TDOT Internal Audit

Policies, Procedures, and Audit Guide

Version 2.2 | Effective 4/1/2015

James K. Polk Building, Suite 1800
Nashville, TN 37243
Phone: 615.741.1651
Fax: 615.532.6760
James K. Polk Building, Suite 1800

TABLE OF CONTENTS

1 GENERAL

1.1 Introduction

To meet the expectations for a more effective, efficient, and fiscally sound government, elected officials, appointed officials, and key decision makers need timely, relevant, and reliable, information. The role of Tennessee Department of Transportation's (TDOT) Office of Internal Audit (OIA) is to provide meaningful information in support of the decision making process and provide an independent evaluation of program objectives in the interest of management accountability and for meeting citizen expectations.

All audit work completed by Internal Audit must comply with the auditing standards promulgated by the Office of the Comptroller General of the United States, commonly known as the "Yellow Book" or generally accepted government auditing standards (GAGAS). To meet the obligations of this critical requirement, the Office of Internal Audit staff can look to this manual as a tool for achieving compliance to GAGAS and providing high quality on-time projects and value added reports.

Used often, this guide should enhance project planning, directing, and control for the In-Charge Auditor and Quality Assurance (QA) responsible for managing the audit project team. All auditors, furthermore, are encouraged to use this manual and seek additional assistance as needed, related to steps or skills in the audit process. The Office of Internal Audit's "Policies, Procedures, and Audit Guide" is a broad statement of auditor responsibilities on audit teams, with emphasis on project management and the role of the In-Charge Auditor. Within this context, OIA strongly encourages team members to review their roles and TDOT Internal Audit expectations and to seek opportunities for personal and professional development within the scope afforded by each project.

In addition to the Yellow Book, the TDOT Internal Audit also utilizes supplementary guidance from *The International Professional Practices Framework,* commonly referred to as "Red Book", issued by the Institute of Internal Auditors as a best practice guide.

1.2 Tennessee Department of Transportation

The Tennessee Department of Transportation is a multimodal agency with statewide responsibilities in roadways, aviation, public transit, waterways, and railroads. The mission of TDOT is to plan, implement, maintain, and manage an integrated transportation system for the movement of people and products, with emphasis on quality, safety, efficiency, and the environment.

1.3 TDOT's Responsibilities

The major duties and responsibilities of TDOT are:

- To plan, build, and maintain the state owned highway and Interstate system of over 14,000 miles (23,000 km).
- Administer funding and provide technical assistance in the planning and construction of state and federal aid road programs for cities and counties.
- Provide incident management on Tennessee's Interstate system through TDOT SmartWay, an intelligent transportation network of cameras and dynamic message signs.
- Staff transportation management centers in the four largest urban cities in Tennessee.
- To provide motorist information.
- Construct and maintain 19 rest area facilities and 17 welcome centers.
- Administer program for control of outdoor advertising adjacent to Interstate and state highways.
- Issue and administer special permits for movement of overweight and over-dimensional vehicles.
- Prepare and distribute city, county and state road maps, aeronautical charts, and airport directories.
- Promote safe driving behaviors on Tennessee highways.
- Provide management, technical and financial assistance, and supervision to public, private, and nonprofit public transportation agencies within the state.
- Administer funding and assistance in location, design, construction, and maintenance of the state's 80 public airports.
- Support improvements in Tennessee's railroads and rail service.
- Inspect over 19,000 bridges, 80 public airports, and all of the state's railroads.
- Maintain state park roads.
- Operate Reelfoot Airpark and ferry operations.
- Respond to initiatives of the Tennessee Aeronautics Commission.
- Provide aerial photography and mapping services to all state agencies.
- Provide aircraft for state executive transportation and economic development recruiting.
- Administer Tennessee's highway beautification programs.
- Provide grants to all Tennessee counties for litter abatement and litter prevention education.
- Provide cycling trails that connect or go through state parks and natural areas.

1.4 TDOT Organizational Structure

TDOT is headed by a single Commissioner who is appointed by the Governor. The department is organized into four regions of the state: Knoxville (Region 1), Chattanooga

(Region 2), Nashville (Region 3), and Jackson (Region 4). Each region is subdivided into five or six districts and those districts are further subdivided into county facilities. TDOT has at least one facility in all of Tennessee's 95 counties. Several administrative offices, including the commissioner and staff, operate from the TDOT headquarters in downtown Nashville, the state's capital city. TDOT has approximately 4,200 employees.

1.5 Authoritative References

AUTHORITATIVE BODIES	REFERENCE
Financial Accounting Standards Board	FASB
Government Accountability Office	GAO
Government Accounting Standards Board	GASB

PROFESSIONAL ASSOCIATIONS	
American Association of State Highway and Transportation Officials	AASHTO
Association of Certified Fraud Examiner	ACFE
American Institute of Certified Public Accountants	AICPA
Association of Local Government Auditors	ALGA
Institute of Internal Auditors	IIA
Institute of Management Accountants	IMA
Information Systems Audit and Control Association	ISACA

RELEVANT PROFESSIONAL STANDARDS, PRONOUNCEMENTS AND GUIDANCE	
Control Objectives for Information and Related Technology	COBIT
Committee of Sponsoring Organizations of the Treadway Commission	COSO
Generally Accepted Government Auditing Standards	GAGAS
Government Auditing Standards	GAS
Statement on Standards for Attestation Engagements	SSAE
International Professional Practices Framework	IPPF

1.6 Additional Audit Development Tools

The Office of Internal Audit lists additional reference materials that can help the audit staff in learning general and specific audit skills and techniques. Suggested reference reading includes:

- *Sawyer's Internal Auditing 5th Edition: The Practice of Modern Internal Auditing*
- *2007 Auditor's Risk Management Guide: Integrating Auditing and ERM*
- *Internal Control – Integrated Framework*, Committee of Sponsoring Organizations of the Treadway Commission

- *Enterprise Risk Management – Integrated Framework*, Committee of Sponsoring Organizations of the Treadway Commission
- *2005 Governmental Accounting, Auditing, and Financial Reporting: Using the GASB 34 Model*, *Government Finance Officers Association*

2 PROFESSIONAL STANDARDS

2.1 Authoritative Standard

The Office of the Internal Audit adheres to Government Auditing Standards (GAS), sometimes referred to as the Yellow Book or GAGAS, as promulgated by the Comptroller General of the United States' Government Accountability Office, Washington, D.C.

- All audits and attestations performed by the OIA shall be conducted in accordance with the GAGAS ethics and general standards at a minimum, as well as the applicable standards for field work and reporting.
- For all audit and attest work undertaken by OIA, auditors shall follow all applicable GAGAS requirements and cite the extent of compliance with those requirements in the audit report.
- Non-audit projects shall be conducted in accordance with Section 12, Non-Audit Services of this Manual.

2.2 Supplementary Standards

The Yellow Book allows the OIA to use other professional standards issued by other authoritative bodies in conjunction with GAGAS such as:

- The AICPA for financial audits and attestations (GAS 2.20 a).
- The IIA for performance audits (GAS 2.21 a).
- The ISACA for information technology engagements (GAS 2.21 e).

Supplementary standards will be utilized whenever the performance audit engagement necessitated its use. A Modified or Unmodified GAGAS compliance statement will be included in the final report as applicable (GAS 2.24).

3 DIVISIONAL ORGANIZATION

3.1 The Division of Internal Audit

Within the Tennessee Department of Transportation, the Division of Internal Audit provides Audit and Assurance, Consulting and Advisory, Education, and Integrity services for the department. The primary focus of the Division is conducting **Performance Audits** designed to ascertain the efficiency, effectiveness, and economy of TDOT's various operational and financial programs, processes, and activities.

- **Audit and Assurance Services** - are prioritized from a Risk Management approach to focus resources on areas of high risks. The ultimate objective is to provide the management structure and senior leadership with information they need to make better decisions - through practical, cost beneficial, recommendations geared toward improving TDOT's operations.
- **Consulting and Advisory Services** - are designed to initiate a collaborative approach to address concerns regarding the ever changing business environment.
- **Education Services** - include providing training on ethical behavior, fraud awareness, internal controls, and the proper use of TDOT assets to department employees.
- **Integrity Services** - are performed to substantiate alleged instances of fraud, waste, and abuse of TDOT funds by department employees, contractors, vendors, and grantees.

3.2 Internal Audit Vision

The vision of the Office of Internal Audit is to become a valuable management resource that facilitates the promotion of good governance by performing high quality audit, assurance, consulting, and investigative works that:

- Address key enterprise risks central to TDOT’s strategies and objectives
- Apply audit work commensurate with material risks.
- Help improve internal controls, transparency, and accountability of operations.
- Promote a tone of openness, cooperation, and mutual trust within TDOT.
- Place emphasis on areas that have heightened sensitivity to management and citizens of Tennessee.

3.3 Internal Audit Mission

The mission of the Office of Internal Audit is to provide objective analysis and information critical to better decision making and enhancing the overall governance capability within TDOT.

3.4 Goals

In executing its mission, OIA will focus on the following goals: Perform all audits in compliance with Government Auditing Standards. Develop the annual audit agenda and individual audit objectives using risk-based analysis - considering the complexity of activity, fiscal impact of operations, previous audit results, applicability of laws, rules, and regulations, changes in organizational structure, effects on public welfare, and the time since the performance of the last audit.

- Perform audits within the assigned time budgets.
- Perform a post audit review approximately 6 months after the completion of each audit.
- Provide auditors sufficient training to maintain professional competence and satisfy GAS.
- Continuing Education Requirements (GAS 3.69-3.78).
- Charge an average of 1,250 hours per auditor to the performance of audits and other OIA services.
- Work towards achieving government auditing benchmarks of Available Project Time (78%) and Direct Project Time (67%).
- Help ensure a 3-year average of Recommendations Implemented of 82% (government auditing benchmark - 86%).
- Adhere to the Ethical Principals cited in GAS and the Code of Ethics of the Institute of Internal Auditors (GAS 1.10-1.14).

3.5 Organizational Values

Integrity – is the characteristic that creates the trust essential for success in the OIA. Integrity is a necessary ingredient to enable each auditor to provide top notch customer service, and lasting personal, professional, and organizational development. The key attributes that exhibit integrity includes:

- Ability to conduct self-examination about their individual roles and how to achieve excellence.
- Responsible stewardship of public resources.
- Obligation to abide by professional standards.
- Focus on quality service.
- Dedication to treat everyone with respect.

Customer Service – is the primary directive for each Office of Internal Audit activity. Our customers are our primary consideration and meeting their needs by providing relevant, accurate, and timely information to enhance the decision making process is essential. Our customer-focused approach means that our customers define quality service, OIA auditors are committed to quality service delivery, the service delivery exceeds customer expectations, and customer feedback is valued and sought.

