DEFINING AUDIT SCOPE: RISK ASSESSMENT AND PLANNING

Each financial compliance, performance, and information systems audit includes risk assessment and planning procedures. We must adequately plan the work to address audit objectives and reduce audit risk to an acceptably low level. The nature and extent of risk assessment and planning procedures depends on the type of the audit, subject matter, and applicable audit standards. The following discusses risk assessment and planning procedures within the Legislative Audit Division (LAD) for financial compliance, performance and information systems audits.

FINANCIAL AUDIT

For financial audits, the type of financial report issued by the agency plays an important role in risk assessment and planning. In addition to the Legislative Audit Committee (LAC), a wide variety of organizations and individuals rely on the results of both financial statement and schedule audits for decision making. The financial teams consider the information needs of those organizations and individuals during the planning process. Table 1 summarizes the types of financial audits issued and the primary audiences for those reports.

Table 1
Type of Financial Audits and Primary User Audience

Type of Report	Primary User Audience
Financial Statement Audits:	
Annual Comprehensive Financial Report (Statewide Audit)	Municipal securities market (bondholders, rating agencies, underwriters, investors, bond counsel), legislators and informed constituents
Montana State Fund	Governing board, legislators and employers
Board of Housing	Governing board, municipal securities market and Federal Home Loan Mortgage Corporation
Facility Finance Authority	Governing board, municipal securities market, program participants
Public Employee's Retirement Administration and Teachers' Retirement Board, and associated pension schedules	Governing boards, state and local government employers and their auditors
University of Montana Montana State University	Governing board; federal, state and private grantors; donors; and municipal securities market
Board of Investments	Governing board, state agencies and local governments, and municipal securities market
Montana State Lottery	Governing board, legislators
Financial Schedule Audits:	
State Agencies subject to the Legislature's appropriation process	Agency management, legislators, municipal securities market, federal indirect cost negotiators

The following summarizes the primary differences between financial statements and financial schedules audits.

Financial Statement Audits

The Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (Uniform Guidance) require financial reporting in accordance with Generally Accepted Accounting Principles (GAAP). The Governmental Accounting Standards Board (GASB) is the organization responsible for establishing GAAP for governments. Financial statement audits are completed for the state of Montana and each of its component units. The Board of Investments and Montana State Lottery also issue GAAP-based program financial statements in response to statutory requirements for annual audits of their operations.

Financial statements are by nature more complex than financial schedules. While financial statements are prepared from the underlying accounting records, adjustments to present the financial activity in accordance with GAAP, correct errors, and eliminate internal balances for presentation purposes are routine. Audit teams are responsible for assessing risk and planning procedures over the compilation and adjustment process, appropriateness of the financial presentation, and reasonableness of underlying account balances and activity.

Financial Schedule Audits

A financial schedule audit is completed for each agency whose financial activity is appropriated by the legislature. The financial schedule format was adopted by the Legislative Audit Committee in June 1996, with elimination of revenue estimates and property held in trust approved in June 2020. The June 1996 minutes indicate, "The Committee discussed what information they wanted included in the financial schedule format and what basic information was necessary to answer questions of constituents regarding budgets." This format focuses on fund equity, revenues and expenditures. It is considered a regulatory basis special purpose framework, meaning the Legislative Audit Committee selected the format to meet legislator information needs. The financial schedules are not intended to report certain information, such as assets and liabilities, that are reported in the state's Annual Comprehensive Financial Report.

The schedules are prepared from the accounting records without adjustment, so planning and risk assessment procedures are more predominantly focused on the underlying account balances and activity. This allows us to report errors existing in the underlying accounting records that may impact other information used by legislators, such as the Legislative Fiscal Division's budget analysis and fiscal reports.

Materiality in Financial Audits

Materiality is a threshold used to ensure misstatements are detected that will influence the judgement of a reasonable user of the financial statements. Consistent with the auditing standards, our determination of materiality involves professional judgement and is affected by our understanding of the information needs of the user audience. We evaluate each of our audits individually when we establish materiality.

We are required to establish materiality using an opinion unit concept because of the unique nature of governmental financial reporting. Opinion units define the portions of the agency's activity to be addressed through the audit. For a few audits, the opinion unit encompasses the entirety of a financial statement. In most situations, multiple opinion units exist. For example, our audit of the state's Annual Comprehensive Financial Report includes 11 opinion units, such as the General Fund and the State Special Revenue Fund.

