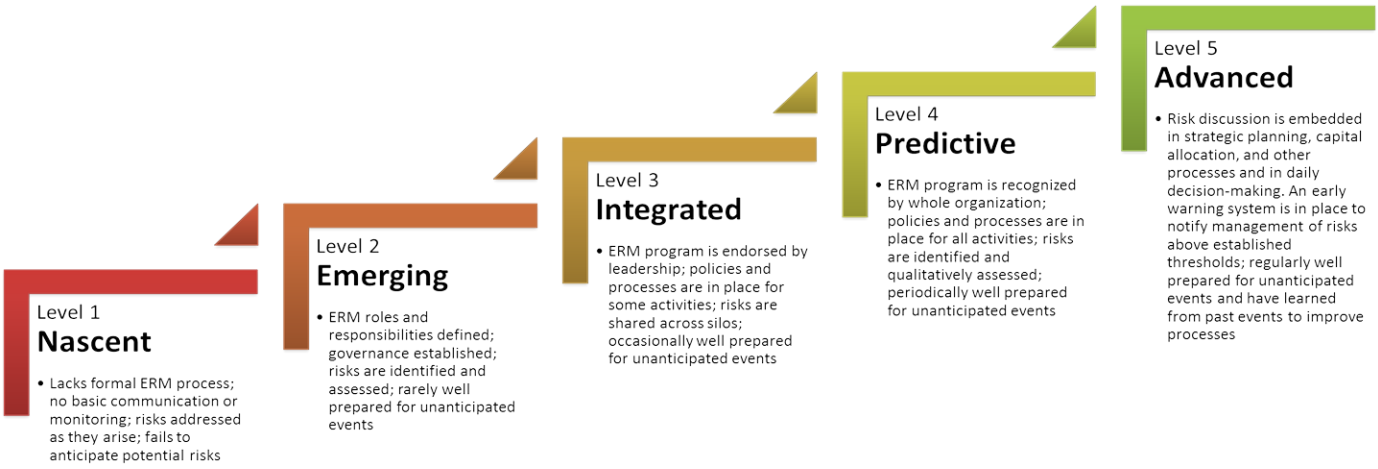
How do organizations monitor the progress of ERM efforts?

Maturity models play an important role to monitor ERM development. Risk maturity is a benchmarking tool, which measures the extent an organization implements ERM in accordance with best practices. Risk maturity can change over time due to internal and external factors. As an organization changes, ERM also needs to evolve to ensure it continues to support the

achievement of its objectives. When necessary, organizations should develop strategies to improve its risk maturity. Maturity scores should increase as ERM programs become more developed and integrated into planning and operations.

According to the Risk Management Society, statistical analysis proves that higher risk maturity levels translate into better performing organizations. Risk maturity goes beyond ensuring an ERM framework is solidly in place. It also requires an organization to assess whether its framework is effective. This means an agency would need to determine if risk management is contributing to its overall performance, is operating as expected and outcomes are achieved. The diagram below illustrates process maturity levels. Note that risk maturity models differ.

A maturity model helps monitor ERM development



Source: Playbook: Enterprise Risk Management for the U.S. Federal Government

Is there risk management software available?

The success of ERM programs depends on clearly communicating risk assessment efforts across the entire organization. Organizations must purchase or develop user-friendly software to communicate this risk information. According to the literature, organizations must use specialized software to fulfill this need. There are several ERM-focused packages available to choose.

Yuma County, AZ looked overseas to find an affordable ERM software package. Yuma uses an online program that everyone in the County has read only access. The software uses a

dashboard and risk register to communicate risk information. Departments and programs can monitor their risk assessments and treatments as well as see others' risk information. The availability of cross-entity information for all participants helps to break down any silos.

What are the challenges of ERM?

ERM must have solid support from the top of the organization. In fact, a high-level champion is a critical factor for building and sustaining a successful ERM program. Another make-or-break barrier to an organization's establishment of an ERM program is siloed data and decision-making. ERM is not an isolated activity. Organizations should fully integrate ERM into its day-to-day management and steadily into its culture. Other challenges include:

- Making sure that all staff understand ERM and demonstrating its value to the organization.
- Committing sufficient resources.
- Placing the ERM program at a high level in the organization and having a clear mandate to implement it.
- Positioning ERM as a strategic management practice and not as an additional task. Organizations should not view ERM as another layer of bureaucracy.
- Working closely with program leaders. An ERM program's role is to provide assistance to others in the organization.
- Changing leadership can stop or slow ERM implementation.
- Developing ERM is an iterative effort that matures over time. Try not to do too much too quickly.