Teamwork – Within the OIA, teamwork is paramount achieve the best results and deliver quality customer service. Internally, OIA auditors endeavor to share knowledge, opportunity, and accountability amongst the group. Auditors strive to develop mutual trust and respect within the group and with our customers. The collaborative approach and valuing diversity are overriding requirements that exhibits teamwork.

Leadership and Learning – leadership and learning go hand-in-hand. Learning at every level of the Division enables leadership opportunities for each auditor. Facilitating a forum for freely exchanging ideas allows for new, creative, and innovative solutions to potential issues. Continuing education, participating in professional organizations, mentoring, and expanding job tasks provides avenues for enhancing each auditors' personal and professional development.

Commitment – unity of purpose and each auditor's distinct focus on meeting organizational objectives is critical in providing quality customer service. Applying commitment converts a job assignment into an extraordinary experience. Commitment demonstrates public service professionalism and allows accountability and responsibility for work outcomes from each auditor of the OIA.

Respect– Each auditor of the OIA is expected to promote, truthful, open, and honest communications between auditors and customers. Each auditor listens and endeavors to understand each other. Auditors share knowledge and resources to achieve organizational goals. Discourse and diverse point of views are encouraged and auditors are afforded the freedom to freely express those without fear.

3.6 Core Strategies

OIA applies core strategies to all work engagements. They apply both inwardly in how we operate and manage our division and outwardly in achieving our goals and desired outcomes for TDOT. They include:

- Being proactive and prevention focused
- Maintaining an Internal Control standpoint
- Maintaining a process-centric, rather than people-centric, approach
- Creating a positive organizational image
- Focused on long-term rather than short-term gains
- Valuing and promoting diversity
- Active communication within and outside of the Division
- Understanding the cost/benefit equilibrium

4 QUALITY CONTROL PROCEDURES

4.1 Quality Control Environment

The Tennessee Department of Transportation (TDOT) Office of Internal Audit is committed to providing the highest quality of service to management and governance structure within TDOT. Quality control planning begins with a foundation of organizational and personal independence, competent staff, continued development of staff, appropriate policies, and procedures for efficient implementation of polices.

Monitoring is needed to ensure adherence to the plans set in place.

Periodic reviews and updates are necessary to evaluate the success of the quality control plan.

4.2 Organizational Independence

Independence of the TDOT Office of Internal Audit is established by meeting the Government Accountability Office's (GAO) independence requirement. Specifically because, the Director of Internal Audit:

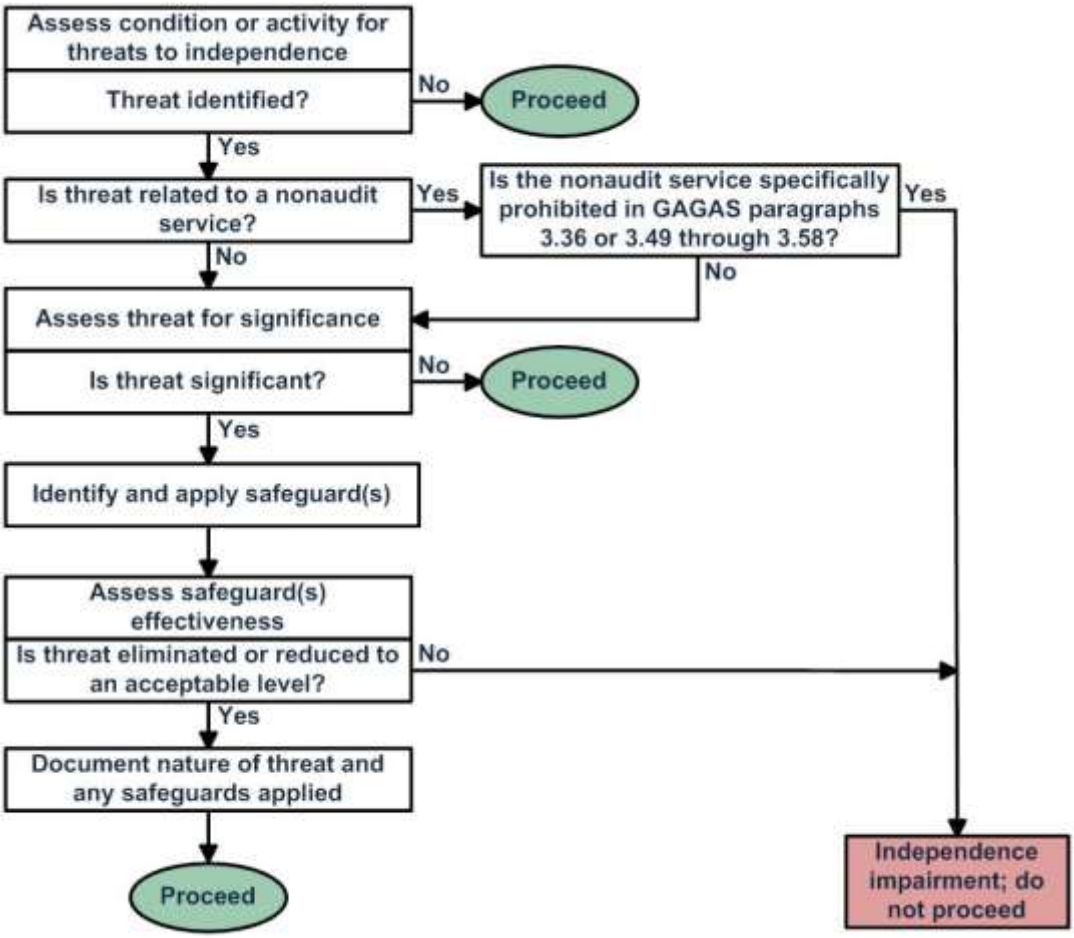
- is accountable to the head or the deputy head of the government entity charged with governance;
- reports the audit results both to the head or the deputy head of the government entity and to those charged with governance;
- is located organizationally outside the staff or line management function of the unit under audit;
- has access to those charged with governance;
- is sufficiently removed from political pressures to conduct audits and report findings, opinions, and conclusions without fear of political reprisals.

4.3 Staff Independence

All individual auditors should be free both in fact and appearance from personal, external, and organizational impairment to independence. Auditor independence will be documented through an Independence Statement for each audit project by the In-Charge Auditor, Assisting Auditors, Audit Principal, and Internal Audit Director. The In-Charge Auditor is responsible for ensuring the independence documentation has been completed by all auditor assigned to assist with the project (GAS 3.30)
If the work of a specialist is used, the specialist ability to perform the work impartially must be assessed (GAS 6.42, 6.44)

If circumstances arise that might be construed as impairment to independence, the auditor must appraise the Principal Auditor or Audit Director as soon as possible after the situation first becomes known.

4.4 GAGAS Conceptual Framework for Independence



Source: GAS 2011 Revision, Appendix II

Independence comprises of ***Independence of Mind*** and ***Independence in Appearance***.
The GAGAS ***Conceptual Framework Approach to Independence*** should be used to identify threats to independence, evaluate the significance of the threats identified, and apply safeguards to eliminate the threats or reduce them to an acceptable level (GAS 3.08).
Auditors should evaluate threats both individually and in the aggregate because threats can have a cumulative effect on an auditor's independence (GAS 3.20).
When threats are not at an acceptable level and require application of safeguards, auditors should document the safeguards applied (GAS 3.24)).

4.5 Professional Judgment

Auditors of the OIA conducting any of the services rendered by the office will exercise reasonable care and professional skepticism throughout each engagement. Reasonable care (due diligence) will be exercised conscientiously, in compliance and accord with the applicable professional standards. Professional skepticism includes an attitude of impartial treatment of information pertaining to engagement matters without assumptions or preconceived notions while applying and maintaining a keen inquisitive stance.

4.6 Staff Competency

Staff competency is derived from a mix of intellect, experience, and education. Maintaining competence through a commitment to learning and development throughout one's professional life enables sound professional judgment. Upon hire, the work history, education, and training transcript of the new employee should be captured. The competency of the assigned staff will be evaluated for each project. If necessary, funding may be secured to enlist the services of required subject matter experts to assist the audit team.

4.7 Continuing Professional Education

To comply with Yellow Book's two-year education requirements an annual, pro-rated, continuing educational and training plan will be devised for each auditor of the OIA regardless of job function. The CPE reporting period begins on January 2013 and goes on a 2-year cycle thereafter, tallied at the end of each calendar year. The pro-rated CPE schedule indicates the cumulative CPE hours each OIA auditor requires at the end of the calendar year, in relation to the auditor's official start date.
For example: a auditor that was hired in March should have (10/12)*40 hours of CPE by the end of December on the first year of hire and (22/24)*80 by the end of December of the second year.

4.8 Record Retention

Audit Work Papers
Hard copy audit working papers and other ancillary items associated with an audit engagement will be maintained by the TDOT Office of Internal Audit for ten (10) years. Hardcopy working papers for the two previous years will be kept in the offices while Electronic work papers will be maintained in perpetuity in cooperation with TDOT's Information Technology Service Division. Audit Reports, Follow-up Reports and Special Reports will be maintained in perpetuity.

Work Papers Pertaining to Investigations

Case Files and reports associated with **substantiated allegations** will be maintained in perpetuity. When office storage space becomes unavailable, they will be transferred to the State Records Center.

Other Office files:
Invoices, purchase orders, travel claims, payroll registers, and personnel information including registers which have been worked will be maintained in the TDOT Office of Internal Audit for a minimum of three years.

4.9 Internal Audit - Internal Quality Control

Work paper sign-off of the preparer signifies the completion of the document attachment, audit step, or project. Evidence of quality assurance review includes the Audit Director, Principal Auditor, or In-Charge Auditor's review comments recorded in electronic format. If a document is subsequently changed after review, the document will be flagged and will require additional approval by a designated reviewer.

The reviewer's sign-off of an audit step documents that the audit objective was met and that sufficient and appropriate evidence exists to support the conclusions and observations of the preparer.

The final sign-off of the Principal Auditor or the Audit Director in the EWP indicates the review of the documentation related to planning, conducting, and reporting of the audit project. It also documents approval of the overall assessment of the collective evidence used to support observations and conclusions of the audit report. After the final sign-off, the project will be frozen from additional documentation revisions through use electronic archiving.

4.10 Electronic Working Papers (EWP)

EWP serves to direct the documentation of audit working papers in order to assist the audit planning and performance, the supervision and review of the audit work, and the recording of audit evidence resulting from the audit work in order to facilitate and support the auditor's opinion. The use of EWP will be tailored to follow the predisposed nomenclature utilized in section 6.11

4.11 Monitoring Audit Progress

In-Charge Auditors are required to report to the Principal Auditor or the Audit Director on the progress of audit projects on the ***first business day of each month***. The report should contain budget and actual milestone dates and hours, audit objective, and results to date. Quantify results of test work and explain the significance and anything value added. The

report should also include the dates of communication with the audit client. Include the person's name, position, the topic discussed, and their reaction to the communication.

