State of Oregon

Audit Committee Handbook

This handbook is intended to be a guidance document. It is not a requirement that this document be used by State of Oregon Audit Committees.

Last Update: 6/15/2020

Table of Contents

State of Oregon
Audit Committee Handbook

This handbook is provided to give new and established audit committees background on the internal audit function and provide tools and resources for assisting audit committee members to successfully carry out their role. The handbook was developed by a subcommittee of the Chief Audit Executive Council (CAEC).

The CAEC exists with the intent of sharing information to promote effective internal audit resources within the State of Oregon. CAEC serves in an advisory capacity to the Chief Operating Officer and Director of the Oregon Department of Administrative Services (DAS). The CAEC's charter outlining its mission, objectives, composition, and responsibilities can be found at: https://www.oregon.gov/das/Docs/CAEC-Charter.pdf. DAS is also responsible for coordinating activities of the Internal Audit Function on a statewide level.

I. Why Audit Committees are Important:

A. Oversees an agency's internal audit function.

B. Plays a key role, standing at the intersection of management, independent auditors, internal auditors, and the Commission, Board or Executive Committee/Leadership of the organization.

C. Helps ensure the effectiveness of governance, risk management, internal control, and compliance processes over strategic, financial, operations, and compliance objectives.

D. Helps support the independence of the internal audit function.

II. Audit Committee Composition:

A. Audit Committee Membership

Composition of the committee is critical to its proper function.

The following is from an Institute of Internal Auditors' (IIA) 2014 paper on audit committees (emphasis added):

> *The key to an audit committee's effectiveness is having members with an appropriate mix of skills and experience relevant to the organization's responsibilities. The ideal composition of the audit committee and attributes of its members depends on a variety of factors such as the organization's size, complexity, and responsibilities.* [1]

Independent members are those who represent the public interest. Independence is an agency reporting relationship as well as a frame of mind and a matter of

[1] https://na.theiia.org/standards-guidance/Public%20Documents/Independent-Audit-Committees-in-Public-Sector-Organizations.pdf

perceived appearance. A committee member who has a mind-set of independence but is a member of the agency may not be accepted by the general public as independent. Therefore, as leading practices advise, both DAS and the CAEC strongly recommend having as many committee members that are external to the agency as possible. Furthermore, agencies should consider having an external member act as chair of the committee or at least someone with which the CAE does not have a reporting relationship.

As a further aid to accountability and transparency, external committee members should consider meeting regularly in a confidential session with the internal auditor without management of the agency present. Additionally, members should not have recently worked for the agency. Members should be cognizant of and disclose personal and professional relationships with management or the members of the internal audit function that may appear to hinder independence and objectivity.

Oregon Administrative Rule (OAR) 125-700-0135 provides the framework for audit committees with this section:

(5) Each agency required to have an internal audit function shall establish and maintain an audit committee.

> (a) The role and function of the audit committee shall be stated in a formal, written charter that describes the authority, responsibilities, and structure of the audit committee. The charter must be approved and periodically reviewed by the audit committee and governing board (or agency head in the absence of a governing board).
>
> (b) The primary purpose of the audit committee is to enhance the quality and independence of the audit function, thereby helping ensure the integrity of the internal audit process.
>
> (c) If the agency has a governing board or commission, the audit committee must include one or more board or commission members. If there is no board or commission, agencies are encouraged to include qualified individuals from outside the agency on the audit committee, to enhance public accountability and transparency, and increase independence of the internal audit activity.

Following the requirements in this OAR provision is a very critical component in making an audit committee a meaningful body that can carry out its intended purpose.

B. Audit committee members should have knowledge and understanding of the regulatory environment and industry the agency operates in. At least one member should have some experience as a public accountant, auditor, principal financial officer, comptroller or IT professional. All audit committee members should

understand the importance of internal controls as well as the roles and responsibilities of the audit committee.