For each opinion unit, quantitative materiality is determined by applying a percentage to a baseline. The baseline is intended to align with the opinion unit's primary purpose or most relevant data, such as revenue collection, distribution of funds, accumulation of assets, or fund balance. In planning, we use the most current financial statements or schedules available when making materiality determinations. Professional judgment is required in determining the most appropriate baseline to use. Consistent with our profession, our quantitative materiality percentages generally range between 6 and 10 percent of the baseline.

Qualitative materiality is considered in conjunction with quantitative materiality. This means we consider extenuating circumstances related to an agency's financial activity and consider it material according to importance rather than size. For example, statutorily required transfers may be qualitatively material because of their importance to a recipient agency's ability to administer certain programs.

Quantitative and qualitative materiality determinations are used to identify activity and balances requiring direct testing within each opinion unit. We use a lesser threshold, referred to as performance materiality, to assess risk of material misstatement and determine the nature, timing and extent of our audit procedures. This threshold reduces the probability that misstatements remaining undetected through the audit process will aggregate to a material misstatement.

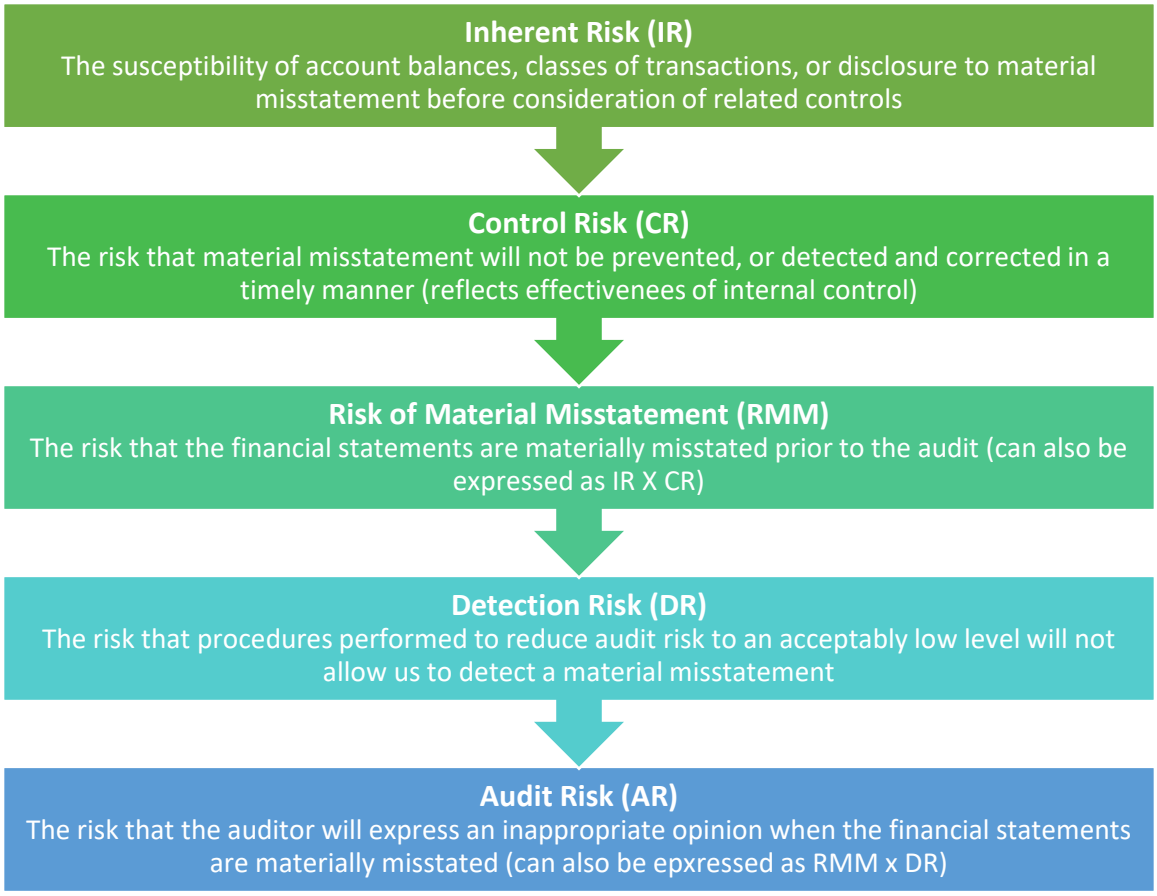
Materiality determinations frequently change in response to an agency's financial activity. Many factors impact baselines and percentages, such as new activity authorized by the legislature or changes in federal funding. We are required to revise materiality as the audit progresses when we encounter new information, such as identifying financial transactions that are missing from the accounting records or the existence of material errors. The materiality determination process specific to our testing of the state's federal financial assistance programs will be discussed in future audit committee hearings.

