FIELDWORK AND THE CONDUCT OF WORK IN AGENCIES

Each information technology, performance, and financial compliance audit project includes a fieldwork stage. This phase of the audit work involves performing the methods and procedures established in the planning stage of the audit necessary to answer the objectives of the audit. The main purpose of the fieldwork stage of an audit is through the completion of the different types of procedures or methods to obtain sufficient and appropriate evidence to provide a reasonable basis for supporting any potential findings and conclusions. The following sections discusses the standards basis, practical approaches, and selected types of testing for the fieldwork stage within the Legislative Audit Division (LAD) for information technology, performance, and financial compliance audits.

INFORMATION TECHNOLOGY AND PERFORMANCE AUDITS

Once audit staff have finalized planning activities and communicated an overview of the objectives, methods, and timing of an audit to the management of the audited entity, the fieldwork stage of an audit begins. The Yellowbook establishes fieldwork standards for performance audits. While the standards don't specifically refer to information technology audits, those examinations also follow performance audit standards. 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). These standards essentially mirror the Yellowbook, in regard to the need to obtain evidence to support findings. Performance audit fieldwork standards outline the overall approach for both performance and information technology audits when conducting fieldwork. The underlying tenet of the fieldwork stage of an audit is the need to gather and assess evidence. Section 8.90 of the Yellowbook begins to outline the requirements for auditors to obtain evidence, including assessing and determining both the sufficiency and appropriateness of that evidence. The Yellowbook requires that auditors evaluate the objectivity, credibility, and reliability of information and evidence provided by the audited entity.

In the planning stage of the work, auditors identified and developed an understanding of the risk to an audit in several key areas and developed objectives and methods to address those risks. In practice, the fieldwork stage consists of following the formal plan established at the end of the planning stage, which outlines the objectives, scope, and specific steps, tasks, procedures, or methods that will be used to answer the objective they have established. These methods are not only tasks to be completed, but also the steps that will provide the evidence needed to support any findings or conclusions. The concepts of audit risk and significance continue to assist auditors in evaluating audit evidence during the fieldwork stage. An important part of auditor's responsibility for assessing evidence is maintaining professional skepticism when using information provided by agency staff over the course of audit fieldwork. This may include obtaining assurance or confidence in the information provided by determining what activities were conducted by the agency to ensure the evidence provided is reliable and accurate. It may

also include conducting independent procedures to test agency staff activities to obtain that assurance, including direct testing or obtaining corroborating evidence. Auditors frame their work and the assessment of evidence gathered from agency staff from a risk-based perspective, considering conflicting information, access issues, the timeframes needed to obtain evidence, and the quality of the agency's internal controls, including information systems controls, over the information. While audit staff generally consider agency staff provide evidence in a good faith manner, in practice audit staff have a responsibility to obtain documentation of that evidence and are unable to take agency staff at their word. And if agency staff do not provide access to evidence in a timely manner, the quality of the evidence degrades with reasonable questions raised regarding the validity and reliability of that information.

Sufficiency and Appropriateness

The concepts of the sufficiency and appropriateness of evidence are threaded through the Yellowbook fieldwork standards and guide auditors in assessing evidence gathered to address the objectives of an audit. Sections 8.99 through 8.102 of the Yellowbook define those concepts as such:

- Sufficiency is a measure of the quantity of the evidence used to support findings and conclusions related to the audit objectives. Useful presumptions which auditors follow when assessing sufficiency include the notions that the greater the audit risk, the greater the quantity and quality of evidence needed; and stronger evidence may allow for less evidence to be needed.
- Appropriateness is the measure of the quality of the evidence used to answer audit objectives and support findings and conclusions. Important concepts considered by auditors include the relevancy, validity, and reliability of the evidence. An important consideration is that a large volume of evidence does not compensate for a lack of relevance, validity, and reliability.

