|  |
| --- |
|  |
| State of Oregon: Internal Audit |
| Risk Assessment Guidance |
|  |

Last Update: April 24, 2014

Table of Contents

I. Introduction 3

II. Enterprise Risk Management (ERM) vs. Risk Assessment 3

III. Identifying the Universe 4

IV. Identifying Risks 4

V. Risk Scoring Methodology 6

VI. Audit Plan Development 7

VII. Reporting 8

VIII. Tools 9

IX. Definitions 9

X. Tool 1 – Risk Assessment by Categories 12

XI. Tool 2 – Risk Assessment by Objectives 17

XII. Tool 3 – Fundamentals Management Map 21

XIII. Tool 4 – Tie-Breaker Questions 22

XIV. Tool 5 – Audit Committee Audit Planning Topic Selection Template 24

XV. Tool 6 – Risk Assessment Summary 25

1. Introduction

This document is designed to provide practical guidance as well as tools and templates for state agencies to use in creating annual internal audit plans based on risk. A risk assessment and audit plan provides a basis to identify areas that may benefit from an internal audit, and allows limited audit resources to be directed toward higher risk areas (with potential more value-add from an audit) thereby maximizing the value of the internal audit function to the agency.

Risk may be viewed through many lenses. For the purposes of this effort, risk is an attribute associated with establishing a goal or objective. That is, once you establish a goal or objective, conditions may exist or events may occur that keep you from achieving that goal or objective. While risk cannot be completely eliminated, it is important to determine whether risk can be cost-effectively mitigated (consider cost/benefit, i.e. don’t implement a $10 control for a $1 risk) and evaluate the relationship between residual risk and the benefits to be realized from achieving the goal or objective (is the reward worth the risk).

Risk and the perception of risk are not static; they are constantly changing. A risk assessment may represent a snapshot in time –or single snapshots of many different areas taken over a certain time period. As new issues emerge, state and federal laws change, technology progresses, and new information becomes available, actual and perceived risk may change.

Inherent risk is the overall amount of risks to completing the objective; residual risk is what remains after controls are applied. Typically risk assessments are performed at the inherent risk level, and audits are conducted to determine what controls have been implemented and whether they are adequate or operating as intended. However, an alternative method is to identify controls in place to mitigate risks so the risk assessment can be completed at the residual risk level. The audit can be performed to determine effectiveness and adequacy of those controls.

There are inherent risks to performing, documenting, and presenting results of a risk assessment that organizations should be aware of. The agency could face public perception risks and impacts if it becomes known that they were aware of a risk but didn’t do anything about it.

1. Enterprise Risk Management (ERM) vs. Risk Assessment

ERM is a systematic process which should occur throughout all functional levels of an organization to continually identify, evaluate and effectively manage real or perceived barriers to the achievement of the organization’s strategic objectives.

Risk assessment is a component of risk management – the process of identifying and assessing by impact and probability factors, those potential events which could inhibit the organization’s ability to meet its objectives.

ERM is the responsibility of Management, and should include a risk assessment process, but go beyond identifying and assessing risks, to selecting a strategy for dealing with identified risks (accept, avoid, mitigate or share) and monitoring the effects of the strategies put in place.

Internal Auditors in state agencies are required to perform risk assessments[[1]](#footnote-1). These assessments may be used for audit planning purposes and may also typically encompass the entire organization, to help ensure auditors are dedicating resources to the highest auditable topics on a cycle approved by the audit committee. An auditor should include the results of the organization’s ERM processes in their assessment, and provide input to Management on any additional risks identified through their risk assessment process.

1. Identifying the Universe

One of the first steps in a risk assessment is to identify the potential audit areas, or audit universe. Varied approaches may be used to do this. Examples of types of documents that can be used to gather this information include, but are not limited to, an agency’s:

* Strategic and/or Business Plans
* Management/Fundamentals Map
* Budget
* Accounting Structure
* Law/Statutes
* Organizational Chart
* Other Background Information on the Organization (i.e. Legislative Informational Binder; website program descriptions)
* Management
* Previous Risk Assessments/ERM Framework
* Previous Internal and External Audit Reports

Items excluded from the universe and reasons therefore should be documented. The documents listed above may also be helpful in determining the goals and objectives for which risks should be identified and assessed.