Risk Assessment Procedures in Financial Audits

Risk assessment procedures also contribute to determining the nature, timing and extent of further audit procedures. Risk assessment procedures include inquiry of management and others, analytical procedures, observation and inspection.

We use this information to assess certain types of risks, summarized in the following table, and identify audit procedures that allow us to achieve low audit risk.

Financial Audit Risk Types



Audit risk is affected by our response to other risk types, specifically control and detection risk. Some procedures, such as comparison between years and review of the financial statements/schedules and associated notes, occur on every audit. Other procedures, such as sampling and data analysis, are designed in response to the agency's inherent risk and effectiveness of their controls. Control risk and detection risk are only reduced through completion of audit procedures. The audit teams also consider fraud risk factors having the potential to result in material misstatements. The AICPA Professional Standards require us to be unpredictable. We expect our audit teams to incorporate new and different approaches in response to the agency's current operations and risk. An audit is an iterative process, meaning we are responsible for modifying our risk assessments and planned procedures when new information and audit evidence is inconsistent with our initial understandings.

As discussed during prior committee education, the AICPA Professional Standards require quality control reviews of certain aspects of audits, such as significant judgments made by the audit team, significant findings or issues, and conclusions supporting the auditor's report. A portion of our quality control review process is completed at the conclusion of audit planning. The Professional Standards also require the engagement partner to take responsibility for the overall quality of the audit; the deputy takes responsibility through discussions with audit teams and review of key planning documents.

PERFORMANCE AUDIT

The Yellowbook indicates that auditors must adequately plan audit work to address audit objectives. Subsequent requirements outline how in planning audit work, auditors must assess risk, with risk defined as the possibility that audit work may not lead to a proper conclusion or the outcome may not be completed or fully supported by the evidence. In an effort to address this consideration of risk for performance audits, section 8.36 of the Yellowbook outlines how auditors must consider several areas and obtain an understanding of the nature and profile and user needs of the program or activity under audit. The Yellowbook indicates that as part of gaining that understanding, it is important to consider the views of users of an audit report, including government officials or other parties who may authorize or request audits.

The Committee's Role In Prioritizing Performance Audits

As referenced in part in state law (§5-13-313, MCA), the Legislative Auditor selects and prioritizes agencies or programs for audit based on risk, considering an agency's or program's financial, operational, and technological risks associated with meeting its intended purpose, goals, objectives, and legal mandates. This section of the law outlines how each odd-numbered year the LAC requests recommendations for agencies and programs from the other branches of government to be considered for an audit during the next biennium. The law provides that this list may be prioritized and must set forth the reasons for being recommended based on risk. Further, this section of the law indicates that the Legislative Auditor reviews this list, including suggestions from legislators and legislative committees, staff recommendations, and any other relevant information and consults with the committee as necessary.

Properly understood, the Legislative Audit Act vests the authority to initiate an audit with the Legislative Auditor, who is required to consider input from multiple sources and then consult with the committee. In practice, the input received by the legislative auditor is subject to prioritization by the LAC every fiscal year. The committee's prioritization process serves as the basis for subsequent decision-making by the Legislative Auditor regarding what and when to audit.