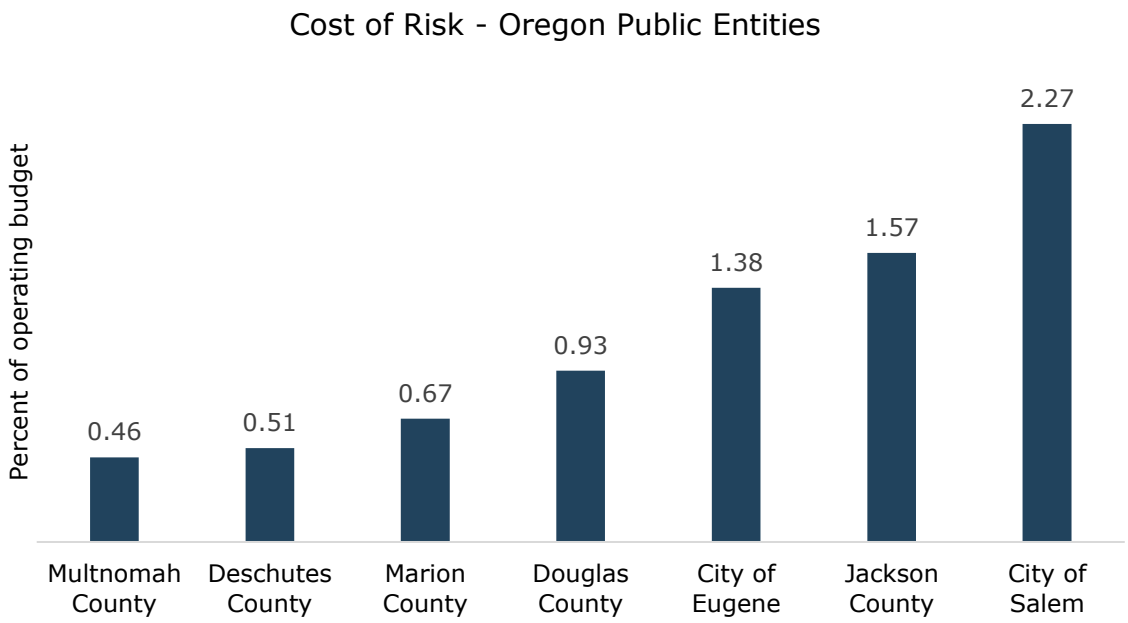
Staffing the ERM program needs a team with knowledge and experience in risk management. The size of the team should be large enough to meet organizational needs but can likely be drawn from existing County resources.

Appendix B: Cost of Risk Benchmarks Well

The cost of risk is a key performance indicator used by the County that compares its risk management costs to other jurisdictions. Total cost of risk includes uninsured claims costs, insurance premium costs and administrative costs. Administration costs include County Attorney, Risk Management personnel, third party administrator and broker costs. The County's cost of risk for combined liability and worker's compensation insurance in FY2017 compares favorably to other jurisdictions. The County's insurance broker prepared the following costs and chart.

County Attorney Legal Costs-Liability	$	1,865,485
Worker's Comp Claims Payments		1,731,994
Risk Management Personnel Costs		539,087
Liability Claims Payments		521,586
Excess Insurance Cost		417,321
Other Insurance		236,599
TPA annual fee		326,340
Broker fee		55,105
Subtotal	$	5,693,517
Less Recoveries	$	162,643
Total Cost of Risk	$	5,530,874
As a Percentage of Operational Budget		0.46%

The County's cost of risk compares favorably to other jurisdictions



Source: Multnomah County's insurance broker who indicated that Multnomah County's cost of risk data combining liability and worker's compensation insurance costs is from 2017, and data from other organizations in the chart is from several years earlier.

Appendix C: Code Revision Suggestions

These suggested code revisions would need to be modified by action of the Board of County Commissioners.

Suggested revisions to the Code:

- Add language to the County Code, referencing the use of an ERM model.
- Change the wording in 7.101 B from "…expenditures may be charged…" to "…expenditures will be charged..."
- A consistent approach to paying insurance premiums should be established in code. Currently some departments pay some policy premiums separately over and above internal service charged dedicated to insurance costs through the Risk Fund. The recommended Risk Management Committee discussing the financial allocation process would assist with ensuring a transparent and fair governance is established.
- Add language to address the need for a Risk Management Committee.
- Change code wording to reflect current name of the state agency responsible for the administration of worker's compensation reserves, the Department of Consumer and Business Services.