III. Roles and Responsibilities of the Audit Committee

The purpose of the audit committee is to assist agency management in carrying out its oversight responsibilities.

A. Oversight of the Internal Audit Function

One of the key responsibilities of the audit committee is to oversee the internal audit function. The audit committee should ensure that the internal audit function has adequate staffing and resources to perform its duties. The committee should also ensure that the Internal Audit structure has adequate independence to the operations of the agency. This is achieved by setting up a structure in which Internal Audit reports functionally (and has direct access) to the audit committee. For administrative purposes, the internal audit function should report to executive management, preferably, the agency head. As part of this reporting structure, the audit committee should approve (or at a minimum, be consulted with) oversight of the Chief Audit Executive, including evaluating, hiring, and terminating.

B. Governance

The audit committee is in a critical position to help ensure management is accountable for reducing the risks that may impede an agency from meeting its mission. Key areas of governance that the audit committee may focus on include:

- Ethics (including tone at the top)
- Enterprise risk management
- Internal control and compliance
- Operational effectiveness and efficiency
- Information Security

Audits, both internal and external, assist the audit committee by providing independent assurance that these areas are appropriately addressed by management.

1. Ethics

Ethics can be defined as: *the application of a moral code of conduct to the strategic and operational management of an agency.* The internal audit function should evaluate the design, implementation, and effectiveness of ethics-related objectives, programs, and activities and report these results back to the committee.

The committee should also consider how ethical issues are reported. Is there a safe method for employees to report potential ethical violations, such as a hotline? Is the Secretary of State's Fraud, Waste, and Abuse hotline advertised to staff and the public at agency locations?

This evaluation will give audit committees an understanding of how ethics are communicated and practiced. It should ensure that the agency has a code of conduct and/or ethics policy. It should also consider how these policies are communicated and practiced. For instance, is there regular ethics/code of conduct training or are employees just required to sign the policy when they start working for the agency without any further training or discussion on the topic?

2. Risk Management (strategic, operational, reporting & compliance)
   The internal audit function should evaluate management's enterprise risk management process and report to the audit committee to provide assurance whether management is strategically considering risks as they manage operations. Committees should ensure that the risk management process is comprehensive and ongoing, rather than partial and periodic. The audit committee should understand the risks of the agency in order to have a more meaningful discussion with management to ensure they are not accepting too high a level of risks without a mitigation strategy.

   It should be noted that while the internal audit function is an important part of this process, risk management is the responsibility of management. The annual risk assessment conducted by the internal audit function for the purpose of identifying high risk topics to include on the audit plan may not be sufficient to be considered the agency's only process of identifying risks.

3. Internal Control and Compliance
   The audit committee should seek assurance that management has effectively implemented policies and procedures to ensure management directives are carried out and comply with applicable rules and regulations. They include a range of activities as diverse as: approvals, authorizations, verifications, reconciliations, review of operating performance, security of assets and segregation of duties. Audits are performed to provide an independent assessment of controls to ensure they are effective.

4. Operational Effectiveness and Efficiency
   The audit committee should keep in mind that one important aspect when evaluating a program is effectiveness. Is it accomplishing what it is supposed to do? Also important to consider is how efficient are the operations; are there opportunities for streamlining processes while not compromising internal controls? Efficiency and internal controls can often be a balancing act for management. Internal audit plays an important role in evaluating operational effectiveness and efficiency, and reporting the results to management and the audit committee.