Yellowbook Independence Standards and Audit Prioritization

The Yellowbook doesn't explicitly outline the role of the LAC in the prioritization of performance or information system audits. Rather it outlines how an auditor must consider the views of key users of an audit report as they plan work. While the performance audit standards don't provide a specific basis for the role of the LAC in prioritizing audit work, historically we have approached the involvement of the LAC in a good faith manner, with the annual prioritization process for performance and information system audits structured as a way to engage the committee in a decision of what topics should be considered priorities. It's an effort to obtain input on what topics should be considered a priority, not what topics must be completed. The prioritization process is a way to balance the need for audit staff to maintain their independence but also consider the views and needs of one of the key users of audit reports, namely the LAC and the broader legislative body.

Once the LAC has prioritized a topic for a potential examination, LAD staff continue to assess the risks to the program or activity as part of a continued planning process and base any decision to move forward with an audit on an assessment of risk. Subsequently, if a decision to move forward with an audit is reached, LAD staff inform the committee of the direction of the audit work. Section 8.20 of the Yellowbook requires that auditors communicate an overview of the objectives, scope, and methodologies and the timing of the audit to applicable parties, including the cognizant legislative committee that has oversight of the audited entity. This step is meant to be a mechanism to inform the LAC of the direction of audit work in an advisory capacity; it is not a process to determine the scope, objectives or methodology for the audit.

Performance Audit Planning Process

The Yellowbook establishes fieldwork standards for performance audits. While the standards don't specifically refer to information system audits, those examinations currently follow performance audit standards. In addition, the Yellowbook may also be used in conjunction with other professional standards issued by other authoritative bodies, such as those issued by the Information Systems Audit and Control Association (ISACA). Performance audit fieldwork standards outline the overall approach for both performance and information system audits when planning and performing an audit. Section 8.03 of the Yellowbook begins to outline several planning factors, including the need for auditors to:

- Adequately plan work, including documenting in an audit plan.
- Plan an audit to reduce risk to an acceptable level.
- Assess significance and audit risk as part of establishing audit scope, objectives, and methodologies.
- Design methodologies to obtain sufficient and appropriate evidence that provides a reasonable basis for finding and conclusions.

In addition to these requirements, the Yellowbook provides guidance which defines audit objectives, audit scope, and audit methodologies, including sufficient and appropriate evidence. Key concepts such as significance, audit risk, and criteria are also defined. Significance generally refers to the type and extent of audit work to perform; risk generally refers to the possibility that audit findings may be improper or incomplete due to various factors, including a lack of sufficient and appropriate evidence; and criteria refers to the expected performance of a program or activity. The Yellowbook gives auditors' the responsibility to communicate an overview of the objectives, scope, methodologies, and timing of the audit to management, those charged with governance, and legislative committees. This section also notes how audit management are required to assign auditors with adequate collective professional competence.

Yellowbook Risk Assessment and Planning Requirements

Key to planning guidance provided by the Yellowbook is the need for an auditor to obtain an understanding of several factors as they plan the audit. Sections 8.03 through 8.86 provide guidance on planning a performance audit. These planning sections of the Yellowbook outline how auditors must assess risk and significance within the context of the audit in several areas as they plan the audit by addressing the following:

- **The nature and profile of the program and the needs of potential users of an audit**
  - Information related to the visibility, age, size, level of oversight, strategic efforts, and awareness of potential user interest and influence.
- **Internal control as it relates to the objectives and scope of an audit**
  - Relevant policies or procedures put in place by management to ensure program activities operate as intended.
- **The relevancy and effectiveness of information system controls**
  - Procedures established by management to ensure the secure an efficient operation of information systems (including data reliability).
- **The provisions of relevant laws, regulations, contracts, and agreements**
  - Any laws, regulations, contract, or agreements with which the program is required to comply.
- **Opportunities for potential fraud**
  - Potential incentives or pressures for individuals to deliberately obtain program benefits inappropriately.
- **Any ongoing investigations or legal proceedings**
  - Any relevant legal actions that have been initiated which could impact the operations of the program.
- **The results of any previous audits or examinations**
  - What corrective actions have been taken to address findings or recommendations from prior audits or examinations.