4.12 Client Survey

In order to receive feedback from audited divisions, audit surveys will be utilized. The survey should be sent by the Audit Director after the completion of the audit project report. It should be sent to the divisional director or his/her designee. Data from surveys will be used to improve the auditing process.

4.13 Peer Review

TDOT Internal Audit will arrange peer reviews to comply with Government Auditing Standards (Yellow Book). The review will be arranged through the Association of Local Government Auditors (ALGA), American Association of State highway and Transportation Officials (AASHTO), or other qualified entities performing Yellow Book Peer Reviews. The results of the review will be made available to the Commissioner and to the public through the TDOT Internal Audit website.

4.14 Performance Reporting

The Audit Director will provide an annual report summarizing the performance of TDOT Internal Audit to the Commissioner and the Deputy Commissioner/ Chief Financial Officer. The report will include tracking of the following performance measures:

- Number of recommendations accepted, partially accepted, or not accepted
- Average percentage of direct time for auditors excluding the Director of Audit
- Audit projects completed as a percentage of audits planned
- Average number of training hours per staff
- Percentage of staff with professional designations

4.15 Additional Quality Control Processes

Additional quality control measures include the following:

- Annual review of policy and procedures contained in the TDOT OIA's Policies, Procedures, and Audit Guide, including the quality control measures
- Audit engagement staff coaching and performance reviews
- Annual update of personnel records

- Annual review of staff f disclosures for first-degree relatives within TDOT, and financial relationships with anyone in TDOT
- Annual review of Continuing Professional Education credits earned
- Frequent staff meetings to discuss issues as they arise
- Reporting to the Commissioner and the Deputy Commissioner/Chief Financial Officer the results of annual performance measures
- Reporting to the Commissioner and the Deputy Commissioner/Chief Financial Officer the results of external peer reviews
- Client surveys

5 AUDIT PROJECT DEVELOPMENT

5.1 Internal Controls

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines internal controls as:

A process, affected by an entity's management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of Financial Reporting
- Compliance with applicable laws, regulations, policies and procedures.

The definition emphasizes that:

- Internal control is a process. It is a means to an end, not an end in itself.
- Internal control is affected by people. It's not merely policy, manuals, and forms, but people at every level of an organization.
- Internal control can be expected to provide only reasonable assurance, not absolute assurance, to an entity's management and board.
- Internal control is geared to the achievement of objectives in one or more separate but overlapping categories.
- Adaptable to the entity structure

COSO Identifies five components of Internal controls, namely:

I. **The Control Environment** – encompasses the overall tone of the department which is critical in influencing the control consciousness of everyone else in TDOT. The control environment provides the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the "tone at the top"; the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility; the way management organizes and develops its people; and the attention and direction provided by senior leadership.

II. **Risk Assessment** – Risk assessment is the identification and analysis of relevant risks to achievement of the objectives. The result of the risk identification and assessment process forms a basis for determining how the risks should be managed.

III. **Control Activities** – are the specific policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

IV. **Information and Communication** – Is an essential part of the management process. TDOT employees must receive a clear message from to senior management that control responsibilities must be taken seriously. Information must be identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication occurs in a matrix, flowing down, across and up the organization. TDOT employees must understand their own role in the internal control system, as well as how individual activities relate to the work of others.

V. **Monitoring** – is a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two.

Internal Control is synergistic and the linkages among the five COSO components form an integrated system that reacts dynamically to changing business conditions. Internal control is most effective when controls are built into the entity's infrastructure and are a part of the essence of the enterprise. "Built in" controls support quality and empowerment initiatives, avoid unnecessary costs and enable quick response to changing conditions.

Evaluations of internal controls occur as a part of the planning phase. Internal controls are evaluated for the adequacy of both design and function. Assessment of internal controls impact the amount of substantive testing that will be conducted in the audit fieldwork phase. Internal control evaluations are assessed and reviewed as a group, in relation to the subject matter under audit, for each engagement.

5.2 Entity-wide Risk Assessment

The Audit Director and the Principal Auditor will maintain and periodically update a risk assessment of activities included in the audit universe of TDOT. All TDOT offices, bureaus or divisions, and individual functions are subject to audit, as well as contracts with vendors and other external parties.

The annual audit plan will be constructed based upon the risks identified in the risk assessment noted above. Risk factors that will be taken into account will include the following:

Risk Factor	Weight
Input from responses to TDOT's Enterprise Risk Management per the Tennessee Financial Integrity Act,	.10
Time elapsed since the date of last audit	.10
Financial exposure	.15
Growth or reorganization	.05
Senior management's concerns	.15
Turnover of key personnel	.05
Regulatory compliance requirements	.10
Complexity of operations	.10
Effects on public welfare	.10
Audit findings from other oversight bodies	.10

Source: TDOT Internal Audit

In addition, input from internal audit staff members will also be considered in the creation of the annual audit plan and in the distribution of audit assignments. In accordance with the standard professional practice, the annual audit plan will be presented to the Comptroller of the Treasury, the Transportation Commissioner, and the Deputy Commissioner/Chief Financial Officer. However, the Audit Director is ultimately responsible for the timing, nature, and scope of all audits performed by the office. In accordance with the Audit Director's duties, any additional audits, special projects, consultations, and other non-audit services will be initiated at the Audit Director's discretion based on available resources.

5.3 Process Risk Assessment

Process risk assessment (PRA) is the identification and analysis of both quantitative and qualitative risks relevant to the achievement of business objectives for any given Division, activity, process, or transaction. It is a scaled down version of the larger Enterprise Risk Management (ERM). PRA forms a basis for determining how risks should be managed by those charged with governance. Risk is assessed on an inherent and residual basis, allowing an entity to understand the extent to which internal controls mitigate the risk factors and how the potential events might impact the achievement of objectives. Risk is assessed from two perspectives: likelihood and impact.

Each audit conducted by the OIA will utilize the risk management approach to optimize audit efforts on areas of high risk.

5.4 Overview of the Audit Process

Regardless of the area under consideration or the function, process, or activity being audited, the process followed in conducting audits and related projects consist of the phases

described below. These phases are broken down in greater detail in the following sections. The phases are:

1. ***Audit Planning*** – The planning phase is normally the most extensive and longest portion of the audit process. Planning determines how the auditors are going to spend their time conducting the audit. Within the planning phase the following occurs:
   - Auditors familiarize themselves with the operations or activities of the audited entity.
   - Background information is collected and documented.
   - Process flow analyses are performed.
   - Internal control evaluations are conducted.
   - Process risk assessment is developed.
   - Finalization of audit objectives is confirmed.
   - Design of audit tests and audit methodologies to be deployed.
   - Production of the Planning Memorandum.

2. ***Fieldwork*** – It is in this phase that the planned activities are implemented. During this phase, the audit consists of some (or all) of the activities below:

   - Collecting the data.
   - Analyzing and evaluating the data.
   - Testing internal controls by testing the validity of assertions such as:

     - ***Occurrence*** — did the activity or transactions actually take place?
     - ***Completeness*** — are all activities and transactions that should have been recorded actually been recorded?
     - ***Accuracy and Cutoff*** — were activities and transactions recorded at the appropriate amounts in the right period?
     - ***Classification*** — were activities and transactions recorded in the proper accounts?
     - ***Existence*** — do assets (and liabilities) exist?
     - ***Rights and Obligations*** — do the audited entity hold or control the rights to its assets and do they owe obligations to their liabilities?
     - ***Valuation and Allocation*** — are assets, liabilities and ownership balances recorded at appropriate amounts? Are adjustments necessary?

   - Evaluating the program, activity, or division for:

     - ***Effectiveness*** – occurs when the expected outcome and actual outcome coincide. (Are we doing the right things?)
     - ***Efficiency*** – occurs when maximum output is derived from the least amount of resources or performing an activity in the optimal manner. (Are we doing it the right way?)

- ***Economy*** – occurs when activities are done at the lowest possible cost without compromising on quality of essentials. (Are we getting value for what we spend?)

- Adequately documenting supporting work for audit observations.
- Communicating audit observations that require management's immediate attention.

3. ***Reporting*** – this phase includes the preparation and presentation of audit observations, the draft report, and the final audit report. The reporting phase includes the conclusions determined from the audit, recommendations for process improvements, responses from management, and necessary corrective actions.

4. ***Follow-up*** – the follow-up procedure, often conducted several months after the final audit report period is employed for three primary reasons:

   - It is used by OIA to determine the status of any corrective actions.
   - Ensure that the actions taken by management are responsive to audit the recommendations, and
   - Corrective actions are effective in addressing audit observations.

6 AUDIT PROJECT INITIATION

Audit teams are expected to have a thorough knowledge of the Yellow Book Standards. The procedures in this and the following chapters do not limit the team's responsibility, but describes TDOT Internal Audit procedures designed to ensure those standards are followed. If more specific procedural information is needed, auditors are encouraged to review references such as "Sawyer's Internal Audit. This chapter describes the general procedures to be followed when initiating a new project.

6.1 Types of Audits

The Audit Director will identify and determine the timing to initiate specific projects. While the majority of assignments will be performance related audits, auditors can be assigned a variety of projects. Project codes and descriptions are listed below.

- AU Financial, performance, or agreed-upon procedures
- SP Advisory Service, Special Request,
- CASE Formal Investigations
- RW Research Work
- IN Office Initiatives
- EV Case Evaluations

6.2 Project Numbering Convention

Project numbers will be prefixed by the two or four character project code, followed by four digit audit fiscal year, followed by a dash, followed by a three digit sequence number. The sequence number is a unique series for each audit type and fiscal year. The project codes are listed above in section 4.1. For example the initial 2013 performance audit project would have the following project number; AU 2013-001, and the second project would be AU 2013-002.

6.3 Audit Step Numbering Convention

Audit steps use an alpha-numeric numbering convention. A standard template has been created for Sections A-C and is included in section 4.11 of this document. The first step in Section A will be labeled, "A.1." The second step will be numbered "A.2.". A subservient documentation under the first step in Section A will be labeled A.1.1 to infinity. A subservient document under A.1.1 will follow the convention A.1.1 a to z, then aa to zz.

Audit programs specific to the audit will begin with **Section D**. The first step in Section D will be D.1. Simple audits may have only one test work section (D) with multiple steps. More complex audits may have multiple sections, Section E, Section F, etc.