1. Identifying Risks

A risk assessment should focus on agency objectives, not possible causes of problems. Specifically, risk is the inverse of a goal or objective for a particular area. For example, if the goal is that “Training meets critical agency needs,” the risk is that “Training does not meet critical agency needs” as oppose to describing all of the events, conditions, or causes that may prevent training from meeting critical agency needs. It is also important to consider at some point the collective risks of a given area. In many instances, goals or objectives may need to be balanced against each other rather than maximizing or minimizing each individually.

Varying methods may be employed for identifying risks to an agency’s objectives. Examples of methods to employ include but are not limited to:

* Individual meetings with Executive Team members, Managers, and other Stakeholders
* An Electronic Survey
* Attending Management Team Meetings across the organization

The process for identifying risks must be documented. Several factors need to be considered, including: anonymity of information received, whether voting software could be utilized, how frequently a full-risk assessment should be conducted or whether a previous one could use an ‘update.’

When identifying risks, internal auditors should consider the following categories of agency operations:

* Strategic/Governance (Organizational)
* Reporting
* Financial
* Operational
* Legal and Compliance Requirements
* Information Technology and Security
* Potential for Fraud, Waste, Abuse and Other Irregularities
* Public or Political Sensitivity (Reputation)
* Customers

Additionally, some Oregon Laws, Administrative Rules and Policies contain ‘mandated audits’ for internal auditors – topic areas which require periodic review by an independent party within the organization. The majority of these mandates are in the process of being removed; however it is important to ensure these high-visibility topics receive adequate consideration during the risk assessment process. In addition to gathering information directly from personnel, some of the following risk factors should be considered independently:

* Whether the organization has implemented a SPOTS (visa card) system (OAM 55.30.00 105.a);
* Whether the organization has a Performance Management program in place, or reports Key Performance Measures (OAR 125-700-0140 1c) and give consideration to integrity or accuracy and adequacy;
* Whether the organization has an employee recognition program in place (DAS Statewide Policy 50.040.01 c);
* Whether the organization provides employee leased housing (OAR 125-040-0000 5 a, b) ;
* Whether the organization has executed a Delegated Authority Agreement with the State Procurement Office at DAS; and
* An assessment of Information Security implementations within the organization (Information Security Plan for the State of Oregon, DAS EISPD) including security policies, plans, processes, procedures and systems.

Results of risk identification work should be documented and appropriately safeguarded. If risk information is taken out of context, a reader could potentially misinterpret a ‘risk’ as something actually happening within an organization. It is important that risk information be shared with Management in a safe environment with the appropriate contextual information. Most Internal Audit functions consider risk assessment information a data classification level 3[[2]](#footnote-2) – Restricted. It may be summarized for more public distribution in a document such as Tool 6 as provided and classified a level 2 – Limited.

1. Risk Scoring Methodology

The Auditor, with input from Management, should develop criteria by which to factor in to calculating a risk score (i.e. things that would impact the impact of the risk to the organization and probability of it occurring). Examples of such criteria include, but are not limited to:

* Complexity
* Interdependence
* Volatility
* Sensitivity
* Visibility of results
* Agency confidence in successfully mitigating the risk
* Subjectivity of that confidence

Weight factors should be assigned risk scores, which can be quantitative (numbers from 1-5 or 1-10) or qualitative (high, moderate, low) or a combination of both (a risk can be categorized as low and given a numerical score between 1 and 3.) the auditor can consider limits to factors so that, for instance, no more than 3% of risks could be classified as ‘highly sensitive.’ Different criteria can be used to adjust risk scores, depending on their overall value to the agency’s mission/operations. Factors assigned are used to calculate a risk score. The auditor should use a template for documenting these results (Tools are provided) and explain any additional methodology applied to calculate risk scores.

There are several factors to keep in mind when considering the risk score. These include the following:

* Scoring risk is a highly subjective process and requires judgment.
* The score is a reflection of many factors.
* Its primary use is as a relative measure.
* The risk score is not a precise measure; and the scores are not scalar.
* A high risk score does **not** mean that someone is doing something inappropriate.
* A low risk score does not necessarily mean that the associated objective is always achieved.

For each entity, division, program, or business process objective identified in the audit universe, risks should be identified and evaluated upon:

* The potential **impact** on the business objectives;
* The **probability** or **likelihood** of that risk materializing.