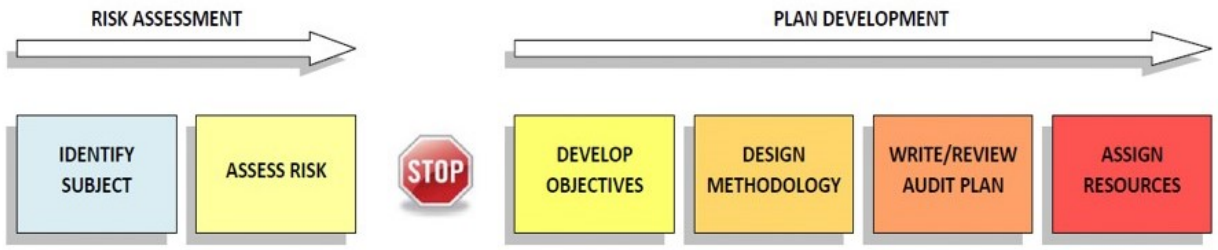
- **Potential criteria needed to evaluate the subject matter of the audit**
  - Relevant laws, regulations, goals, policies standards, best practices, agreements, or benchmarks that can be used to measure or evaluate program operations.
- **Sources of relevant evidence**
  - Identifying sources of information that can be used as evidence, including the type and amount of evidence needed to meet the sufficient/appropriate standard.
- **The work other auditors or specialists conduct**
  - Determining whether other auditors or specialists have conducted or are conducting work to relevant to the current examination.

Obtaining an understanding of the program during planning assists an auditor in assessing risks associated with the program and the effects of those risks on any potential audit objectives, scope, or methodologies. Section 8.90 of the Yellowbook outlines how the focus of these planning efforts is to ensure that over the course of the work, auditors obtain sufficient and appropriate evidence to provide a reasonable basis to answer audit objectives and support any potential findings and conclusions. In the context of identifying and gathering evidence, sufficient evidence refers to the quantity of evidence and appropriateness refers to the quality of the evidence. The quality and quantity of evidence needed is directly related to the type of work to be conducted and the focus of the audit objectives. The types of evidence may be physical evidence obtained directly by an auditor, documentary evidence which already exists, or testimonial evidence consisting of statements made by individuals or groups of individuals. Each type of evidence has its own strengths and weakness and generally is used in combination with each other to provide support for audit findings. Overall, the nature and types of evidence used are based on the professional judgement of auditors relative to audit objectives and audit risk.

LAD Performance Audit Planning Process

In practice, LAD has developed audit processes which implement the requirements of the Yellowbook to ensure that the required factors outlined in the standards are considered. Regarding performance audits, while LAD had made an artificial distinction between assessment and planning work, in the eyes of the Yellowbook it's all planning. However, we make a distinction where we use the consideration of risk as an opportunity to make a decision regarding if a performance audit should move forward or not. This is a policy-based practice that we have incorporated into our work, to provide a line regarding if we believe any identified risk is prevalent enough to conduct audit work. The assessment is conducted by examining various audit selection criteria that are based on those key areas identified from the Yellowbook. These criteria have been developed to help guide the decision-making process for determining if a performance audit should proceed beyond the audit assessment phase with the development of an audit plan, which would then define the scope, objectives, and methodologies employed to

conduct the work. The following figure broadly illustrates the risk assessment and planning continuum for a performance audit.



How is a Performance Audit Assessment Conducted?

Performance audit assessment and planning begins with the LAC prioritization process. Generally, upon determination an audit should be completed of an agency or program via being ranked highly in the LAC performance audit prioritization process, an audit assessment begins. Audit assessments essentially consist of research, review of program materials, interviews with agency management/staff and other applicable individuals, observations of program operations, review of available data, and development of support-based conclusions of risk. These conclusions are based on the auditor's evaluation of established audit selection criteria. The selection criteria help the auditor evaluate the risks associated with a specific state government program and assist LAD management in determining what resources are needed and will be expended on assignments. It is important for auditors to provide their professional judgment on whether or not a performance audit should proceed and why they believe this. The assessment of risk involves both qualitative and quantitative considerations. Factors such as the time frames, complexity, or sensitivity of the work; size of the program in terms of dollar amounts and number of citizens served; adequacy of the audited entity's systems and processes to detect inconsistencies, significant errors, or fraud; and auditors' access to records also impact audit risk. If a performance audit is determined feasible and warranted as a result of the audit assessment, then the assessment is a foundation of the audit planning process. If a determination is made to not conduct a full-scale audit, the assessment provides supported justification for this determination. This assessment results in the development of an internal formal memo documenting and supporting any decision.