Since the objectives of an audit can vary widely, the level of work needed to ensure the sufficiency and appropriateness of that evidence can also vary widely to answer those objectives. The level of assurance or confidence needed by audit staff when gathering and assessing evidence is directly related to the type of audit objective. For example, if an audit objective focused on the performance of a specific program or activity, auditors likely would need to test the quality of any information that was compiled by an agency through individual document review to assess the information's reliability and validity. If an audit objective were to focus on verifying specific quantitative results presented by an agency, auditors would likely obtain evidence of the accuracy of the information through the use of statistical sampling. In practice, professional judgement assists auditors in making these kinds of determinations. In this sense, auditors use their professional knowledge, skills, and abilities, in good faith and with integrity, to diligently gather information and objectively evaluate evidence.

Types of and Appropriateness of Evidence

The types of audit approaches and evidence collected by auditors may be categorized as physical, documentary, or testimonial. Section 8.104 of the Yellowbook describes those types of evidence as follows:

- Physical evidence is obtained by direct inspection or observation of people, property, or events. This type of evidence might be documented by auditors through summary memos, photographs, videos, charts, maps, or physical samples. For example, an auditor might travel with program staff to observe a particular program activity and summarize that observation and experience in a detailed memo describing how that activity is conducted.
- Documentary evidence is information that already exists, such as emails, contracts, accounting records, invoices, spreadsheets, database extracts, physically or electronically stored information, and other management information on program performance. For example, when assessing a particular activity or program, auditors would likely obtain and inspect agency complied information regarding the outcomes of a program, such an annual report or other summary statistics.
- Testimonial evidence is gathered through questions, interviews, focus groups, public forums, or surveys. For example, a routine and frequent activity conducted by auditors is speaking directing to agency staff, recipients, or other stakeholders regarding the operations of a programs.

When gathering, examining, and assessing evidence, auditors frequently use analytical procedures, comparisons, or other structured approaches to determine the quality and quantity of evidence. Whether gathered through observation, inquiry, or inspection, each type of evidence has its own strengthens and weaknesses. In practice, auditors must continually judge the appropriateness of the evidence they gather. Some general approaches the Yellowbook provides to guide auditors in this regard include:

- Evidence obtained where controls are effective is generally more reliable than if controls are weak or absent.
- Evidence gathered through direct physical examination, observation, analysis, or inspection is generally more reliable that indirectly obtained evidence.
- Examination of original documents is generally more reliable than copies.
- Testimonial evidence gathered when individuals may speak freely is generally more reliable than circumstances in which individuals may be intimidated.
- Testimonial evidence obtained from an unbiased individual with direct knowledge is generally more reliable that from a biased individual with indirect or partial knowledge.
- Evidence from a knowledgeable, credible, and unbiased third party is generally more reliable than from agency management or others with a direct interest in the agency.

Other guidance in this portion of the Yellowbook regarding determining the appropriateness of evidence include the guidance that testimonial evidence can be helpful in interpreting or corroborating physical evidence, while documentary evidence may be useful in supporting or challenging testimonial evidence. Surveys generally provide self-reported information about existing conditions or programs. When sampling is used, the appropriate method will depend on the audit objectives, including the need for a statistical or nonstatistical approach.

Overall Assessment of Evidence

Lastly, section 1.108 of the Yellowbook takes a holistic view of evidence, directing auditors to perform and document an overall assessment of the collective evidence used to support any findings and conclusions, including any assessments related to reliability and validity. Concepts such as significance, corroborating factors, and risk are considered, with auditors required to perform additional steps if limitations or uncertainties are identified. While the Yellowbook stresses the need for an overall assessment of evidence, it recognizes that concepts such as sufficiency and appropriateness are relative and may be considered on a continuum rather than as absolutes. In practice, this assessment of evidence happens in several ways within LAD, including on a continuously basis, with audit work subject to layers of supervision to ensure that audit staff are correctly interpreting the results of audit testing and evaluating the sufficiency and appropriateness of the evidence. In addition, at the conclusion of fieldwork, prior to the development of findings, audit staff develop summaries memos assessing their collective work. These memos are subject to supervisory review to ensure that evidence is evaluated in the context of related findings and conclusions, including providing a reasonable basis of support for those findings relative to the audit objectives. An important consideration outlined in the Yellowbook is that evidence is not sufficient or appropriate when it carries a high risk of an improper or incorrect conclusion, when there are limitations given the intended use, or it does not provide an adequate basis for addressing the audit objectives. As part of that overall assessment of work, during the fieldwork stage, any evidence and analysis conducted by LAD staff is always and continually presented and communicated with agency staff to obtain their input to ensure that we are understanding the nuances of any program activity and approaching the work in a fair and balanced manner.

