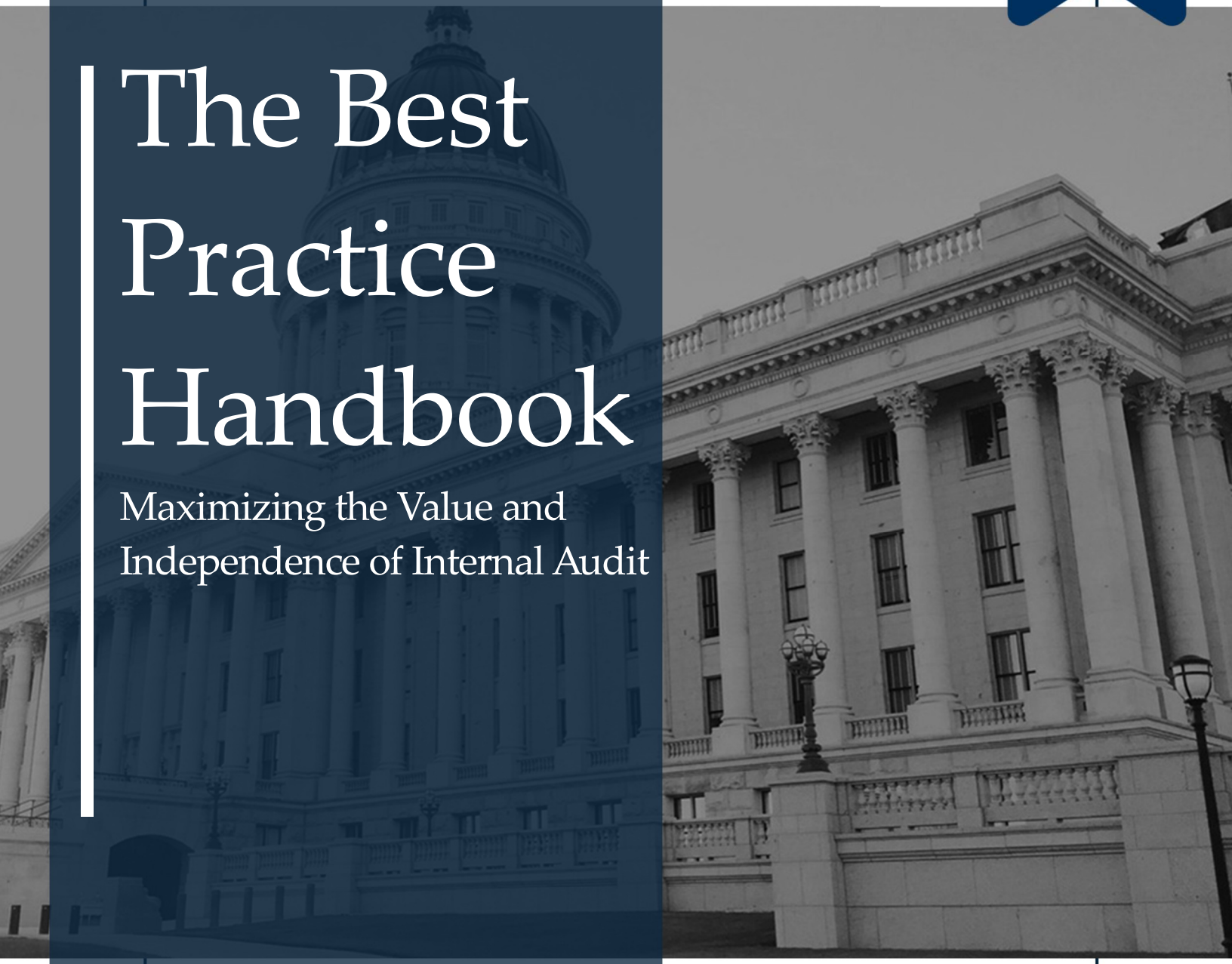
Report No. 2026-07

LEGISLATIVE AUDITOR GENERAL

The Best Practice Handbook

Maximizing the Value and Independence of Internal Audit



A Handbook for **UTAH GOVERNMENT EXCELLENCE**

LEGISLATIVE
AUDITOR GENERAL

Audit Subcommittee

President J. Stuart Adams, Co-Chair
President of the Senate

Senator Kirk Cullimore
Senate Majority Leader

Senator Luz Escamilla
Senate Minority Leader

Speaker Mike Schultz, Co-Chair
Speaker of the House

Representative Casey Snider
House Majority Leader

Representative Angela Romero
House Minority Leader

Audit Staff

Kade R. Minchey, Auditor General, CIA, CFE

Brian Dean, Manager, CIA, CFE

Brent Packer, Audit Supervisor

Rusty Facer, Audit Supervisor

Brittni Anderson, Staff

Office of the Legislative Auditor General

Kade R. Minchey, Legislative Auditor General

450 N State Street, Suite N385 North Capitol Building | Salt Lake City, UT 84114 | Phone: 801.538.1033

Audit Subcommittee of the Legislative Management Committee

President J. Stuart Adams, Co-Chair | Speaker Mike Schultz, Co-Chair

Senator Kirk Cullimore | Representative Casey Snider

Senator Luz Escamilla | Representative Angela Romero

April 16, 2026

TO: THE UTAH STATE LEGISLATURE

Transmitted herewith is our report:

"The Best Practice Handbook: Maximizing the Value and Independence of Internal Audit" [Report #2026-07].

The Best Practice Handbook: Maximizing the Value and Independence of Internal Audit is a resource for all government organizations in the state of Utah. In the handbook, we describe the blueprint for high-value auditing. Governance, Strategy, Execution, and Impact are the four critical spheres of influence that help maximize the value of internal audit. This handbook is meant to provide best practices for internal auditors, organizational leaders, and oversight bodies that supplement audit standards provided by entities such as the Government Accountability Office and the Institute of Internal Auditors.

Policy makers and leaders need more than compliance and financial opinions. They need accountability with actionable solutions. High-impact auditing leads to meaningful improvements for organizations. We encourage executive leaders, oversight bodies, and internal audit to collaborate and improve internal auditing.

This report is published initially under an "Open Comment Period." The purpose of the open comment period is to receive feedback from a broad audience on how to make this report as useful and practical as possible. Once the open comment period concludes, we will publish a final version based on feedback we have received.

Sincerely,

Kade Minchey

Kade R. Minchey, CIA, CFE

Auditor General

kminchey@le.utah.gov

Acknowledgments

Special thanks to the members of our internal audit workgroup for their insights and guidance throughout the development of this handbook.

Rebecca Cushing, Audit Manager — Department of Environmental Quality
Debbie Davis, Chief Audit Executive — Utah State Board of Education
Chris Harding, County Auditor — Salt Lake County
Scott Healy, Internal Auditor — Granite School District
Mike Hurst, Director of Internal Audit — Utah Transit Authority
Wayne Kidd, Internal Audit Director — Administrative Office of the Courts
Travis Lansing, Chief Audit Executive — Salt Lake Community College
Scott Tingley, Internal Audit Director — Department of Government Operations
James Welchel, Director of Internal Audit — Department of Workforce Services

Additional appreciation is extended to the organizational leaders, governing body members, internal auditors, county auditors, and other partners who helped with the development of this report through interviews, surveys, and providing feedback that further advanced the quality of this product.

LEGISLATIVE AUDITOR GENERAL

AUDIT SUMMARY

REPORT 2026-07 | APRIL 2026

Office of the Legislative Auditor General | Kade R. Minchey, Auditor General

BEST PRACTICE HANDBOOK

THE BEST PRACTICE HANDBOOK: MAXIMIZING THE VALUE AND INDEPENDENCE OF INTERNAL AUDIT

BACKGROUND

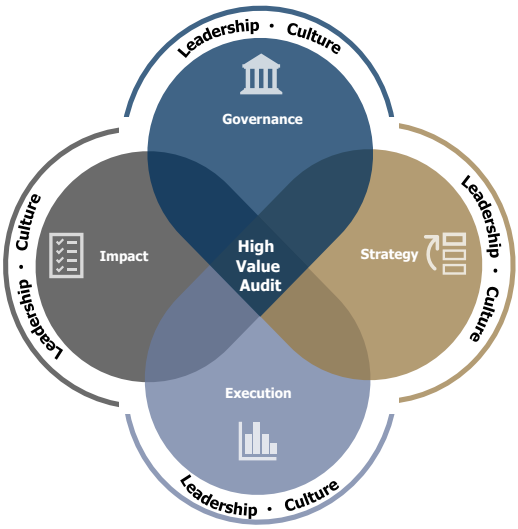
This is the fourth Best Practice Handbook released by our office. The most recent one, *The Best Practice Handbook: Diagnosing Root Causes and Driving Results*, focuses on identifying the causes of poor performance and intervening on those causes.

This Handbook is designed to maximize internal audit's (IA) capacity to consistently produce relevant, reliable, and actionable information, which is IA's primary product. It is intended to supplement audit standards.

Utah Code 36-12-15 requires our office to monitor and report on the health of government organization's IA functions, and to make recommendations to increase the independence and value added of IA functions throughout the state.

Increasing the value of IA increases the value of the organization's products and services. We encourage leaders to use this Handbook to improve their internal audit functions and their organizations.

THE FOUR SPHERES OF INFLUENCE



Governance: Organizational leaders provide enough independence, authority, and capacity for auditors to do their job, and organizations apply effective risk management.

Strategy: Organizational and audit leaders select audits based on organizational risk, strategic objectives, and key questions.

Execution: Auditors develop highly relevant, reliable, and actionable information, while organizational leaders hold audit leaders accountable.

Impact: Organizational and audit leaders work together to track and implement recommendations made in audits.

CALL TO ACTION

Auditor General Kade Minchey:

We are calling for a new era in Utah government auditing. Policymakers and leaders need more than standard compliance and financial opinions written in stereotypical report formats. They need accountability with actionable solutions. They need high-impact auditing that leads to meaningful improvements. They need recommendations that improve organizations. Let's collaborate to innovate and shape the future of auditing."

Maximizing the value and independence of internal audit requires action from three stakeholders:

- Internal Auditors (Section 1)
- Organizational Leaders (Section 2)
- Oversight Bodies (Section 3)

Table of Contents

Introduction

Leaders exist to advance the missions of their organizations. Government organizations' missions are vital to the well-being of the Utah citizenry. For example, missions of Utah agencies include

Department of Public Safety

Keeping Utah Safe through dedicated public service and partnerships to protect Utah's great quality of life.

Department of Health & Human Services

[S]upport and serve all individuals and communities…through effective policy and the operations of an effective and efficient seamless system of services and programs…

Utah State Board of Education

Academic and organizational excellence in Utah education for an elevated, educated citizenry.

Utah Department of Agriculture and Food

To support the development of Utah's agriculture and food industries, serve as a steward of our natural resources, safeguard public health, protect consumers, and ensure a quality food supply.

To drive these and all missions forward, leaders must take decisive action to transform organizational effort into results. Good information is central to achieving those results. Without good information, leaders don't have the necessary feedback loops to make good decisions. Organizations are then vulnerable to ineffectiveness and inefficiency, and leaders fail to advance the mission.

Internal audit (IA) is designed to meet leaders' needs for good information. Good information is highly relevant, reliable, and actionable to key stakeholders. By providing this type of information to key stakeholders, auditors can strengthen the organization's ability to create, protect, and sustain value. This empowers every organization's core purpose—to reliably produce a set of outcomes.

Too often internal audit isn't recognized for its central role in organizational success. Without a

Increasing the value of internal audit increases the value of the organization's products and services.

robust internal audit function, leaders won't have the information they need to make the best decisions. Without good decisions, the organization is prone to inefficiency, ineffectiveness, fraud, waste, and abuse.

This Handbook is written to help organizational and audit leaders better leverage the audit function. Increasing the value of internal audit also increases the value of the organization's products and services. Though written to support Utah government organizations, we believe this Handbook is applicable to all organizations—public or private, large or small, new or mature.

As **organizational leaders** prioritize their need for relevant, reliable, and actionable information, organizational improvements can accelerate. As internal audit leaders strengthen their capacity to consistently provide this kind of information to stakeholders, they'll be a catalyst for change in their organizations.

Organizational leaders: For purposes of this report, we define this as management level staff such as executive or division directors.

Such a profound shift requires transforming government auditing practices. Utah Legislative Auditor General, Kade Minchey, has released a "Call to Action" inviting all leaders to shift toward value-first, high-impact auditing in government.

Auditor General Kade Minchey:

"We are calling for a new era in Utah government auditing. Policymakers and leaders need more than standard compliance and financial opinions written in stereotypical report formats. They need accountability with actionable solutions. They need high-impact auditing that leads to meaningful improvements. They need recommendations that improve organizations. Let's collaborate to innovate and shape the future of auditing."

This Handbook outlines many of the best practices that offices can adopt to increase their ability to provide this type of information to stakeholders.

We recently presented an audit in our Legislative Audit Subcommittee meeting that found an agency's reports to the Legislature were not including the information needed. In the subcommittee, one senator expressed concern with information being omitted. The senator said, "As Legislators, when we don't have information it makes it really hard." In response, the agency director acknowledged "You can't do your jobs if we're not giving you adequate feedback." The same is true for leaders, who cannot do their jobs if they do not know where the issues are. The director went on to say, "…this is another good illustration of why auditing is so important, because without the audit we wouldn't have known that those [issues were occurring]."

We invite all leaders to apply the best practices found in this Handbook and to advance the missions of their organizations for the benefit of the citizens of the state of Utah.

The Blueprint for High-Value Auditing

Leaders' use of high-quality information from auditors to act and make decisions leads to

- Successful achievement of organizational objectives
- Stronger governance, risk management, and control processes
- Improved decision-making and oversight
- Enhanced reputation and credibility with stakeholders
- Ability to serve the public interest

Better information drives better decisions, and better decisions drive better outcomes.

In short, better information drives better decisions. And better decisions drive better outcomes.

The Institute of Internal Auditors (IIA), explains the purpose of internal audit.[1]

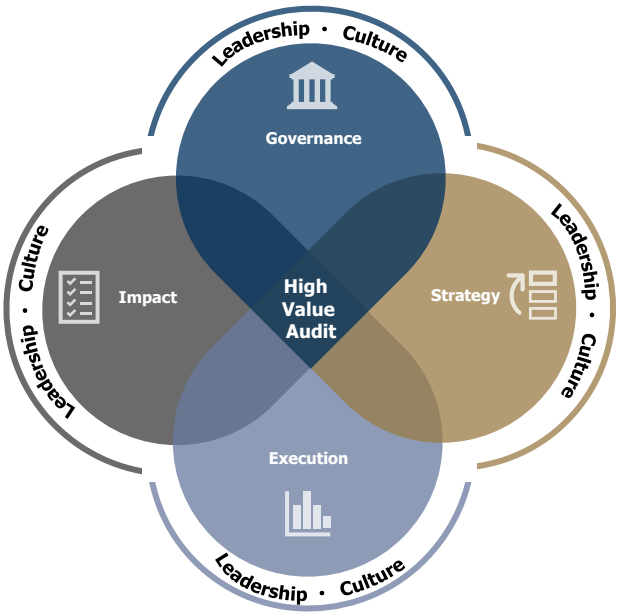
[1] ***Utah Code*** 63I-5-102 (9)(c), the Utah Internal Audit Act names two sets of audit standards that apply to audit functions. The first is the International Standards for the Practice of Internal Auditing issued by the Institute of Internal Auditors. The second is the Government Auditing Standards issued by the Comptroller General of the United States. We reference both extensively throughout this resource.

Purpose of Internal Audit:

"Internal auditing strengthens the organization's ability to create, protect, and sustain value by providing the board and management with independent, risk-based, and objective assurance, advice, insight, and foresight."

Utah Code further states that IA "objectively evaluates the effectiveness of agency, division, bureau, or office governance, risk management, internal controls, and the efficiency of operations…"[2] IA offices should strive to perform these critical functions.

To maximize the value of the audit function, all leaders must excel in four critical spheres of influence: governance, strategy, execution, and impact.



Governance: Organizational leaders provide enough independence, authority, and capacity for auditors to do their job, and organizations apply effective risk management.

Strategy: Organizational and audit leaders select audits based on organizational risk, strategic objectives, and key questions.

Execution: Auditors develop highly relevant, reliable, and actionable information, while organizational leaders hold audit leaders accountable.

Impact: Organizational and audit leaders work together to track and implement recommendations made in audits.

Source: Auditor generated.

Highly relevant, reliable, and actionable information is IA's primary product.

These spheres are vital because they empower audit offices to have the ability to produce highly relevant, reliable, and actionable information for stakeholders, which is IA's primary product.

For Any of These Four Spheres to Have Any Effect on Organizational Outcomes, They Must Be Accompanied by Strong Leadership and Culture. We believe successful transformation largely hinges on these two catalysts. Organizational leaders

[2] ***Utah Code*** 63I-5-102(9)(b).

must nurture a culture that embraces the audit function and welcomes its involvement. By committing to advancing internal audit, leaders are committing to advancing the organization's mission. At the beginning of each section, we discuss the vital role of leaders to shape culture and advance the four spheres of influence.

Organizational Leaders and Oversight Bodies Enable Audit to Succeed

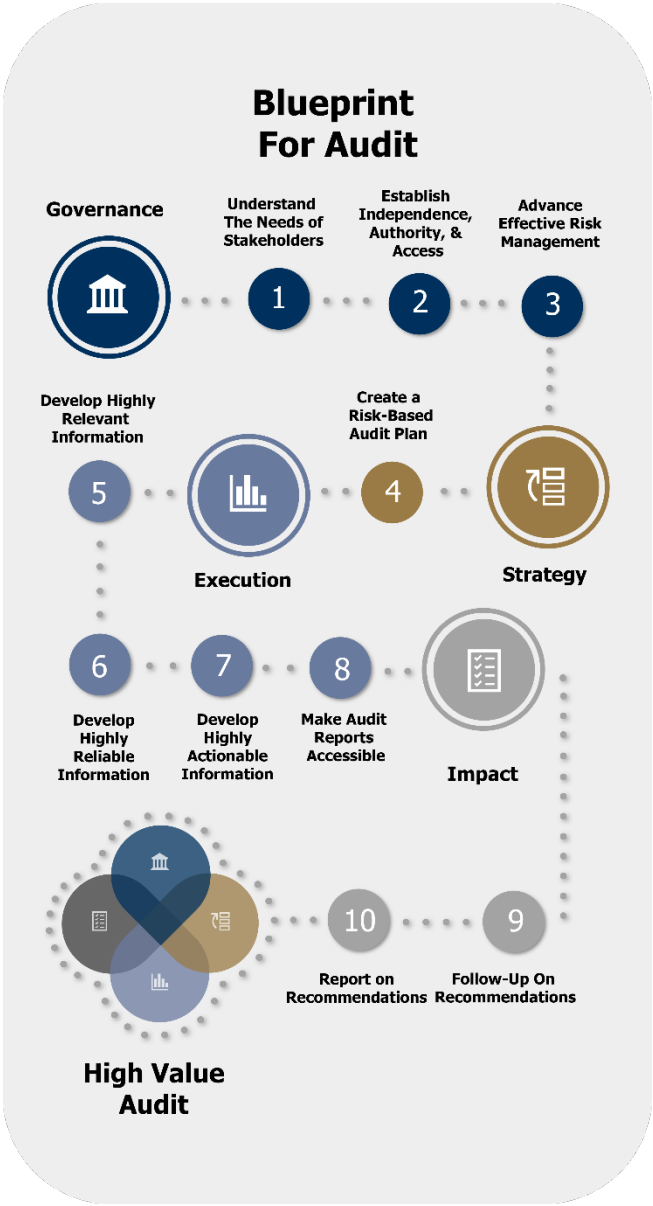
For organizations to make meaningful changes based on the work of internal auditors, organizational leaders and **oversight bodies**[3] must set the conditions that allow IA to succeed. Because the following stakeholders play a critical role in the audit process, this Best Practice Handbook is organized to show how each group helps achieve high-value audit work:

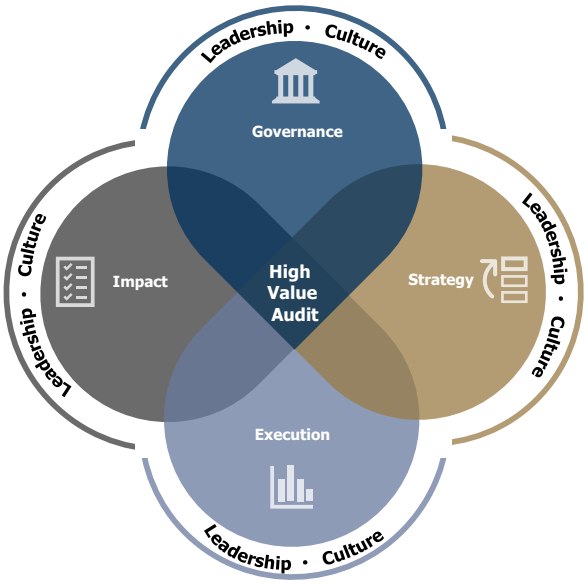
- Section 1: Internal Audit
- Section 2: Organizational Leaders
- Section 3: Oversight Bodies

Oversight bodies: For purposes of this report, we define this as groups with governing power such as the Legislature, boards, or commissions.

Each section explains how these stakeholders can leverage the four spheres of influence to maximize the value of internal audit. If all three groups implement these best practices and foster a culture of change, organizations will have the information they need to make good decisions and therefore achieve good outcomes.

[3] In this report, we highlight that for internal audit to succeed, they must report to the highest level of the organization. Because government organizations have significant differences between their structures, the highest level of the organization can include executive leaders, boards or commissions, legislative bodies, the Governor, or directly reporting to voters.





Information About This Report

Section 1 covers best practices for internal auditors. There is overlap in content and examples between sections of this report because internal auditors, organizational leaders, and/or oversight bodies approach issues from different perspectives.

Leadership & Culture

Without strong audit leaders creating and supporting an innovative culture, there will be no high value audits. Utah's former Chief Innovation Officer encouraged leaders to eliminate the "It's not my job" mentality. Auditors can improve efforts to avoid "It's not my job" by focusing on driving real, positive improvements. This focus creates a culture of excellence both within the audit office and in the organization.

While it's important for all professionals to "stay in their lane," we believe audit directors can and should widen their lane. Too often we see stereotypical audits that could have offered much more value for the organization. By being creative and innovative, internal audit can demonstrate their value. Once executive leaders can see the value of good audits, it can grow into more impactful work.

Section 1
Internal Audit

Internal audit (IA) should be a tool to create better organizations with better outcomes. Highly relevant, reliable, and actionable information is an essential part of what IA should offer. In short, IA should provide better information, which drives better decisions. And better decisions drive better outcomes.

Better information drives better decisions, and better decisions drive better outcomes.

This section addresses the four spheres of influence through the audit lens. Creating good **governance**, employing solid **strategy**, **executing** at a high level, and ensuring audits have **impact** can guarantee IA is providing the highest possible value.

Governance: The Foundation for Audit Value

Auditing is one of three vital functions to good organizational governance.[4, 5] This prominently positions IA to have an outsized impact on the organization. Audit leaders should capitalize on this opportunity to contribute to the success of the organization. While it is important to "stay in your lane," we believe audit leaders should "widen their lane" to build capacity to develop whatever type of information their stakeholders need.

Governance: Broadly establishes the structures and processes necessary to direct, inform, manage, and monitor the organization.

In this section, we refer specifically to the **governance** of internal audit. In order to provide the most value, IA's governance must allow for audit leaders to

- Know the stakeholders' needs
- Use independence and authority to do their work
- Assist organizational leaders to perform adequate risk assessments

[4] *The Best Practice Handbook: A Practical Guide to Excellence for Utah Government*, 2023.

[5] Effective governance broadly establishes the structures and processes necessary to direct, inform, manage, and monitor an organization. When the governing body applies principles of good governance, it fosters organizational success and augments the value the organization provides.