Determination of Impact (The effect the occurrence of that risk will have upon the achievement of goals and objectives):

* High or 4-5: The effect will cause the agency to not achieve its goals and/or objectives.
* Medium or 3: the effect will cause the agency to operate inefficiently and/or expend unplanned resources to meet goals and objectives.
* Low or 1-2: There will be no measurable effect upon the achievement of institutional goals and objectives.

Methodology to determine Impact Value:

* Identify consequences to the organization if a risk were to become a reality.
* Value the effect on the organization for each consequence (high, medium, low).
* Assign impact value of an identified risk based upon the value of its highest potential consequence.

Determination of Likelihood or Probability (The chance the risk will occur):

* High or 4-5: The risk will become a reality frequently.
* Medium or 3: The risk will become a reality infrequently.
* Low or 1-2: The risk will rarely become a reality.

The combined assessment provides a red, yellow, or green status which indicates whether the risk should be included in the audit plan. The rationale for inclusion or exclusion of risks from the audit plan should be documented on the evaluation summaryas follows:

* Green status (low priority; scores 1-2) – risk not recommended for inclusion in the audit plan, unless a mandatory audit requirement.
* Yellow status (medium priority; score 3) – risk could be considered for inclusion on the plan subject to available resources.
* Red status (high priority; scores 4-5) – risk recommended to be included on plan; if not included for audit coverage the Internal Audit Function should ensure they are communicated to Management for an opportunity to address.

1. Audit Plan[[3]](#footnote-3) Development

Audit plans provide a roadmap for internal auditors to follow in conducting audit activities and help ensure the internal audit function maximizes its value to the organization. Creating annual audit plans based on a risk assessment also ensures that the internal audit function has not limited itself to addressing only fiscal or compliance issues, but has also considered a wide variety of factors to identify efficiency or economy gains for the state agency.

After deriving the final risk score for each individual risk, various statistics may be calculated for each risk area. Reports should be generated for Management and the Audit Committee to consider top risks and risk areas for further exploration. Room should be left in an audit plan for Management requests, even of low risk audit topics, if there is derived value for Management for the time to be spent performing the work. Auditors should document justification for including or removing high and medium auditable risks from the Audit Plan.

See Tools 4 and 5 for example of a questions and a worksheet that can be used to help an Audit Committee, Auditor, or Management Team make a decision prioritizing which high and potentially medium risk areas should be included in an Audit Plan. Tool 5 includes aspects of: availability of audit evidence, the likely existence of a reasonably efficient audit methodology, the level of effort estimated to complete the audit, the volatility of the program or process under audit, the existence of recent independent reviews, and the likelihood that recommendations for improvement or other value would result.

An audit plan should include estimated resources needed to complete the plan compared to available internal audit staff. This information can help an Audit Committee determine if the internal audit function is ‘right-sized’ for the level of assurance they desire to the assessed risks of the organization. In assigning resources to planned audit activities, time should be reserved for sick and vacation leaves, training, reasonable participation in other agency activities/committees, and time to respond to agency questions and non-formal consulting activities, as applicable.

Audit plans should not be considered ‘set in stone’ and the internal audit function should be free to amend plans in response to change in the organization or when new information surfaces. Amendments should be vetted through the Audit Committee. The level of risk of proposed changes should be used in the decision process to change the audit plan (i.e. be cautious of removing high risk audit topics and replacing them with too many low risk ones).

1. Reporting

Results of the risk assessment should be summarized and reported to appropriate parties, which may include: the agency’s Management team, the Audit Committee, Board or Commission, the Department of Administrative Services and the Oregon Audits Division (Secretary of State.) The amount of detail included should be determined based on the audience the report is intended for. Auditors should also determine a method for reporting to Management and the Audit Committee on high risks that will not be covered by the annual audit plan. Tool 6 has been provided as a template for this type of report.

1. Tools

The tools provided each approach doing a risk assessment in slightly different ways. There is no right or wrong way to do a risk assessment. Choose a tool or tools that work best for you and your organization.