FINANCIAL AUDITS

Fieldwork and communication standards for financial audits are primarily established through the auditing standards issued by the American Institute of Certified Public Accountants (AICPA). The AICPA Professional Standards align with the Yellowbook.

Fieldwork

During fieldwork, the auditor obtains evidence to support the audit opinion rendered in the Independent Auditor's Report. The auditor must obtain sufficient appropriate audit evidence on

which to base their conclusions. Sufficient is a measure of quantity of audit evidence. The quantity of audit evidence necessary is affected by the auditor's assessment of the risks of material misstatement and the quality of the audit evidence obtained (that is, its appropriateness).

The AICPA outlines two types of tests: tests of controls and substantive procedures (also known as detection tests). Tests of controls are designed and performed to determine if agency controls are working appropriately. This may involve looking at documents to determine if all reviews required by the agency occurred, or to determine if a monthly process, such as a reconciliation, was completed each month. Substantive procedures include tests of details, such as account balances and disclosures, and analytical procedures. The following table summarizes the types of substantive procedures performed during financial audits.

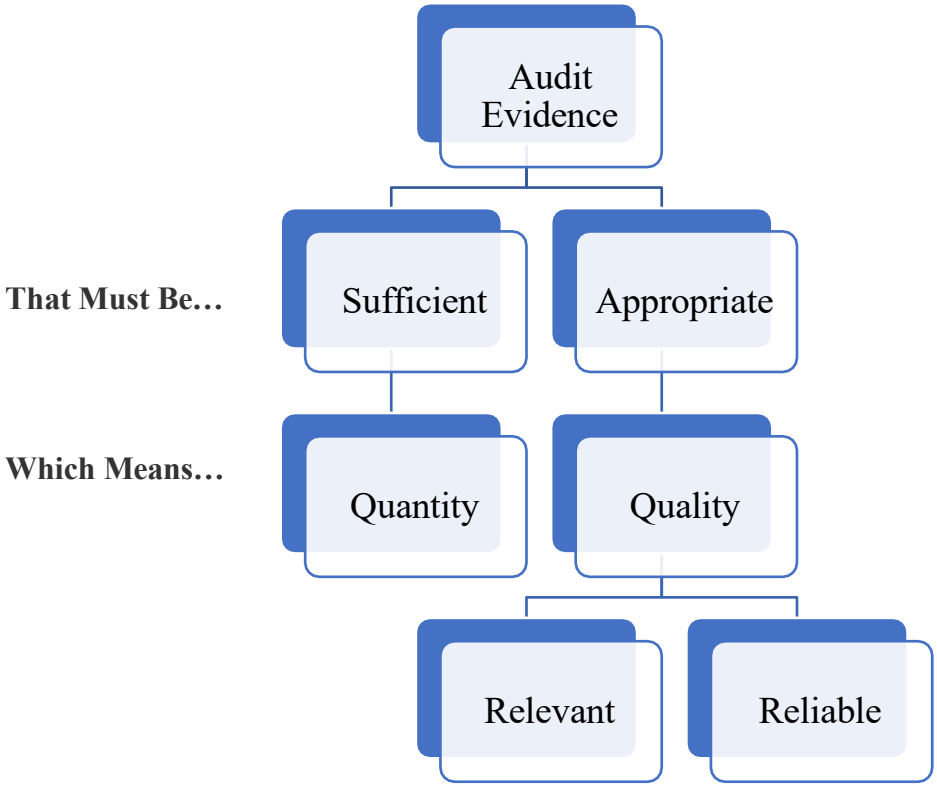
Type of Substantive Procedures	
Type of Procedure	Description
Inquiry	Asking knowledgeable agency staff about activity being tested. Inquiry alone does not provide sufficient audit evidence. We often inquire about differences in financial amounts between years.
Inspection	Looking at documents from the agency or an external source. This is often used in combination with other procedures, such as sampling or inquiry.
Observation	Watching a process taking place. Observation commonly occurs with inventory counts or mail and check processing.
External Confirmations	Requesting a third party verify the accuracy of data. This is commonly used to confirm the balance of accounts or loans receivable.
Recalculations and Reperformance	Manual or automated recalculations are commonly performed when an agency uses complicated mathematical formulas. An example is allocation of taxes among various funds according to percentages established in state law.
Data Analysis (Analytical Procedures)	Consists of evaluations of financial information through analysis of plausible relationships among both financial and nonfinancial data. Examples include reviewing when cyclical revenue is received against expectations and confirming routine activity, such as rent payments, occur each month.
Sampling	The selection and evaluation of less than 100 percent of the population. We commonly use judgmental and sequential sampling plans.
Service organization reports	Many agencies outsource aspects of their business activities to external organizations. These service organizations receive audits that are provided to the agency. We rely on these audits by considering what the service organization auditors identified, how that impacts the agency we are auditing, and consider the service organization auditor competency and qualifications.
Use of Specialists	The most common specialists we rely on are actuaries. Sometimes we hire an actuary. In other cases, we rely on management's actuary after considering the actuary's independence, competence, and qualifications, as well as the type of work they performed.