Governance 1: Audit Leaders Must Be Intimately Familiar With the Needs and Key Questions of Stakeholders

Audit leaders should prioritize meeting the needs of their stakeholders. This requires a strong understanding of what those needs are. Ways for audit leaders to stay informed include:

- Attend and participate in organizational leadership meetings
- Meet with governing bodies regularly and frequently
- Ask questions about leaders' knowledge gaps
- Be familiar with the organization's strategic plan and its goals

After understanding these needs, audit leaders should then align their work with the resulting concerns. Then, they must promote the work IA can do.

Some people view IA as merely a tool for financial verification or compliance. This view limits the likelihood that organizational leadership will turn to audit when they need to know if a program is having an intended effect, or if a division could operate more efficiently. It is crucial that stakeholders understand not only what audit is doing, but what it can do. Audit leaders need to make sure stakeholders understand what is possible.

Audit leaders must help stakeholders understand not only what audit is doing, but what it can do.

In recent years, the Utah Legislature has expanded our office's responsibilities partially because audits we performed showed them what performance auditing can provide. Some of our additional ongoing oversight responsibilities include the following:

- Reviewing local education agencies
- Reviewing the Utah System of Higher Education and its institutions
- Monitoring the health of internal audit
- Creating a statewide high-risk list
- Performing investigative audits

We believe these responsibilities show the Utah Legislature's understanding that we can offer high-quality information in critical areas that matter to the state's progress.

Once management understands IA's potential value, IA has to step up to provide that value. Audit leaders should focus on cultivating the office's ability to produce different kinds of information. This empowers the office to be versatile

in meeting stakeholder needs. Leading with value should always be the foundation for all that the audit office does.

The Salt Lake County Auditor provides another example of how to "widen the lane" of internal audit and help meet the needs of the stakeholders. The county auditor worked with stakeholders to strengthen their audit authority, increase the requirements for auditor qualifications, and enable more performance audits to be done in the county. While not every internal audit shop needs these types of changes, every audit director should look for ways they can better meet the needs of their stakeholders and provide value to the organization.

Internal Audit Best Practice 1

Internal audit leaders should understand stakeholder needs and key questions so they can focus audits on the most important risks, use resources effectively to meet organizational priorities, and provide recommendations that lead to meaningful improvements.

Governance 2: Audit Charters Should Establish Audit Independence and Capacity

Audit charters should be written to strengthen audit independence and capacity, key attributes to good audit governance. Although organizational leaders are responsible for ensuring auditors have the independence and capacity to perform high-value audits, IA is responsible for shoring that up with their audit charter.

Audit Charter: A document that includes the audit functions, mandate, position, reporting structure, scope of work, services, and other items.

Independence first ensures the information provided by the audit function is unbiased. Essentially, independence positions reliable, accurate information as the foremost objective. It establishes safeguards to protect the motivations of auditors. Without independence, bias is prone to enter the information development process through perverse incentives. The Institute of Internal Auditors (IIA) states that the audit function can only fulfill its purpose when the audit director reports to the highest level of the organization.

Independence: The freedom from conditions that impair the internal audit function's ability to carry out its responsibilities in an unbiased manner.

One way audit functions can strengthen independence is by using a formal charter. Charters should be customized to fit the needs of the board and senior management and the organizational operating environment.

Audit charters also explicitly grant IA functions the necessary **authority** to perform their work. For example, the ***Utah Constitution*** grants the legislative auditor its authority.[6]

Authority: Unrestricted access to the highest reporting level, as well as records, personnel, and physical property.

Utah Constitution:

"The legislative auditor shall have authority to conduct audits of any funds, functions, and accounts in any branch, department, agency or political subdivision of this state and shall perform such other related duties as may be prescribed by the Legislature. The legislative auditor shall report to and be answerable only to the Legislature."

This authority ensures OLAG can perform the work required of the legislative branch. At the time of OLAG's establishment, the first Auditor General, Dr. Lennis M. Knighton,[7] stated

Dr. Lennis M. Knighton, Utah's First Legislative Auditor General

"…the scope of audit inquiry for a legislative auditor should be as broad as is the legislature's need for assistance in its oversight responsibility, limited only by the availability of resources and the competence of the audit staff."

We believe all audit functions should have an equally broad scope of audit inquiry relative to their agencies. For IA functions in Utah, ***Utah Code*** 63I-5-102 requires internal audit to be independent, and audit charters should reaffirm this standard.

Governing bodies and organizational leaders must invest time and attention to strengthen IA's organizational independence and authority. In turn, it's up to audit leaders to zealously guard that independence and authority. If either is threatened, audit leaders should report those breaches to their governing authority. Threats to independence or authority include:

[6] ***Utah Constitution***, Article VI, Section 33 [Legislative auditor appointed].

[7] Dr. Lennis M. Knighton is considered one of the fathers of performance audit. In 1975, there was a national trend to establish legislative performance audit offices. These offices were created to meet the growing need for meaningful oversight, including a focus on efficiency and effectiveness in state government.

- An entity that is being audited refusing to supply the auditors with necessary data
- Management telling auditors not to look at a high-risk area
- Management refusing to fund internal audit unless they change a negative audit finding
- Auditors being asked to work on a program they may soon audit

Additional Resources

Best Principles for Utah Audit Charters (Appendix A)

IIA Model Internal Audit Charter

Example Utah Audit Charters (Appendix A)

IA directors should ensure that audit functions work with organizational leaders to maintain the strict independence and authority listed in their charters. These values allow IA to continue to provide high-quality information and value to their organizations.

For many years the Department of Natural Resources' (DNR) internal audit director was also the department's finance director. The Office of the State Auditor had continued concerns for 26 years about the independence of DNR's internal audit function. When we audited DNR, we also shared the same concern. DNR finally split the positions after our audit. This helped to resolve organizational independence and objectivity concerns for the internal audit function.

Internal Audit Best Practice 2

Internal audit should ensure they create and periodically review the audit charter that addresses how they will maintain independence and authority.

Governance 3: Internal Audit Can Increase Value by Advancing Effective Risk Management

When organizations practice effective risk management, they are more likely to

- Create and protect value

- Achieve core objectives
- Make informed decisions
- Address uncertainty
- Continually improve as an organization

Importantly, IA assists organizational leaders as they develop effective risk management practices. Specifically, we believe IA should facilitate the establishment and maturity of Enterprise Risk Management (ERM) frameworks without compromising their independence.[8]

Risk: the possibility that something will happen that adversely affects the organization's achievement of their objectives.

Effective risk management is crucial to organizational success. **Risk** is the possibility that something will happen that adversely affects the organization's achievement of their objectives.[9] If the organization's risks aren't mitigated, it will be less successful in advancing its mission. ERM is considered an effective, agency-wide approach to manage organizational risk. All organizations can benefit from applying an integrated approach to risk management.

We believe IA has a prime opportunity to advise leaders on Enterprise Risk Management best practices.

Managing risk is organizational leadership's responsibility. However, we believe IA has a prime opportunity to advise leaders on ERM best practices.[10]

Additional Resources

Enterprise Risk Management Template (Center for High Impact Auditing)

Enterprise Risk Management Tool Guidance (Appendix B)

Resources were developed with the support of our audit leaders' workgroup.

The Governor's Office requires executive branch agencies to submit annual risk assessments. It also provides guidance on performing "Entity-Wide Risk

[8] Enterprise Risk Management (ERM) is an agency-wide approach to identifying and addressing the organization's combined risks.

[9] *Standards for Internal Control in the Federal Government*, U.S. Government Accountability Office, 2025.

[10] The Internal Audit Foundation anticipates IA will spend about 70% more of its time doing advisory work by 2035 (*Internal Audit: Vision 2035, Creating Our Future Together*, Institute of Internal Audit, 2023). We believe advising on effective risk management can increase the value internal audit provides.

Assessments," which we view as synonymous with ERM. Many organizations fall short of established best practices for risk management.

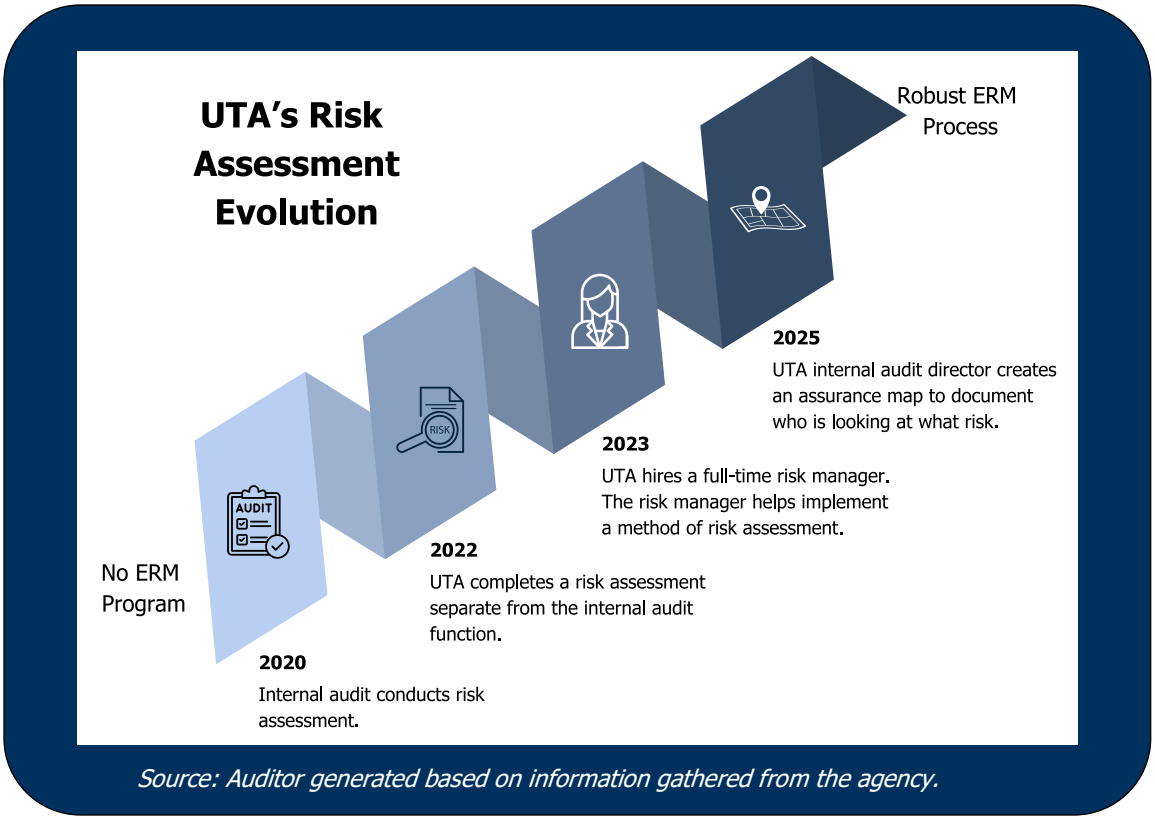
Section 2 of this report outlines organizational leaders' best practices in ERM. We encourage audit leaders to support organizational leaders as they apply these best practices. As organizations improve their ERM, it will set the stage for prioritizing high-risk audit work in the audit plan.

CASE STUDY
Utah Transit Authority

The Utah Transit Authority (UTA) did not have an effective risk management system in the past. In 2019, an effective risk assessment could have mitigated the effects of a $51 million write-off, including more than $13 million in land. In response to a 2019 recommendation from the Federal Monitor, UTA agreed to establish an enterprise risk management (ERM) program. The evolution of its ERM program is depicted on the graphic on the next page.

UTA's current risk assessment process reportedly involves employees at all levels, from management down to those who supervise one employee. UTA documents all risks, categorizes and organizes them, and assigns a person to oversee them. UTA risk management consults with management to remediate identified risks. As an additional step, the internal audit director uses an assurance map to document who is looking at the highest-level risks and any gaps in the coverage. This robust risk assessment process not only helps document their risks but ensures that the agency is managing its risks.

This risk assessment process did not happen overnight but rather was an iterative process. Both the risk manager and the internal audit director have played an active role in integrating a robust risk assessment process into the agency. We believe their efforts to follow up on risks to ensure they're mitigated and to document gaps in handling risks has strengthened UTA's governance.



Source: Auditor generated based on information gathered from the agency.

A mature ERM will also help to strengthen the organization's control environment, reducing demands on the audit function as strong controls and consistent monitoring reduce risks to the organization.[11]

Risk response should begin with the most serious risks. The purpose is to reduce risks to a reasonable or acceptable level. Internal audit's role in this process should include further auditing the most serious risks to give management the information they need to mitigate that risk. We encourage audit leaders to facilitate and support the development of an effective ERM through their advisory work.

> According to a 2025 OLAG audit, the Utah Office of the Inspector General of Medicaid Services (OIG) provided little evidence of independent oversight of Accountable Care Organizations (ACOs) since 2018. ACOs manage nearly one-and-a-half billion dollars in Medicaid spending. By failing to prioritize oversight of such a large risk, the OIG limited its impact and put over $1 billion at risk of waste.

[11] *Standards for Internal Control in the Federal Government*, U.S. Government Accountability Office, 2025.

The Utah State Board of Education (USBE) has not conducted an agency-wide risk assessment. The internal audit team performs a risk assessment to help build their audit plan, but management does not direct an enterprise risk management process. This is concerning as management should be conducting an enterprise risk assessment process, separate from internal audit's risk assessment for the audit plan. Internal audit should continue to advocate for management to implement an agency-wide risk assessment.

The Utah Courts System's internal auditors identify risks based on previous audits and feedback from centralized court leadership, then sample them to conduct risk assessments. They do not always use each individual court's leadership to determine what risks they should evaluate. Without some leadership's involvement, we believe internal auditors may be missing risks. Leadership at every court should be involved in identifying and ranking risks. The same is true of every organization where auditors are asked to help facilitate or advise on the risk management or assessment process.

Internal Audit Best Practice 3

Internal audit should advise organizational leaders on effective enterprise risk management. They should then use the results of enterprise risk management to help guide their auditing efforts.

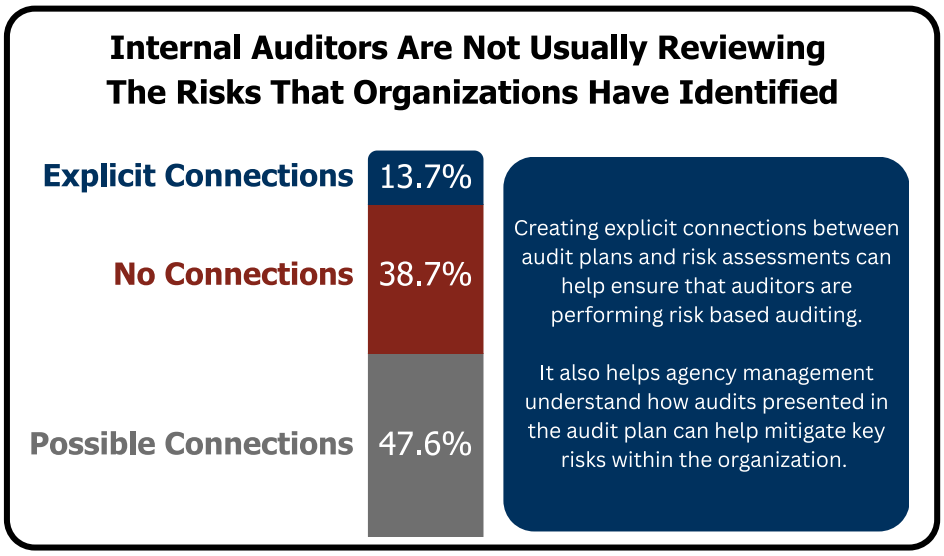
Strategy: Audit Leaders Must Advocate for Impactful Work

Strategy 4: Agency Risk Assessments and Critical Goals Should Drive Audit Work

IA is a scarce resource. So, audit leaders should focus on work that addresses the most critical risks and goals. The opportunity for meaningful impact begins with which areas IA examines. This is another example of how audit directors can widen their lane. Either through their own risk assessment process or through findings of the ERM, IA can use these as opportunities to inform the most critical areas of an organization.

The Global Internal Audit Standards require audit leaders to annually develop an audit plan based on the organization's strategies, objectives, and risks.[12] ***Utah Code*** directs the audit leader to develop audit plans based on the findings of periodic risk assessments.[13]

From a selected sample, we found nearly 40% of audit plans were not directly tied to the organization's risk assessment. This suggests that either IA work is not aligned to the most critical risks in the organization, or that the organization's risk assessment is poor. Unless IA is used to address information gaps in the most critical areas, it will have limited impact.



Source: Auditor generated using agency risk assessments and audit plans.

[12] *Global Internal Audit Standards*, Standard 9.4. Institute of Internal Auditors, 2024.

[13] ***Utah Code*** 63I-5-401 (1)(f).

Audit leaders should include high-risk areas when developing audit plans. Certain threats should always be top concerns. For example, some of the common risks we look for in our audits include the following:

- Loss of life
- Large dollar impact
- Poor effectiveness and efficiency
- Public harm
- Statutory or contract violations

Audit leaders should focus on work that addresses the most critical risks and goals.

If an area has one of these risks, IA can provide substantial value in directing leaders on how they can mitigate the threats.

When audits focus on minor concerns or lower objectives, it doesn't leave time for higher-value work. In contrast, concentrating limited audit resources on the biggest needs can reduce the frequency and intensity of organizational issues. It can also keep those issues from being discovered by outside entities.

> The Department of Health and Human Services' (DHHS) internal audit office conducts investigations of individuals, often related to Medicaid fraud. When time is spent on non-audit responsibilities that could be taken care of by other entities, they limit their ability to focus on work that only the independent audit function can provide the organization.

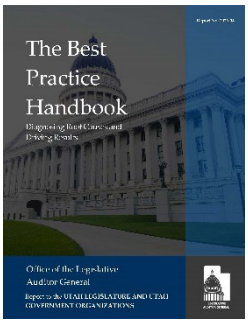
Additionally, ***Utah Code*** requires audit plans to adequately cover efficient and effective use of agency resources.[14] Organizational leaders must make hard decisions on how to best advance the mission of the organization. In our report, *The Best Practice Handbook: Diagnosing Root Causes and Driving Results*, we explain that stakeholders need and want to know what works in their organizations.

[14] ***Utah Code*** 63I-5-401 (2)(a)(iv).

The Best Practice Handbook: Diagnosing Root Causes and Driving Results

"Stakeholders consistently need information on how to make government work well for the citizens of the state. They want to know the causes of issues so that they can intervene effectively. They also want to know if policies, programs, and initiatives are successful. If successful, stakeholders want to know how to expand. If unsuccessful, they want to make changes to promote better outcomes. In short, stakeholders are interested in the type of information that enables them to make government better."

Audit leaders can add value by developing information for organizational leaders that would otherwise be unknown. IA should seek opportunities to answer stakeholders' key questions. Organizational leaders can rely on this information to make the best decisions. These decisions direct the work toward meaningful activity that produces desirable results.



Audit leaders can and should educate their governing bodies and management on how to best leverage the IA function. They should strive to identify the most critical challenges facing the organization and include these areas in their audit plans. By leading with organizational risk, IA can position its work to be meaningful and impactful.[15]

Internal Audit Best Practice 4

Internal audit should focus their work on the most critical risks and goals of the organization. Internal audit should also develop information for organizational leaders that otherwise would not be known. As organizational leaders rely on information that auditors provide to make decisions, the organization can effectively advance its mission.

[15] We acknowledge that some audits are required or may be necessary despite their limited impact. We encourage audit leaders to determine the proper proportion of risk-based audit work. We also encourage audit leaders to consider working with stakeholders to reduce the frequency of low-risk and low-impact audits.

Execution: Auditors Should Produce High-Quality Information and Communicate Clearly

IA exists to help organizations improve. To play that role, audit leaders must provide value to stakeholders. Auditors' value comes from providing highly relevant, reliable, and actionable information.[16] Several factors influence IA's ability to consistently produce this kind of information. As IA builds capacity, it can amplify its value as it supports organizational leaders in the advancement of the organization's mission.

CASE STUDY
Department of Alcoholic Beverage Services

Our 2025 audit of the Department of Alcoholic Beverage Services (DABS) found that their IA didn't consistently provide high-quality information. Several of IA's audits didn't meet basic expectations for relevance and reliability, which contributed to ongoing problems within the agency.

IA Information Wasn't Relevant

In just one example, IA's less-relevant information contributed to serious inventory issues. The audit plan included a request for an audit of the agency's IT system. The system supports their financial transactions, inventory management, and point-of-sale operations. The audit was requested to review of one of the highest-risk areas of the organization. Instead, the audit was delayed for a year and half. When it was finally released, the audit focused on the system's contract, rather than the controls that management needed evaluated. Because of this less relevant information, the system continued to allow issues that enabled theft and poor inventory practices.

[16] Auditors both enhance the value of existing information through verification and provide new information through information development. We focus in this subsection on strategies and best practices for developing new information to drive good decisions and organizational improvement.

IA Information Wasn't Reliable
Other audits contained incorrect or outdated information. In several instances, internal audit did not verify information with management before issuing the report and did not ensure the findings reflected the most current conditions. These practices led to unreliable recommendations that were not useful to decision-makers. Over time, problems such as these weaken trust in the audit function and reduce the likelihood that management will act on recommendations.

Execution 5: Information Must Be Relevant

To increase the value of information, auditors must pursue **audit finding** with strong **effect.** Examples of strong effect include public danger, large dollar impact, and program ineffectiveness. Without effect, the audit finding may not be worth reporting. We call this "dollars chasing pennies." In simple terms, effect answers the question: Does this problem matter?

Effect answers the question: Does this problem matter?

Auditors can ensure information is highly relevant by clearly defining **audit objectives**. Auditors should focus objectives on critical risks and goals. Good audit objectives are

Audit Finding: A rigorous, action-oriented answer to an important question.

Effect: The impact, outcome, or consequence of a finding.

Audit Objectives: What the audit is intended to accomplish.

A good objective helps the audit team to determine an appropriate methodology. Without a clear question it is impossible to find a clear answer. Pursuing strong effect and setting good audit objectives empowers the audit team to focus its efforts on the most valuable and meaningful information.

Without a clear question it is impossible to find a clear answer.

Internal Audit Best Practice 5

Internal audit should make sure information is relevant. To be relevant, they must pursue strong effect. Auditors should define the audit scope and objectives and tie these to stakeholder needs. Auditors must determine when stakeholders will need information and scope the audit to provide important information at the time key decisions or changes will be made.

Execution 6: Information Must Be Reliable

Reliable information is the bedrock of the audit profession. Information must be accurate to drive good decisions. Inaccurate information from IA leads to bad organizational decisions and ruined audit credibility. Auditors must take audit standards seriously, collect appropriate evidence, and support their findings. Otherwise, the information they provide will likely not be reliable. Decisions made on unreliable information can harm the organization. If IA doesn't provide reliable, accurate information, it is useless to the organization.

Quality Assurance Confirms the Accuracy of Findings. Auditors must collect enough evidence to convince a knowledgeable person of their findings. They should document the evidence so that another auditor or similarly competent person could repeat the work and come to the same conclusions. This can be done by supporting each finding in a report with evidence. Auditors should provide a trail of evidence that could lead a reviewer from the **workpapers** to the conclusions. In large audit shops, supervisors should review the evidence and ensure that it supports the findings, conclusions, and recommendations of the report before the audit is released. While a supervisory review is not practical in single-person audit functions, auditors should still provide a trail of evidence that could lead a reviewer to the conclusion found in the report.

Workpapers: Documentation of work done that supports information in audit findings and conclusions.