How Does Performance Audit Planning Continue Post Assessment?

If a decision is made to move forward with an examination, then the audit team will continue on with the planning process. Through continued review of program materials, agency interviews, and observations of program operations, auditors will deepen and refine their understanding of the risk by determining the scope of the examination. There are several factors that contribute to the scope of an audit. The scope of an audit can generally be thought of as the boundary of the

audit, such as which aspects of a program will be examined, what documents are needed to conduct the examination, the period of time reviewed, and where information is located. As part of this determination of scope, auditors develop audit objectives, which can be thought of as the questions about the program that the auditors want to answer based on the evidence gathered and measured against established criteria or expectations. The purpose of developing the scope and objectives of the audit is to keep staff focused on examining the areas that they think present the most risk. The truth is that an audit examination can't look at everything, so auditors try to focus on the larger risks identified during assessment work.

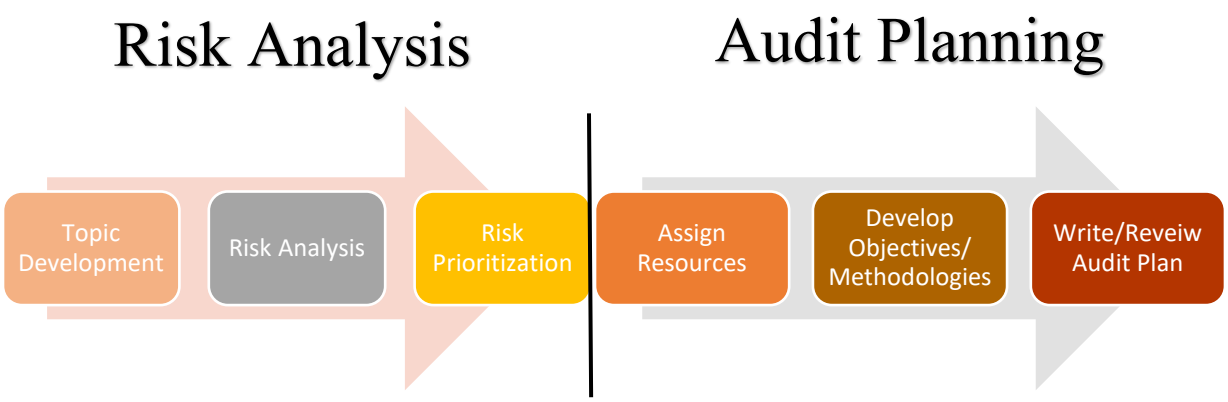
The development of scope and objectives is a way of organizing and refining the work into a relatable and manageable structure. While the scope of the audit outlines the boundaries of the work, objectives provide the specific direction. Consequently, objectives should be action-oriented, with language that explains what you hope to accomplish and measure. As part of this planning process, auditors also need to develop the specific steps, tasks, procedures, or methodologies that they will conduct to answer the objective they have established. These methodologies are not only the tasks to be completed, but also the steps that will provide the evidence needed to support any findings or conclusions. Auditors typically develop methodologies through a process whereby they identify a methodology, obtain agency input, and then develop the procedure to conduct. Once an auditor has done all this and likely cycled through these steps several times, a formal plan is written to document the direction or the work. Resources and timeframes will be also be established to conduct the work, defining staff involved, the number of hours to be expended, and when the project is expected to be delivered. At this point, audit staff formally communicate the plan to an agency, obtaining their input, and audit fieldwork begins.

INFORMATION SYSTEMS AUDIT

Similar to Performance audit, information systems audits follow the same overall approach guided by section 8.03 of the Yellowbook, noted above. However, information system audits also incorporate the guidance of ISACA as an international professional association for Information Technology (IT) governance. The IT Audit Framework (ITAF) is the professional standard developed by ISACA. Therefore, information systems have a different means for developing an audit plan, while still following the same general process as performance audits and meeting the standards of the Yellowbook. For example, section 8.03 of the Yellowbook is covered in similar standards within ITAF, as shown below.