Type of Substantive Procedures	
Type of Procedure	Description
Group Audits	Some audits have components or component units audited by other auditors. Auditing standards allow us to rely on the work done by other auditors in some circumstances after considering the work they performed and their qualifications and competence. University foundation financial activity is audited by other firms. That activity is presented in university financial statements, so we make reference to the work of those auditors.
Reliance on Information Systems	Many information systems process or directly determine financial amounts. With the help of IS auditors we perform tests of the system. We often test system access and mathematical processes.
Direct and Material Laws and Regulations	Some laws or regulations directly determine a material financial amount. The Yellowbook extends this consideration to grant and contract agreements. In these instances, we determine agency compliance with that law as part of gathering evidence to support our audit opinion. An example is ensuring an agency complies with a law that sets an amount for a license.
Management and Legal Representations	Management is required to acknowledge their responsibilities and indicate they believe they fulfilled their responsibilities, in writing. We also obtain a written representation from legal counsel regarding outstanding litigation against the agency and possible contingent liabilities. We obtain management and legal representation at the end of every audit.

In performing substantive procedures, the auditor needs to consider the nature, timing, and extent of procedures as well as the appropriateness of the audit evidence. This is the quality of audit evidence, or its relevance and reliability in providing support for the audit opinion. Auditors need to evaluate audit evidence by considering if it is relevant and reliable. Auditors need to think about the source of the information and whether it corroborates or contradicts assertions in the financial statements. Audit evidence needs to be sufficiently precise and detailed for the auditor's purpose as well as accurate and complete. Most fieldwork involves obtaining audit evidence, evaluating its relevance and reliability, and resolving inconsistencies and doubts over reliability.

The AICPA Professional Standards indicate reliability increases when:

- The evidence is obtained from independent sources outside the agency.
- The evidence is generated internally, and related agency controls are effective.
- The evidence is obtained directly by the auditor, rather than indirectly or by inference. For example, an auditor observing a control is better than inquiring about the control.
- The evidence is in documentary form rather than obtained orally.
- The evidence is original documents rather than copies of original documents.



Communicating with Management and Those Charged with Governance

While performing the work described above, we often find potential issues related to financial misstatements, internal control deficiencies and noncompliance with state and federal laws and regulations or contractual agreements. We communicate these issues to management throughout the audit. The Yellowbook indicates early communication is important because of the significance and urgency for corrective action.

Both the Yellowbook and AICPA Professional Standards also require that we communicate certain information to those charged with governance of the agency, such as boards and commissions with oversight responsibilities. In addition to issues we identify, we also communicate any disagreements with management, significant estimates made by management, and the responsibilities of the auditor and management. Recent changes to AICPA Professional standards require us to communicate even more with those charged with governance, including information about significant risks we identify, planned scope and timing of the audit, and significant unusual transactions.