Internal Audit Best Practice 6

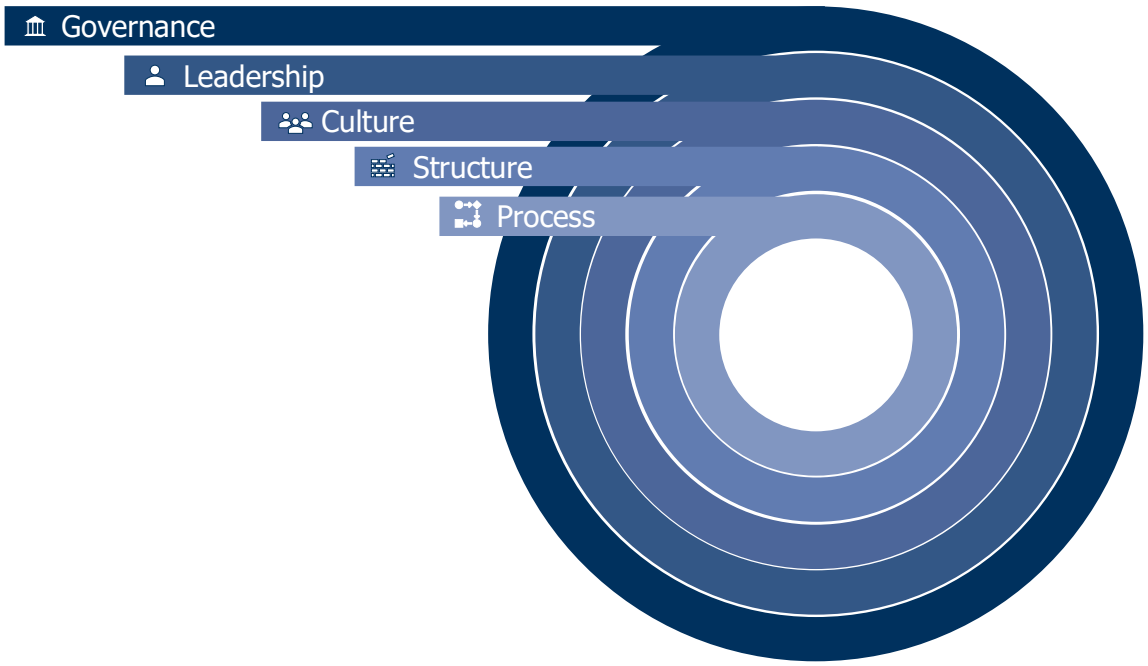
Auditors' information must be reliable. Internal audit (IA) should consistently follow audit standards, tailor audit methodologies to produce accurate information, and support findings in a way that a knowledgeable person could agree that the findings are correct.

Execution 7: Information Must Be Actionable

To maximize the value IA provides to the organization, information must be actionable. When IA identifies problems without offering clear recommendations for improvement, decision-makers may be limited in their ability to use the information to drive meaningful improvement. Auditors should include recommendations to correct identified deficiencies wherever possible. However, for the recommendation to correct the identified deficiency, auditors must first identify the root cause of the issue.

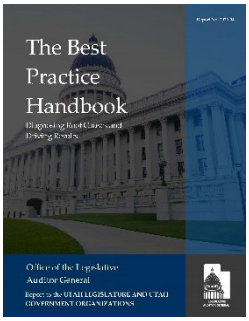
Identifying Cause Is the Key to the Real Solution. In 2026, we released our report, *The Best Practice Handbook: Diagnosing Root Causes and Driving Results*. In the report, we introduce the Five Layers of Cause Framework to assist leaders, auditors, and evaluators in identifying the root causes of organizational issues. Figure 1.3 illustrates the Five Layers of Cause Framework.

Figure 2.1 The Five Layers of Cause Framework, Ordered from Most to Least Impactful. Good governance is vital to organizational success, while process is more limited in its impact.



Source: OLAG's Five Layers of Cause Framework.

The list is hierarchical, ranking the layers from most to least impactful. Generally, when an organization has a governance weakness, that weakness flows downstream to issues across all other layers. In contrast, when an issue resides at the process level, it tends to be less pervasive.



Recommendations that target the set of causes leading to a deficiency often achieve the best return on investment. In addition, solutions tend to last longer because they move beyond treating symptoms. We encourage auditors to read our Handbook on diagnosing root causes and to apply the Five Layers of Cause Framework in their audits.

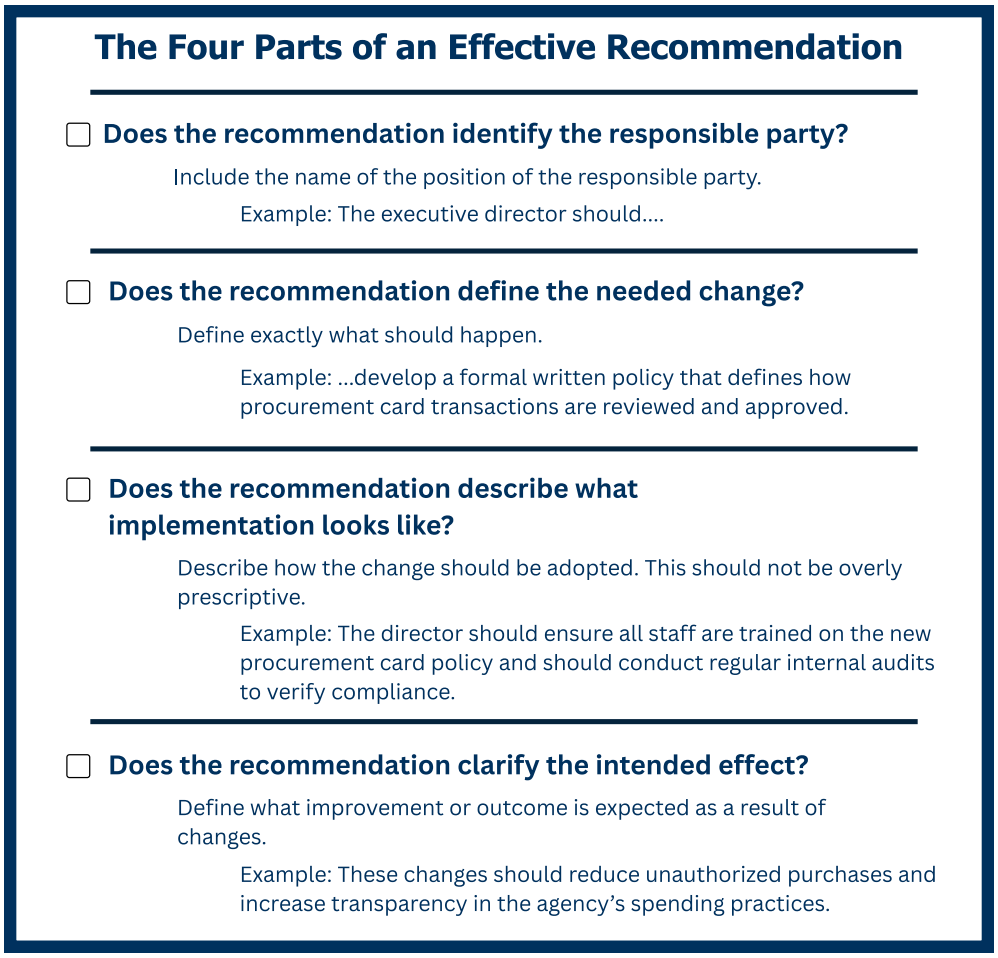
Click here to read *The Best Practice Handbook: Diagnosing Root Causes and Driving Results.*

Recommendations Must Drive Improvement. Implemented recommendations should increase the organization's effectiveness, efficiency, or compliance.

Effectiveness refers to whether objectives were achieved, while efficiency is getting the most from available resources.

Auditors must write recommendations that address the root causes of their audit findings. When the agency implements recommendations but it doesn't produce the intended changes and outcomes, either IA wrote the recommendation poorly, identified the wrong cause, or both.

We believe effective recommendations include four parts. Auditors should include all four parts to ensure the right changes are made and intended outcomes are realized.



Source: Auditor generated.

We have developed the four-part recommendation through experience and auditee feedback. Many of the problems that arise during implementation can be avoided by writing effective recommendations.

Auditors should focus on high-level recommendations that are not overly prescriptive. While process changes are important, detailing every process change the auditee should make is overly cumbersome. Ticky-tacky findings may not merit a change. Instead, auditors should look for patterns in the audit findings that point to deeper, more systemic issues. Recommendations that focus on superficial symptoms of the problem are unlikely to sustainably resolve the issue.

Internal Audit Best Practice 7

Auditors must ensure their information is actionable. To write effective recommendations, auditors must properly identify the root causes of their audit findings. Recommendations should be designed to intervene on the causes of the issue. Recommendations should

1. Identify the responsible party
2. Define the needed change
3. Describe what implementation looks like
4. Clarify the intended effect

By focusing actions on changing the conditions causing negative outcomes, auditors can empower leaders with the knowledge they need to make good decisions and improve their organizations.

Execution 8: Audit Reports Should Be Accessible to Stakeholders

Stakeholders must be able to understand audit reports quickly. Increasingly, information is abundant and comes from all directions. In addition to being relevant and reliable, IA must focus on making information immediately understandable to cut through the noise. If stakeholders can't understand the report, they are less likely to implement its recommendations. Making information quickly understandable takes time and effort. IA must make reports understandable, because increasingly, stakeholders won't take the time to understand unclear information. Auditors' main goal should be to improve their organizations; if their findings are too dense to understand, they will fail at that goal.

If stakeholders cannot understand the audit report, auditors will fail at their main goal—to help organizations improve.

Clear communication is important for more than making decision-makers' lives easier. It also communicates the professionalism and, therefore, the reliability of the audit function.

Harvard Business Review: Better Business Writing

"You may think you shouldn't fuss about your writing – that good enough is good enough. But that mind-set is costly. Supervisors, colleagues, employees, clients, partners, and anyone else you communicate with will form an opinion of you from your writing. If it's careless and sloppy, they may assume your thinking is the same. And if you fail to convince them that they should care about your message, they won't care. They may even decide you're not worth doing business with. The stakes are that high."

Some ways IA can make reports useful and accessible to stakeholders include:

- **Intensive planning**—A quote often attributed to Abraham Lincoln says, "Give me six hours to chop down a tree and I will spend the first four sharpening the axe." It is easy to write everything one knows on paper. The effort comes through planning what is most relevant to include, and more importantly, what not to include.
- **Simplified language**—It is important to write in a way that you would want to read. Dense, technical writing is neither persuasive, nor helpful. If management wanted a technical report, they could bypass audit entirely and go straight to the source. Simplifying and summarizing helps show IA's value. In 2010, the federal government enacted the Plain Writing Act.[17] It was designed "to enhance citizen access to Government information and services by establishing that Government documents issued to the public must be written clearly." State and local auditors should follow suit.
- **Figures and graphics**— "A picture is worth a thousand words." This aphorism is repeated over and over because it's true. Technical or number-heavy ideas are often communicated most clearly with a graphic. Forbes Communication Council says, "Rather than sifting through dense blocks of text or complicated data sets, viewers can grasp key points at a glance, enhancing comprehension and retention." Allowing decision-makers to "grasp key points at a glance" should be a goal of audit communication.

[17] Public Law No. 111-274.

Internal Audit Best Practice 8

Internal audit must communicate in the simplest, most accessible ways. Some ways to accomplish this include planning the simplest reports, simplifying language, and relying on figures and graphics to help stakeholders make decisions based on the best information.

Impact: Internal Audit Must Confirm Recommendations Are Implemented

Audit effectiveness is largely defined by the benefits achieved from implemented recommendations. The bottom line of audit work is improved organizations, saved tax dollars, and better service to the public. Recommendations transform good information into actionable steps organizational leaders can take to produce desirable results. Auditors should take the time to monitor whether recommendations have the intended results. This requires formal, consistent **follow-up** on audit recommendations. We encourage IA to make implementation status transparent to stakeholders to promote accountability.

Follow-Up: Monitoring and verifying management's implementation of audit recommendations.

Impact 9: Internal Audit Should Meaningfully Follow-Up On the Implementation Status of Recommendations

Organizational leadership is responsible for implementing audit recommendations, but internal auditors must regularly determine the status of implementation. For OLAG audits, ***Utah Code*** requires the chief officer of the audited organization to develop an audit response plan that includes the following elements: [18]

Elements Required in OLAG Audit Responses

- **Identifies how the entity will implement each recommendation**
- **Identifies an individual responsible for implementing a recommendation**
- **Establishes a timetable that identifies benchmarks for the entity to implement the recommendation**
- **Specifies an anticipated deadline by which each recommendation will be fully implemented**

Defining these elements long before follow-up begins promotes robust accountability and clarity. Our office follows up at least annually until recommendations are implemented. This involves evidence reviews and, in some cases, additional audit work.

IA functions should set follow-up intervals appropriate for the nature of their organization and the audit work.

See OLAG's Audit Response Guide

[18] ***Utah Code*** 36-12-15.3.

These intervals should be frequent enough to maintain accountability and avoid recommendations falling by the wayside. We are concerned that when auditors wait to follow up until after full implementation of recommendations, or not at all, management may not address them. The following examples show what happens when management does not address risks:

> A recent audit of Utah State University (USU) found that the internal audit office did not follow up on audits to track recommendations or encourage their implementation. This may have contributed to USU leadership not reviewing, prioritizing, or addressing the recommendations. In one audit, this allowed overspending to continue despite important recommendations that could have been more quickly addressed.

> Despite being required by the Department of Natural Resources' (DNR) policy, their internal audit function did not perform follow-ups on prior audit findings. Some of the audit recommendations were intended to address variances in inventory and strengthen controls over finances. DNR was continually assuming risks for which auditors identified but never followed up on.

Ultimately, the frequency for follow-ups should be conducive to recommendation implementation. In part, the frequency and timing of follow-up should match the urgency of the deficiency. If follow-up indicates that a significant recommendation is not progressing, auditors should consider additional steps, including elevating follow-up to a higher level of the organization. Audit leaders should work with organizational leaders to set intervals that reflect both the speed and urgency of implementation.

Similarly, meaningful follow-up assessments should be conducted based on the risk's significance. Internal auditors should not accept, without verification, that recommendations have been implemented. More significant recommendations, such as those involving the potential loss of life, may need further testing to ensure recommendations have been implemented.

Meaningful follow-up assessments should be conducted based on the risk's significance.

GAO Guidance for Audit Follow-Up:

"For more significant recommendations, implementation actions should be tested. For key or critical recommendations that have not been implemented within a reasonable time, another audit or strategy may be warranted."

Auditors should use their judgement to determine the adequate level of review needed to ensure recommendation implementation. In some cases, this may include performing a follow-up audit or conducting test work based on the audit's risk level.

Internal Audit Best Practice 9

Internal auditors should follow up on audit recommendations and conduct additional audit work as necessary to ensure that internal changes are made.

CASE STUDY
Utah Department of Corrections

Our office reviewed Utah's prison medical system in 2021 and found significant concerns with how the Clinical Services Bureau provided care for inmates. Some of these concerns included:

- Problems with patient monitoring
- Problems with providing care for diabetic inmates
- Noncompliance with national accreditation standards
- Needed improvements with administrative oversight

After the first audit, the Department of Corrections (UDC) management asked internal auditors to review the recommendations and provide updates on their implementation. This review was unfinished when UDC reported to the Legislature that most of the recommendations were implemented. Internal audit's review likewise reported to UDC management that many of the same audit recommendations had been implemented.

Because the Legislature was interested in ensuring implementation, they authorized an OLAG In-Depth Follow-Up of Healthcare in State Prisons that was completed in 2023. Of the recommendations OLAG reviewed,

nine recommendations UDC had reported as implemented were still in process, and some remained significant risks to the department.

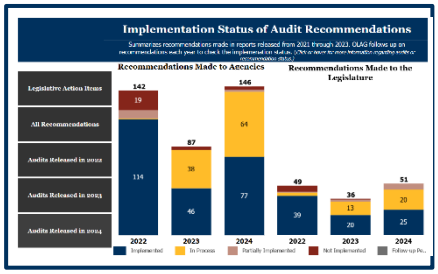
In 2023, prison medical services were moved to the Department of Health and Human Services (DHHS). In 2024, DHHS's internal audit followed up on the 2023 OLAG report and said that many of the recommendations were implemented. However, a second OLAG follow-up, released in 2025, found many recommendations were not yet implemented.

We interviewed both internal audit groups who often marked recommendations implemented if a policy was in place, with only some instances of limited testing. In high-risk situations, especially those that affect people's lives, IA needs to do more intensive work to ensure that processes are working.

Impact 10: Tracking and Reporting on Recommendation Progress

After following up on audits, our office reports the status of all recommendations for at least three years publicly on our website. We use four categories to indicate the status of our recommendations:

1. **Implemented**—Recommendation was fully implemented.
2. **In process**—Additional time is needed for full implementation.
3. **Partially implemented**—Not all portions of the recommendation will be implemented.
4. **Not implemented**—Recommendation was not implemented.



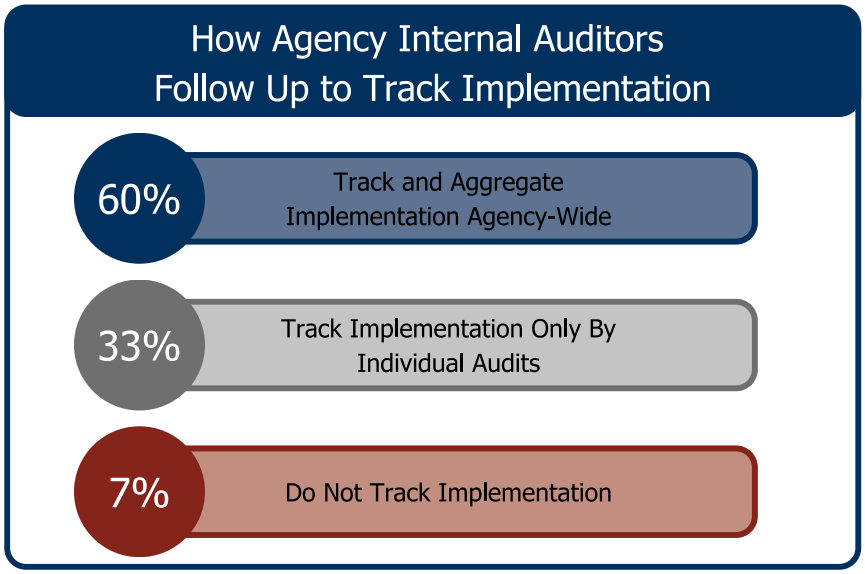
Tracking and publishing this information provides transparency for the Legislature. They can use this information to take legislative action or hold agencies accountable for implementation. In audited agencies, this information tells management where there is still work to be done. Organizational leaders can use this knowledge to hold the people responsible for making the necessary changes.

IIA Internal Audit Standards:

"Internal auditors must confirm that management has implemented internal auditors' recommendations or management's action plans following an established methodology, which includes:

- *Inquiring about progress on the implementation.*
- *Performing follow-up assessments using a risk-based approach.*
- *Updating the status of management's actions in a tracking system."*

To help promote accountability and transparency, internal auditors should create and use a system to track recommendation implementation. Tracking should be done each time the auditor follows up, as determined by their established timelines. Most auditors at agencies required to have an internal audit function already do some form of follow-up, as noted in the graphic.



Source: Auditor generated using agency follow-ups or other documented information.

While any sort of implementation tracking provides auditors with an idea of what management is doing to correct problems, we believe that aggregated, agency-wide data can be the most important. This is an area that allows internal auditors to provide value to the organization because this information gives organizational leadership knowledge of what work still needs to be done. Like our recommendation dashboard, this allows leaders to hold the right people accountable.

Without acting on information from audits, agencies may not address problems, and the same risks may remain.

Without acting on information from audits, agencies may not address problems, and the same risks may

remain. Internal auditors can encourage change by providing information on the status of recommendations to organizational leadership.

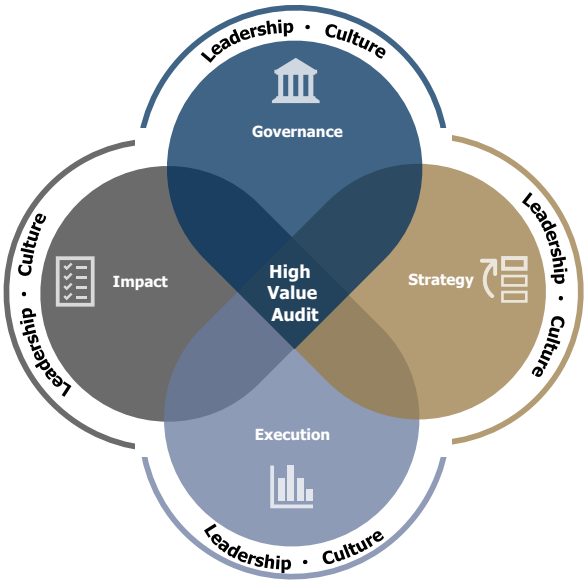
Internal Audit Best Practice 10

Internal auditors should track recommendation implementation agency-wide to help inform organizational leadership of what changes still need to be made to correct audit findings.

Blueprint For Organizational Leaders

Information About This Report

Section 2 covers best practices for organizational leaders. There is overlap in content and examples between sections of this report because internal auditors, organizational leaders, and/or oversight bodies approach issues from different perspectives.



Leadership & Culture

Effective leadership can have a powerful impact on the success of an organization. Leaders largely influence the culture of the organization through the tone they set at the top. For internal audit (IA) to provide the most value to the organization, organizational leaders must embrace the audit function. They should use their position to welcome opportunities for improvement as identified by auditors. For example, one organization in Utah created the "Audit Ready Framework."

Anthony Pugliese, the CEO of the Institute of Internal Auditors, describes the need for a change in how leaders view audit. He says, "Historically, internal audit has been viewed strictly within the realm of compliance and assurance services. However, as the threat environment continues to change and become increasingly complex, boards and senior management should look to shift their perception of internal audit and view them first and foremost as a strategic partner and advisor when it comes to risk management." We encourage leaders to turn to IA to answer their most pressing questions and address their most critical risks.

Section 2
Organizational Leaders

Leaders must make decisions even if they don't have enough good information. This can expose the organization to risk. There have been countless examples of leadership and organizational failure because of missing or bad information. We believe internal audit (IA) is an underused resource that leaders can leverage to make sure they have the information they need to make good decisions.

We believe internal audit is an underused resource that leaders can leverage to make sure they have the information they need to make good decisions.

The internal audit function is designed to produce some of the most reliable information. For example, audit standards[19] require:

- Independence
- Objectivity
- Thorough documentation
- Quality management
- Adherence to ethics
- Professional judgment
- Competence

These are only a few of the many standards auditors follow to ensure the information they provide is highly reliable.

Reliable information is essential to the success of every leader and organization. To make sure the information auditors provide is the most useful, leaders must help auditors know what is most relevant. Leaders should determine which types of information are most needed to make key decisions, then request them from IA. Leaders who concentrate audit resources on the most critical risks and goals of the organization will be more successful.

[19] Audit standards focus heavily on assuring the quality of information provided to stakeholders. See the *Government Auditing Standards* (Yellow Book) and *Standards for Internal Control in the Federal Government* (Green Book) produced by the U.S. Government Accountability Office, and the *Global Internal Audit Standards* (Red Book) produced by the Institute of Internal Auditors.

Governance: Leaders Must Ensure Audit Independence and Capacity, and Apply Enterprise Risk Management

Leaders exist to advance the mission of their organization. To accomplish this, leaders rely on others to give them the information they need to effectively manage the organization. When information is inaccurate, irrelevant, or inactionable, it is less useful to stakeholders.

Because of their unique role and authority in an organization, leaders must rely on IA for accurate, relevant, and actionable information. IA must be independent of the organization and possess sufficient capacity so that it can produce this high-quality information. In addition, organizational leaders must apply effective Enterprise Risk Management (ERM) to strengthen their organizations and inform the selection of audit work.

Governance 1: Organizational Leaders Must Establish Audit Independence

Independence empowers IA to develop unbiased information. It establishes safeguards to protect the motivations of auditors. Essentially, independence positions reliable information as the foremost objective. Without independence, auditors may intentionally or unintentionally bias information. For example, if an auditor reports to the finance director, they may be less likely to find flaws in finance's operations. When leaders protect IA independence, they can then trust the information IA provides.

Independence: The freedom from conditions that may impair the ability of the internal audit function to carry out internal audit responsibilities in an unbiased manner.

When leaders protect IA independence, they can have trust in the information IA provides.

Organizational leaders can work with oversight bodies to safeguard audit independence. Where applicable, organizational leaders should take steps to secure IA independence, including:

- Ensuring IA reports to the highest level of the organization
- Approving IA's charter defining authority and responsibilities, especially independence and access to information
- Ensuring IA is located organizationally outside of staff and management functions that IA may eventually audit
- Protecting IA from potential reprisals for reporting on deficiencies

- Making sure IA has access to leaders charged with governance
- Limiting non-audit work

By safeguarding IA independence, leaders protect the reliability of information provided by auditors. Leaders can then confidently rely on the information when making important decisions. If they do not protect IA independence, they may act on inaccurate information.