6.4 Work Paper Numbering Convention

Working papers will follow the numbering convention used for the audit procedure step, plus a numeric extension. For example, the first supporting attachment or exhibit for procedure step A.1 will be A.1.1; the second work paper will be labeled A.1.2 and so on. The pattern continues consistently with the numbering system. Thus, the working paper binder will accept one document as B.11, which is a specific procedure step and allow another as B.1.1 a specific work paper related to procedure step B.1.

6.5 Project Administration and Initiation

The entrance conference will be arranged by the Principal Auditor. Prior to the entrance conference, the In-Charge Auditor will be assigned by the Audit Director or Principal Auditor. The In-Charge Auditor will be responsible for:

- Opening and closing the project in the binder as well as the Internal Audit drive
- Completion of the Project Budget Request
- Completion of the Auditors' Independence Statement
- Directing staff assignments
- Composing the Process Risk Assessment
- Composing the Planning Memorandum
- Ensuring documentation of work in the electronic working paper database
- Meeting milestone dates and time budgets
- Composing the draft report
- Assisting the Principal Auditor and the Audit Director with staff performance evaluations

6.6 Engagement Letter/ E-mail

The Audit Director or Principal Auditor will normally send an engagement letter or electronic mail to the audit client at least two weeks prior to the start of the audit. The announcement will request that the client respond within five days naming a point of contact for the audit. Unannounced audits, such as surprise cash counts, inventory and asset management reviews, do not require an engagement letter.

6.7 Office of Internal Audit Kick-Off Meeting

After the project engagement announcement has been finalized, the Audit Director or Principal Auditor will hold a kick-off conference with the assigned project team. During the conference initial audit objectives, expectations, budgets, and milestones will be determined and presented to the audited function in the form of an opening audit agenda.

6.8 Project Budget Request

In order to complete assigned tasks on each engagement in an efficient and effective manner, preliminary time budgets and milestone dates are completed by the In-Charge Auditor, submitted to the Principal Auditor, then forwarded to the Audit Director for final approval. Time is allocated by audit phase and aggregated by total hours. Milestone dates should consider the impact of staff additional assignments, development days, planned leave, and holidays on the overall calendar schedule. Milestone dates should be developed using an assumption of a maximum of 37.5 hours per week per auditor.

If staff assigned believe that actual time spent completing an assigned task will exceed estimated hours, communication between staff assigned and the In-Charge Auditor is required. If necessary, the In-Charge Auditor should include a revised time budget and estimated milestone dates in the Planning Memorandum. Significant revisions required after the approval of the Planning Memorandum should be approved by the Audit Director using a Revised Project Budget Request form.

6.9 Entrance Conference

The Principal Auditor will arrange the date and location of the entrance conference and will normally request that the Division Director and/or Deputy be in attendance as well as other key individuals. This meeting should be used to solicit the support of the audit client and include an inquiry on the audit client's perception of the objectives, scope, and related risks for the project.

6.10 Creating a New Project

The In-Charge Auditor will create a new project in the electronic working paper database following the number convention in Section 4.2, and will input budgeted hours, milestones, and staff assignments.

6.11 Audit Programs

Audit programs will consist of four parts—the project management steps, the reporting steps, the audit planning steps, and the specific test program steps. Sections A-C consists of the standard format used for the **administering, planning, and reporting** of audit projects. Sections D-Y will contain the specific test methodology used to achieve audit objectives and Section Z will contain audit data analytics performed.

The standard audit program steps A through C have been established to provide consistency in the administration, planning, and reporting of audit projects. These steps are outlined below.

A: Project Management
- A.1 Project Budget Request
- A.2 Engagement Letter
- A.3 Project Independence Statement
- A.4 Entrance Conference Record
- A.5 Confidential Information Protection Measures
- A.6 Project Wrap-Up

B: Reporting
- B.1 Internal Audit Initial Draft Report
- B.2 Discussion Draft Report and Exit Conference
- B.3 Management Letter (If Applicable)
- B.4 Final Report

C: Planning
- C.1 Information Survey
- C.2 Process Mapping
- C.3 Computer Application Systems
- C.4 Process Risk Assessment
- C.5 Fraud & Illegal Acts Evaluation
- C.6 Coordination with External Parties
- C.7 Planning In-Progress Meeting with Audit Management
- C.8 Planning In-Progress Meeting with Audit Client
- C.9 Planning Memorandum

D: Audit Objective 1
- D.1 Audit Test 1

E: Audit Objective 2
- E.1 Audit Test 1
- E.2 Audit Test 2

Z: Audit Analytics

For further references refer to the Performance Audit Template in the production Library folder/tab. This will have each individual step broken down.

7 AUDIT PLANNING

Planning is the most critical part of the audit. A well thought out and planned engagement is the key to audit efficiency. Planning involves acquiring a knowledge of the audited entity and their essential operations; delineating the scope of work; setting broad objectives that will be specifically defined at the conclusion of the audit survey; assessing inherent risks and their corresponding controls (and the resulting residual risks); developing the approach or methodology to meet the audit objectives; allocation of audit resources; and the anticipation of problems and making required adjustments.

7.1 Planning and Preliminary Survey

Auditors must adequately plan and document the planning of the work necessary to address the audit objectives.

Auditors must plan the audit to reduce audit risk to an appropriate level for the auditors to provide reasonable assurance that the evidence is sufficient and appropriate to support the auditors' observations and conclusions.

The preliminary survey should familiarize the audit team with the operations being reviewed and should identify potential problem areas.

Auditors should gain an understanding of the:

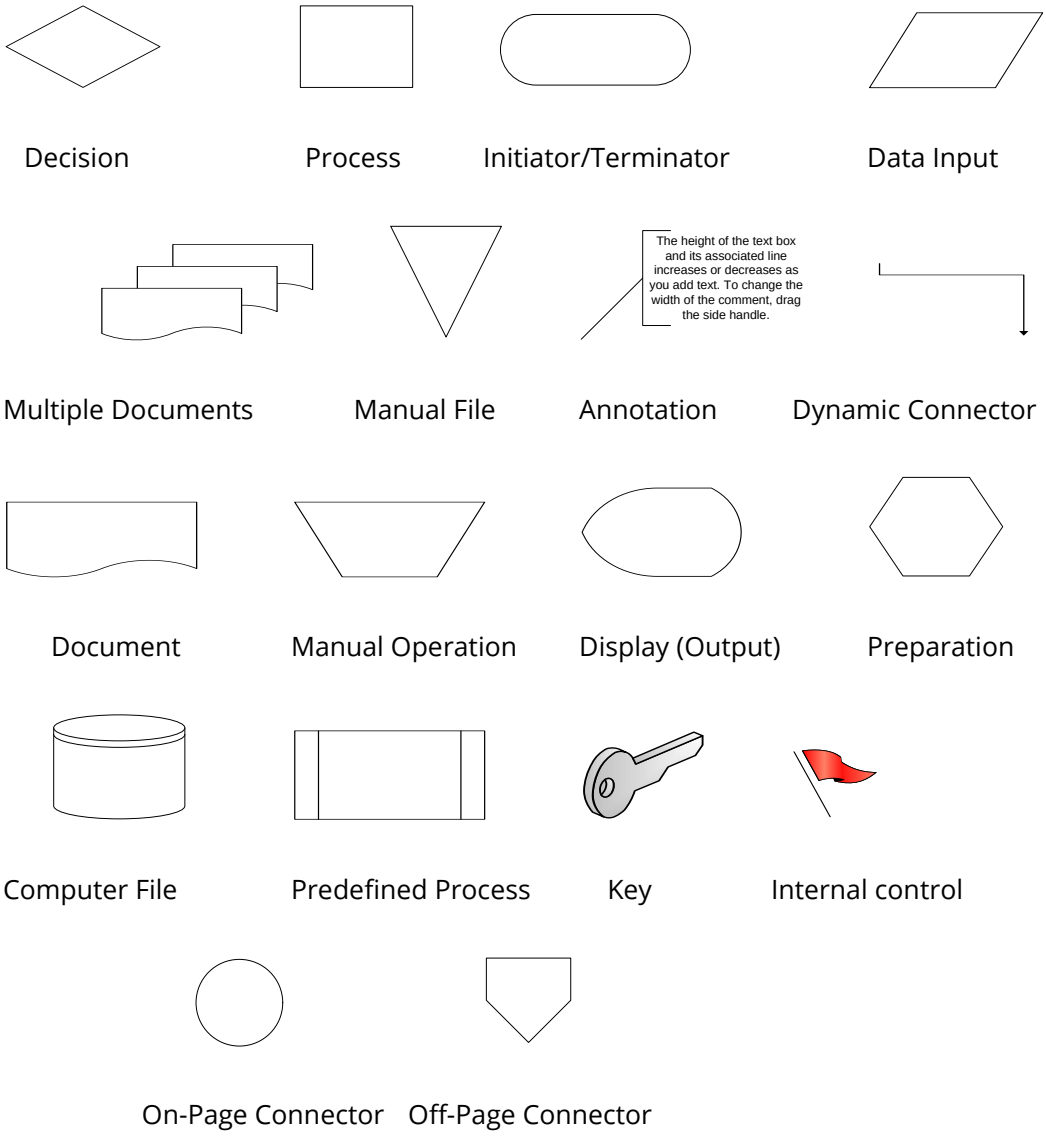
- nature of program to be audited
- financial transactions and flow of resources
- internal controls relative to the audit objectives
- information systems
- reports provided to upper management
- pertinent and applicable laws and regulations
- potential for fraud and abuse
- results of previous audits

The most frequently used surveying techniques are: questionnaires, reviews of executive or management reports to TDOT management, interviews of personnel, direct observation of work processes, process walkthroughs, reviews of contracts and procedure manuals, analysis of financial and non-financial trends, and benchmarking to other similar entities.

The Auditor's preliminary work should be documented by detailed narratives, process-flowcharting, or any other acceptable method. The information obtained will be used to prepare the ***Process Risk Assessment*** and ***Planning Memorandum***. During the survey applicable work processes should be documented in a flow chart.

7.2 Process Flowcharts

The TDOT Office of Internal Audit has devised a standard set of symbols and a flowcharting format that will be used for creating visual representations of process flows.



Source: TDOT Internal Audit

Symbol Application:

A. **Decision** - Indicates a question or branch in the process flow it shows a point in the process where a decision is made that leads to different processing steps.