SAMPLING AND OTHER STATISTICAL ANALYSIS

It is often not possible or reasonable within the timeframe of an audit for an auditor to examine every item in the population of interest to answer an audit objective. When this is the case, an

auditor must determine an appropriate sampling approach to use a subset of the population for the purpose of evaluating the entire population or answering the audit objective. Resource constraints, such as staff and time, and the nature of the population of interest often contribute to the need for sampling. For example, if the population of interest is large, and manual review of documentation is necessary, sampling would likely be required. The appropriate sampling approach depends on the audit objectives. Auditors must determine both an appropriate sample size and sampling method in the context of obtaining sufficient and appropriate evidence for answering an audit objective. In addition to sampling, more advanced statistical approaches and analyses are sometimes required to answer an audit objective.

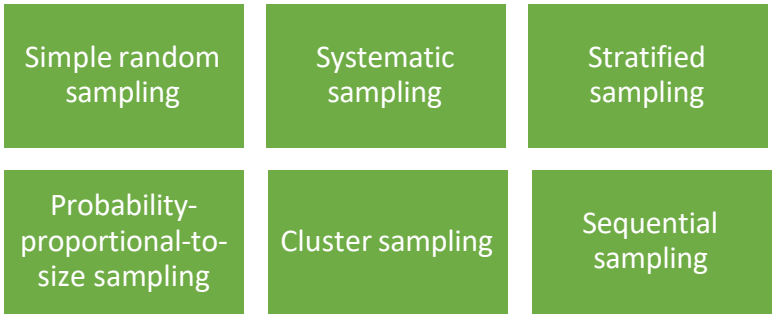
Determining a Sampling Method

When sampling is required, the first decision an auditor must make is whether a statistical or nonstatistical approach should be used. Statistical sampling draws from the field of applied statistics. Nonstatistical sampling draws from the auditor's experience and professional judgment. Section 8.107 of the Yellowbook emphasizes that use of a statistical sampling approach generally results in stronger evidence than that obtained from nonstatistical techniques. In that sense, a statistical approach is often preferred. However, a targeted selection (or nonstatistical approach) can be effective if the auditor has isolated risk factors or other criteria to target the sample selection.

The decision between a statistical or nonstatistical approach depends on whether a representative sample is needed to answer the objective. A sample is representative if it mirrors the characteristics of interest in the population. When this is the case, the auditor can use the sample to make estimates for the population with a known degree of accuracy. When the auditor determines a statistical approach is necessary, they must then identify an appropriate sampling method. Several factors influence the choice between sampling methods, including:

- The nature and quality of items within the population
- Availability of auxiliary information about the sampling units
- Accuracy requirements and the need to measure accuracy
- Whether detailed analysis of the sample is expected
- Resource constraints or other operational concerns

The auditor must consider these elements and select a sampling method that will provide appropriate evidence within the resource constraints of the audit. There are several common sampling methods used in our audits. Some examples of common statistical sampling methods utilized in our audits are:



Each of these methods invokes probability sampling techniques and involves random selection of items within the population. For example, in the case of simple random sampling, each item in the population has an equal probability of being selected, and a sample of the appropriate size is randomly selected. These techniques allow us to use mathematical theorems to make estimates and conclusions about the population from which the sample was chosen. These estimates and conclusions are then used as evidence or part of the evidence in supporting any findings.

When a nonstatistical sampling approach is fitting, auditors must still ensure the sample is sufficient and appropriate for answering the audit objective. A nonstatistical sampling approach limits our ability to make inferences about an entire population. However, this approach can produce sufficient and appropriate evidence in some circumstances. The most common nonstatistical sampling method used by our office is a judgmental sample. For a judgmental sample, the auditor selects items for a sample based on his or her experience and professional judgment. For example, an auditor may be aware of specific types of items in the population that are higher risk. The auditor may choose to focus on these known high-risk items in the population and may not need to make estimates about the entire population to answer the audit objective. All sampling approaches are subject to review, and input from other members of the team with experience in the area being reviewed is typically obtained.