Internal audit must be positioned independently. Management at the Department of Natural Resources (DNR) made excuses for years as to why they could not separate the roles of internal audit director and finance director. The Utah State Auditor found a number of issues with DNR's financial controls during this period. Managers must be active in ensuring that auditors have the independence necessary to fulfill their responsibilities.

Organizational Leaders Best Practice 1

Independence reduces bias because it reduces perverse incentives. Leaders should ensure internal audit (IA) reports to the highest level of the organization, approve IA charters on authority and access, and protect IA from potential reprisals. Taking these and similar steps will safeguard the independence of IA and increase the reliability of the information it produces.

Governance 2: Organizational Leaders Must Ensure Sufficient Audit Capacity

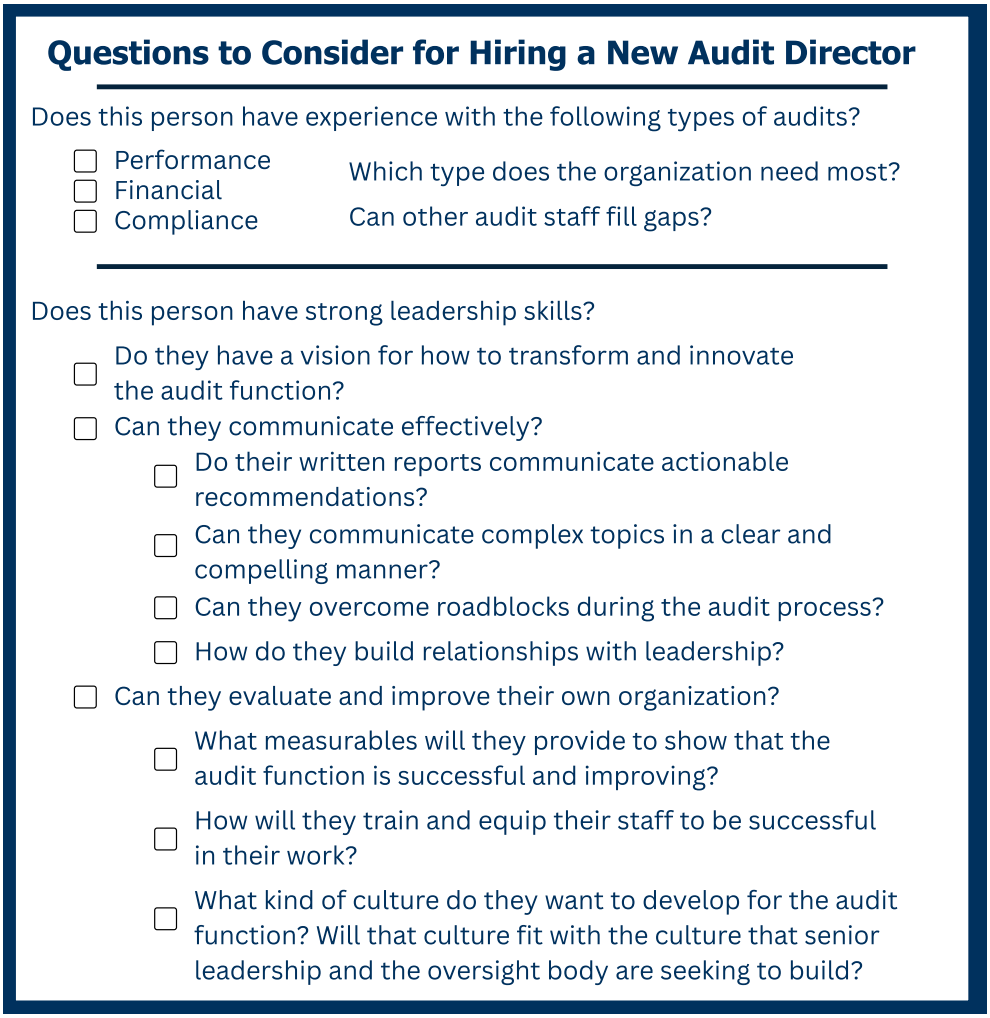
As described by Dr. Knighton in the Introduction, audit functions should only be limited by the availability of resources and the competence of the audit staff. We refer to this as **capacity**. Leaders should ensure IA has the necessary capacity to provide the information the organization needs.

Capacity: The resources and competencies necessary for IA to develop high-quality information.

Organizational leaders can be responsible for hiring the audit director. It's important that the person they select has the skills and ability to provide the types of information stakeholders need. As we discuss in the next subsection, there are several types of audits. Leaders should understand the audit types and what kind of question each can answer. They should then hire an audit director who can complete the

desired types of audits. For example, if a leader needs information on organizational performance, an audit director who can only do compliance-based auditing may not be a good fit.

Leaders should also look for traits that indicate the candidate's ability to advance the maturity of the IA function. Audit directors should be innovative and effective at change management. Audit leaders must also be relentless in pursuit of value for their stakeholders. A mature IA function can drive innovation, add strategic value, and contribute to organizational success. Questions leaders may consider can be seen in the following graphic.



Source: Auditor generated.

Leaders should select an audit director with the necessary competencies and character to provide them with the information they need to make good decisions.

Funding for IA should fit the scope of audit responsibilities. Similarly, the nature of the work in some organizations is more prone to risk. Audit coverage should carefully align with those increased risks. Ultimately, we believe funding should match both the leaders' needs for high-quality information and the value of the work audit performs. The following examples demonstrate the importance of dedicating capacity to IA:

> The Utah Department of Agriculture and Food (UDAF) didn't have an auditor when we completed audits of the agency in 2021. UDAF systemically lacked internal controls. This led to grant compliance issues, improper reimbursements, underutilized vehicles, insufficient fees, and minimal accountability. Many of the control weaknesses could have been prevented or minimized if UDAF had internal auditors.

> From 2009 to 2021, the Department of Human Services reduced its number of internal auditors by more than half. With limited resources, the internal auditors focused on reactive issues such as fraud and conflicts of interest, rather than on preventative work like reviewing and improving internal controls.

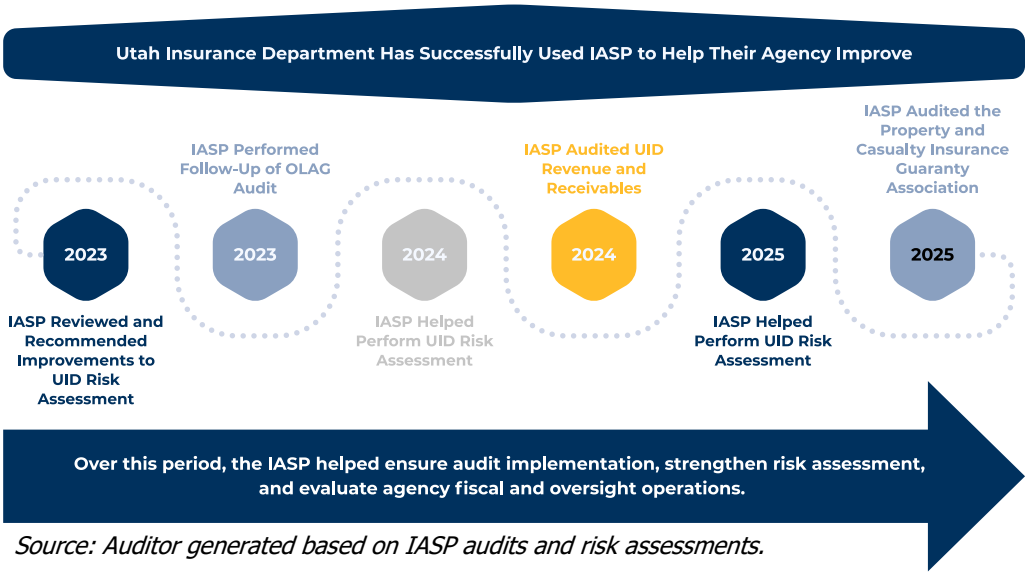
> Despite being statutorily required to have an internal auditor since 1996, the Department of Commerce still does not have an internal auditor. Executive directors should ensure audit capacity by hiring a competent internal audit director and embracing IA.

When IA is lacking, organizations are more prone to ineffectiveness, inefficiency, fraud, waste, and abuse.

Agencies Can Use the Internal Audit Services Program (IASP) to Increase Capacity. The Legislature appropriates money to the Department of Government Operations to fund the IASP. Use of their services is entirely voluntary. Despite being state funded, only a few agencies use this resource. One agency that has proactively used the IASP program to strengthen their organization is the Utah Insurance Department (UID). The following graphic shows how UID has

If agencies more proactively request audit resources through the IASP they could more effectively identify, test, and mitigate their risks.

used the program to help assess risk and strengthen programs.



Source: Auditor generated based on IASP audits and risk assessments.

We encourage state agencies to consider using IASP, particularly if the agency does not have IA. Increasing the capacity of IA can help organizations manage risk and achieve objectives.

Organizational Leaders Best Practice 2

Organizational leaders should ensure internal audit (IA) has sufficient capacity, meaning competencies and resources. Leaders should recruit and hire an audit director who can produce the type of information needed by stakeholders. Funding should match leaders' needs for high-quality information and the value that IA provides.

Governance 3: Leaders Should Apply Best Practices In Enterprise Risk Management

When organizations effectively manage risk, they are more likely to

- Create and protect value
- Achieve core objectives
- Make informed decisions
- Address uncertainty
- Continually improve as an organization

Risk is the possibility that something will happen that adversely affects the organization's achievement of objectives.[20] Managing risk is leadership's responsibility. When leaders fail to appropriately manage risks, it can have serious consequences, as seen in the following examples:

Risk: The possibility that something will happen that adversely affects the organization's achievement of objectives.

Utah's School and Institutional Trust Lands Administration (SITLA) did not have a formal risk mitigation plan. SITLA updated its risk assessment yearly, but none of the 40 risks identified in 2020 had been eliminated when an OLAG audit on SITLA was released in 2024. SITLA did not have a risk response or monitoring plan, and it was difficult to know if a risk could be removed from the list. The poor risk assessment likely contributed to the unaddressed major financial and environmental risks at a landfill property.

The Office of the State Auditor recently highlighted misuse of funds occurring in Iron County. After a hotline tip, the county auditor and state auditors were able to uncover approximately $188,000 in missing cash from building permit payments that occurred over several years. These missing funds likely would have been identified if proper controls were in place.

Responsibility for overseeing risk ultimately rests with the organization's highest leadership level. Organizational leaders are primarily responsible for identifying risks and developing strategies to mitigate them. IA is responsible for objectively reviewing the effectiveness of the organization's risk management. IA is also responsible for ensuring that they choose audits based on risk.

[20] *Standards for Internal Control in the Federal Government* (Green Book), U.S. Government Accountability Office, 2025.

The Governor's Office Strengthened Risk Management

The Governor's Office has made a push in recent years to strengthen agency risk assessments. The office released guidance on how to perform an "Entity-Wide Risk Assessment," outlining many of the best practices for effective risk management. Because the Governor's Office was proactive in advancing effective risk management, our observations are primarily positive.

The Governor's Office released a best practices guide on effective risk management that has had a meaningful, positive impact on organizational practices.

For example, the Governor's Office requires agencies to submit an annual risk assessment, creating accountability. Good governance should include risk assessment oversight, which is already taking place. The guidance clearly explains the different roles of internal audit and management. It defines risk and control types, provides a robust control framework, and offers direction on timing and frequency. We are encouraged with the work that the executive branch through the Governor's Office is doing with risk assessments. Requiring all executive branch agencies to conduct a risk assessment is a strong indicator of good leadership. Conducting risk assessments is a critical step to ensuring government is operating in a sound and effective manner. With permission, we have included the Governor's Office guidance in our resources available to all organizations.

Governor's Office Guidance:

"Obtaining robust information on risk allows management, in the face of finite resources, to assess overall resource needs, prioritize resource deployment and enhance resource allocation."

Additional Resources

Governor's Office Risk Assessment Guidance (Appendix C)

Conducting a risk assessment is an essential first step to an effective ERM. To explore opportunities to build on this success, we reviewed 2024 executive branch agency risk assessments. The following graphic summarizes the results of our review and illustrates some areas where risk assessments can be strengthened:

Executive Branch Agencies' Risk Assessment Elements

Governor's Office Recommended Risk Assessment Elements		Percentage of Agencies with Element Present in Risk Assessment
Identified Risk	Agencies have identified risks	100%
Risk Type	Agencies have determined risks to be strategic, operational, or another type of risk	57%
Risk Likelihood	Agencies have determined the probablity something will occur	95%
Risk Impact	Agencies have determined the impact the risk would have on their organizations	95%
Risk Score	Agencies have determined a scale based on the likelihood and impact of a risk	71%
Risk Response	Agencies have included a response to the risk: avoid, transfer, mitigate, accept	57%
Other Important Elements Included on Risk Assessments		**Percentage of Agencies with Element Present in Risk Assessment**
Risk Description	Agencies include the context of the risk	38%
Mitigating Activities	Agencies include documentation to show there is a mitigation strategy in place	67%
Risk Owner	Agencies have named a person or office responsible for the risk	52%
Risk Level	Agencies have rated risks on a scale of high, medium and low	65%
Follow-Up	Agencies track the status of the risk	24%

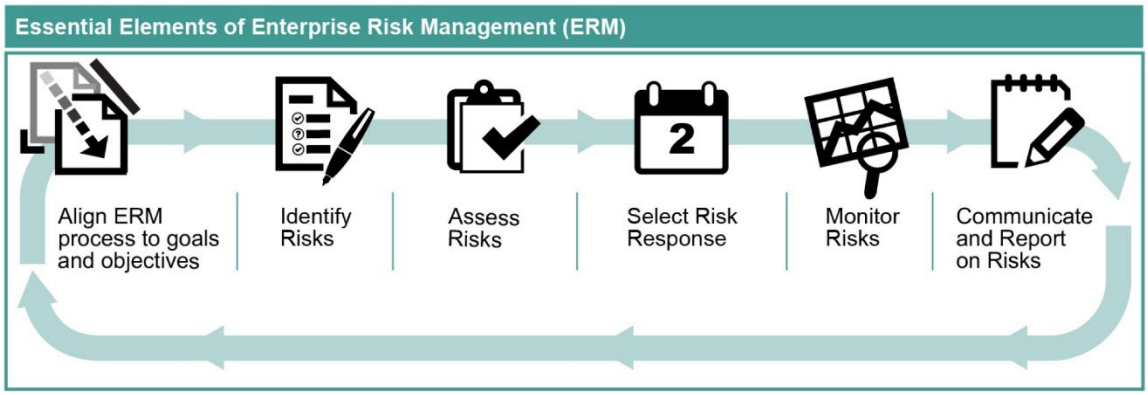
Source: Auditor generated based on agency risk assessments.

We are encouraged that core components of risk assessment, such as risk identification, risk likelihood, and risk impact, are consistently included. Most agencies are also scoring risks, which facilitates risk prioritization. Leaders can use this information to understand their unique risk landscape.

Agencies can also take steps to further strengthen their risk assessments, such as following up on the status of risks and including risk descriptions. Crucially, all organizations must determine the appropriate risk responses so that risks are not just identified, but managed. By sustaining momentum and shoring up loose ends, agencies can assess resource needs and enhance resource allocations.

ERM is a best practice for strengthening governance by managing organizational risk.[21] It also creates a risk-aware culture that accounts for risks in strategic planning, resource allocation, and daily processes such as decision-making.

The U.S. Government Accountability Office (GAO) defines six essential elements for establishing an ERM. Agencies can improve their risk assessments by incorporating these elements.



Source: Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk. *2016*.

ERM focuses on how risks interact, instead of allowing them to remain siloed. For example, a risk in one part of the organization could potentially magnify a risk in another part of the organization. Similarly, risk mitigation strategies can solve one problem and unintentionally create another. Using ERM to look at the entire organization's inventory of risks allows leaders to understand which risks are most important to address. This is essential when prioritizing which risks merit the most attention. Management and IA can use it as a tool to develop internal audit plans.

The following briefly outlines the six essential elements of ERM:

1. **Align ERM Process to Goals and Objectives.** If an organizational objective isn't threatened, there is no risk. So, after identifying risks, leaders should clearly connect them to the strategic objectives that are threatened. ERM further avoids treating individual risks within silos. This integrated approach is

Risks only exist in relation to objectives.

[21] Enterprise Risk Management (ERM) is an agency-wide approach to addressing the organization's combined risks. It integrates organizational strategies, risks, and risk responses in one place. The Governor's Office Guidance describes how to do an "Entity-Wide Risk Assessment," which we view as similar to ERM.

designed to improve mission delivery, reduce costs, and focus mitigation strategies toward key risks.

2. **Identify Risks.** Leaders should create a comprehensive list of risks. Each leader in an organization is responsible for managing risk at their level. Risks should be grouped by type (strategic, operational, hazard, etc.). Administering a risk survey to organizational leaders can be a useful approach, particularly for gathering a variety of perspectives. Risk analysis models and stress testing can also be effective strategies for identifying key risks. Organizational leaders should strive to develop a culture that encourages employees to identify and discuss risks openly. Even if risks are outside the agency's control, they should still be identified. That said, if the risk is highly unlikely or unimpactful, it probably doesn't need to be addressed. Establishing a risk committee is one way to facilitate and oversee risk identification.

Each leader is responsible for managing risk at their level.

3. **Assess Risks.** Two factors form the core of risk assessment—likelihood and impact. Risk velocity—how quickly the risk could threaten the objective—may also be important. Leaders should score risks based on these factors.

Likelihood and impact are the core factors for assessing risk. Velocity may also be important to consider.

We have developed two resources—The Enterprise Risk Management Template and Tool Guidance[22]—to assist organizational leaders in developing and strengthening an ERM framework using best practices. These resources are available on our website, under the Center for High Impact Auditing page (https://olag.utleg.gov/CfHI.jsp). Resources were developed with the support of our audit leaders workgroup.[23]

[22] The Tool Guidance is also available in Appendix B.

[23] We received an initial risk assessment template from the audit director at the Utah Department of Government Operations. The audit leaders' work group helped us to further refine these tools.

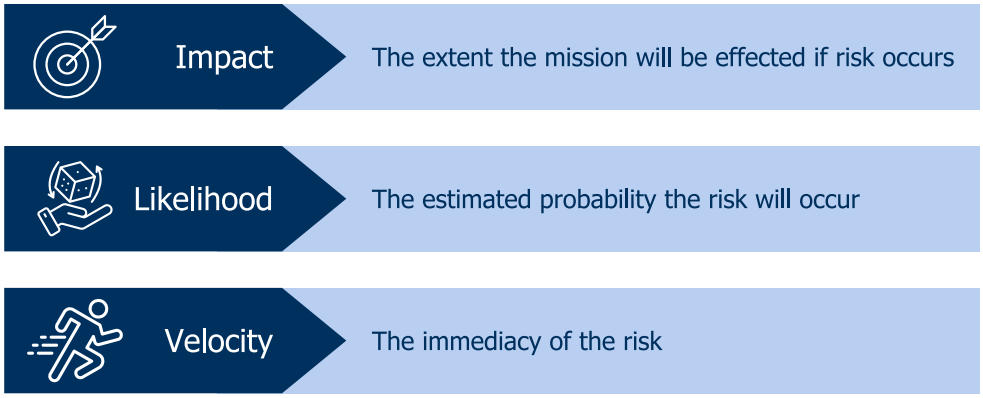
Additional Resources

Enterprise Risk Management Template

Enterprise Risk Management Tool Guidance (Appendix B)

Resources were developed with the support of our audit leaders' workgroup.

An ERM brings together all major risks from across the organization. Leaders score and rank risks based on their impact and likelihood, and possibly velocity, as seen in the following graphic.



In assessing risk, leaders should define their risk appetite. Agencies can be too risk-averse. In fact, failing to innovate and avoiding opportunities because of the risk involved is a risk in and of itself. Risk can never be fully eliminated. So, leaders should weigh the costs of a potential risk's impact against the opportunity cost of remaining with the status quo. As discussed next, leaders may be able to mitigate or transfer the risk in some situations. This enables leaders to innovate without assuming a lot of risk.

4. **Select Risk Response.** The guidance from the Governor's Office describes four primary risk responses. Leaders should determine which response or responses are most appropriate for a particular situation. Regardless of which response leaders choose, they should assign ownership to each risk and document the strategies in the ERM.

There are four primary risk responses—mitigate, transfer, accept, and avoid.

- **Mitigate**—Reduce the impact and likelihood of the risky event. This involves applying internal controls.

- **Transfer**—Contract with a third party to administer the program or activity, thus reducing the risk and loss exposure to another organization.
- **Accept**—Retain the risk and develop plans to cover the financial or non-financial consequences.
- **Avoid**—Eliminate the risk by choosing not to participate in programs or activities considered too risky.

5. **Monitor Risks.** The risk landscape is always changing. Some mitigation strategies may eliminate a particular risk. Leaders need to monitor these landscape changes and determine whether risk responses are still effective. As IA performs work in high-risk areas, audit reports can inform leaders about whether controls are effective. Leaders should use audit reports to strengthen controls and monitoring practices, as previously discussed.

The risk landscape is always changing. Leaders should continually monitor whether risk responses are effective.

6. **Communicate and Report on Risks.** Many stakeholders are invested in the success of organizations. Beyond organizational leadership, the Utah Legislature, the Governor, the community, and the taxpayer have a stake in the organization's success. Leaders must apply best practices in risk management to advance their missions. Leaders can communicate risk through a dedicated risk management report or include it in other performance management reports. This increases transparency to stakeholders and allows the agency to share its progress.

Many stakeholders are invested in the success of organizations. So, leaders should communicate risk strategies.

Additional Resources

Enterprise Risk Management Maturity Model (Appendix D)

Risk Likelihood and Impact Rubric (Appendix E)

We encourage leadership to establish the six essential elements of an ERM. Leaders should avoid trying to do too much too quickly. Instead, we recommend an incremental approach that builds maturity over time. By developing mature risk management strategies, leaders can advance the mission of their

organizations and achieve meaningful results. The following examples show where some agencies have not fully integrated management in the risk assessment process.

Leadership from each court is not involved in helping identify risks at the Utah Courts System, which is contrary to best practices that say management holds the responsibility for managing risks at an agency. The lack of involvement from each court means that some may be assuming risks that are unidentified and consequently unaddressed. Court leadership should take on a bigger role in the risk management process and manage and own their risks.

Without an agency-wide risk assessment, the Utah State Board of Education is missing the opportunity to direct internal audit to some of the largest areas of risks. It is concerning that an organization charged with general control and supervision over the public education system that distributes over $8.4 billion yearly is not systematically assessing risks within its organization.

Organizational Leaders Best Practice 3

Effective risk management is essential to organizational results. Organizational leaders should develop and strengthen an Enterprise Risk Management (ERM) framework. Leaders may apply the U.S. Government Accountability Office's six essential elements of ERM.

Strategy: Leaders Should Select Audits Based on Organizational Risk, Strategic Objectives, and Key Questions

Organizational leaders should select audits that review high risks and advance critical goals. If audit leaders develop the audit plan for approval, organizational leaders should review the proposal for these same factors. Organizational leaders also should use IA to answer their key questions. As discussed previously in this section, IA is designed to provide reliable information. Organizational leaders must work with IA to ensure the information it provides is highly relevant to their needs and those of the organization.

Strategy 4: Stakeholders Should Use Audit to Advance the Mission of the Organization

IA is well suited to address the information gaps that cause poor decisions and poor performance. Robust and dependable audit standards serve as the backbone for reliable information development. Similarly, audit's broad range of work offers a broad perspective. In short, audit provides better information, which drives better decisions. And better decisions drive better outcomes.

Better information drives better decisions, and better decisions drive better outcomes.

Leaders Should Understand the Types of Audits They Can Request. Not all audits are the same. In fact, there are several types of audits that influence the information developed. Different types of audit work provide different kinds of information.