IV. Internal Audit Function Oversight

As part of the oversight of the internal audit function, the audit committee should periodically review and approve key documents and reports. These can include:

Document to Review	What to Look For
Audit Committee Charter	• Does the audit committee charter follow best practices? • Does the audit committee include qualified members who are not part of the agency?
Internal Audit (IA) Charter	• Does the IA charter follow best practices? • Is adequate independence given to the internal audit function?
Annual Risk Assessment	• Does the risk assessment cover all areas of the agency? • Was an appropriate methodology used by the internal audit function that included input from management, key external stakeholders and the committee?
Audit Plan	• Does the audit plan adequately address the risks identified in the risk assessment? • Will internal audits be focusing on the highest risk areas of the agency? • Is the plan realistic given the amount of audit resources? • Is there a need to outsource some audit topics?
Audit Reports (Internal or External)	• Does the audit report include the objectives of the audit, and if so, were those objectives met? • Does the audit clearly outline the issues found and make recommendations for management to address them? • Is management's response included with the report? Are the responses adequate in that they will address the issues identified timely?
Follow-up on prior audit recommendations	• Has management implemented the recommendations outlined in the previous report?
Annual Report to DAS	• Does the report accurately reflect the internal audit function activity for the year? • Is the report in compliance with policies/procedures, IA OAR and ORS?
Performance Metrics	• Is the internal audit function measuring and reporting on information that helps the audit committee gauge the internal audit function's

Document to Review	What to Look For
	success, efficiency and effectiveness of work performed? • Is there action the audit committee should take to improve the internal audit function's performance?
Quality Assurance and Improvement Program	
External Quality Assurance Reviews (Peer reviews)	• Does the internal audit function section generally conform to standards? • What areas are needed for improvement? • Does the CAE have a plan to address the areas for improvement?
Internal Quality Assurance Programs	• Does the internal audit function section have an internal quality assurance improvement program that includes both periodic and continuous reviews? • Does the internal audit function section report the results to the audit committee? • Does the internal audit function section identify areas needing improvement as well as timelines for implementation?

A. Internal Audit Reports
In order to assist the audit committee in fulfilling their governance role, the internal audit function should report out on their assurance activities. These reports should address:

- Risks that could hamper the achievement of strategic and operational objectives
- Fraud risks
- Internal controls and the safeguarding of assets
- Compliance with laws, rules, regulations, policies, and contracts
- Evaluation of policies and practices
- Opportunities for operational efficiencies

Reports should include responses from management, which identify how they intend to address the recommendation or risk identified. The audit committee should help ensure that management is appropriately addressing the issue and is not accepting a level of risk that is too high.

B. Involvement in External Audit Activities
Many agencies are frequently audited by external parties, such as the Secretary of State Audits Division and various federal government agencies. If an agency chooses

to hire a firm to perform an audit or review, the audit committee should be involved in the hiring and selection process.

The audit committee should receive and review reports from external audits just like internal audits. External audit reports, much like internal reports discussed above, often include recommendations. The audit committee should ensure that management has appropriately responded to the recommendations in the report, as well as provided follow up information when requested by internal audit.

V. Types of Audits

A. Financial Audits

Financial audits are performed to express an opinion as to whether the financial statements are presented accurately in accordance with accounting principles. The purpose of this type of audit is to enhance the degree of confidence of intended users in the financial statements. Most agencies do not produce their own financial statements. Financial information is combined with other state agencies and appears in the state's Comprehensive Annual Financial Report (CAFR) which is produced by DAS. Other agencies, such as Lottery, PERS, and the Oregon University Systems, produce their own financial statements. In these audits, auditors will review the entire financial statements, notes, and schedules.

The Secretary of State Audits Division is the constitutional auditor of public accounts and is responsible for performing the financial audits for state agencies. In some cases, the Audits Division may contract with a CPA firm to conduct the audit on their behalf. Additionally, federally funded programs may be audited for compliance with regulations and appropriate management of grant funds.

Significant audit findings relating to financial reporting and federal compliance are published in the state's Statewide Single Audit Report. Audit Committees should be familiar with how their agency's financial information is reported, either through a stand-alone financial statement or how it is included in the state's report.

B. Performance or Operational Audits

Performance audits identify improvements an agency or program can apply to better achieve its objectives and mission. These audits may be performed by internal or external auditors. Recommendations may be directed at improving management practices and procedures to increase efficiencies, generate savings, and produce better results. The scope of the audit may include the following:

- Program effectiveness (Is a program achieving its goals and objectives in the most efficient manner?)
- Internal control (Are controls sufficient to achieve goals and objectives?)