B. **Process** - Shows a process or action step.
C. **Initiator/Terminator** - Terminators show the start and stop points in a process. When used as a Start symbol, terminators depict a *trigger action* that sets the process flow into motion.
D. **Data Input** – Indicates inputs to a process, usually in a computer environment.
E. **Document** – Indicates production of a tangible document.
F. **Multiple Documents** - indicates production of multiple tangible documents.
G. **Manual Operation** - Shows which process steps are not automated.
H. **Manual File** - Denotes a storage location, generally for hard-copy documents, such as a filing cabinet. It may also be used to represent a temporary storage such as a drawer or even a clipboard.
I. **Preparation** – Any process step that is a preparation process flow step, such as a set-up operation.
J. **Display (Output)** – Indicates a process flow step where information is displayed to a person (e.g., PC user, machine operator).
K. **Predefined Process** – Indicates a process step or series of process flow steps that are formally defined.
L. **Computer File** – The most universally recognizable symbol for a data storage location, this flowchart shape depicts a database.
M. **Annotation** – Used to add additional notes to the flowchart and reference the notes to a symbol on the flowchart.
N. **Key** – indicates a key process
O. **Internal Control** – Indicates internal control points.
P. **On-Page Connector** - Continues the flow on the same page. On-page connectors are defined with an alpha character starting with A.
Q. **Off-Page Connector** - Continues the flow to another page. Off-page connectors are defined with an alpha character and the reference to the page to which the flow is going, or the page from which the flow has come, depending on the nature of the connector.

The flow of the process should proceed from left to right and from top to bottom beginning at the leftmost corner of the sheet. ***Swim lanes*** will be utilized to represent separation of process flows through multiple functions.

7.3 Risk and Significance Assessment in Audit Planning

Risk assessment is the identification and analysis of relevant risks to achievement objectives. The purpose of risk assessment is to focus audit work on important program elements or audit areas that may be at risk. The risk assessment is completed during the planning phase and updated throughout the audit process.

While gaining an understanding of the program itself, the internal controls, information systems controls, financial flow, legal or regulatory requirements (including the potential for fraud or abuse) and the results of previous audits, auditors are required to assess the risk

and significance of each of these components in relation to the audit objectives as well as the effect each may have on the audited entity's ability to achieve its objectives. Work papers should fully document this assessment. All significant processes within the scope of the audit should be evaluated.

Identifying risks and vulnerabilities enables the audit team to determine appropriate issues for audit and maximize effectiveness. There should be no preconception of the adequacy of existing procedures and controls. In order to document the risks identified during the planning phase, a Risk Register is completed. The Risk Register summarizes and evaluates information that will be used to identify potential audit issues and develop audit programs. The Risk Register includes several elements from type of risk to mitigating controls. Some (not all) of the things that should be considered are:

- Which programs or activities are susceptible to fraud, waste, abuse, or mismanagement
- Where are the large dollar volume transactions taking place and what are the controls
- Has management expressed any concerns about specific programs, activities, or transactions?
- Areas that have inherent risks
- Prior audit observations
- Nature of transactions
- Level of internal control
- Amount and type of oversight

Additional assistance in developing a Risk Register can be found in Paul Sobel's book *2007 Auditor's Risk Management Guide: Integrating Auditing and ERM*, chapters 7 through 10.

7.4 Consideration for Fraud

In planning the audit, auditors should assess risks of fraud occurring that is ***significant within the context of the audit objectives***.

7.4.1 Fraud Risk Assessment

Audit team members should utilize the fraud risk assessment form to inquire with management of the audited function any known instances of fraud within the program, the auditees understanding of departmental ethics requirements, knowledge of departmental policy on fraud, and concerns regarding existing (or non-existent) internal controls within the function's scope of activities.

7.4.2 Fraud Roundtable

Audit team members should discuss among the team fraud risks, including factor such as individuals' incentives or pressures to commit fraud, the opportunity for fraud to occur, and rationalizations or attitudes that could allow individuals to commit fraud. Auditors should gather and assess information to identify risks of fraud that are significant within the scope of the audit objectives or that could affect the findings and conclusions. For example, auditors may obtain information through discussion with officials of the audited entity or through other means to determine the susceptibility of the program to fraud, the status of internal controls the entity has established to detect and prevent fraud or the risk that officials of the audited entity could override internal control.

7.4.3 Professional Skepticism

Professional skepticism is an attitude that includes a questioning mind and working practices that encompass a critical assessment of audit evidence. Since evidence is gathered and evaluated throughout the audit, professional skepticism should be exercised throughout the entire audit process. An attitude of professional skepticism in assessing risks assists auditors in assessing which factors or risks could significantly affect the audit objectives. Exercising professional skepticism means that the auditor should not be satisfied with less than persuasive evidence.

7.4.4 Auditor Responsibilities

If auditors **identify factors or receive information** indicating that a fraud, significant within the context of the audit objectives, has occurred or is likely to have occurred, they should:

- Design procedures to provide reasonable assurance of detecting such fraud.
- Extend the audit steps and procedures, as necessary, to (1) determine whether fraud has likely occurred and (2) if so, determine its effect on the audit findings.

If the fraud that may have occurred is not significant within the context of the audit objectives, the auditors may conduct additional audit work as a separate engagement, or refer the matter to other parties with oversight responsibility or jurisdiction.

Assessing the risk of fraud is an ongoing process throughout the audit and relates not only to planning the audit but also to evaluating evidence obtained during the audit

7.5 Consideration of Previous Audits

Auditors must give consideration to the results of previous audits and attestation engagements that could affect the current audit objectives. TDOT Internal Audit has reading copies and/or an index of audits for at least the past five years which should be used to research for prior audit material.

7.6 Other Planning Considerations

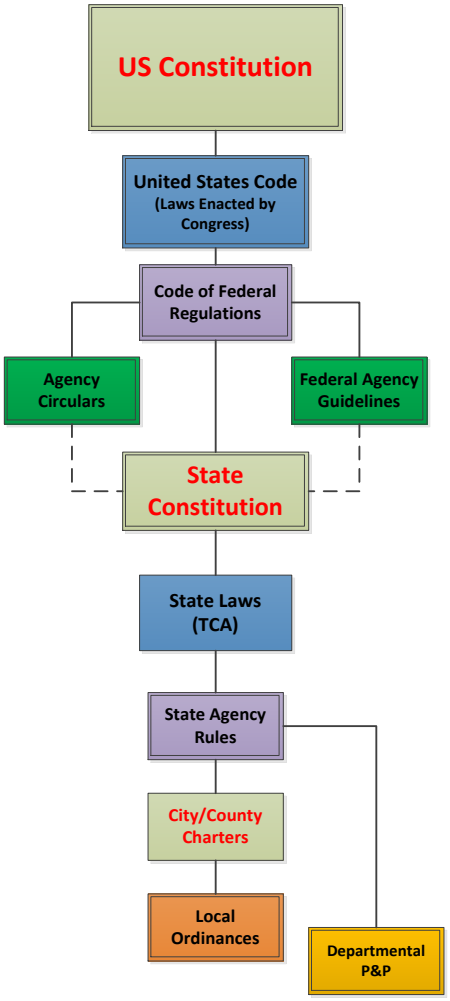
During the planning phase, consideration should be given to:

- Appropriate criteria for test work evaluation such as contracts, division procedures or best practices
- Format and location of records to be accessed

This information should be documented in the audit-planning memo.

7.6.1 Hierarchy of Criteria

The *hierarchy of laws* establishes the *supremacy of criteria* when attempting to define the overarching guidance for a particular subject matter. When establishing criteria from which to evaluate an activity, process, function, or organization, the auditor must note the overarching legislative or administrative rules that apply and use them through the objective application of the criteria. For questions regarding criteria application, it is the audit in-charge's responsibility to discuss these matters with the Principal Auditor or the Audit Director for resolution.



Source: TDOT Internal Audit

7.7 Planning Memorandum

The Planning Memo should document essential background information and present key decisions about the objectives and scope. The Planning Memo will provide an audit plan for meeting the objectives of the audit.

A Planning Memorandum should be created by the Auditor In-Charge within 30% to 40% of the budgeted project time. The attachments for the Risk Register and the Planning Memo in the electronic working paper database will include the Principal Auditor and Audit Director as a reviewer. Approval should be obtained prior to beginning fieldwork.

After obtaining approvals of the audit plan, the In-Charge Auditor is responsible for entering the specific audit program steps (Steps D-Z) into the electronic working paper database.

7.8 Directing Staff Assignment

Audit supervisors or those designated to supervise auditors must properly supervise audit staff.

The In-Charge Auditor will provide first level supervision for all audit staff assigned to the project. The Principal Auditor will supervise and direct In-Charge Auditors and as well as unassigned auditors.

The Audit Director is ultimately responsible for all audit staff and the success of each audit project and will provide such direction as required to enable accomplishment of TDOT Internal Audit objectives.

8 AUDIT FIELDWORK

Based on the results of the audit planning, the auditor develops an Audit Program that consists of the audit objectives, scope, methodology, and related concerns. The audit program includes detailed audit steps, tasks, and procedures to test if the identified controls or procedures the audited entity has in place to prevent, eliminate, or minimize identified threats are working as intended.

The Audit Program guides audit staff through the steps necessary to complete audit fieldwork. In fieldwork, auditors obtain and analyze program data and information to determine if the identified controls are working as intended. This is accomplished by completing the audit steps identified in the Audit Program. The objective of the fieldwork is to develop audit observations and put recommendations that enable the correction of an improper condition or to enable improved operational processes.

8.1 General

When completing work assigned, several factors should be considered by the auditor to ensure that the audit objectives were met. Below are listed some general statements that should be addressed prior, during, and after field work:

- Always read the planning memorandum before starting all audit work
- Ensure you have an understanding of the division, function, or process
- Approach your work and the audited entity's representations with an appropriate degree of ***professional skepticism***. Look for substantiation for representations
- Always ask questions if you do not understand something
- Ask yourself if you are doing too much work
- Ask yourself if the work makes sense
- Once you decide on an appropriate scope or sample, clear it with the In-Charge Auditor
- If you think you know a more efficient method to obtain the audit objective do not be afraid to make recommendations
- Review the entire audit program prior to beginning your work
- Before you start your work ensure that you understand the audit objective of each step, the amount and type of work each step requires, and what you will do if the results of the test are unsatisfactory
- Remember that supervisors are relying on your work and your judgment
- Your working papers should stand alone
- Never sign-off on an audit step until you have fully completed the work

8.2 Custody of Audit Work Papers

Work papers are the property of TDOT. They should remain under the control of the TDOT Internal Audit and should be accessible only to authorized personnel. **Audit reports are considered open records**; however audit working papers are considered sensitive and appropriate care should be taken to prevent disclosure to individuals making an official public records request. TDOT Management and other members of the organization may request access to audit work papers. Such access may be necessary to substantiate or explain audit observations or to utilize audit documentation for other business purposes. Sharing of work papers, which do not contain confidential information, with audit client management is encouraged. Other requests for access to work papers are subject to the approval of the Audit Director or Principal Auditor.