The following is a brief list of the types of audits that stakeholders may request:

- **Performance**—Evaluates the efficiency and effectiveness of organizational performance. The goal is to improve operations, enhance performance, reduce costs, and facilitate decision-making.
- **Financial**—Assesses whether financial reporting is reliable and accurate by evaluating the integrity of financial information and reviewing the effectiveness of internal controls over financial reporting.
- **Compliance**—Determines whether activities conform to their mandates or specific requirements. The goal is to assure adherence to policies and standards.

- **Attestation**—Assesses information provided by a party other than the auditors. The goal is to provide an independent opinion of the information.

As evident in this list, audit can strengthen and improve every facet of the organization. We believe all information types are valuable depending on stakeholder needs.[24] We encourage leaders to request the types of audit best suited to the information they need. An understanding of audit types can also support organizational leaders during the recruitment and hiring process. Candidates should be able to deliver the desired information to stakeholders.

***Utah Code* requires efficiency and effectiveness evaluations to be adequately represented in audit plans.**

Utah Code requires IA to include two types of audits in audit plans—performance and compliance.[25] Leaders should ensure both are adequately represented. Other types of audits should be included as needed.

Shifting perception of IA means shifting organizational culture. It also means hiring versatile and innovative audit directors. We encourage leaders to expand their view of IA and recognize the breadth of information that it can provide.

Organizational Leaders Best Practice 4

Leaders should understand the different types of audits available. Leaders may request audits based on the information they need about the risks of the organization. Leaders should also hire directors that can provide the necessary information.

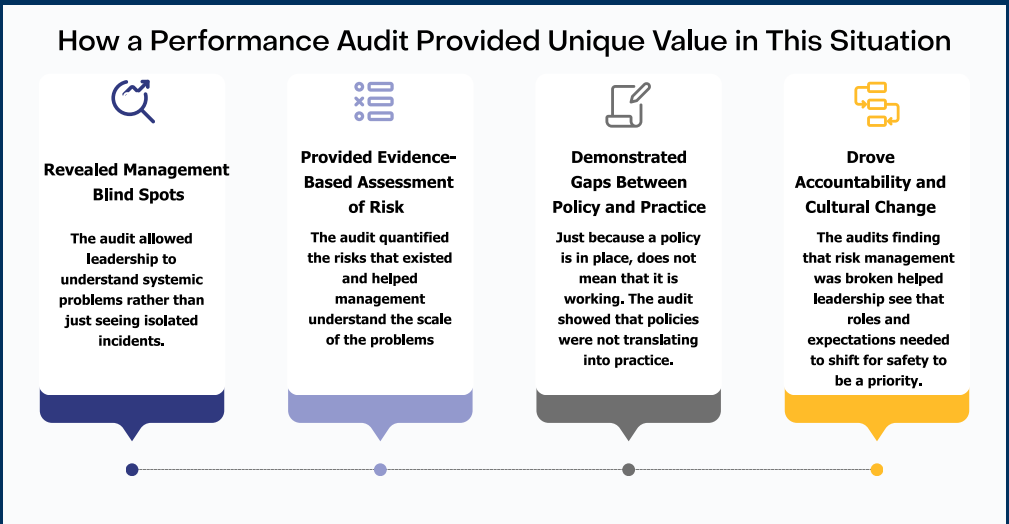
CASE STUDY
The Power of Performance Audits

Our 2019 performance audit of the University of Utah's (U of U) laboratory safety practices demonstrates the critical value that performance audits can provide to organizational leaders.

[24] We have tried to write this report in a way that can be applied to all types of audits. However, we acknowledge that our office primarily does performance audits, which influences our perspectives.
[25] ***Utah Code*** 63I-5-401 (2)(a).

What the audit found:

- Persistent safety deficiencies at the lab, with 44% of research groups having at least one major chemical safety deficiency. This exposed the University to the possibility of life-threatening incidents.
- Risk management for lab safety was broken. Some labs had significant repeated deficiencies without adequate oversight or corrective action.
- The University was at risk of significant legal exposure and endangered employee health by not following OSHA requirements.
- Serious incidents had already occurred. While the U of U did not have any fatalities, similar failures in risk management at other similar facilities have proved fatal.



Source: Auditor generated.

Leaders can direct auditors towards performance audits to get these types of valuable findings and information.

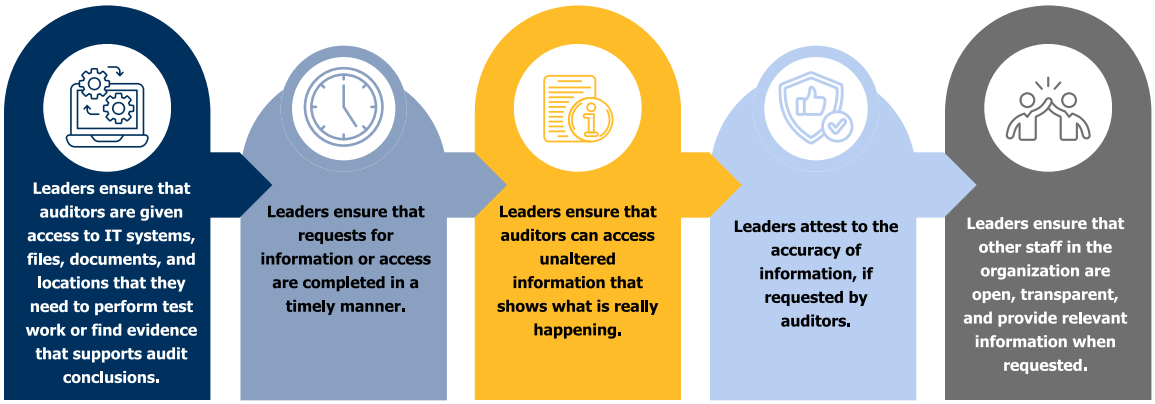
Execution: Leaders Can Help Enable And Strengthen Audit Work

Leaders can help auditors produce the most relevant, helpful information. Their actions and attitudes can either enable or impede audit work. For audit results to be as complete as possible, auditors need leaders to facilitate access to information. Oversight bodies, leaders, and IA should coordinate to make any necessary changes. Leaders should also hold the audit function accountable. These steps can strengthen audit findings and lead to better recommendations.

Execution 5: To Enable Internal Audit to Provide Accurate Information, Leaders Should Provide Access and Remove Roadblocks

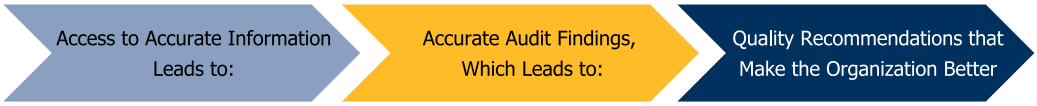
For auditors to perform their job effectively, they need access to accurate information. While the audit charter, statutes, and policies may require that auditors are given information, in practice, leaders still need to ensure that this occurs.

Leaders Should Facilitate Access During the Audit Process



Source: Auditor generated based on IIA and GAO standards.

There are times when auditors can face roadblocks from staff or leaders that can slow the work down or lead to incomplete findings. If leaders have created opportunities for open communication with audit staff, they will learn of any roadblocks and verify that these problems are quickly resolved.



Source: Auditor generated based on IIA and GAO standards.

When auditors cannot access accurate information, it limits stakeholders' access to accurate information.

To make the necessary communications as smooth as possible, auditors should have a point of contact from senior leadership to address audit issues, such as access. When auditors cannot access accurate information, it limits stakeholders' access to accurate information. An example from one of our audits shows how damaging it can be to limit access during an audit.

A 2025 OLAG audit found that Utah's Attorney General had not been transparent with the public and other stakeholders about how he was fulfilling his responsibilities. During the audit process, auditors repeatedly requested information within the scope of the audit. We were denied the information. During our investigative process, we obtained information that appeared to have been withheld. These barriers significantly limited our ability to assess important functions of the Attorney General. Access concerns like these can make it difficult for auditors to provide meaningful recommendations or provide the information that stakeholders need to make decisions.

Organizational Leaders Best Practice 5

Leaders should facilitate access to accurate information during the audit process.

Execution 6: Leaders Should Coordinate with Auditors and The Oversight Body to Ensure Audit Effectiveness

Organizational leaders should help IA maintain independence by avoiding undue influence over the audit function. At the same time, there must be effective coordination during the audit process, especially when there are changes. Changes can stem from the auditors' assessment of risks or from adjustments that leaders want to request.

Leaders or the oversight body should communicate any new concerns that were not included in the original audit plan. Although the oversight body makes the final decision to approve changes, organizational leaders should raise these issues and explain why the proposed changes are important. This coordination allows auditors and the oversight body to evaluate whether changes are necessary.

Because many oversight bodies in government organizations serve part-time or may not understand the day-to-day operations of the internal audit function, they can delegate administrative reporting to the organizational leader. In these situations, leaders should maintain regular communication with the oversight body to ensure accountability. Leaders should provide enough information when concerns arise so the oversight body can give effective feedback and conduct performance evaluations, especially when the audit function is not fulfilling its responsibilities.

> Our 2025 audit of the Department of Alcoholic Beverage Services (DABS) found a lack of coordination and oversight between the internal audit function, the department leadership, and the commission. The poor coordination and oversight allowed an audit that could have addressed significant issues to be delayed. The audit was requested to address key risks; it did not cover those risks. If there was greater coordination, issues like timeliness and change of scope could have been addressed by the commission. Without this coordination, the DABS' main IT system lacked key controls. This allowed theft and inventory practice issues to continue even though the audit could have addressed these control deficiencies.

In Some Government Organizations, There Is No Oversight Body Directly Overseeing the Auditor. When this occurs, the organizational leader assumes both the leadership role and the oversight role. This arrangement requires less coordination but places greater responsibility on the leader to balance both perspectives. Leaders who serve in both roles should review Sections 2 and 3 of this best practice handbook to understand the best practices that apply to each role.

Organizational Leaders Best Practice 6

Leaders should coordinate regularly with the auditor and oversight body to ensure audit effectiveness.

Impact: Leaders Should Act on Audit Recommendations and Cultivate a Culture that Embraces Audit

Organizational leaders could have the best information in the world, but if they don't act on it, the organization won't improve. High-quality information is vital, but it isn't enough to produce desirable outcomes. Leaders should work with IA to track progress on recommendations. IA should devote sufficient time to validating self-reported information from those responsible for implementing audit recommendations. When organizations do not take implementation of audit recommendations seriously, the value audit provides is greatly diminished.

Impact 7: Organizational Leaders Must Act on Audit Recommendations

IA provides organizational leaders information needed to make good decisions. This may include findings such as weak **internal controls** or other risks. Auditors should then make recommendations to address these deficiencies. It is up to management to work with IA to determine how best to act on recommendations. Ultimately, it's the organizational leader's responsibility to implement recommendations. When leaders do not take meaningful action, the risk areas IA identified will remain. This was recently the case at Utah State University (USU).

Internal Controls: Processes that help support an organization's achievement of objectives.

> A recent OLAG audit of USU identified many problems, including weak controls and spending concerns. For example, IA had identified issues with staff lodging limits, and organizational leaders failed to act for over a year. Many other issues identified in the report could have been addressed if USU leadership implemented internal audit recommendations.

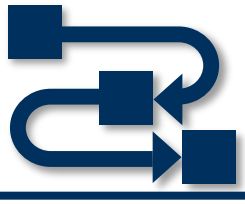
One way leaders can ensure recommendations from IA reports are implemented is by creating an audit response plan at the conclusion of every audit. For example, ***Utah Code*** requires the chief officer of OLAG-audited organizations to submit formal responses every 180 days until we agree the recommendations have been implemented.[26] ***Utah Code*** also requires agencies to submit responses at the end of audits that include the information in the following graphic:

[26] ***Utah Code*** 36-12-15.3

Elements Required in OLAG Audit Responses

- **Identifies how the entity will implement each recommendation**
- **Identifies an individual responsible for implementing a recommendation**
- **Establishes a timetable that identifies benchmarks for the entity to implement the recommendation**
- **Specifies an anticipated deadline by which each recommendation will be fully implemented**

See OLAG's Audit Response Guide



Not every organization needs such a thorough follow-up process. However, leaders should document the who, what, when, and how of their response to each recommendation. Detailing these specifics enables clear responsibility and real accountability.

The GAO's Green Book standards provide similar guidance.[27] Organizational leadership is responsible for determining the appropriate corrective actions to fix control deficiencies, including those identified in internal audits. However, it is not enough to provide a response to internal audits; leadership must act. Without action, leaders are accepting the risk. The Department of Natural Resources (DNR) experienced this issue with a series of mineral extraction audits:

> For over a decade, internal auditors told DNR that there were problems with mineral royalty payments, such as issues with royalty rate calculations, royalty payments, data documentation/ submission, and oversight. DNR management was aware of the issues and wrote responses to the internal audits, but never fully implemented IA's recommendations. Several years later, our audit found the same issues and discovered that varying sodium chloride rates represented an annual deficit of about $170,000. Without recommendation implementation, agencies continue to make the same mistakes.

Agencies' reaction to deficiencies should be timely. Delaying action means that the risks remain and continue to create problems for the organization.

[27] *Standards for Internal Control in the Federal Government* (Green Book), U.S. Government Accountability Office.

As leaders work to implement recommendations, they should document the actions taken to fix problems. These can include completion dates, milestones, or measurable progress. Continued documentation helps IA track the status of recommendations.

Audit findings are only fully complete when leadership has corrected the deficiency or made improvements. If leadership chooses not to implement an audit recommendation, they should document why they believe the audit findings don't need action. Alternatively, if leadership determines a different plan to implement recommendations, they should inform their internal auditors of these changes. Whatever the decision, organizational leadership is ultimately responsible for remedying identified deficiencies.

Organizational Leaders Best Practice 7

To ensure accountability, leaders should document the who, what, and when of their plans to implement audit recommendations. Leadership should act on audit recommendations to ensure that risks are properly managed or eliminated.

CASE STUDY
Department of Corrections

In 2014, the Utah Department of Corrections' (UDC) internal auditors released a report on recruitment and retention that identified multiple areas where UDC was falling short on recruitment and retention efforts. The audit identified high turnover rates and attributed them to the implementation of mandatory overtime. The audit stated, "Perhaps the most serious problem the Utah Department of Corrections (UDC) faces now and in the future is the need to attract and retain sufficient numbers of high-quality correctional officers."

This audit made several recommendations to UDC to try and fix the turnover challenges. However, leadership failed to act on that information and didn't make any changes until 2019 when they hired a recruiter. UDC did not adopt a formal recruitment strategy until 2021.

In 2022, the prison location moved from Draper to a new location, called the Utah State Correctional Facility (USCF). Instead of increasing hiring to

meet an increased demand for correctional officers at the new prison, UDC lost 91 more officers than it hired in 2022. When our office released an audit of the prison in late 2023, staffing had reached crisis levels. Low staffing levels led to dangerous and harmful outcomes in the prison.

UDC, however, is a good example of change that happens when management cares about fixing an issue and implements audit recommendations. After a leadership shift, the new executive director implemented audit recommendations and took other actions that helped fix staffing levels and cultural problems in the department. Within two years, inmate assaults decreased, no officer assaults occurred in three months of a 12-month period, and staffing levels greatly improved.

When leadership failed to act on audit recommendations, the risks remained. But by working to implement audit recommendations and taking additional actions, conditions at USCF greatly improved.

Impact 8: Good Implementation Requires Oversight and Accountability

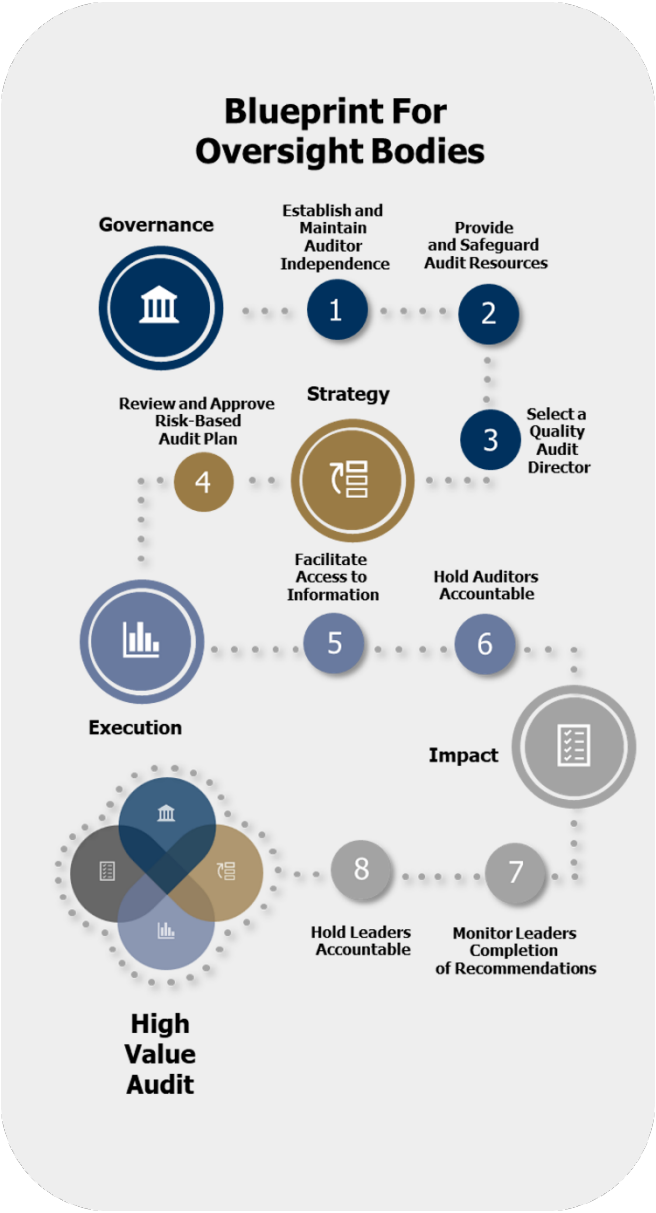
Organizational leaders must take decisive action to implement audit recommendations and remediate deficiencies. This initial action must then be monitored to oversee progress, holding individuals accountable for full implementation. Accountability is driven by the tone at the top. If leaders don't hold individuals responsible for implementing audit recommendations, they may not get implemented, and problems will persist. One way organizational leadership can hold individuals accountable for implementing recommendations is performance appraisals. The Department of Health and Human Services (DHHS) is a good example of how management can take steps to improve implementation in agencies.

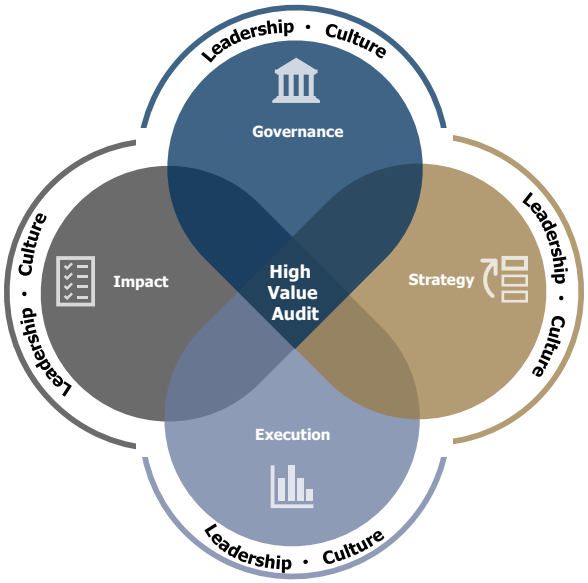
DHHS executive leadership placed implementing audit recommendations on management's performance plans. DHHS also posts its implementation rates publicly. We believe that increasing the stakes for implementing audit recommendations encourages management to follow through.

We believe that when leadership holds individuals responsible for implementing audit recommendations, they set a tone that says IA recommendations are important. This can help encourage lower-level management to take recommendations seriously and facilitate change.

Organizational Leaders Best Practice 8

Leadership must hold individuals responsible for implementing audit recommendations.





Information About This Report

Section 3 covers best practices for oversight bodies. There is overlap in content and examples between sections of this report because internal auditors, organizational leaders, and/or oversight bodies approach issues from different perspectives.

Leadership & Culture

Oversight bodies are in a unique position to influence leadership and culture in the organization and its internal audit. Primarily, they can set a culture of accountability for leadership. Selecting both organizational and audit leaders who genuinely want to make the organization better can help ensure collaboration and better outcomes.

Oversight bodies can also provide a positive tone at the top. This tone can influence the organization and its acceptance of internal audit. The GAO Green Book describes tone at the top as reenforcing "the commitment to doing what is right, not just maintaining a minimum level of performance necessary to comply with applicable laws and regulations, so that these priorities are understood by all stakeholders, such as...employees and the public." This tone can help build a culture of internal audit and staff throughout the organization working together to make meaningful changes.

Section 3
Oversight Bodies

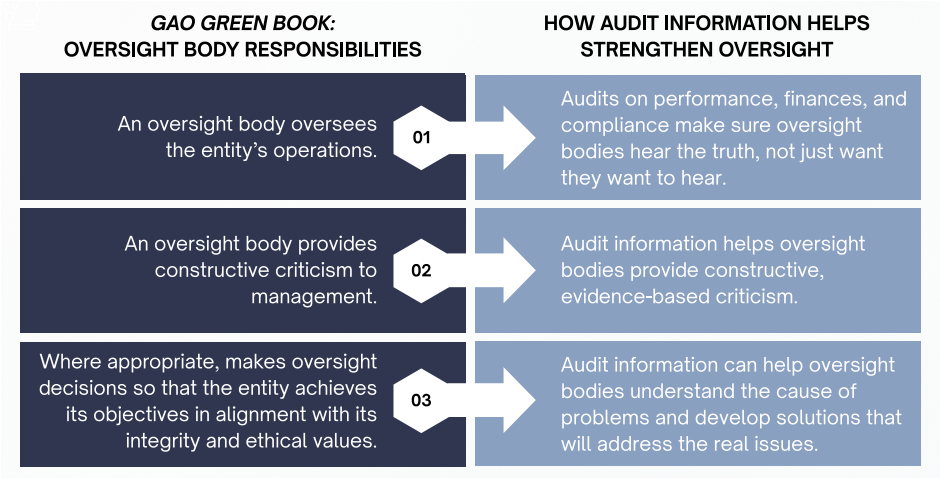
To provide effective oversight of organizations, these bodies need high-quality information.

Because auditors can provide valuable, unbiased information, oversight bodies should strengthen audit governance, strategy, execution, and impact. Most public and private entities have oversight bodies that help provide accountability to the organization. In government, elected or appointed officials oversee functions at the federal, state, and local levels. To provide effective oversight of organizations, these bodies need high-quality information. Internal audit can play a key role in providing oversight bodies with objective and credible information that informs good decision-making.

This section describes ways in which oversight bodies can direct and affect each of these areas. We have also included a description of the current landscape of internal audit (IA) provided in ***Utah Code,*** including who is required to have audit and where there are still gaps**.**

Oversight Bodies Roles Can Be Strengthened By IA's High-Quality Information

The Government Accountability Office's *Standards for Internal Control in the Federal Government,* known as the "Green Book," describes three important responsibilities that government organizations' oversight bodies have. Each of these responsibilities can be strengthened by the quality information that audit provides, as described in the following figure:



Source: Auditor generated from GAO Green Book and audit standards.

While audit is not the only source of high-quality information, effective internal audit provides objective assurance, insight, and advice that enhances value in the organization.

Without objective and risk-based information, oversight bodies and other leaders can make decisions that hurt an organization's ability to provide value.

Without any objective and risk-based information, oversight bodies and other leaders can make decisions that hurt an organization's ability to provide value. Because of the important services that government provides, this can put health and safety at risk, place the organization in a difficult financial position, or cause significant regulatory deficiencies because of noncompliance. The following example shows where the lack of good information led to poor decision-making. In similar situations, internal audit can be used to ensure that quality information can be used to make better decisions.

> Park City School District (PCSD) did not comply with environmental or school construction regulations. Even though administrators should have acted to ensure compliance with these regulations, PCSD moved contaminated dirt without proper cleanup. Regulators shut down the construction projects, introducing delays and increased costs. Having enough information to understand the risks prior to the project could have minimized costs and increased public safety.