In financial audits, auditors use standard procedures and rely on accounting principles to determine the audit objectives. In contrast, performance audits are research-based, and often require the auditor to determine the criteria against which a program will be

evaluated. These audits apply a variety of methodologies beyond accounting procedures.

C. Information Technology Audits
Information technology (IT) audits are a subset of performance audits. They are designed to determine whether computer systems adequately protect public funds and electronic information, and whether they operate as intended. Recommendations are directed at improving electronic information security, practices and procedures. There are two broad categories of IT audits: general control reviews and application control reviews. General control reviews relate to the overall information processing environment and has a large effect on the organization's computer operations. Application controls apply to the processing of individual accounting applications and help ensure the completeness and accuracy of transaction processing, authorization, and validity.

Types of general controls include:
- IT Governance Controls
- Data Center Physical Security Controls
- Change Management Controls
- System and Data Backup and Recovery Controls
- Computer Operation Controls
- System Development Life Cycle Controls
- Logical Access Controls over Infrastructure and Data

Types of application controls include:
- Data Capture Controls
- Data Validation Controls
- Processing Controls
- Output Controls
- Error Controls

D. Compliance Audits (often performed in conjunction with other performance audit objectives)
Compliance audits determine whether a program is in compliance with a specific law, rule, policy, or other guidance in conducting its operational and administrative programs.

E. Investigations
Investigations may be performed if there are allegations of fraud, waste, or abuse. The goal of the investigation is to determine if the allegations are supported. These types of investigations are generally performed by the Secretary of State Audits Division and/or Oregon State Police. Internal audit may be involved to help coordinate an investigation and recommend control improvements as necessary. The audit committee should be aware of these investigations and ensure that corrective action is

taken. Auditors who perform or take on roles related to an investigation should ensure they have the proper training to perform these duties.

F. A single audit can include multiple types of audits as described above. The scope of the audit work to be performed is usually determined in the planning phase of the audit; though in some cases it may be necessary to make changes to an audit scope as work is performed, which should be communicated with the auditee.

VI. Additional Considerations

a. Single-person functions: Audit committees of one-person shops should be aware of some anomalies created from such a situation. Auditors may face, and need support in:
   - Meeting professionally recognized standards.
   - Completing the annual audit plan due to emerging priorities and time limitations.
   - Balancing administrative functions and consulting engagements when there is limited audit time available.

b. Contracted functions: Audit committees with oversight over contracted internal audit services should be aware of some anomalies created from such a situation:
   - Auditors may be unfamiliar with details of business – focus may be on internal controls and compliance audits instead of programmatic audits.
   - Management may not be comfortable discussing issues with hired auditors.
   - Auditors may lack understanding of government functions.
   - Auditors may be unable to perform additional work outside of original contract scope without amendment process.
   - Consulting services may be limited.

VII. Best Practices

The following list are things for audit committee members to consider and discuss with the agency to help support the internal audit function and ensure it is adding value to its fullest capacity.

a. <u>Seat at the Table</u>
   It is important that the CAE be integrated with the leadership team of the organization. This can be accomplished by having the CAE attend executive team meetings, strategic planning meetings, leadership meetings, or board / commission meetings. The CAE should utilize opportunities to develop rapport with management, strategic understanding, and insight where possible into risk factors.

b. <u>Meet with CAE, External Auditor, Agency Director/CFO</u>
   1. External Auditor – The CAE should meet regularly with external auditors and report back to the audit committee the scope, findings, and recommendations from external auditor engagements. The CAE should act as a liaison between the external function and agency management. This relationship allows the CAE to be aware of potential risk areas within the agency for future planning

and can ensure external auditors are connected with appropriate parties to complete their audit objectives.