8.3 Work Papers with Confidential or Sensitive Information

The auditor **shall not** publicly disclose any information received during an audit that is considered proprietary in nature by any local, state or federal law or regulation. Sensitive observations or any information likely to result in increased attention should be safeguarded and only discussed with TDOT Internal Audit personnel assigned to the project or appropriate personnel within the audited entity. Care must be taken to ensure audited entity information is not discussed within hearing range of others (such as in hallways, elevators, restaurants or outside.) When in doubt whether information should be safeguarded, consult with the Principal Auditor or the Audit Director.

When confidential information (such as individuals' names linked with their social security numbers, health related conditions linked to personally identifiable data, juvenile court records, bank account information) must be included in audit working papers, minimize the volume of information retained. Whenever possible, you should redact all personally identifiable information in the work papers. All documents or electronic files containing confidential information should be labeled and secured at all times. Confidential electronic files should never be stored on portable storage devices (flash drives), compact disks/DVD media, or transmitted by e-mail.

8.4 Security of Audit Work Papers

While an audit is in progress, the work papers must be safeguarded to ensure that they are not misplaced, stolen, altered, or obtained by unauthorized personnel. After the audit is completed, work papers are to be maintained electronically in the work papers folder/database or in a secured location.

Extraneous documents and electronic files should be disposed of after the project is finalized and the report is released to the Commissioner and Deputy Commissioner/Chief Financial Officer. If the hard copy documents contain confidential or sensitive information, they should be shredded.

8.5 Documenting Work Papers

Auditors must prepare audit documentation related to planning, conducting, and reporting for each audit. Auditors should prepare audit documentation in sufficient detail to enable an experienced auditor, having no previous connection to the audit, to understand from the audit documentation the nature, timing, extent, and results of audit procedures performed, the audit evidence obtained and its source and the conclusions reached, including evidence that supports the auditors' significant judgments and conclusions.

The degree of documentation is based on the judgment of the individuals responsible for forming an opinion, the nature of the project, and the adequacy and effectiveness of the system of internal controls. Audit documentation should be economical to prepare and review. Work papers should be complete but concise and usable as a record of work performed. Auditors should include in their work papers only what is essential and they should ensure that each document included serves a purpose that relates to an audit objective or procedure. Work papers should be prepared for the ease of use by the team members and the reviewer.

Each work paper prepared by the auditor should include:

- Audit project number and project name
- Work paper number and title
- Prepared by
- Prepared date
- Data source

Furthermore, audit documentation should include the objective, source, scope, criteria, work performed, results, and conclusion of the audit procedure as follows:

PURPOSE: This should consist of a "brief" description of the purpose for the particular working paper. This can best be accomplished by explaining what is expected to be accomplished and why.

SCOPE: This should establish the boundaries for time frame and the population being reviewed. This may include "as of date", date range, number of transactions in the total population, and number of transactions tested.

CRITERIA: This should include the specific regulations, procedures, business practices or other standards that are relevant to this audit procedure.

WORK PERFORMED: A full explanation of the work done to accomplish the objective. It should include a description of the sample selection and methodology. Additionally, it should describe the system name, report, and parameters used to extract information from computer applications. Consequently, this is where 95% of each working paper's documentation should reside.

REFERENCE SOURCES: This should include a listing of all reference sources (e.g. name, position, phone number, email address, etc.) interviewed or consulted in conjunction with the procedures section below. It should also include any computer application, web site references, regulations, procedures, or other documents/references that are relevant to this audit procedure.

RESULTS and CONCLUSIONS: Description of applicable test paper results and any exceptions and reasons for the exceptions. The amount of detail will depend on whether there are observations (i.e., a finding usually equals more detail). For less significant weaknesses noted, indicate the reason why the issue is not considered to be significant and how it is disposed of, such as: (1) no exception was noted, or (2) issue was communicated to management during the project status meetings.

Conclusions should consist of a "brief" statement on the overall adequacy and effectiveness of the internal controls tested within the working paper. If no significant errors were noted, then conclude that the internal controls appear to be adequate and effective. If there were exceptions, adjust the conclusion accordingly; as appropriate refer to audit observations.

When the preparer signs off, it signifies that the paper is ready for review; however, the preparer should also notify the reviewer either verbally or by email.

Any work saved to the hard drive of a computer while in the field should be transferred to a network drive at the earliest possible occasion. Daily back-ups should be created until the work papers can be transferred to Office of Internal Audit shared network drive. Sensitive or confidential information should not be saved on the auditor's laptop hard drive.

In very limited instances hard-copy or manual work papers will be maintained. These supporting work papers should be bound and cross-referenced.

8.6 Statistics and Sampling

Statistics and Sampling are complex subject matters that are important in developing an understanding of the data. Applying the principles of statistics, OIA can test a relatively small sample that enables the office to draw conclusions about a test population with measurable reliability. Sampling uses a small part of the population to determine parameters and characteristics of the whole population. It is the policy of the OIA to utilize statistical, rather than non-statistical, sampling whenever applicable and reasonable.

It is imperative that the auditor consider that:

- A sample MUST represent the population for sampling to be valid.
- A population MUST be complete for sampling to be valid.
- Sampling MUST take into account the cost/benefit consideration.
- The auditor MUST design the sampling methodology to fit the testing objectives.

WHAT OIA SAMPLES:

ATTRIBUTES	**VARIABLES**
Have qualitative underlying variables	Have quantitative underlying variables
Answer "yes/no" questions, e.g., "Are you male"?	Answer numeric questions, e.g., "How many males"?
Do not assert degree, "I am twice as male."	Make assertions of degree, e.g., "I am twice as old."
Group information into classes	Do not group information into classes
Are discrete	Are continuous
Are finite	Are infinite
Use the mode (frequency) to measure central tendency	Use the mean (average) to measure central tendency
Cannot be less than 0%	Can be less than 0
Cannot be greater than 100%	Can be greater than 100

TYPES OF SAMPLING

Random Sampling – Confirmatory

- ***Simple Random*** – random sampling of a homogenous population
- ***Stratified Random*** – breaks the samples into strata within a given group; groups are determined by their members' similarities
- ***Cluster (Area)*** – group samples by spatial arrangement.

Purposeful Sampling – Exploratory AKA non-statistical sampling is used to evaluate characteristics of the population; cannot be used to infer valid assertions about a population.

PRIMARY AUDIT SAMPLING METHODOLOGIES

Attribute Sampling – are utilized when testing internal controls or when testing compliance. This method can be used to confirm or reach a conclusion about a population, proportion, percentage, or total number of items.

- **Discovery/Acceptance Sampling** – used to identify critical errors or irregularities in a population when the occurrence rate is assumed to be zero (discovery) or close to zero (acceptance), such as for fraud detection.
- **Attribute Estimation Sampling –** used to identify critical errors or irregularities in a population when the occurrence rate is assumed to be high (> 10%).

Variable Sampling - used to confirm and reach conclusions about a population in terms of dollar amount in the context of substantive testing (reasonableness). Used when amounts are more important than rates.

Monetary Unit Sampling (PPS)- uses attribute sampling to estimate dollar amounts; increases the likelihood that larger amounts are selected and tested.

Sampling Strategies

- **Systematic (Interval) Sampling** – sample selection by taking the n^{th} item in the population.

- **Stop and Go (Sequential) Sampling –** used when the objective is to minimize sample size. Multiple samples are taken and the criteria for selecting subsequent samples are determined by the results of the prior sample

Elements of Sampling Mathematics

Confidence Level - Relates to the percentage of times the sample is within the specified margin of error (how it accurately represents the population). The auditor must note that there is no way to ensure that any given SINGLE sample is representative and most likely, we will not utilize multiple sampling (repetition). So in order to gain more "confidence" in our sample, the best method is to increase the sample size.

As a standard practice, the OIA utilizes a 95% confidence level for sampling and statistical assessment in all fieldwork testing conducted, whether testing attributes or variables.

Alpha Risk - This is the risk of stating that controls or balances are incorrect when in fact they are not

- **In Attribute Sampling - represents** the risk of under reliance.
- **In Monetary Unit Sampling -** the risk of incorrect rejection.

Beta Risk - This is the risk of stating that controls or balances are correct when in fact they are not.

- **In Attribute Sampling -** represents the risk of over reliance.
- **In Monetary Unit Sampling -** the risk of incorrect acceptance.

ALPHA RISK VERSUS BETA RISK		When, in Fact, They Are	
		Good	Bad
Tests Say Controls Or Balances Are	Good	Correct	Beta Risk
	Bad	Alpha Risk	Correct

Standard Deviation – indicates the spread of the data in a population or a sample.

Tolerable Error Rate - indicates the maximum acceptable error rate or upper error limit.

Expected Error Rate – (p-hat) relates to the percentage of the population being sampled expected to be in error or non-compliance. Usually based on past experience (also called expected population deviation rate), if not determined use 50%.

Desired Precision (Margin of Error) – Relates to the amount of deviation from the estimate the tester is willing to accept.

Post Sampling Tests

The GAO has established a criterion test for sampling precision called the "relative error" of the sample.

$$\textbf{\textit{Standard Error}} = \frac{\textbf{\textit{Sample Standard Deviation of the Sample}}}{\sqrt{\textbf{\textit{Sample Size}}}}$$

- Where the Sample Standard Deviation of the Sample is:

$$= \frac{\textbf{\textit{Standard Error of the Sample}}}{\textbf{\textit{Sample Statistic}}}$$

- Where the sample statistic is the attribute error percentage (for attribute testing) or sample mean (for variable testing)
- Attribute error percentage is = $\boldsymbol{\theta} = \sqrt{[\boldsymbol{p}(\mathbf{1}-\boldsymbol{p})\boldsymbol{n}]}$
- If not within 15%, the results may be considered unacceptable and the expected error rate must be decreased.

Methods for Estimating Population Parameters Based on the Sample Statistic

I. Control Method
II. Attribute Estimation Method
III. Ratio Method
IV. Mean-per-unit Method
V. Difference Method
VI. Regression Method
VII. Extrapolation

It is imperative that the auditor consider that:

- Both alpha and beta risks represent the probability that the sample is not representative
- The confidence level, the alpha and the beta risks, precision, and tolerable rate are set by the auditor.
- There are no standard methods for sampling, estimation, or extrapolation exists; methods must be tailored to the project objective.
- Systemic problems create sample biases.
- Multiple methods are always better than singular processes
- Sampling results should never form the sole basis of an assertion
- Always report an error rate and an error amount
- Extrapolations should provide information regarding the upper and lower limit.

8.7 Documenting Sample Selection

The sample should include all of the columns that were in the original data file. However, the test work may require only a fraction of those columns (i.e., name, voucher number, voucher date).