This example shows that even smaller, more local government organizations can have significant problems when they make decisions without good information. When oversight bodies are able to get more information from sources like internal audit, they can help the organization improve.

Different government oversight bodies play different roles, which means they can influence the success of internal audit in different ways. Some governing bodies can direct funding, allocate resources, or provide direct oversight of the internal audit function. Others may play a more advisory role. The following best practices, drawn from the Government Accountability Office's Yellow and Green Books and the Institute of Internal Auditors' Internal Audit Standards, show how oversight bodies can help set the conditions for auditors to provide value to

the organizations they oversee. In some cases, multiple oversight bodies will need to work together to implement these practices effectively.

Governance: The Oversight Structure Can Determine the Success of Internal Audit

Oversight bodies play a key role in audit governance. They can help the auditor successfully perform their work by directing audit function's resources, policies and procedures, audit charter, and culture.

Governance 1: Oversight Bodies Can Help Establish And Maintain Auditor Independence

Independence is pivotal to a successful audit function. Oversight bodies should value this independence as it helps ensure they are getting accurate and unbiased information. When reviewing **audit charters**, oversight bodies should ensure that they

- Define the standards and safeguards that protect the internal auditor's ability to work without interference or influence.
- State that the auditor will not take part in management activities.
- Place the auditor in the organizational structure where audited staff do not oversee their work.

Independence: The freedom from conditions that impair the internal audit function's ability to carry out its responsibilities in an unbiased manner.

Audit charter: A document that includes the audit functions, mandate, position, reporting structure, scope of work, services, and other items.

Another way that oversight bodies can help provide organizational independence is encouraging open communication and transparency with the auditor. This includes holding regular meetings with the chief audit executive without management being included.

Oversight Bodies Best Practice 1

Oversight bodies should help establish and maintain auditor independence by approving the internal audit charter and by helping ensure accurate and unbiased information.

Governance 2: Oversight Bodies Can Provide and Safeguard the Resources that an Internal Audit Function Needs to Succeed

Oversight bodies with appropriations authority can support audit work by allocating enough funding for the audit function to operate effectively. Oversight bodies without appropriations authority should hold management accountable

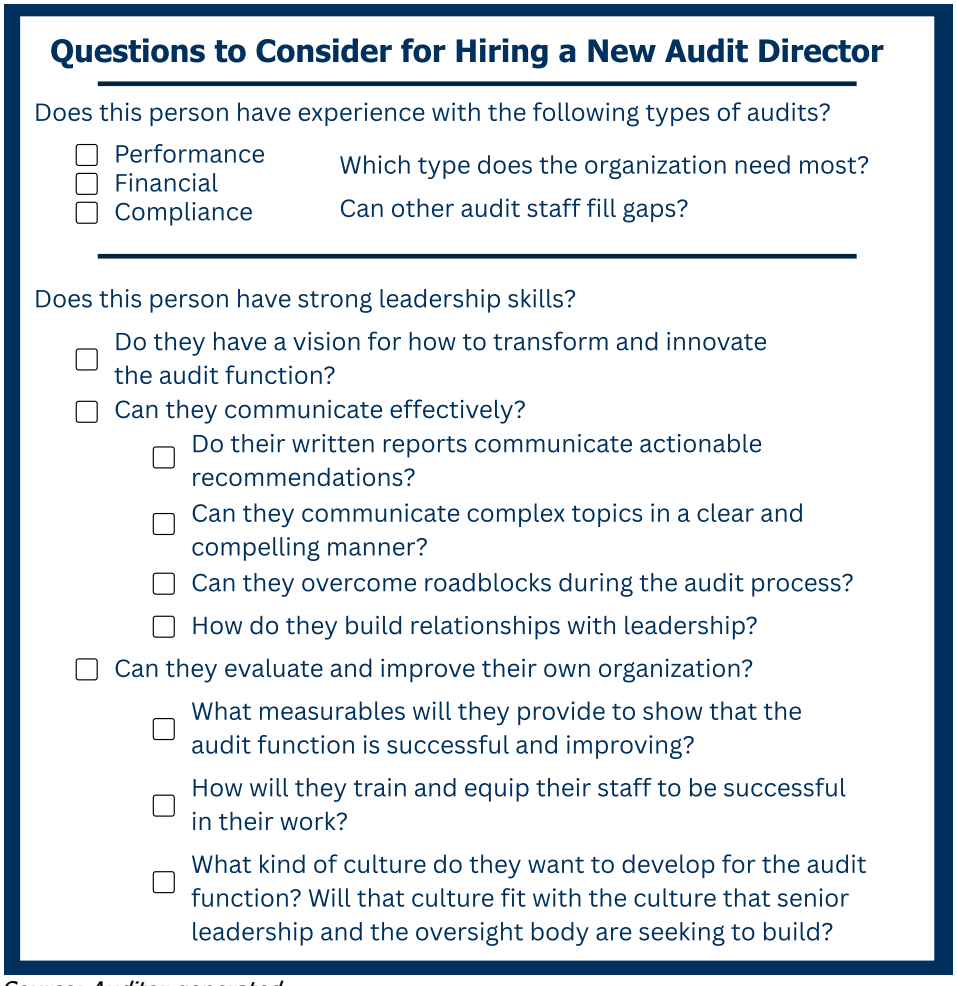
for proposing budgets that support adequate staffing and ongoing professional development for internal audit staff.

Oversight Bodies Best Practice 2

Oversight bodies should provide and safeguard the resources that an internal audit function needs to succeed.

Governance 3: Oversight Bodies Can Influence the Selection of a Quality Audit Director

Oversight bodies may be the hiring authority for the internal audit director. If they are not that authority, they often still have influence with organizational leadership. Audit director selection is extremely important to driving the success of the audit function and providing value to the organization. Several important aspects are important to consider during the process, including what is shown in the following graphic:



Source: Auditor generated.

While these questions are not the only options for interviews with a new audit director, the two key areas that matter are:

- Can this person provide the types of information that the oversight body and management need to make the needed changes to the organization?
- Does this person have the vision and leadership skills to make a real difference, both for the audit function and the organization?

One example of how an internal audit function can grow under strong leadership is the Utah State Board of Education (USBE). When the current audit director was hired, only one of five audit positions was filled. The office also lacked a strategic plan, had no policy and procedure manual, and was not completing self-assessments. Over the next 10 years, the internal audit director helped grow the office to nine staff and implemented a strategic plan, a policy and procedure manual, and a regular self-assessment process. By strengthening these foundational practices, increasing accountability, implementing professional development and demonstrating value, the audit function earned greater trust from the board. As a result, more work has been asked of the internal audit function, and the board has been willing to support continued investment to meet these needs.

Audit standards suggest that a robust internal audit function can perform all three major audit types, but the organization's audit staffing largely determines what kind of information IA can offer the oversight body. Leadership capabilities matter because IA can be a challenging role, requiring a driven, vision-oriented approach to ensure that the work is provided in a way that will add value to the organization.

Oversight Bodies Best Practice 3

Oversight bodies should either direct or effect the selection of a quality audit director to ensure the organization is getting the most value from the internal audit function.

Strategy: Oversight Bodies Can Help Ensure the Organization Is Appropriately Responding to Risk

Oversight bodies can help strengthen and develop the overall agency **risk** assessment. After the risks have been determined, they can then ensure IA is asked to review key risks. The oversight body should work with IA to verify that these key risks are adequately addressed by audits in the **audit plan**.

Risk: The possibility that an event will occur and adversely affect the achievement of objectives.

Strategy 4: Oversight Bodies Can Review and Approve the Annual Risk-Based Audit Plan

To ensure the audit plan is as effective as possible, oversight bodies should review it to confirm that it aligns with

Audit Plan: The plan auditors use to regularly track the audits that they will perform in the future.

- Legislative mandates
- Organizational priorities
- Risks identified in organizational risk assessments
- Risks that the oversight body sees that may not be in the risk assessment

The oversight body, organizational leadership, and internal audit must work together to ensure an audit plan covers the most important things. When they do work together, the organization is much more likely to be able to achieve its goals.

Oversight Bodies Best Practice 4

Oversight bodies should review and approve the annual risk-based audit plan to ensure it covers the most important things.

Execution: Oversight Bodies Can Help Remove Barriers for Internal Audit

While oversight bodies should not exercise undue influence or control over the audit process, they can play a role in ensuring audit value.

Execution 5: Oversight Bodies Can Facilitate Access to Information and Help Remove Barriers

IA should tell oversight bodies if they are having trouble getting access to information, or the groups they are auditing are delaying responses. Once the oversight bodies know about these issues, they should intervene with management to hold them accountable. Without that intervention, IA may be forced to give the oversight body incomplete or inaccurate data. Also, these delayed responses waste limited IA resources, leaving the organization open to risks they would otherwise have had time to address.

> The Utah Legislature has supported efforts to improve access to information when auditors need it. After OLAG experienced difficulties obtaining certain records from auditees, the Legislature strengthened statute to ensure that critical information cannot be withheld during an audit. During the 2025 General Session, lawmakers created a formal process for handling privileged items so auditors can review necessary materials while preserving legal protections. When oversight bodies take steps that support auditor access to information, they improve the quality of audit work and reinforce the effectiveness of the audit process.

For the oversight body to ease IA's access, it must first know about the barriers. This is another reason it is essential that the auditor has the authority to communicate directly with oversight members, and why that should happen regularly and frequently.

Oversight Bodies Best Practice 5

Oversight bodies should facilitate access to information and help remove barriers.

Execution 6: Oversight Bodies Should Hold the Internal Auditors Accountable for Their Work

Oversight bodies are uniquely suited to provide accountability for IA. Ways to provide this accountability include:

- Requiring IA to report key performance indicators
- Participate in performance reviews of audit leaders
- Ensure that as priorities change and the audit plan changes, those changes are documented

If oversight bodies believe IA shouldn't change the audit plan they can request that the original plan continue.

IA should periodically complete an external review.[28] External reviews by another audit professional can help find ways that internal audit could be strengthened. Oversight bodies should ensure that IA is completing external reviews and working to improve any deficiencies.

Finally, if the internal audit function is not providing value to the organization, oversight bodies should assess whether to require changes, including evaluating the

- Competency of the audit function and leader
- Availability and sufficiency of resources
- Potential impact of audits IA conducts
- Value of the audits IA performs

When oversight bodies provide true accountability, IA can reach its full potential to provide value to the organization.

Oversight Bodies Best Practice 6

Oversight bodies should hold the internal auditors accountable to ensure their work has the most positive impact on the organization it can have.

[28] If the internal audit function follows IIA standards, external reviews are required every 5 years. If the internal audit function follows the *GAO Yellow Book* standards, external reviews are required every 3 years.

Impact: Oversight Bodies Can Help Ensure the Organization Implements Audit Recommendations

Oversight bodies can have significant impact by ensuring that audit recommendations are implemented. They can do this by first, communicating their expectation that recommendations will be completed, and second, holding management accountable for doing so. Ensuring the implementation of recommendations

- Contributes to a tone at the top of respect for IA
- Helps increase the value of internal audit
- Supports meaningful organizational change

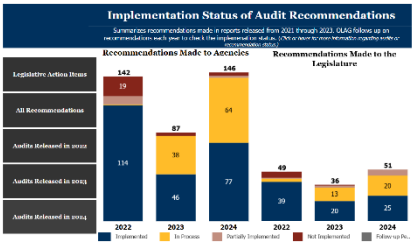
Impact 7: Oversight Bodies Can Monitor Management's Response to Recommendations

Oversight bodies are responsible for ensuring that management completes recommendations. The steps to appropriate oversight of recommendations include:

- Reviewing and understanding the initial recommendation in the audit.
- Reviewing management's initial response to the audit recommendation. Is the response reasonable, does it include sufficient steps to address the recommendations, and does it include a timeline that is appropriate to complete the recommendations?
- Periodically revisiting recommendations' implementation.

Oversight bodies can ensure that IA follows-up on recommendations and that management's response shows progress or verifies that the audit recommendation has been completed.

Our office uses a dashboard on our website that reports to the Legislature the status of all recommendations for three years. This provides transparency for the Legislature. They can use this information to take legislative action or hold agencies accountable for implementation.



Oversight bodies could expect IA to provide similar information so they can likewise provide accountability.

Oversight Bodies Best Practice 7

Oversight bodies should monitor management's completion of recommendations.

Impact 8: If the Organization Isn't Implementing Audit Recommendations, Oversight Bodies Should Hold Leaders Accountable

If organizational leaders have created a culture where findings can be ignored and recommendations don't get implemented, oversight bodies must hold those leaders accountable. Ways to maintain accountability include:

- Requesting further follow-up work from the auditors to determine what changes management still needs to make
- Requiring management to account for the delays
- Ensuring corrective action occurs when leadership is ignoring audit recommendations

Oversight bodies shouldn't allow management to decide that they won't implement recommendations if there isn't a sufficient alternative plan or management cannot articulate why the recommendation no longer applies.

Oversight Bodies Best Practice 8

Oversight bodies should hold leaders accountable for overdue or ignored findings.

Currently, Utah's Audit Landscape Varies by Organization

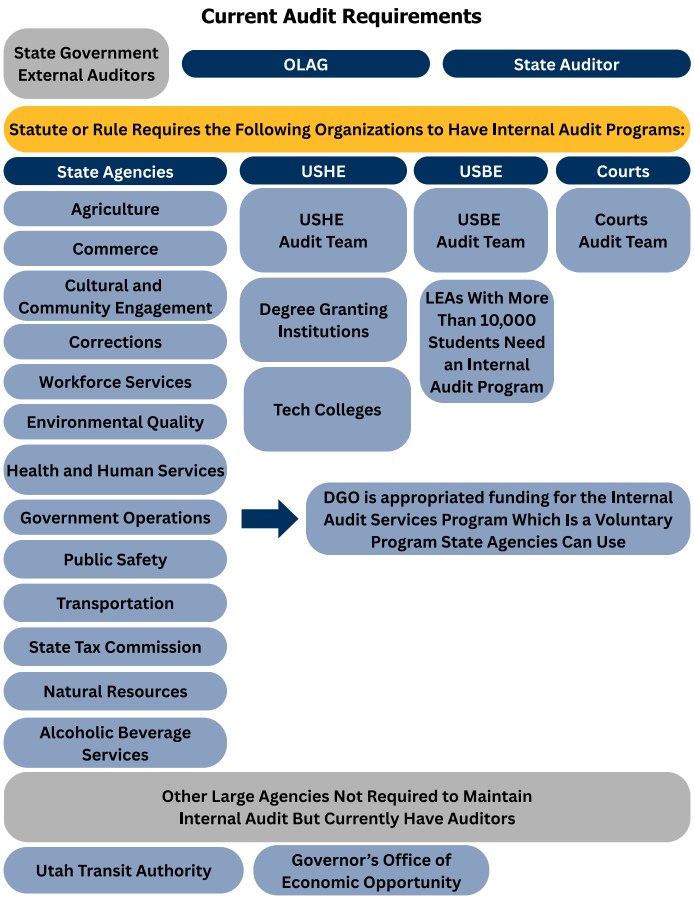
This section helps Utah's oversight bodies understand who is required to have auditors, how they are overseen, and what gaps remain in audit coverage.

Utah law does not require every organization to have an internal audit function. This section helps Utah's oversight bodies understand who is required to have auditors, how they are overseen, and what gaps remain in audit coverage. Other political subdivisions of the state could have internal audit; however there are no state statutory requirements for their audit functions.

Utah Internal Audit Act Requires Some Entities to Have an Internal Audit

The Utah Internal Audit Act, first passed in 1995, added internal audit coverage to government entities.[29] The statute provides auditors so that agencies can have independent evaluations of finances, performance, and compliance. The following graphic shows state organizations currently required to have an auditor.

[29] ***Utah Code*** 63I-5



Source: Auditor summary of Utah Internal Audit Act and Utah Rules. USHE, USBE, and Courts audit teams can perform audits of their whole systems.

Many organizations have an audit committee appointed by either the Governor or the oversight board or commission responsible for the entity that oversees internal audit functions. Some entities haven't appointed an audit committee. In these cases, the agency director retains the authority of the audit committee.

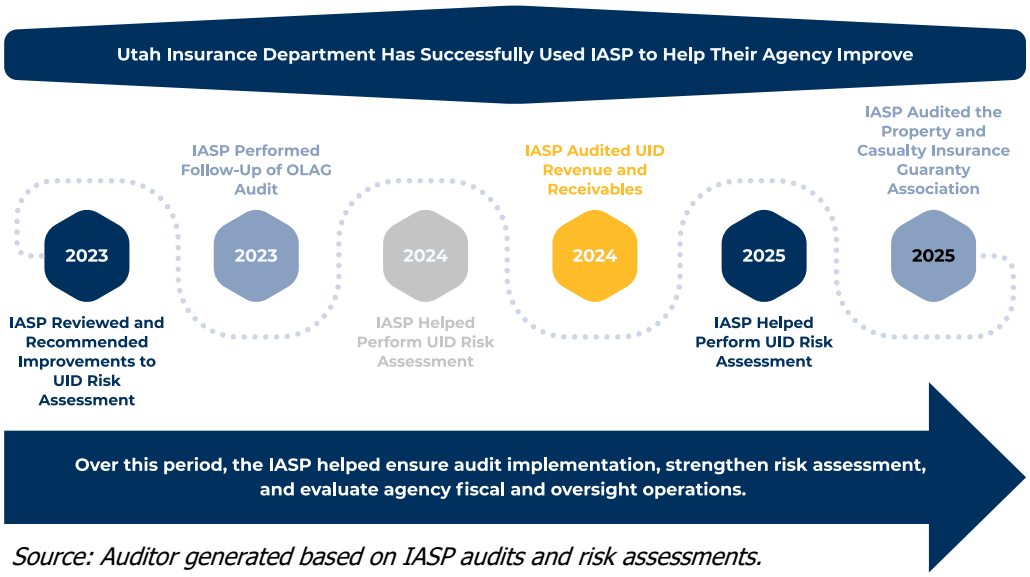
There are seven agencies with a budget of more than $10 million that are not required to have an internal auditor:

- Department of Veterans and Military Affairs (VMA)
- Utah National Guard (UNG)
- Attorney General's Office (AG)
- Utah Insurance Department (UID)
- School and Institutional Trust Lands Administration (SITLA)
- Department of Financial Institutions (DFI)
- Labor Commission

The total annual budget for these seven agencies is more than $340 million, with over 1,400 employees. For the reasons discussed in this report, we believe such large and complex organizations could use internal audit services to help ensure that these resources are used efficiently and effectively. One option that these agencies could use is the Internal Audit Services Program (IASP).

If agencies more proactively request audit resources through the IASP they could more effectively identify, test, and mitigate their risks.

Agencies Could Use the IASP, a Department of Government Operations Program, to Help Provide Some Audit Coverage. The Legislature appropriates money to the IASP to help provide audit services to other agencies. Use of their services is entirely voluntary. Although the IASP is state funded, only a few agencies use this resource. One agency that has proactively used the IASP program to strengthen their organization is the Utah Insurance Department (UID). The following graphic shows how UID has used the program to help assess risk and strengthen programs:



Source: Auditor generated based on IASP audits and risk assessments.

If agencies requested audit resources through the IASP more proactively, they could more effectively identify, test, and mitigate their risks.

Many County Auditors Can't Effectively Act as an Internal Audit Function

While counties have an elected auditor position, this may not mean that they have an internal audit function. Statutorily, county auditors must perform financial and accounting duties for their county unless the county council assigns

those responsibilities elsewhere.[30] In many counties, the elected auditor also performs the duties of the elected county clerk. Performing financial, accounting, or other duties can limit auditors' time and ability to objectively perform internal audits for the county. This means that many counties in Utah do not have a fully objective internal audit function. However, it doesn't mean that counties do not have significant risks that internal auditing is suited to help reduce. Internal auditors have expertise that can help strengthen internal controls, mitigate risk, and make operations more efficient. The following examples show what can happen in counties with ineffective internal controls that could have been strengthened through audits.

A former Kane County treasurer transferred funds from county accounts to a personal bank account, paid for personal cell phone services, and likely took cash from county funds. Inadequate separation of duties and internal controls allowed over $90,000 to go missing without detection.

Two former Cache County attorneys appeared to have used taxpayer money for their own personal gain. These attorneys appeared to have used other Cache County employees, the Cache County case management software, and grant funding reimbursements for private contracts they were performing. Inadequate oversight and controls likely allowed these resources to be utilized for private purposes.

While auditing does not remove all the opportunities for fraud, it can help provide assessments of internal controls that can help limit fraud. As mentioned throughout this report, audit can also help ensure efficiency and effectiveness, compliance, and accurate financial reporting. The following example shows one way that audit can be used to perform these functions:

[30] ***Utah Code*** 17-69.

In Davis County, the county commission wanted to understand whether there were concerns with the contract that was in place with the county shooting range. The county auditor was asked to review the contract and operations of the contractor to help the commission decide whether to continue with the contract. The auditor found gaps in accountability, which led to operational and financial risk because of a lack of internal controls. Based on the audit, the county commission was able to make informed decisions about what to do with the contract and shooting range going forward.

As these oversight bodies consider their risks and attempt to assign internal audit assignments to the county auditors or their staff, they should assess whether they have the objectivity and capacity to perform that work. If not, external auditors, greater resources, or changes to auditor responsibilities may be needed.

Except for counties of the first class, county performance audits are performed under the authority of the county legislative or executive bodies.[31] As these oversight bodies consider their risks and attempt to assign internal audit assignments to the county auditors or their staff, they should assess whether they have the objectivity and capacity to perform that work. If not, external auditors, greater resources, or changes to auditor responsibilities may be needed. In some larger counties, auditors have separated internal audit duties by delegating audit responsibilities to a county auditor's office staff member.

[31] Counties of the first class are those with more than 1,150,000 people. Salt Lake County is currently the only county of the first class in Utah.

Complete List of Best Practices

Complete List of Best Practices: Internal Audit

This report recommends the following 10 best practices.

Best Practice 1

Internal audit leaders should understand stakeholder needs and key questions so they can focus audits on the most important risks, use resources effectively to meet organizational priorities, and provide recommendations that lead to meaningful improvements.

Best Practice 2

Internal audit should ensure they create and periodically review the audit charter that addresses how they will maintain independence and authority.

Best Practice 3

Internal audit should advise organizational leaders on effective enterprise risk management. They should then use the results of enterprise risk management to help guide their auditing efforts.

Best Practice 4

Internal audit should focus their work on the most critical risks and goals of the organization. Internal audit should also develop information for organizational leaders that otherwise would not be known. As organizational leaders rely on information auditors provide to make decisions, the organization can effectively advance its mission.

Best Practice 5

Internal audit should make sure their information is relevant. To be relevant, they must pursue strong effect. Auditors should define the audit scope and objectives and tie these to stakeholder needs. Auditors must determine when stakeholders will need information and scope the audit to provide important information at the time key decisions or changes will be made.

Best Practice 6

Auditors' information must be reliable. IA should consistently follow audit standards, tailor audit methodologies to produce accurate information, and support their findings in a way that a knowledgeable person could agree that the findings are correct.

Best Practice 7

Auditors must ensure their information is actionable. To write effective recommendations, auditors must properly identify the root causes of their audit findings. Recommendations should be designed to intervene on the causes of the issue. Recommendations should

1. Identify the responsible party
2. Define the needed change
3. Describe what implementation looks like
4. Clarify the intended effect

By focusing actions on changing the conditions causing negative outcomes, auditors can empower leaders with the knowledge they need to make good decisions and improve their organizations.

Best Practice 8

Internal audit must communicate in the simplest, most accessible ways. Some ways to accomplish this include planning the simplest reports, simplifying language, and relying on figures and graphics to help stakeholders make decisions based on the best information.

Best Practice 9

Internal auditors should follow up on audit recommendations and conduct additional audit work as necessary to ensure that internal changes are made.

Best Practice 10

Internal auditors should track recommendation implementation agency wide to help inform organizational executive leadership of what changes still need to be made to correct audit findings.

Complete List of Best Practices: Organizational Leaders

This report recommends the following eight best practices.