Yellowbook	Planning Standards	ITAF	IT Audit and Assurance Standards Statements
Planning Standards	Adequately plan work, including documenting in an audit plan;	**1203 Engagement Planning**	IT audit and assurance practitioners shall develop and document an IT audit and assurance engagement audit program that describes the step-by-step procedures and instructions to be used to complete the audit.
Planning Standards	Plan an audit to reduce risk to an acceptable level;	**1201 Risk Assessment in Planning**	IT audit and assurance practitioners shall consider subject matter risk, audit risk and related exposure to the enterprise when planning audit engagements.
Planning Standards	Assess significance and audit risk as part of establishing audit scope, objectives, and methodologies;	**1201 Risk Assessment in Planning**	The IT audit and assurance function shall use an appropriate risk assessment approach (i.e., data-driven with both quantitative and qualitative factors) and supporting methodology to develop the overall IT audit plan and to determine priorities for the effective allocation of IT audit resources. IT audit and assurance practitioners shall identify and assess risk relevant to the area under review when planning individual engagements. IT audit and assurance practitioners shall consider subject matter risk, audit risk and related exposure to the enterprise when planning audit engagements.
Planning Standards	Design methodologies to obtain sufficient and appropriate evidence that provides a reasonable basis for finding and conclusions.	**1204 Performance and Supervision**	IT audit and assurance practitioners shall document the audit process and describe the audit work and the audit evidence that support findings and conclusions.

Information system audits still follow the same guidance and use the same definitions for audit objectives, audit scope, and audit methodologies and use the same standards for sufficient and appropriate evidence. The planning factors described in the Yellowbook are also considered throughout the IS audit risk analysis and planning process, just through different processes. The following figure shows the overall process with various decision points throughout risk analysis and planning for IS audits.



How is Information System Risk Analysis Conducted?

IS audit has many risk assessment methodologies available to adequately analyze and prioritize risks. These range from simple classifications of high, medium and low, based on auditor's judgment, to more quantitative approaches that provide a numeric risk rating. There are other methodologies that are a combination of the two. Our office has chosen a process that combines simple classifications and a secondary review that is more quantitative. Overall, the risk analysis process includes gathering information about risks throughout the state IT environment, deciding about where to focus further risk analysis, and a quantitative method to develop a risk rating. Initial information gathering comes from various places, including:

- Boards, committees, budget hearings, and other meetings
- Other audit functions
- Legislative requests
- Hotline calls

This initial information is formed into areas of audit, or topics. A simple classification of high, medium, and low, are determined based on initial information, including nature and profile, reason for attention, impact to state government operations, and potential for fraud. The topics considered high risk are then further reviewed in a more quantitative way. This process includes reviewing 44 aspects of controls, nature and profile, governance, and interest within seven domains: Regulatory Requirements, Topic of Interest, Security Management, Impact of System Failure/Issue, Management/Governance, Fraud & Abuse, and Nature and Profile. Auditors spend time researching and contacting agencies in similar means to the Yellowbook (knowledge gained through inquires, observations, and reviewing documents) to determine a high, medium, or low risk for each aspect. This determination is then translated into a numeric score for the domain and the topic overall. The topics are then ordered by risk score. The highest scores are selected for the audit list of that year and are approved by the deputy to move into the planning process. Unlike performance audits, there is no further assessment to determine if an audit is warranted. The "cut off" for highest scores depends on other work needing to be completed by the IS audit

team over the course of the year, including assistance to other audit functions and system compliance audits.

How Does Information Systems Audit Planning Continue Post Risk Analysis?

After the highest risk topics are reviewed and approved by management, the IS audit officially moves into the planning stage. Following the general audit process outlined in ITAF, audit staffing and scheduling occurs next followed by further detailed planning of the audit. Similar to the Yellowbook, ITAF also requires communication with those charged with governance and oversight, such as audit committees. However, Yellowbook discusses communicating an overview of the objectives, scope, and methodology and the timing, while ITAF discusses communicating an audit schedule. After the list of highest risk audit topics is determined and other potential work to complete in the year are defined, a schedule of those risk-based topics is presented to the LAC. We ask the committee to prioritize the topics to identify where we should focus resources first in our audit schedule for the year, rather than to determine where we further assess risk, like performance. After prioritization is completed by the committee, auditors are then assigned to the audit schedule based on availability. From this point, the auditor reviews previous information and formally engages in the audit with the auditee to complete the planning process like performance audit described above.