1. **Risk Assessment by Categories:** This is a risk assessment **documentation** tool. It documents different types of risks for each business objective or organizational unit identified. It ranks the sum of the risks on a 1-10 scale, which can be modified to fit the agency needs. Risk categories could be modified to fit an organization’s needs (for example, only assess by COSO Categories – Strategic, Reporting, Operational and Compliance.) This tool includes a **Risk Rating Guide** whichcan help the auditor and other risk rankers make decisions on high, medium, and low risks based on the factors presented.
2. **Risk Assessment by Business Objectives:** This is a risk assessment **documentation** tool. It addresses risk, assessment, and audit plan information per business/process objective reviewed. It includes a High, Medium, Low matrix.
3. **Fundamentals Management Map:** This is a risk assessment **presentation** tool for agencies who have utilized the NOW Fundamentals Management Map in their Strategic Planning or Governance processes. This tool aligns risk with Core Processes.
4. **Tie-Breaker Questions:** This is a **second-tier** tool which can be utilized in the event you have two or more high or medium risk areas or audit topics that you are trying to prioritize between. Not every question needs to be asked; use your judgment as to which answers will best help you or your Management team or Audit Committee make a decision in each case.
5. **Audit Committee Audit Planning Topic Selection Template:** This tool can be used with an Audit Committee, Management Team, or even Audit group to assess and prioritize several audit topics, or to help make decisions on where to spend limited internal audit resources.
6. **Risk Assessment Summary:** This is a mandatory reporting tool required to present the results of the annual risk assessment and audit planning process to the Department of Administrative Services and is included in the annual reporting database. Many agencies also use this reporting template for the submission required to the Secretary of State, Division of Audits.

Most of these tools have been adapted from Rick Wright’s book “The Internal Auditor’s Guide to Risk Assessment.” The NOW Management Map was adapted from the Fundamentals Map created by Mass Ingenuity.

1. Definitions
   1. 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 include financial, performance, compliance, systems security and due diligence assurance engagements.
   2. Risk: The possibility of an event occurring that will have an impact on the achievement of an agency’s mission, goals, or objectives.
   3. Inherent risk: the risk that an activity would pose if no controls or other mitigating factors were in place.
   4. Residual risk: the risk that remains after controls are taken into account, or the net risk after controls and/or other mitigating factors are considered.
   5. Risk category: A specific type or class of risk.
   6. Impact (or consequence): the extent to which a risk event might affect the enterprise.
   7. Likelihood (or probability): the possibility of a given event, or consequence, will occur.
   8. **Levels of Risk**
      1. Functional-level risk: Risk related to specific functions within an organization and tied to the operational, financial, and compliance categories.
      2. Entity-level risk: Risk that impacts the entire entity and is found in the strategic risk category.
   9. **Risk Categories**
      1. Compliance/regulatory risk: the possibility of an event or condition occurring that influences an organization’s ability to achieve organizational objectives by conforming to value-adding internal policies, guidelines, and commitments; or external requirements of governing bodies.
      2. Control risk: the risk that loss will not be prevented or detected by internal controls. This category assesses the strength of management processes and controls.
      3. Customer risk: risk of loss of customers or negative impact to customers because of business process or decisions.
      4. Financial risk: the risk that is related to the financing operations of an organization, generally concerned with an organization’s cash flows and related transactions.
      5. Fraud risk: the risk of loss due to intentional misappropriation of assets or intentional misstatement of financial reporting.
      6. Information technology risk: risk of loss due to inadequate security, confidentiality, integrity, capability, or availability of systems affecting an organization’s operations, assets customers, shareholders or employees.
      7. Operational risk: the possibility of an event or condition occurring that will influence the ability of an organization to achieve its objectives through the transformation of inputs into outputs (i.e. processes, people, strategies, external events).
      8. Reporting risk: The type of risk the company is exposed to if the internal and external reporting is inaccurate.
      9. Reputation risk: the potential that negative publicity regarding an organization's business practices, whether true or not, will cause a decline in the customer base, costly litigation, or revenue reductions.
      10. Strategic/governance risk: The possibility of an event or condition occurring that will enhance or threaten an organization’s prosperity and existence in the long term.

1. ORS 184.360 requires state internal audit functions to perform an agency-wide risk assessment in conformance with professional auditing standards. The risk assessment must be used as the basis for the selection and performance of one internal audit per calendar year. [↑](#footnote-ref-1)
2. This does not mean the document is exempt from public records disclosure; just that it should be safeguarded from disclosure to unintended parties. [↑](#footnote-ref-2)
3. For purposes of this guidance document, ‘Audit Plan’ means the list of audits planned to be resourced and conducted during the upcoming year. [↑](#footnote-ref-3)