Best Practice 1

Independence reduces bias because it reduces perverse incentives. Leaders should ensure internal audit (IA) reports to the highest level of the organization, approve IA charters on authority and access, and protect IA from potential reprisals. Taking these and similar steps will safeguard the independence of IA and increase the reliability of the information it produces.

Best Practice 2

Organizational leaders should ensure internal audit (IA) has sufficient capacity, meaning competencies and resources. Leaders should recruit and hire an audit director who can produce the type of information needed by stakeholders. Funding should match leaders' needs for high-quality information and the value that IA provides. State agencies should consider using the internal audit service program.

Best Practice 3

Effective risk management is essential to organizational results. Organizational leaders should develop and strengthen an Enterprise Risk Management (ERM) framework. Leaders may apply the U.S. Government Accountability Office's six essential elements of ERM.

Best Practice 4

Leaders should understand the different types of audits available. They should request audits based on the information they need and hire directors that can provide the necessary information.

Best Practice 5

Leaders should facilitate access to accurate information during the audit process.

Best Practice 6

Leaders should coordinate regularly with the auditor and oversight body to ensure audit effectiveness.

Best Practice 7

To ensure accountability, leaders should document the who, what, and when of their plans to implement audit recommendations. Leadership should act on audit recommendations to ensure that risks are properly managed or eliminated.

Best Practice 8

Leadership must hold individuals responsible for implementing audit recommendations.

Complete List of Best Practices: Oversight Leaders

This report recommends the following eight best practices.

Best Practice 1

Oversight bodies should help establish and maintain auditor independence by approving the Internal Audit Charter, and by helping ensure accurate and unbiased information.

Best Practice 2

Oversight bodies should provide and safeguard the resources that an internal audit function needs to succeed.

Best Practice 3

Oversight bodies should either direct or affect the selection of a quality audit director to ensure the organization is getting the most value from the internal audit function.

Best Practice 4

Oversight bodies should review and approve the annual risk-based audit plan to ensure it covers the most important things.

Best Practice 5

Oversight bodies should facilitate access to information and help remove barriers.

Best Practice 6

Oversight bodies should hold the internal auditors accountable to ensure their work has the most positive impact on the organization it can have.

Best Practice 7

Oversight bodies should monitor management's completion of recommendations.

Best Practice 8

Oversight bodies should hold leaders accountable for overdue or ignored findings.

Appendices

A. Best Practices for Utah Audit Charters and Two Example Charters: Department of Workforce Services and Utah Transit Authority

To access this tool online, go to:

https://olag.utleg.gov/CfHI.jsp

Best Principles for Utah Audit Charters

An organization's internal audit function supports the organization's success. The Institute of Internal Auditors states "internal auditing strengthens the organization's ability to create, protect, and sustain value by providing the board and management with independent, risk-based, and objective assurance, advice, insight, and foresight."[1] Ensuring that internal audit is independent, objective, and competent helps internal audit be effective at fulfilling its mission to bring value to the organization. Audit charters support the governance structure of the audit function and set expectations for how auditors, organizational leaders, and oversight bodies collaborate to support the organization.

This document provides guidance on four key principles that should be within an audit charter to set auditors and organizations up for success. We recommend that internal auditor directors, senior management, and oversight bodies review this document then evaluate their own audit charter for improvements.

PRINCIPLE #1
Access to Leadership

The internal audit function must be granted full access to the oversight body and senior management so that they can support organizational decision making. It is critical that auditors be allowed to report on risk-based audit findings and make recommendations on a regular basis to improve the organization. An audit charter should grant internal audit access to the board and senior management and set expectations for how they will interact with and oversee internal audit.

PRINCIPLE #2
Access to the Organization

For internal audit to do its job and evaluate the organization, internal audit staff need access to the organization. This means access to documents, information, and any other resources that could help audit staff in their efforts to produce high-impact reports. An audit charter should grant audit staff this access and ensure that management cannot infringe upon the internal audit function's authority.

[1] The Institute of Internal Auditors. "Global Internal Audit Standards." Page 15.

PRINCIPLE #3
Risk-Based Auditing

To support the organization, auditors should focus on high-impact auditing and be allowed freedom to influence the scope of the work they perform. The areas an auditor evaluates should be specified in an annual audit plan and the audit plan should be risk-based. Risk-based audit plans can help ensure the audit function is aligning its work with the organization's top priorities. Audit charters should clarify that the internal audit function will focus on risk-based auditing and will seek to tie the annual audit plan to the organization's biggest risks.

PRINCIPLE #4
Non-Audit Work

Auditors should maintain their objectivity so they can fulfill their professional duties to the organization. The Government Accountability Office Government Auditing Standards specify that auditors should be aware of threats to their independence. One threat to independence that the standards identify is referred to as management participation threat, which arises when auditors are involved in managing any part of the entity they are auditing. Management participation threat "will lead an auditor to take a position that is not objective."[2] To maintain objectivity, auditors should avoid being directly involved in managing the organization as much as possible. Audit charters should set clear expectations regarding the importance of allowing auditors to remain free from any conflict of interest.

[2] Government Accountability Office, Government Auditing Standards 2024 Revision, page 32.

DEPARTMENT OF WORKFORCE SERVICES

AUDIT BOARD CHARTER

PURPOSE

To establish an Audit Board to assist the Executive Director in fulfilling oversight responsibilities found in *Utah Code* 63I-5-301(3). These responsibilities include establishing an independent objective internal audit activity designed to evaluate and improve the efficiency and effectiveness of operations, safeguarding of assets, compliance with applicable laws, regulations, policies, procedures, and contracts, risk management and control processes of the Department.

AUTHORITY

Utah Code 63I-5-302 assigns the powers and duties of the audit committee to the Executive Director when the governor has not appointed an audit committee. The governor has not appointed an audit committee; therefore, these powers and duties are exercised by the Executive Director.

COMPOSITION

The Executive Director and Deputy Directors comprise the Audit Board. Because powers and duties of the "audit committee," as defined in statute, are exercised by the Executive Director, Deputy Directors advise, assist, and carry out responsibilities under the direction of the Executive Director.

MEETINGS

The board will meet at least once per year. The Director of Internal Audit is responsible for documenting decisions by the Executive Director and any action items from the board meetings. No formal minutes will be prepared.

RESPONSIBILITIES AND DUTIES

- Appoint and evaluate the Director of Internal Audit.
- Approve the remuneration of the Internal Audit Director.
- Adopt formal policies that define the Department's internal audit activities.
- Approve the Internal Audit Division's charter.
- Ensure that the Director of Internal Audit and staff have access to all records, data and other Department information that the Director of Internal Audit or staff consider necessary to carry out their assigned duties.
- Approve the internal audit plan and all major changes to the plan.
- Review Internal Audits performance relative to the plan.
- Approve the Internal Audit Division's budget and resource plan.
- Review final audit reports and responses (both internal and external) and ensure appropriate action is taken.

Casey Cameron
Casey Cameron (Sep 28, 2021 11:53 MDT)

Casey Cameron, Executive Director

09/28/2021
Date

*DWS is in the process of updating its Audit Board Charter to align with the 2024 Global Internal Audit Standards from the Institute of Internal Auditors

INTERNAL AUDIT CHARTER

FOR THE UTAH TRANSIT AUTHORITY

The Board of Trustees ("Board") has established the Internal Audit Department ("Internal Audit") within the Board Strategy and Governance office as a key component of the Utah Transit Authority's ("UTA") governance framework.

This Internal Audit Charter serves as a framework for Internal Audit in the performance of its duties and is intended to provide a basis for the Chief of Board Strategy and Governance to evaluate the Internal Audit function.

The components of this Internal Audit Charter include:

- Mandate
- Scope of Work
- Responsibilities
- Audit Plan
- Reporting
- Independence and Authority
- Standards of Audit Practice

MANDATE

The mandate of Internal Audit is to improve UTA's operations and systems of internal controls and add value through independent, objective assurance, and consultative support. Internal Audit helps UTA accomplish its objectives through a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance activities and processes.

SCOPE OF WORK

The scope of Audit coverage is organization-wide including all departments and business units of UTA.

To fulfill its mandate, Internal Audit assesses whether UTA's network of risk management, control, and governance processes, as designed and represented by management, is adequate and functioning in areas such as:

- Risk identification and management
- Operational control
- Accurate, reliable, and timely financial, managerial and operating information
- Compliance with policies, standards and procedures
- Adherence to applicable laws and regulations
- Management's achievement of goals and objectives
- Economic acquisition, efficient use, and adequate protection of resources
- Support of management in their interaction with the various internal organizations and external regulatory authorities as needed

RESPONSIBILITIES

The Director of Internal Audit and the Internal Audit staff have responsibility to:

- Develop an annual Audit Plan using appropriate risk-based methodology (including risks or control concerns identified by management, the Audit Committee and external Audits) and submit that plan to the Audit Committee for review and approval
- Perform independent and objective audit engagements of the key processes and related internal controls supporting operations and financial reporting as part of the audit process
- Communicate audit engagement results and recommendations to management and the Audit Committee as part of the audit process
- Follow-up with management to assess whether Action Plans are completed by management within the mutually agreed timeframe to address the risks and deficiencies identified
- Perform safety related audits required by the Federal Transit Administration.
- Support UTA management in their interaction with the external financial auditors
- Assist UTA management to facilitate other external compliance audits generally managed through other departments within UTA
- Assist UTA in identifying the characteristics of adequate systems of control
- Maintain a professional audit staff with sufficient knowledge, skills, experience and professional certification to meet the requirements of this Charter
- Establish and maintain a Quality Assurance and Improvement Program ("QAIP") in accordance with the Global Internal Audit Standards, published by the Institute of Internal Auditors.
- Ensure that a peer review is conducted every five years, and that results are communicated to the Audit Committee
- Keep the Audit Committee informed of emerging trends and best practices in internal auditing
- Assist the Audit Committee in any other way in connection with the discharge of Committee duties and responsibilities
- Prepare and present reports to the Audit Committee summarizing the status of Internal Audit's work at least quarterly but could be more frequently as directed by the Audit Committee
- Design and roll-out programs and practices around ethics, with support from UTA's Legal Counsel
- Assist in the investigations of suspected misconduct or fraudulent activities within the organization and notify management and, in the event of significant ethical violations, the Audit Committee.
- Develop a Strategic Plan for Internal Audit that documents a long-term vision, objectives, and supporting initiatives for Internal Audit
- Maintain an Assurance Map outlining audit and monitoring activities across the organization

AUDIT PLAN

The annual Audit Plan is developed each year based upon input from UTA leadership and the Audit Committee and is submitted to the Audit Committee for review and approval.

The annual Audit Plan is comprised of topics or processes to be the subject of audit engagements, and may include, but is not limited to, a combination of the following:

- Assessments of compliance with UTA's policies and procedures
- Reviews of internal controls related to significant processes and IT systems to determine if they are properly designed and functioning as intended
- Reviews of financial and operating information
- Assessing if corporate assets are properly safeguarded
- Reviews of computer-based systems focusing on data security, disaster recovery, and effective use of resources
- Reviews of internal controls designed to ensure compliance with external laws and regulations,

including accounting rules and applicable regulations
- Operational audits focusing on improving efficiencies or effectiveness with a goal of contributing to cost reduction efforts
- Strategic audits, such as reviews of due diligence activities and the execution of UTA's strategic objectives
- Requested consulting services, the nature of such services are determined in collaboration with management. Internal Audit may not provide any audit services for a period of one year following the conclusion of the consulting over an area where they consulted.

To develop the annual Audit Plan, an overall risk-based approach is used to ensure that the Internal Audit function provides the greatest possible benefit to UTA. On an ongoing basis, matters considered in developing the annual Audit Plan include the following:

- Strategic and operational plans of UTA
- Risk for potential loss to UTA
- Opportunities to achieve operating benefits
- Existence of known errors, irregularities or control weaknesses
- Results of previous audits
- Changes in operations, systems or controls
- Changes in regulatory or other requirements
- Requests from management, Audit Committee and external auditor

Each year, Internal Audit will work with UTA's leadership to perform risk assessment activities designed to identify and prioritize UTA's key risks. This information will be used to identify priorities to be addressed by the annual Audit Plan.

Based on the risk assessment performed, the Director of Internal Audit will present a proposed annual Audit Plan to the Audit Committee for approval. The Audit Plan is a list of topics or processes that will be the subject of audit engagements. Any significant deviation from the approved Audit Plan, such as adding a large audit engagement or removing an audit engagement, will be submitted to the Audit Committee for review and approval. Small changes, such as changing the type of engagement performed or small requested audit engagements can be carried out without Audit Committee approval and will be reported in the Director of Internal Audit's quarterly report to the Audit Committee.

The Audit Plan will be developed in a manner that allows for the coverage of UTA's highest risk areas. The Director of Internal Audit, in consultation with the Audit Committee, will determine when certain critical risks and controls require more frequent coverage.

REPORTING

A report will be issued by the Director of Internal Audit to the Audit Committee following the completion of any engagement phase (preliminary assessment, audit, follow-up). The report will document observations and recommendations. Management must be offered the opportunity to provide a written response to be included in the report. The written response can document agreement or disagreement with the results and an action plan, if applicable. The report will be provided to the Audit Committee members and discussed at a future Audit Committee meeting. Reports may be restricted from public release if classified as protected under the provisions of the Governmental Records Access and Management Act (Utah Code, §63G-2-101, *et seq*.).

Other engagement types will have a report issued by the Director of Internal Audit outlining any findings, recommendations, and management Action Plans. The report will be provided to the Audit Committee members and discussed in a future Audit Committee meeting.

The Director of Internal Audit may report urgent issues to the Chief of Board Strategy and Governance, as necessary.

INDEPENDENCE AND AUTHORITY

To provide for Internal Audit's independence, the Director of Internal Audit reports to the Chief of Board Strategy and Governance, which position reports directly to the Board of Trustees. All Internal Audit personnel will report to the Director of Internal Audit. The Director of Internal Audit will meet at least once every quarter, but more frequently if necessary, with the Audit Committee. The Audit Committee may choose to meet with the Director of Internal Audit in private and apart from UTA management, if the meeting satisfies the criteria for a closed session under Utah's Open and Public Meetings Act (Utah Code §52-4-101, *et seq*.).

To maintain its independence, Internal Audit will have no direct operational responsibility or authority over any of the activities under scope of its review. Accordingly, Internal Audit will not be responsible to develop or install systems or procedures, prepare records, or engage in any other activity that would normally be audited but may perform a consulting role without any decision-making authority. Because the Director Internal Audit is a member of UTA's Ethics Committee, Internal Audit cannot audit the ethics program. Any auditing of the ethics program will be outsourced to a third party, at the discretion of the Chief of Board Strategy and Governance.

Internal Audit is authorized to have unrestricted access to all company activities, records, property and personnel. Restriction to these accesses imposed by any employee or management of UTA, which prevents Internal Audit from performing any duties, will be reported immediately to the Executive Director, Chief of Board Strategy and Governance, or directly to the Audit Committee, based on circumstances as determined by the Director of Internal Audit.

STANDARDS OF AUDIT PRACTICE

Internal Audit will adhere to mandatory elements of The Institute of Internal Auditors' Global Internal Audit Standards. Additionally, Internal Audit must adhere to laws and regulations specific to Internal Audit activities, with applicable jurisdiction, including Utah Code 17B-2a-801, Utah Public Transit District Act.

Revision/Review History:

Date	Action
3/28/2018	Board of Trustees adopted Internal Audit Charter by R2018-03-03
6/10/2019	Audit Committee presented with revised Internal Audit Charter for review on 4/29/19; Audit Committee approved the Charter on 6/10/2019.
2/10/2020	Revised Internal Audit Charter reviewed and approved by Committee on 2/10/20 with minor verbiage updates.
2/1/2021	Internal Audit Charter presented and approved by the Audit Committee with no changes.

1/31/2022	Committee adopted revised Internal Audit Charter. Revisions included title changes for staff functions and updates to audit processes including establishment of a QAIP, documentation of a peer review process, and expanded standards of audit practice.
3/6/2023	Audit Committee Charter duties and responsibilities amended to include the Committee's review and approval of the Internal Audit Charter annually. Committee approval of revised Internal Audit Charter that adds responsibility for EEO investigations, safety audits, and removes duties to facilitate UTA's annual risk assessment which will be done by management.
9/23/2024	Language was added to reflect new standards adopted by the Institute of Internal Auditors (IIA) that comply with State of Utah law, and to clarify audit types. Removed language about investigating discrimination and retaliation claims which will be done by the Office of the Attorney General.
2/13/2025	Language was added to reflect a change in audit standards published by the Institute of Internal Auditors. The organizational reporting structure was updated. The nature of consulting activities was clarified. Details of specific audit practices was removed to better align with the document being a charter and not an operating procedure document. The reporting section was updated to reflect the practice of management providing written responses to reports.
3/9/2026	Language was added to document the Director Internal Auditor's role on the Ethics Committee and require audits of UTA's ethics programs to be outsourced to an independent auditor.

B. Enterprise Risk Management Tool Guidance

To access this tool online, go to:

https://olag.utleg.gov/CfHI.jsp

Legislative Auditor General

Center for High Impact Auditing

Enterprise Risk Management Tool Guidance

Risk assessment is a coordinated activity designed to direct and control threats to achieving the organization's goals and objectives. Enterprise Risk Management (ERM) is an agency-wide approach to identifying and addressing the organization's combined risks. The ERM template was developed with the help of our audit workgroup.[1] It is intended to be a resource. The template provides a place to record many common elements found in an effective ERM.

While the template provides a foundation for applying ERM principles, leaders may want to customize the template according to their industry and environment. Organizational leaders' primary role is to advance the missions of their organizations. ERM should be designed in a way that helps leaders in this role.

The template has two tabs. The first, "Key Definitions," provides a common language used for understanding and talking about risk. As stated in the Governor's Office guidance,

> *A risk assessment without shared definitions and an understanding of the product it will produce will likely be viewed as not successful;*

We agree and have included definitions in this tab. We have also added definitions to make the resource as flexible as possible for a broader audience.

The second tab, "Template", is where leaders can begin to fill out their ERM. It is divided into three sections—risks, objectives, and responses—to facilitate an integrated approach to risk management. In the course of our research, we encountered multiple existing resources on how to effectively develop an ERM. We encourage leaders to read and apply the principles and practices found in these resources. They are linked below.

Additional Resources

U.S. Government Accountability Office: Enterprise Risk Management

U.S. Chief Financial Officers Council & Performance Improvement Council: Playbook: Enterprise Risk Management for the U.S. Federal Government

[1] The Internal Audit Director at the Department of Government Operations provided the original template that we modified and reviewed with the audit workgroup.

C. Governor's Office Risk Management Guidance

To access this tool online, go to:

https://olag.utleg.gov/CfHI.jsp

Legislative Auditor General

Center for High Impact Auditing

ENTITY-WIDE RISK ASSESSMENT

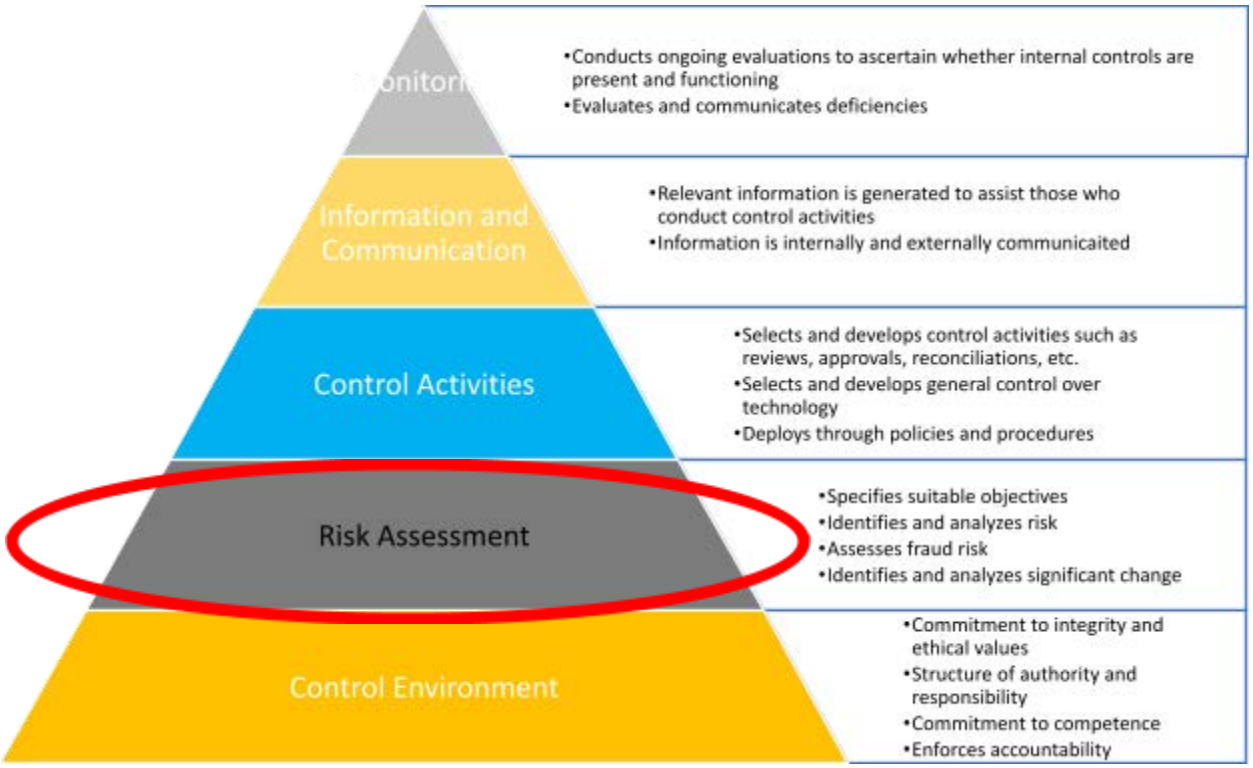
Introduction

All executive branch agencies must conduct an annual risk assessment using a methodology which applies leading practices. Agencies should share two or three high or critical risks and their plans to address them.

Effective risk assessment enables organizations to better anticipate challenges so they can get ahead of them. Obtaining robust information on risk allows management, in the face of finite resources, to assess overall resource needs, prioritize resource deployment and enhance resource allocation. A risk assessment without shared definitions and an understanding of the product it will produce will likely be viewed as not successful; therefore, the definitions below help establish shared definitions and understanding.

Definitions

COSO's Internal Control Framework – A generally accepted internal control framework that defines how to respond to and manage risk and that is designed to help organizations enhance the likelihood of achieving their objectives. Risk assessment is one component of this framework as illustrated below.



Internal Audit – The individuals who operate independent from management to provide assurance and insight on the adequacy and effectiveness of governance and on the management of risk, including internal controls.

Internal Control – The processes, actions and activities designed to create reasonable assurance of the achievement of objectives.

Management – The individuals, teams and support functions assigned to provide products and/or services to the organization's clients.

Risk – Anything that threatens an organization's ability to achieve its goals.

Risk Assessment – One of the five components of the COSO Internal Control Framework. It addresses how an organization identifies, assesses and manages risks related to the achievement of objectives. Typically results in a report on risk by priority.

Risk and Control Types – Risks and controls are often grouped into types (such as strategic, operational or hazard) to facilitate risk identification and control development.

Risk Rating – A scale by which a risk is compared to how likely/probable it is to occur and what impact it would have on the achievement of objectives when it occurs.

Risk Types – A classification label used to identify and characterize the variety of risk to which an organization is exposed. Typical risk types include:

- Strategic Risk – Risks that arise when an organization's strategy fails to deliver expected outcomes. These are the risks taken when making strategic decisions. They are typically mitigated through formal decision-making processes that vet the data involved in choices and that check for decision bias. They also include organizational impacts by diverting resources to a strategic choice. Examples include:
    - Ethics, conflicts of interest, bias in decision-making processes.
    - Strategic decisions that are unclear or poorly communicated.
    - The introduction of new programs or services.
    - Changes in senior management.
    - Changes to customer demands or expectations.
    - Financial challenges (e.g., underfunded programs).
    - Problems with suppliers, vendors or other stakeholders.
- Operational Risk – Risks that arise from inadequate or failed internal procedures, employee errors, cybersecurity events or external events. These are the risks that arise due to an absence of or weakness in operational controls. As management sets up operations, there is an expectation that people with needed skills are involved, processes are efficient and effective, and technology is enabling and supportive. There is also an expectation that management has oversight mechanisms needed to enable operational success and capacity growth over time. Examples include:
    - Weakness in governance and management oversight controls.
    - Unclear objectives and accountabilities.
    - Misalignment of people, processes and technology.
    - Inadequate or failed internal processes.