Response Letters

March 20, 2019

Jennifer McGuirk, County Auditor
501 SE Hawthorne Blvd, Suite 600
Portland, OR 97214

Dear Auditor McGuirk:

Thank you for the opportunity to review and comment on the *"Risk Management, Adopting Enterprise Risk Management will help the Count better manage its risks"* audit.

We feel we have the fundamental structure in place to develop an enterprise risk management program that will mature over time. We will utilize an existing leadership committee already practiced in identifying and mitigating risk that includes the COO, CFO, and County Attorney for the creation of a Risk Committee. With the guidance of the Risk Services Manager, the Risk Committee will receive training, develop an operational framework, and be tasked with prioritizing the recommendations outlined in the audit.

The audit identifies two areas that we consider a top priority for the committee to undertake. The audit's analysis of the levels of settlement authority in comparable public sector entities demonstrates an area where the Committee could perform a risk assessment and offer recommendations. The Committee could also assist in evaluating the use of administrative leave to determine an approach that best meets the County's needs and objectives.

The Risk Management team is currently assisting management in implementing localized ERM activities where compliance or funding requirements dictate it. Expanding on this activity, and utilizing the newly acquired Risk Management Information System (RMIS) to prioritize and document risk assessments, will allow program maturation once objectives are clearly defined.

The audit also addresses sections on employee safety and health that demonstrate the need for management involvement in the employee safety effort. We agree with this assessment. The Risk Management loss prevention team is dedicated to assisting both employees and management in providing a safe and healthy workplace. They will continue to work with management, employees, the Safety Steering Committee, and building safety committees to achieve safety best practices.

Thank you for reviewing the Risk Fund and operations within the Finance and Risk Management Division. We are pleased with the opinion that the traditional risk management operations function well and look forward to establishing ERM processes as part of County governance.

Sincerely,

Mark Campbell
Chief Financial Officer

cc: Marissa Madrigal, Chief Operating Officer/DCM Director
Jenny Madkour, County Attorney
Michelle Cross, Risk Services Manager

Multnomah County Sheriff's Office

501 SE HAWTHORNE BLVD., Suite 350 • Portland, OR 97214

Exemplary service for a safe, livable community

MICHAEL REESE
SHERIFF

503 988-4300 PHONE
503 988-4500 TTY
www.mcso.us

March 15, 2019

Multnomah County Auditor's Office
Attn: The Honorable Jennifer McGuirk
501 SE Hawthorne, #601
Portland, OR 97214

Dear Auditor McGuirk,

The Sheriff's Office has received and reviewed the Auditor's Report regarding Risk Management to include survey results regarding workplace safety and providing a better understanding of employee's perception of the County's safety culture. As a professional within the criminal justice system for over 28yrs, I am keenly aware of the challenges within risk management for large public safety organizations. As Sheriff, I value and encourage a positive work environment recognizing that I am not only responsible for the community's safety but also my staff. Individuals working in law enforcement and corrections face potentially dangerous conditions on a daily basis in order to fulfill our vision of a safe and livable community. MCSO appreciates the Auditor's recommendation to the County to become more prepared by adopting an Enterprise Risk Management Model. We agree; this model provides for a more proactive and preventative approach versus the traditional way of managing loss.

The Sheriff's Office is committed to the overarching goal of learning from the employees about specific workplace safety concerns. To meet this goal, the Sheriff's Office is in the early stages of implementing the Employee Information System (EIS). This program supports the goal of developing and encouraging its members to grow professionally by supplying information to supervisors that will allow them to better develop, manage and support staff through consistent reinforcement.

Information that will be pre-programed within the Employee Information System will include commendations, complaints, control events, traumatic incidents and training history. The Supervisor of the involved employee can take non-corrective action designed to give members feedback on their performance and promote best practice, such as coaching, commending, debriefing, counseling, monitoring referral to the Employee Assistance Program (EAP), etc.

This new program will give an opportunity for the employee to offer a response within the EIS entry, which will be reviewed by both the employee's supervisor and manager.

Furthermore, the Sheriff's Office has already implemented a new way to capture and monitor the incidents where staff are assaulted. Prior to October 2018, this data was not accurately captured. This data will be used to monitor the number of employees being assaulted in their workplace and help us develop strategies to reduce or respond to these situations.

Lastly, the Sheriff's Office plan to create a follow-up survey with its employees to better grasp the specificity of workplace safety concerns. This survey would be completed by the end of 2019, with results sent to the Auditor's Office by March 2020.

Respectfully,

Michael Reese
Sheriff