The description of the sampling selection methodology should be adequate such that a reader is able to repeat the sample selection based on the information provided. The sample selection information can be included in the test work narrative; however a sample selection chart may also be used. The following elements are to be documented:

- **Test Objectives** – Describe what is to be accomplished by performing the testing.
- **Population Description** – Describe the entire population from which the sample will be pulled, including the size of the entire population in the audit period.
- **Sample Size** – Identify what quantifiable number of items will be tested. And, how the decision was made for the size to be tested.
- **Sample Selection Criteria** - Describe in detail how the actual sample was selected. State whether the sample was selected randomly or judgmentally.

Note: A random sample must truly be random where a random number generator is used and judgmental actions are avoided. A judgmental methodology incorporates other considerations or anomalies such as higher dollars, divisional account, or responsible party groupings.

There may be instances where MS Excel, Audit Command Language (ACL) or other computer assisted audit techniques are used in the sample selection process. If ACL is used to select a sample, the elements described above should still be documented. The ACL log information can be used as additional support for the sample selection process.

8.8 Test Work Paper Format

Each test should be well thought out and documented in a logical manner. It may be necessary to have a team meeting to discuss test work and the best way of documenting the tests.

Test work papers will usually be documented in Microsoft Excel worksheets. Ideally, the file will include separate tabs for:

- the original population
- the sample to be tested
- the test work and summary of exceptions
- the narrative describing the test work

To provide concise, clear and organized documentation of the testing performed and the results achieved, test work papers should also include the documentation work paper elements identified in section 4.3 above.

General guidelines to follow:

- The spreadsheet should be formatted so that it can be printed cleanly on one page, if possible, using a 10 point or larger font size.
- Only relevant columns of original data should be included in the test spreadsheet.
- Sample item numbers are sequential numbers and placed in the left column of the schedule.
- All cells should be filled in. Information not available or not applicable should be designated as “n/a”.
- Prepare columns effectively to correspond to the audit program. Each testing attribute will usually be a single column in the test paper. If the attribute is better understood by including several columns for the specific test in order for additional information to be shown, then include several columns. For example, instead of just “deposits made timely,” columns could be included to show the “date of cash receipt,” “date of deposit,” and “calculated number of days for deposit to be made.”

The auditor should discuss with the In-Charge Auditor the degree of column headers.

- A comment column for additional information, such as pointing out specific anomalies, may be used.
- Tick marks can be used to identify the source or purpose of data contained in the spreadsheet. **Microsoft Word has an extensive selection of symbols that may be inserted as tick marks.**
- **Exceptions should be noted by a letter, usually beginning with "A". The explanation in the legend on the work paper may be brief if a more expanded description is placed in the Summary of Exceptions.**
- The Exception Legend should be referenced to the Summary of Exceptions. "Exception cleared" may be stated after the exception explanation in the exception legend.
- **Notes are labeled by a superscript number**. Notes are not exceptions from the testing performed, but represent modifications or variations to the audit program or procedure which are necessary to complete the audit step. **Notes may also be further explanations of conditions noted**. In some cases it might be necessary to obtain documentation to support the note. Reference to the supporting documentation may be indicated in the Comment column for the sample item number or in the Notes Legend.
- Tick marks, exceptions, and notations should be in bold font or highlighted in some manner and should be identified in a legend.

8.9 Work Paper Tick Marks

Tick marks are used to simplify documenting work completed and conditions found usually during fieldwork. A legend that defines each tick mark should be provided and located near the tick marks used. If the tick mark legend is not in the working paper where the tick mark is used, then the working paper should be referenced to the tick mark legend.

Tick marks should be concise and should adequately explain the results of the audit procedure performed. It should be evident to the reader as to whether or not an error or weakness was noted. Items tested should never be left blank.

The Office of Internal Audit utilizes a standard set of tick marks for commonly used actions. All tick marks are to be in RED. Tick mark explanations should be in pencil or computer generated. Seen below is some of the standard tick marks used throughout the audit cycle.

Symbol:	Denotes:
☑	Footed
⊠	Cross-Footed
⊠	Agreed to the GL
♏	Not Material
✉	Provided by Auditee
✪	Not Applicable
⌖	Calculated
☮	Data Obtained from Information System
✸	Data Provided by External Parties
❖	Created by Auditor

Figure 1 – TDOT Internal Audit Standard Tick Marks

8.10 Summary Work Paper

Auditors must obtain sufficient, appropriate evidence to provide a reasonable basis for their observations and conclusions.

A summary work paper may be used to synopsize the data contained in supporting work papers relative to the audit objectives being accomplished. The process of summarizing focuses on the important and relevant details and is not a complete re-telling of the information.

Summaries provide a logical flow between the related supporting work papers and can facilitate report writing and the review process. The summary should note any issues or observations from the test work and should direct the reader to Section C "Audit Observations".

Each audit step for the project should have a Narrative or Summary. This may not be necessary if only one audit procedure was performed to satisfy a conclusion for a specific objective.

8.11 Audit Issues and Observations

During the planning and test work phases, potential audit issues will be logged into the electronic folder or the EWP as audit observations and will be cross-referenced to the

appropriate audit work paper. **Auditors will communicate these issues to the audit client**.

After discussion with the audit client, the issues will either be cleared or will be fully validated. When an issue is not cleared, care should be taken to adequately develop an audit finding. Auditors should report observations by providing credible evidence that relates to the audit objectives. These observations should be supported by sufficient, competent, and relevant evidence. They also should be presented in a manner to promote adequate understanding of the matters reported and to provide convincing but fair presentations in proper perspective. The finding should provide selective background information to provide the context for the overall message and to help the reader understand the finding and significance of the issues discussed.

To the extent possible, in presenting observations, auditors should develop the elements of condition, criteria, cause, and risk/impact (effect) to assist officials of the audited entity or oversight officials of the audited entity in understanding the need for taking corrective action. The four elements of a well-developed audit finding are:

Condition	What was found?
Criteria	What standard applied? (Reference and detailed description of what should have been found)
Cause	Why did it happen? (be sure to get the "root" cause)
Risk/Impact/Effect	What happened or could happen? Dollar value? Effect on service delivery?

The Audit Team should work with management to develop sound recommendations for audit observations. Cost effective recommendations that will add value to TDOT should be developed for each finding. A sensible corrective action plan should be agreed with by the audit client management. Discussions regarding planned actions to address the recommendations should be documented.

Observations deemed not material to the overall objectives of the audited entity and presenting only insignificant risk to TDOT, will not normally be included in the report; but, may be provided to audited entity management in a "Management Letter". Management Letters are public information.

In order to track accepted audit recommendations for follow-up, the observation must be recorded after they have been approved.

8.12 Work Paper Review

Work papers should be reviewed as soon as they are prepared to provide timely feedback to the preparer.

Prior to the beginning of the fieldwork phase, all documentation pertinent to the administrative and planning phases should have been entered into the work papers binder and database and reviewed.

All work papers will have a minimum of one level of review. The In-Charge Auditor should review all documentation prepared by the audit team. The Principal Auditor will review documentation prepared by the In-Charge Auditor. Work papers prepared by the Principal Auditor will be reviewed by the Audit Director. This will ensure accurate and sufficient information for planning and performing the audit.

While content is more important than format, the reviewer **will verify**:

- All planned objectives and supporting audit steps were completed or justification provided for exclusion.
- Work papers are sufficient, accurate and reliable.
- The conclusions reached were reasonable, logical, and valid.
- Observations have sufficient and appropriate supporting documentation based on the significance of the issue.
- The working papers were prepared in accordance with GAGAS standards and TDOT Internal Audit procedures.

The reviewer will record significant comments in the work papers. The preparer will need to respond to the comments and sign-off. The reviewer sign-off signifies that corrections were adequately performed.

8.13 Issues Needing Further Study

If, during the audit, auditors identify significant issues that warrant further work, but the issues are outside the scope of the current project, they should document the issue and discuss it with the Principal Auditor or Audit Director. The Audit Director will make final decisions whether to expand the scope of the audit, add the issue to the audit plan as a separate audit, or retain the information for future risk assessments.

8.14 In-Process Review of Fieldwork

Near the end of fieldwork (90% of budget field work hours complete) the Auditor In-Charge will prepare documentation and meet with the Principal Auditor and Audit Director to discuss the audit project progress. The documentation will:

- Provide an answer to each objective

- List the scope area, observations with root cause and risk/impact
- Describe the communications with client management (whom and how)
- Validate auditor and calendar days to complete draft report

8.15 Meeting with Audit Client Director

After the Fieldwork In-Process Review, the In-Charge Auditor and/or Principal Auditor will meet with the Division Director and/or Deputy to discuss the progress of the audit to date.

8.16 Identification of Fraud or Other Activities

If an auditor discovers a situation where possible fraud or other questionable activity has likely taken place, notification should be made immediately to the In-Charge Auditor. Once it is determined by the In-Charge Auditor that a problem likely does exist, the In-Charge Auditor should immediately notify the Principal Auditor or Audit Director. The following are possible concerns:

- An illegal act that is a violation of a law, and or a regulation
- Noncompliance of a provision of a contract or grant agreement
- Abuse - when the conduct of a government organization, program, activity, or function falls far short of societal expectations for prudent behavior

The Principal Auditor or Audit Director will make a determination whether additional work needs to be performed or whether audit procedures should be suspended as a result of the concern. If necessary, the Audit Director will report the irregularity to the Commissioner or the Deputy Commissioner/Chief Financial Officer, the TDOT Legal Counsel, or the Tennessee Comptroller of the Treasury. If the incident appears to be criminal in nature, the appropriate law enforcement agency will be notified.

9 REPORTING

Auditors must issue audit reports communicating the results of each completed performance audit.

After every engagement, a draft report (or other form of communication) is completed. The draft report is completed by the audit team (main responsibility to the Auditor-in-Charge) and preliminarily reviewed by the Principal Auditor. Final review is completed by the Director of Audit. While the reporting format is standardized, some variation exists based on the type of engagement.