    - Human error.
    - System downtime or failure.
    - Inadequately trained staff.
    - Breakdown of process controls.
- Hazard Risk – The many things that could go wrong, mostly external to the organization. Management typically controls these risks by funding functions to address them (e.g., insurance, communications, information security, legal, safety, etc.) Examples include:
    - Damage to the organization's credibility or reputation.
    - Compliance with laws, rules or policies.
    - Information security.
    - Human resource incidents (e.g., workplace harassment and employee discipline).
    - Cybersecurity events (e.g., data breaches).
    - Fraud.
    - External events (e.g., earthquakes or pandemics).

Conducting an Entity-Wide Risk Assessment

1. Who is Responsible?
   Management is responsible for managing risks to the entity; therefore, ensuring a risk assessment is conducted is ultimately their responsibly. Internal audit standards and leading practices put internal audit in a position to lead or participate in conducting the entity-wide risk assessment.

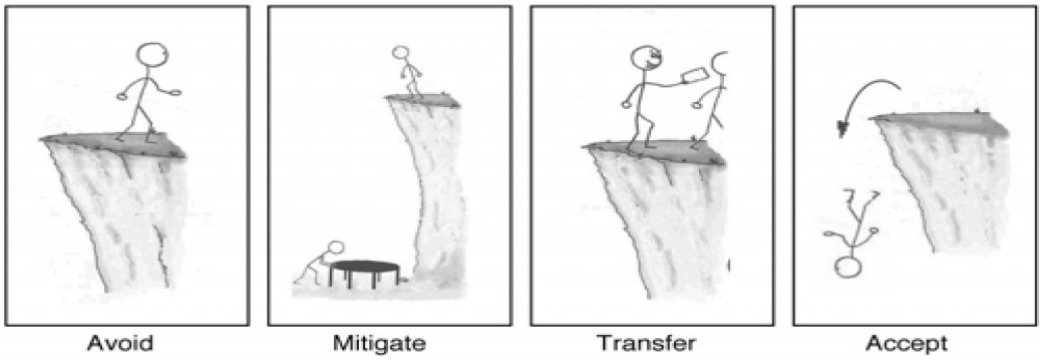
   Defining risks requires an analytical mind that can take off the operational hat and put on a value-preservation hat. It is possible that several individuals may be needed to form a risk assessment leadership committee to execute it with competence.

2. Develop a Risk Assessment Strategy
   The following should be considered when developing a risk assessment strategy:

   - Timing – Choose a period of time when key individuals can give sufficient attention and thought to the assessment (e.g., not during a legislative session).
   - Frequency – Risk assessments should be conducted at least annually.
   - Methodology:
     - Background – Gain an understanding of what is at risk, including the operational structures, strategic plans and objectives of the organization.
     - Scope – This is critical to the risk assessment being viewed as successful. Scoping entails the following:
       - Knowing which risk types will be covered and how they will be prioritized, given the time and resources available.
       - Defining if the risk assessment will be wide covering all areas of the organization or deep in only a few areas of the organization.
     - Research – Based on the scope of the risk assessment, define and collect risks through research, interviews, surveys or workgroups with identified personnel.
     - Risk Type – Defining potential risks by risk types in advance is helpful to all involved as it aids in communication and in the development of risk assessment methodology. This can help management view risk through the internal controls

they have naturally put in place as they seek the success of strategic and operational objectives.

- Rating - Rate the impact and likelihood/probability of identified risks.
- Risk Response - Develop a risk response that may include one of the following:



  - Avoid – Eliminate the risk by choosing not to participate in programs or activities considered too risky.
  - Mitigate – Reduce the impact and likelihood/probability of the risky event by applying internal controls.
  - Transfer – Contract with a third party to administer the program or activity, thus transferring the risk and loss exposure.
  - Accept – Retain the risk and develop plans to cover the financial or non-financial consequences.

- Communicate the results to appropriate parties in a written format.

3. Utilizing Risk Assessments

   Management should utilize risk assessments to develop risk management strategies and the annual audit plan.

D. Enterprise Risk Management Maturity Model

To access this tool online, go to:

https://olag.utleg.gov/CfHI.jsp

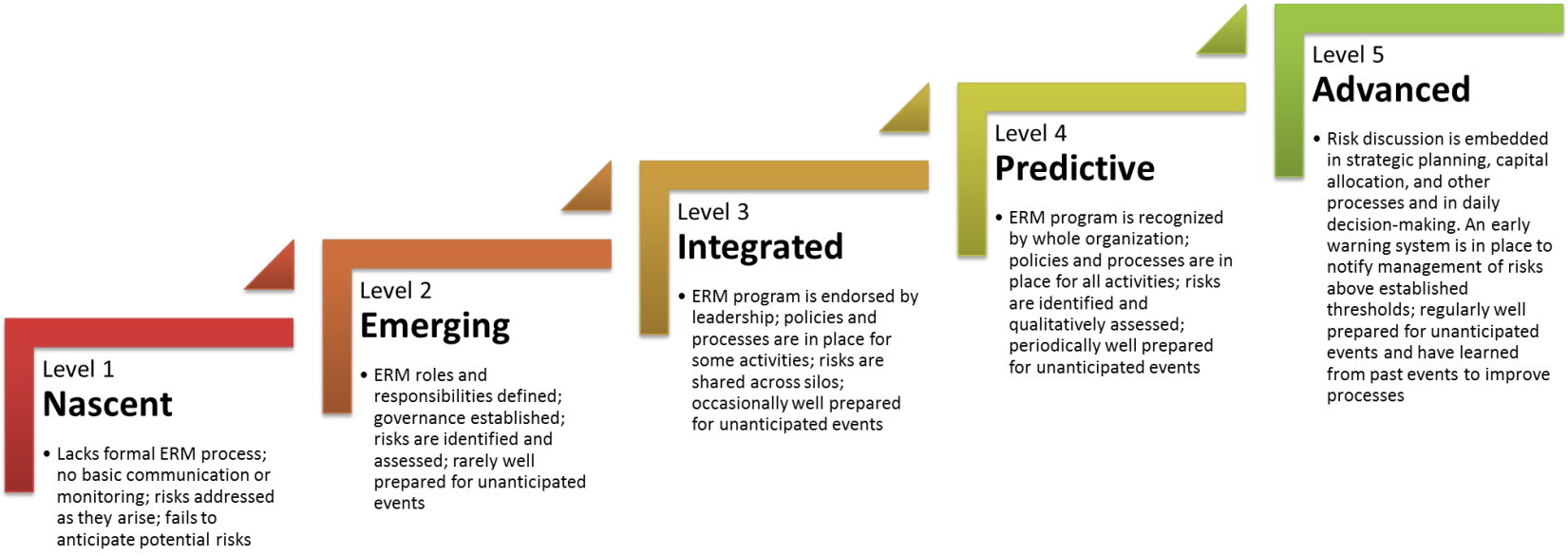
Legislative Auditor General

Center for High Impact Auditing

U.S. Chief Financial Officers Council & Performance Improvement Council
Playbook: Enterprise Risk Management for the U.S. Federal Government

Maturity Models

Five Step Maturity Model (Example)



Maturity Across Eleven Areas (Example)

Maturity Sub-Factors	Maturity Levels				
	1 Nascent	2 Emerging	3 Integrated	4 Predictive	5 Advanced
CULTURE					
Alignment	Failure to have congruence between the overall goals of the organization and specific units and their personnel	Select unit functions are aligned to overall goals	Relationships between all unit functions and overall goals are consistently communicated and understood by personnel	Functions across units are synchronized to support achievement of overall goals	Unit functions across the enterprise are aligned to support achievement of overall goals
Governance	Dysfunctional policies, processes, and controls with lack of even basic communication and monitoring	Governance program is established	Quality policies, processes, and controls are in place for select processes	Quality policies, processes, and controls are in place for all processes	Policies, processes, and controls are in place to protect the enterprise and are consistently communicated and monitored
PROCESS - ANALYTICAL					
Policy	No Risk Management (RM) policy is written	RM policy is written for select applications	RM policy is written for all applications	RM policy integrated into organizational policy	RM concepts are embedded in [AGENCY] policy throughout the enterprise
Method	No guidance of preferred RM methodologies	Guidance developed for select RM methodologies	Guidance developed for overall RM framework, enabling integration between processes	Interrelationships between RM processes are defined and leveraged	RM methodologies enable efficient and effective management and communication of risk across all processes and throughout the enterprise
Risk Tolerance	No formal documentation or consistent understanding of risk tolerance	Established risk tolerance for select applications	Established risk tolerance for all risk applications	Risk tolerance applied consistently for select applications	Clear identification and acceptance of risk tolerance throughout the enterprise
PROCESS - ORGANIZATIONAL					
Roles & Responsibilities	Limited formalization of RM roles and responsibilities	RM charter is written, formally establishing RM roles and responsibilities	Policy for managing risk endorsed by leadership	Organization Is fulfilling RM policy	Clear designation of RM roles and responsibilities from top to bottom and across the enterprise
Resources	Pockets of self-taught RM competence performed by part-time personnel	Some full-time RM resources supported by formal training	RM organization that is a mix of part- and full-time resources is supported by formal [AGENCY] training program	Risk duties are integrated into workforce, including position descriptions	Minimal overhead required to administer RM activities as they are performed as part of business culture

Maturity Sub-Factors	Maturity Levels				
	1 Nascent	2 Emerging	3 Integrated	4 Predictive	5 Advanced
IMPLEMENTATION					
Risk Identification, Assessment, and Communication	Risks are identified and assessed on an ad hoc basis. Uncertainty is ignored	Risk is systematically identified and assessed for select processes. Uncertainty is largely ignored	Risk data are seamlessly shared across processes. Uncertainty is expressed qualitatively for select processes	Risks are effectively and efficiently identified and qualitatively assessed across all levels of the enterprise. Uncertainty is expressed qualitatively.	Risks are effectively and efficiently identified and quantitatively assessed, including return-on-investment estimates, across all levels of the enterprise. Uncertainty is expressed quantitatively
Tools	Different tools are used by different groups to assess and manage risks for different processes	Standard tools are used across the enterprise	All RM processes use the same tools and data are integrated across select processes	All RM processes use the same tools, and data are integrated across all processes, and select processes leverage [AGENCY] enterprise data sources	RM tool is integrated with all appropriate enterprise tools and data sources
OUTCOME					
Anticipated Risks	Long history of failing to adequately address anticipated risks before they occur or expending substantial resources on relatively minor risks	Consistently failing to adequately estimate the frequency or consequence of anticipated events or over expending resources on relatively minor risks.	Consistently estimating the frequency or consequence of anticipated events and occasionally adequately managing anticipated risks and reduction of resources applied to relatively minor risks	Consistent prevention and/or adequate management of anticipated risks. Focus of resources on anticipated high-risk events	Sustained record of preventing and/or managing anticipated risks and learned from the events to avoid recurrence of related events while also integrating the information throughout the performance management process
Unanticipated Risks	Long history of failing to anticipate potential risks	Rarely executed well-prepared responses to unanticipated events	Occasionally executed well-prepared responses to unanticipated events	Periodically executed well-prepared responses to unanticipated events and learned from the events to avoid recurrence	Regularly executed well-prepared responses to unanticipated events and learned from the events to avoid recurrence of related events while also integrating the level of understanding throughout the performance management process

Five Step Maturity Model (Example)

1. **Level 1: *Ad hoc.*** Undocumented; in a state of dynamic change. Depends on individual heroics rather than well-defined processes.
2. **Level 2: *Preliminary.*** Risk is defined in different ways and managed in silos. Process discipline is unlikely to be rigorous.
3. **Level 3: *Defined.*** A common risk assessment/response framework is in place. An organization-wide view of risk is provided to executive leadership. Action plans are implemented in response to high priority risks.
4. **Level 4: *Integrated.*** Risk management activities are coordinated across business areas. Common risk management tools and processes are used where appropriate, with enterprise-wide risk monitoring, measurement, and reporting. Alternative responses are analyzed with scenario planning. Process metrics are in place.
5. **Level 5: *Optimized.*** Risk discussion is embedded in strategic planning, capital allocation, and other processes and in daily decision-making. An early warning system is in place to notify the board and management of risks above established thresholds.

E. Risk Likelihood and Impact Rubrics

To access this tool online, go to:

https://olag.utleg.gov/CfHI.jsp

Legislative Auditor General

Center for High Impact Auditing

Likelihood Criteria

	Staffing (Levels & Experience)	Operational Procedures	Guidance	Problem History	New Program, Phase or Component	Complexity	Outside Control	Potential for Waste, Fraud and Abuse	Work Force Development and Training	Agency Involvement	Consultant Use	Other
Likelihood Level	Is the staff assigned to the effort sufficient? Do they have a clear knowledge, understanding, and ability with the program area or objective and its implications	Are there documented and relevant procedures for this program area or objective of the program?	Is there relevant guidance?	Have there been significant problems or ongoing series of problems related to this program area or objective?	Is program area or objective of the program is truly novel?	Is there a high level of intricacy or challenge associated with the program area or objective?	Is there an opportunity for outside agencies to assert control or interference?	What is the opportunity waste, fraud, and abuse?	Is there program in place to keep training and development in place for the personnel related to this program area or objective?	Is our division office staff actively is involved in managing the program area or objective?	Are consultants actively being applied as primary resources in the effort?	Are there other areas of concern related to this program area or objective that are not addressed in the frequency criteria? (Document the criteria below)
Almost Certain	Severely understaffed or no experience: It is unrealistic to expect the staff assigned not to need supplementation or augmentation before the end of the effort	None: There are no documented or relevant procedures	None: There are no documented or relevant guidance	A lot of: There are historical events that tie directly to the problem history	Cutting Edge: No one has addressed this type of work in this program area or objective before	Almost Certain: The program area or objective involves integration of multiple agencies, consultants and contractors	Almost Certain: Numerous outside agencies and the public have the opportunity and ability to voice concerns, influence or direct	A lot of: There is almost no oversight and a almost no ability to identify waste, fraud and abuse	None: There are no training or mentoring programs	None: Division office personnel have no visibility or no management control	A lot of: The Agency is using a broad range of consultant to address the program area or objective	
Likely	Understaffed or no experience: Staff assigned will be over utilized and likely incapable of completion of with out immediate training.	Some: There are some documented procedures or tangentially related procedures	Some: There is some documented guidance or tangentially related guidance	Some: There have been some incidents of problems related to this program area or objective in this type of program	Done in other transportation agencies: This type of work has been done in other transportation agencies, but no experience at this agency	Likely: The program area or objective involves integration of multiple agencies	Likely: One or two outside agencies and the public have the opportunity and ability to voice concerns, influence or direct	Some: There is some oversight, but certain gaps in our ability to identify waste, fraud and abuse	Limited: There are training and/or mentoring programs, but no funding and/ or leadership commitment	Limited: Division office personnel have visibility but no management control	Some: The Agency is sharing significant responsibilities with consultants related to this program area or objective	
Possible	Understaffed or some experience: Staff assigned will be over utilized and run the risk of being incapable of completion if additional responsibilities are assigned, or lack experience	Out-of-date: There are documented procedures, but they are out-of-date with existing laws and regulations.	Out-to-date: There are documented guidance, but they are out-of-date with existing laws and regulations.	Possible: There are rumors or organizational legend of problems related to this program area or objective in this type of program	Some experience: Some people have done this type of work in the past or have done related work	Possible: This program area or objective involves integration of Agency and one other outside agency	Possible: One or two outside agencies have the opportunity and ability to voice concerns, influence or direct	Possible: There is oversight, but possible gaps in our ability to identify waste, fraud and abuse	Some: There are training and/or mentoring programs, but they are not universally available	Some: Division office personnel have management control over some aspects of the program area or objective	Limited: The Agency is sharing limited responsibilities with consultants related to this program area or objective	
Unlikely	Adequately staffed or competent: Adequately staffed or competent	Good and up-to-date: Procedures are good and up to date.	Good and up-to-date: Guidance is good and up to date.	None: There have been no significant or ongoing problems.	Old news: It's what we do, routine	Unlikely: This program area or objective involves only Agency personnel	Unlikely: There is virtually no opportunity or ability for outside agencies to voice concerns related to this program area or objective	None: There is virtually total oversight and a high opportunity to identify waste, fraud and abuse	A lot of: There are training and mentoring programs, broadly available to personnel	A lot of: Division office personnel have active management control over most aspects of the program area or objective	None: The Agency has full responsibility for all aspects of this program area or objective	

Impact Criteria

	Financial	Reputation	Business Operations	Legal and Compliance	Infrastructure Assets	Resources and Effort Required	Human and Natural Environment	Safety	Civil Rights	Economic
Catastrophic	Large unacceptable financial loss, severe budget variance. Critical long term impact on budget/finances, not recoverable within current or next fiscal year. Critical business functions could be vulnerable or ineligible. Systematic and extensive major fraud. Results in qualified audit opinion.	Very significant harm to image with substantial impact on effectiveness. Significant adverse community impact and condemnation. Consistent extreme negative media attention (months). Irreconcilable community loss of confidence in the organization's intentions and capabilities and possibly in the government. Secretary level intervention	Large and unacceptable operational impact, long term business interruption. System failure and overall survival of the organization is threatened. Full business disruption for more than one week or a key service more than two weeks. Majority of critical programs cannot be achieved. Secretary level intervention	Material compliance infraction. Significant prosecution and fines. Major litigation involving class actions. Major non-compliance with legislation.	Significant or critical infrastructure assets are destroyed. Significant or critical infrastructure assets are unusable for months.	Impact cannot be managed within the organization's existing resources and threatens the survival of the organization. Department Secretary level intervention.	The event will permanently affect the human and natural environment. The impact covers a wide area and is difficult to contain. The effects are irreversible. Threat to survival of flora, fauna, and or cultural heritage.	Many fatalities.	Program or critical component of a program declared unconstitutional the US Supreme Court, thereby effectively eliminating it nationally. Complete inability to achieve any of the program's objectives, or any objectives of a critical component of a program.	Significant, long lasting negative impacts to the economy of a major metropolitan area, a State or the nation
Major	Very significant financial loss, major budget variance. Significant impact on budget/finances/eligibility, not recoverable within current or next fiscal year. Significant fraud waste or abuse. Leads to material weakness.	Major embarrassment leading to significant impact on effectiveness. Considerable and prolonged community impact and dissatisfaction publicly expressed Community loss of confidence in the organization's and capabilities (weeks) Consistent negative media attention (weeks) Administrator or Executive Director level intervention	Unacceptable operational impact, short term business interruption. Continued capability of the organization is threatened. Full business disruption for up to one week or a key service up to two weeks. One or more critical programs, projects, or agency priorities cannot be achieved	Reportable compliance infraction. Major breach of regulations. Major litigation.	Non critical infrastructure assets are destroyed. Significant or critical infrastructure assets are unusable or restricted for weeks.	Impact requires significant long term management and organizational resources to respond.	Medium to long term impact to the the human and natural environment. The impact covers a wide area but can be contained. Able to be remediated but will require dedicated expert resources.	Fatalities or permanent disabilities.	Long-term impact on the protected rights, intended benefits, or ability to implement effective nondiscrimination programs. Numerous and continuous complaints in multiple program areas that cannot be addressed timely.	Significant economic disruption to a major metropolitan area or entire State
Moderate	Significant financial loss and variance to budget. Major impact on budget/finances/eligibility, may be recoverable within current year, but requires reprioritization. Limited instances fraud waste or abuse. Leads to several audit findings.	Moderate embarrassment impacting short term effectiveness. Community impact and concerns publicly expressed (days) Negative media attention (days) Loss of confidence by the community in organization processes Administrator or Executive Director level concern	Moderate operational impact, business not interrupted. Effectiveness and efficiency of major elements of the organization are reduced. Full business disruption for one day or a key service disruption up to one week. Ability to achieve one or more critical programs, projects, or agency priorities is reduced.	Significant compliance infraction. Serious incident requires investigation and legal representation to determine legal liability. Non compliance with regulation.	Some assets, not including significant or critical assets, are unusable or restricted for weeks.	Impact requires management and resources from a key area of the organization to respond.	Medium term impact to the the human and natural environment. Limited to a small area. Able to be remediated but will require intervention or management by external parties.	Injuries requiring medical treatment with possible fatalities.	Impact results in noncompliance affecting protected rights or intended benefits. Issues are addressed, but over unreasonably long period of time. Numerous complaints in one or more program areas.	Some economic disruption to a metropolitan area or portion of a State; impacts may or may not be long lasting
Minor	Minor financial loss, small budget variance. Slight but noticeable impact on budget/finances/eligibility, recoverable within year. Minor instances of fraud waste or abuse. Leads to audit findings.	Minor embarrassment, but no harm to image or reputation. Local community impact and concerns Occasional or once off negative media attention	Minor operational impact, business not interrupted. Effectiveness and efficiency elements of the organization are reduced, Partial business disruption for less than three days. Opportunity or ability to achieve objectives or deliver outcomes is affected.	Minor compliance infraction. Complex legal issue to be addressed.	A number of assets are unusable or restricted but can be replaced within an acceptable timeframe.	Impact requires additional local management effort and redirection of resources to respond.	Short term impact to the the human and natural environment. Able to be remediated through existing processes. Minimal threat to flora, fauna, and or cultural heritage	Injuries requiring medical treatment.	Minor impact on protected rights or intended benefits with isolated lawsuits and/or complaints that do not involve cross-cutting program issues.	Some economic disruption to a metropolitan area or portion of a State, but effects are both manageable and short term
Insignificant or Neutral	Minimal impact on budget/finances/eligibility. Recoverable within current year. Some waste or abuse. Leads to immaterial audit findings.	Isolated local community or individual issue-based concerns	Negligible impact on the effectiveness of the organization. Isolated or short term business service disruption.	Legal issues managed by routine procedures.	Assets receive minimal damage or are only temporarily unavailable or restricted.	Impact can be managed through routine activities.	No measurable impact to the the human and natural environment. No action required for management or containment. No impact to flora, fauna, and or cultural heritage.	Incident with or without minor injury.	No measureable impact to protected rights or intended benefits of individuals.	Some localized, short-term economic disruption

Heat Map

	Likelihood	Unlikely	Possible	Likely	Almost Certain
Impact	Description	The event could possibly occur, but is unlikely at this time.	The event could occur under specific conditions and some of those conditions are currently evidenced.	The event is most likely to occur in most circumstances.	The event is expected to occur in most circumstances or is happening now.
Catastrophic	Large unacceptable financial loss, severe budget variance. Very significant harm to image with substantial impact on effectiveness. Large and unacceptable operational impact, long term business interruption. Qualified audit finding.				
Major	Very significant financial loss, major budget variance. Major embarrassment leading to significant impact on effectiveness. Unacceptable operational impact, short term business interruption. Leads to material weakness.				
Moderate	Significant financial loss and variance to budget. Moderate embarrassment impacting short term effectiveness. Moderate operational impact, business not interrupted.Leads to reportable findngs.				
Minor	Minor financial loss, small budget variance. Minor embarrassment, but no harm to image or reputation. Minor operational impact, business not interrupted. Leads to audit findings.				
Insigificant or Neutral	Minimal or no measurable operational impact. Can be managed with routine activities. Leads to immaterial audit findings.				
	How to use this Tool: Assess your risk for levels of impact and likelihood. Find where the two values intersect. Use this intersection value to sort your risks and help with risk prioritization. Use your prioritization to help decide which risks require response strategies.				

THE MISSION OF THE LEGISLATIVE AUDITOR GENERAL IS TO

AUDIT · LEAD · ACHIEVE

WE HELP ORGANIZATIONS IMPROVE

olag.utah.gov