2. Agency Director – The CAE and the agency director should meet on a regular basis regardless of the administrative reporting relationship. It is important that the CAE and the director both understand that part of the mission of internal auditing is to provide advice to management. The CAE and the Director should have a working relationship and communicate frequently.

c. Strategic Plan and Performance Measures

The audit committee should review and approve the strategic plan and performance measures of the internal audit function. It is one of the core principles of internal audit to demonstrate quality and continuous improvement. Performance measures established for the internal audit function help to ensure that the function is performing adequately.

d. Confidential sessions as needed

It is important that the CAE feel comfortable calling confidential sessions with the audit committee chair and/or external audit committee members without the presence of management. External members should also be able to meet alone with management or the person the CAE reports to.

e. Participation in Statewide Internal Audit Community

The CAE should be encouraged and provide time on the audit plan to participate in the statewide internal audit community. The Chief Audit Executive Council and the local chapter of The Institute of Internal Auditors both have opportunities for networking, training, and participation in statewide policymaking and initiatives.

f. Consistency with Statewide Internal Audit Practices

The CAE should connect with DAS's statewide internal audit coordinator and the CAEC leadership to connect with resources such as mentorship programs and statewide guidance including handbooks, policies, and training.

g. QAIP and QAR

As part of meeting internal audit standards, audit shops must have a quality assurance and improvement program (QAIP) and well as undergo regular Quality Assurance Reviews (QAR). As part of DAS's statewide coordination, if internal auditors from an agency participate in 2 review teams, then a team of auditors from other state agencies will conduct the QAR when the agency is due (every 5 years for redbook standards). Participation in this reciprocal program takes significant time on audit plans. Audit committees should understand the requirements and benefits of these program and support internal audit resources toward quality assurance efforts and participation. Agencies and the audit committee can also choose to contract for a QAR.

h. Audit Committee Composition – External Membership

Some state agencies and internal audit shops are able to support completely external audit committees. This model provides the highest level of independence from management and has many benefits such as transparency, community participation, and direct governance. Agencies with governing commission or board are more likely to be able to incorporate this model. There are special considerations when the CAE reports functionally to an external audit committee

or if an audit committee is a subcommittee of a commission or board. Agencies should reach out to other state agencies with external audit committees to learn more about special considerations. Currently, PERS, Lottery and the Oregon Parks and Recreation Department have fully external audit committees.

VIII. Audit Committee Resources

a. Internal Audit Jumpstart materials: https://www.oregon.gov/das/Pages/audit-jumpstart.aspx
b. The Institute of Internal Auditors: Public Sector guidance: https://na.theiia.org/standards-guidance/leading-practices/Pages/Public-Sector.aspx

Appendix I – Potential Questions for the Audit Committee

1. What keeps you up at night?
2. What risks are over the horizon?
3. What risks are not assessed?
4. What processes are not assured?
5. What is your business model?
6. Are your Governance, Risk Management, and Compliance (GRC) structures robust enough to support your strategy?
7. How do you gain assurance that roles and responsibilities are appropriately articulated and understood throughout the organization?
8. What charters, committees, and advisory councils are in place?
9. How is accountability assured?
10. How do you gain assurance that rank and file staff trust the message and the messenger regarding the ethical climate of the institution?
11. What are the metrics for fraud and ethics incidents?
12. How robust is the ethics training?
13. How do you gain assurance that transparency and reporting are adequate and appropriate for all stakeholders?
14. Who owns responsibility for stakeholder relations?
15. How do you gain assurance that the risk management process identifies, considers, assesses, and manages all strategic, operational, reporting, and compliance risks?
16. Who owns risk management in your enterprise?
17. How do you gain assurance that monitoring and communication activities are sufficiently robust?
18. How do you gain assurance that your internal audit function is compliant with Standards and has appropriate competencies and capacity?
19. How do you gain assurance that all employees, contractors, consultants, suppliers, and vendors understand your vision, values, strategic direction, and the importance of GRC?