Determining Sample Size

In addition to the sampling approach and sampling method, the auditor must determine the sample size necessary to identify evidence that is sufficient for answering the audit objective. In a statistical sample, the sample size is calculated to achieve a desired level of statistical power, which requires a consideration of audit risk and what is meaningful within the context of the audit objective. In practical terms, the calculation of sample size for a statistical sample is based on a desired or an acceptable margin of error. Margin of error refers to a quantifiable measure of uncertainty in an estimate. Auditors often use our in-house sample size calculator to calculate the sample size for a statistical sample. For nonstatistical samples, auditors often determine the sample size based on the population size, resource constraints, and what sample size a reasonable person might consider sufficient for answering the audit objective. Additionally, federal audit guidance sometimes dictates minimum sample sizes based on various risk elements for financial audits

Other Statistical Analysis in Fieldwork

Outside of basic sampling techniques, auditors sometimes use more advanced statistical techniques for answering audit objectives. That is, sometimes more rigorous and complex analyses are necessary to answer a question that cannot be answered using simple or standard sampling techniques. Auditors must sometimes integrate advanced data analytics into their fieldwork. Examples of statistical analyses included in our work recently are:

- Advanced survey techniques, such as randomized vignettes, can be used to elicit beliefs, attitudes, or behaviors of respondents with respect to presented scenarios. LAD staff used a vignette survey design to assess willingness of attorneys to contract with the state (*Public Defender Workforce Management – 19P-04*).
- Regression analysis allows for the examination of the relationship between two or more variables. LAD staff assessed the relationship between probation officer caseload and their ability to contact offenders on supervision using a regression analysis (*Montana's Probation and Parole Practices: Supervising According to Risk – 20P-05*).
- Linear programs are optimization techniques. In a recent audit, we used a two-stage stochastic linear program for optimizing the inventory of vehicles available for short-term rental by state employees (*Cost and Management of the State Motor Pool – 21P-03*).
- Cost-benefit analyses compare the total costs and benefits of a project or decision. A recent audit included a cost-benefit analysis to determine the ideal reapplication cycle for real property tax exemptions (*Real Property Tax Exemptions: Improving Information Management and Informing Policy Decisions – 21P-06*).
- Simulation techniques can be used to model and analyze complex systems. Our audit on the accuracy of bonus points included a simulation to determine if the results for bonus point holders aligned with expected probabilities (*Analyzing Bonus Point Accuracy – 23P-01*).
- Spatial analyses are used to consider the spatial context of data. LAD staff conducted a spatial analysis using suitability modeling to determine where Montana needed affordably housing the most for awarding tax credits for low-income housing (*Supporting Low-Income Housing: The Montana Board of Housing and Its Role in Awarding Tax Credits – 23P-04*).
- Quasi-experimental techniques can be used to identify similar groups for comparison to determine the effectiveness of programs. We have used such techniques (e.g., propensity score matching) to assess the effectiveness of contracted community corrections programs and tax increment financing programs (*Effectiveness of Contracted Community Corrections Programs in Reducing Recidivism – 18P-05*; *Tax Increment Financing Administration and Impact – 17P-03*).

INFORMATION TECHNOLOGY AUDIT TESTING AND DATA RELIABILITY

As part of fieldwork, auditors frequently rely on computer-based information as a key part of gathering audit evidence or may need assurance an automated control can be relied on. Information technology (IT) audit testing consists of identifying controls in place to mitigate risk, assessing those controls and gathering evidence, and documenting the work and developing findings. Controls can range from application settings, processing, or structure to management

processes and governing practices. Two separate IT audits exist to focus in on this broad spectrum of IT controls with slightly different approaches based on the nature and scope of the work.

IT Management Audits

IT operations, management, and governance all play a role in how technology functions. Therefore, IT management audits focus on those practices that are more pervasive and affect all technology assets. These are usually referred to as general IT controls. These are more about how the IT function works and less about how any particular system works, so the scope of these audits is more at the agencywide level. Multiple frameworks exist for IT auditors to use when assessing general IT controls. Commonly used frameworks are noted below:

- **Control Objectives for Information and Related Technology (COBIT):** Standards for Information Technology (IT) management and governance. These standards outline control practices to reduce technical issues and business risks. This framework is developed by the Information Systems Audit and Control Association (ISACA). While COBIT is not required by state policy, many of its practices align with state policy and it is a well-known, international framework.
- **Information Technology Infrastructure Library (ITIL):** A set of detailed practices for IT activities such as IT service management (ITSM) and IT asset management (ITAM) that focus on aligning IT services with the needs of business. This guidance helps organizations address new service management challenges and utilize technology efficiently. ITIL is not required by state policy, either, but is applicable to organizations with centralized IT service divisions.