Questions for your Chief Audit Executive

1. What is the criteria for establishing the annual and long-range audit plan?
2. What assurance do you have that you are in compliance with Standards?
3. Does your risk assessment include all known risks to the organization?
4. How do you prioritize IA efforts?
5. Are there areas of high priority where IA work has been deferred?
6. What is the level of respect internally for IA?
7. What are management's practices for responding to IA reports?
8. Who in management has reviewed the risk assessment?
9. What risk factors do you consider in developing the audit plan?
10. How will you provide assurance for governance processes?
11. Has IA identified areas of serious concern relative to the corporate internal control environment?
12. Are there other matters that you believe should be of concern to the committee?

13. Putting yourself in the audit committee's position, are there questions you believe we should ask?
14. What processes are not being assured this year due to resource constraints?
15. What processes have never been assured?
16. What are your risk-assessment and risk-based auditing methodologies?
17. What professional certifications do you and the staff hold, e.g. CPA, CIA, CISA?
18. What are the metrics to ensure the audit processes meet objectives?
19. How much resource and time does it take to publish a final audit report?
20. What is the process to follow with management to complete actions to resolve residual risk?
21. How do you track and report aged open actions?
22. Do you believe that management is taking risk beyond their delegation levels or in excess of the organization's risk appetite?

Appendix II– Glossary[2]

a. Audit: An objective examination of evidence for the purpose of providing an independent assessment on risk management, control, or governance processes for the organization. Examples may include:
   - Financial
   - Performance/Operational
   - Compliance
   - Systems Security
   - Information Technology
   - Due Diligence Assurance Engagements

b. Auditee: The subsidiary, business unit, department, group, or other established subdivision of an organization that is subject to an assurance engagement (audit).

c. Audit Committee: A committee that provides oversight of auditing and internal control for the agency and helps ensure the independence of the internal audit function. The purpose of the audit committee is to assist agency management in carrying out its oversight responsibilities.

d. Audit Customer: The unit/management seeking services in a consulting engagement.

e. Enterprise Risk Management: A process affected by an entity's board of directors, management, and other personnel, applied in a strategy setting across the enterprise. The process is designed to identify potential events that may affect the entity, manage risks to be within its risk appetite, and provide reasonable assurance regarding the achievement of entity objectives.

f. Governance: The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

g. Internal Auditing: An independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management control, and governance processes.

[2] Definitions provided by multiple sources including, but not limited to, the IIA International Professional Practices Framework (the Red Book) https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Standards-Glossary.aspx.

.

h. Internal Audit Function (Activity): A department, division, team of consultants, or other practitioner(s) that provides independent, objective assurance (audit) and consulting services designed to add value and improve an organization's operations.

i. Internal Control: A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of:
   - Effectiveness and efficiency of operations
   - Reliability of financial reporting
   - Compliance with applicable laws/regulations

j. Opportunity: The possibility that an event will occur and positively affect the achievement of objectives.

k. Risk: The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact (the effect) and likelihood (the probability the event will occur).

l. Risk Assessment: The identification and analysis (typically in terms of impact and likelihood) of relevant risks to the achievement of an organization's objectives, forming a basis for determining how the risks should be managed.

m. Tone at the Top: The entity-wide attitude of integrity and control consciousness, as exhibited by the most senior executives of an organization.

n. Audit User: A party who relies on the internal auditor's assessment of evidence and conclusion (aka Stakeholder).

o. Description of Internal Audit Services

	Assurance (Audit)	Consulting
Purpose	Assess evidence relevant to subject matter of interest to someone and provide conclusions regarding the subject matter.	Provide advice and other assistance, generally at the specific request of engagement customers.
Who Determines Nature and Scope	The internal audit function.	Mutually agreed upon between customer and internal audit function.
Parties Involved	Auditee, Internal Auditor, and User	Customer and Internal Auditor