These frameworks are large, complex sets of hundreds of management practices. Complete and perfect implementation of either framework would require far more resources than are warranted in most cases. Therefore, the goal of IT management audits is to provide the agencies with recommendations on where to make progress to reduce risk. The scope of the audit is limited to the highest risk areas, and a progress scale is used when identifying where an agency is at and what a practical recommendation would be. The scale used to communicate our assessment of the agency ranges from incomplete or incapable to organized and well-defined. By using this scale, we can help agencies take steps towards improvement, rather than asking for perfection.

System Security and Reliability Audits

On the other side of general IT controls are the controls that are specific to a system and more directly affect how the system functions. These specific controls are reviewed in our other type of IT audit, referred to as Security and Reliability Audits. The scope of this work is the set of controls specific to the system, automated within the system, and only management practices that directly impact that system. Criteria for these audits are more specific to state requirements. State law requires agencies to have certain practices and safeguards in place to secure information, and state policy further defines what those safeguards should be. These audits identify compliance with those safeguards and state law. State policy is based off national standards issued by the National Institute of Standards and Technology (NIST) to define security standards and risk management procedures. These standards provide a catalog of security and privacy controls for

information systems. NIST is a physical sciences laboratory and is part of the United States Department of Commerce. Due to using state requirements as criteria for these audits, the communication of assessment is different. However, the goal is still to communicate agencies' progress towards compliance, rather than compliant or noncompliant. The reports also focus on areas of higher risk, rather than an entire assessment, due to the number of systems that need to be assessed and the recurring nature of these assessments. Both types of audits play a role in helping auditors understand the IT control structure they need to rely on for determining data reliability or assurance of automated controls. IT audit documents this work, develops findings, and discusses the audit with agencies in the same manner, under the Yellowbook standards, as performance audits. Therefore, the other functions in the division can rely on this work whenever they need to assure IT controls are in place as part of their work.

A Practical Example: Data Reliability

An example of how other audit functions can rely on the work IT auditors conduct is when determining data reliability, or the level in which someone can trust the data will help inform the right decisions. This kind of testing is used by auditors as a methodology when there is a risk that data or reporting provided by the agency is inaccurate. It is also used to reduce the audit risk that our analysis uses data that is not complete, accurate, or appropriate. In either case, a review of the automated controls within the system that manages and produces the data as well as a review of the quality of the data output is necessary. IT audits provide an understanding of automated controls. This understanding comes more directly from the security and reliability audits, but IT management audits can also cover some relevant management practices that should be considered by other auditors as well. For the security and reliability audits, there are specific safeguards within state requirements that more directly impact the reliability of data. Those are identified below:

- **Access Control**: These controls help to ensure that only authorized users can access sensitive information and that any actions taken by those users can be traced back to them. In other words, this area is all about controlling who can see what, and making sure that there are no unauthorized actions taking place.
- **Awareness and Training**: This area is responsible for ensuring that people who use and create information systems have the necessary knowledge and awareness in aspects to the business process and information security.
- **Configuration Management**: These controls ensure that systems are properly configured and that changes are made in a controlled and consistent manner. They also intend to prevent unauthorized changes from being made to the system itself, not just the data.
- **Contingency Planning**: These controls prepare agencies to respond to disruptions and minimize the impact of potential disruptions on their operations.
- **Identification and Authentication**: These controls focus on the identities of users and devices. This includes controls such as multifactor authentication, which requires users to provide more than one form of identification before being granted access to a system.
- **System and Information Integrity**: These controls help to reduce improper information modification or destruction in the system.

After the reliability tests are complete, the auditor can then determine if the data is reliable, or if there are issues. When issues are identified, the auditors must review the sufficiency of the data to identify if there is enough quality data to answer an objective or complete the analysis. An auditor may have to change analysis steps based on the audit risk related to the data. This may include gathering a larger sample or using source data instead of system data. It is also possible that the results of this review identify data that is not reliable, and the analysis approach needs to be adjusted.