Characteristics of a Well-Written Report:

- ***Significant*** – significance indicates that matters included in the final report be impactful in effect (e.g., dollar value, lost productivity, public endangerment, etc.).
- ***Useful*** – indicates that a report is structured to the interests, needs, and, benefits of the users.
- ***Timely*** – reports should be issued with alacrity to enable prompt use of the information for decision making.
- ***Accurate*** – infers that the information presented is supported by objective evidence that was verified and passed the quality assurance processes.
- ***Complete and Concise*** – reports should contain clear and sufficient information to facilitate the reader's understanding yet succinct but simple enough not to clutter the facts with unrelated, insufficient, or excessive verbiage.
- ***Persuasive*** – reports should be written in a convincing tone and a respectful manner. Conclusions and recommendations should follow a logical train of thought derived from the facts. The information presented in the report should explain the significance of the findings, the reasonableness of conclusions
- ***Objective and Balanced*** – audit reports should be presented in a fair and impartial manner; without exaggerations or undue emphasis on deficiencies. The report should contain complete information to provide the reader with the proper perspective and the tone should be constructive to illicit a favorable reaction to the recommendations

All audit reports will be prepared in accordance with *Government Auditing Standards* unless full compliance is inhibited and a qualified statement is required. When the audit does not comply with applicable GAGAS requirements, due to scope limitations, restrictions on access to records, laws, regulations, or other issues impacting the audit, the in-charge auditor will document the departure from the GAGAS requirements; how the departure impacted the audit, and the conclusions in both the work papers and in the report.

9.1 Audit Draft Report Overview

The In-Charge Auditor will provide a cross-referenced draft report to the Principal Auditor, who is responsible for reviewing supporting working papers and refining the draft report. All significant information should be cross referenced to the appropriate work paper of reference document. The Principal Auditor will provide the draft report to the Audit Director who will authorize its release to the audit client. An exit conference will be schedule to discuss the issues identified in the audit draft, and, ideally, agree upon a plan of action. Management of the audited entity will be given ten (10) business days to return their written response at which time the Final Audit Report will be issued.

"Discussion Drafts" (issued prior to the Draft report) may also be utilized. Such documents may be used from time to time in order to determine approximate levels or agreement or disagreement on audit observations and flush out additional information from the audited entity.

9.2 Audit Draft Report Template

The audit draft report should utilize the audit draft template which contains the following sections: Introduction, Observations and Recommendations, and General Audit Information. The In-Charge Auditor should obtain the current TDOT Internal Audit report template from the Director of Audit. The report should use the "Century" font with size "11" and should contain only one blank space after a period.

9.3 Introduction

The Introduction section contains a brief discussion of the audit and why it was performed. It contains sub-sections for project description, background, and objectives. If other matters need to be discussed, a sub-section for other matters is appropriate.

- The Audit Project Description sub-section will be captioned to identity the name of the function, contract, etc., that was audited. It will include a brief description of the audit project and the significance of the audit.

- The Background sub-section is used to provide information not otherwise obvious to the reader, but necessary to put audit observations in perspective. The background may include a brief description of the activity mission, operation, and magnitude along with information pertinent to request audits, follow-up audits, and audits with prior interim reports issued on the same audit area.

9.4 Objectives and Conclusions

Audit Objectives will be identified from the audit planning memorandum. Each objective will be written in a format such that it can be answered with "Yes", "No", "Generally yes", "Generally no", and "Indeterminable". Objectives describe the work conducted and results of the work performed to meet the objectives outlined.

Conclusions will answer the objectives with "Yes", "No", or "Yes, except for…" For audit conclusions that are indeterminable, other qualitative factors may be utilized to fully assess the activity, transaction, process, or function that is being audited.

Objective Response	Response Description	Quantitative Algorithm
Yes	Audit conclusions, in response to audit objectives that fall into this grade results from predominantly affirmative test results	Test results indicate ≥ 95% affirmative rate. Conversely, test results might indicate ≤ 5% exceptions
Generally yes	Objective responses falling within this category are predominantly affirmative with a few negative exceptions	Test results indicate a response factor that is < 95% but > 50% affirmative
Generally no	Objective responses falling within this category are predominantly negative with a few affirmative exceptions	Test results indicate a response factor that is < 95% but > 50% negative
No	Audit conclusions, in response to audit objectives that fall into this grade results from predominantly negative test results	Test results indicate ≤ 5% affirmative rate. Conversely, test results might indicate ≥ 95% exceptions
Indeterminable	Audit conclusions, in response to audit objectives that fall into this grade results from equivalent affirmative and negative test results	Test results indicate a response factor that is = 50% affirmative or negative

9.5 Observations and Recommendations

The Observations and Recommendations section will follow the Introduction section.

- Observation—each observation will be consecutively lettered beginning with "A"
- Background—will provide additional information pertinent to the finding.
- Discussion—this section should include the criteria, root cause, and effect. Complex issues may require sub-captions in this area.
- Recommendation—each recommendation will be marked with the letter of the finding and consecutively numbered, i.e. "A-1", "A-2". Multiple recommendations and responses may be grouped together or listed individually as needed.

- Management Response will be summarized here, and will point to the appendix containing the verbatim response.
- Summary of Management Response -- briefly state management's concurrence or non-concurrence, and identify the location within the report of the complete Management Response Template.
- Evaluation of Management Responses—if management does not concur, an evaluation of their response is required by the standards. This section can be deleted if not needed.

9.6 General Audit Information

The General Audit Information section will contain sub-sections for Statement of Compliance, Scope and Methodology, and Staff Acknowledgement.

- ***Statement of Compliance with GAGAS***. Use the following wording for an unmodified compliance statement:

  > We conducted this performance audit from ___ to _____, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our observations and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our observations and conclusions based on our audit objectives. Our audit included tests of management controls that we considered necessary under the circumstances.

  If GAGAS were not followed, the statement must be modified to explain the departure from standards.

- ***Scope and Methodology***. Scope is the extent of coverage or the time period covered by the audit. Methodology describes in detail how audit objectives are accomplished. If the audit involved sampling, specify whether statistics, haphazard, or judgmental sampling was used, the size of the sample, what was sampled (line items, units, transactions, etc.), dollar value of the sample size, and time period relating to the universe from which the sample was selected. If the sample includes only data with special characteristics or within certain parameters, the characteristics or parameters should be identified. It is desirable to also identify the size of the universe if it can be determined with minimum effort and if the results can be extended to the entire population. The auditor should also describe comparative techniques and criteria used to evaluate test work.

- ***Staff Acknowledgement*** will list the names and credentials of the audit team. The list will identify the project Quality Assurance.

9.7 Exclusion of Confidential Information

When dealing with sensitive or confidential information, options for reporting are available. Sensitive or confidential information may be deleted in certain cases or limited-official-use reports may be issued. Tennessee Code Annotated § 10.7.504 provides exceptions to public records containing confidential information.

9.8 Audit Draft Report Formatting

The Audit Draft template form has the "Draft" watermark imbedded in the background of the document. The background will contain the "Draft" watermark until the transmittal letter is prepared by the Audit Director and the report is ready for release.

The "track changes" feature may be used when revising a document prepared by another person. In the word processing software, go to "Review" and select "Markup". Revisions and comments will need to be accepted and the "track changes" feature will need to be disabled before sending or printing the document.

9.9 Audit Draft Report Reviews

The preparer of the draft report will provide a copy to project Quality Assurance or to the Principal Auditor who will review and refine the draft as needed and will use the "track changes" feature to highlight revisions that are made. These changes will be accepted by the preparer. The Principal Auditor will provide a "clean" copy of the report to the Audit Director who will also use the "track changes" feature when revising the work of another. The changes will be accepted by the Principal Auditor.

The Principal Auditor should remove the "Track Changes" using the remove hidden data add-on feature of Microsoft Word. Additionally, only one prior version of the draft report should be retained, all other versions should be deleted.

9.10 Audit Draft Report Cross Referencing

The audit draft report must be cross-referenced to the supporting work papers retained in the electronic working paper folder/database. The cross reference will include work paper number, sub-page number, and in some instances section or paragraph number. The test of a well cross-referenced report is that an independent person not involved in the audit is able to vouch the information included in the report to the supporting work papers and verify all statements of fact. The Principal Auditor must ensure that these cross-referencing procedures are followed so that reports can be promptly verified and issued.

9.11 Independent Verification of Draft Report

The Principal Auditor will provide a cross-referenced copy of the draft report to the Audit Director for verification prior to the draft report or discussion draft report being issued to the audited entity.

a) The verifier's responsibilities are to ensure that:

- Numerical data and computations in the report (including supporting schedules, tables, graphs, etc.) are mathematically correct and/or factually supported in the working papers
- Comments and conclusions are consistent with the facts developed
- Statements of fact, and the report as a whole, are expressed clearly, understandably, and in proper tone

b) Verifiers must go beyond the summary schedules and finding sheets to source documents in making their verifications of the information reported. However, they are not responsible for the scope of the audit, the quality of the work, or the content and organization of the working papers or report. These are the responsibilities of the Principal Auditor.

c) The verifier must initial next to each item verified. If anything in the report is questionable, it should be noted on the report. The verifier should note any unsupported information along with any questions or comments.

d) After verification is completed, the cross referenced draft will be given back to the responsible In-charge Auditor. The In-Charge Auditor shall make needed changes.

e) After the verifier ensures that changes were made, he/she will sign the first page of the draft. A scanned copy, which includes the sign-off, will be included or attached in the electronic folder

9.12 Exit Conference

The In-charge Auditor will arrange an exit conference at the conclusion of fieldwork to review audit observations with key individuals impacted by the audit observations. **Exit conferences should not focus merely on areas with significant issues; those areas performed in a notable or exceptional manner should also be discussed.**

The time frame for receiving management's response should be discussed and agreed upon. Generally, the response should be received within 10 workdays. A work paper documenting the exit conference should be included in the audit program 'Section B – Reporting'. It is expected that the Principal Auditor or the Audit Director attend the exit conference.

9.13 Management Response Template

The In-charge Auditor will prepare the management response template based upon observations in the draft report and an example transmittal letter from the audit client Director to the Director of Audit. The template will contain a summary of the audit observations and recommendations with space for management comments and the proposed action plan.

9.14 Audit Draft Report Distribution List

After the exit conference, the Principal Auditor will provide a copy of the draft audit report and the response template to the Director of the Audited Entity, Legal Counsel, and any other Director / Function that may be impacted.

The agreed-upon time frame for receiving management's response should be re-iterated in this communication.

If you provide the draft report electronically, be sure to remove the "Track Changes" using the remove hidden data add-on feature of Microsoft Word. Additionally, all prior versions of the draft report should be deleted.

9.15 Untimely Management Response

If management response is not received within the agreed upon time frame, the Principal Auditor must determine the cause and decide if additional time is needed.

If the response to the draft report is not received, the Audit Director should notify the Commissioner and the Deputy Commissioner/Chief Financial Officer that the report will be issued without a response. At the end of the 3rd day after such notification, the audit report can be issued with the following statement: "**Comments were not received prior to report publication**."

9.16 Internal Transmittal Letter

The Principal Auditor will prepare a transmittal letter to be printed on TDOT Internal Audit letterhead. The transmittal letter will be addressed to the director of the audited entity. It will include:

- An opening paragraph describing the audit and whether it was conducted as part of the annual audit plan or management's request. It will include the following verbiage:

  "This report is intended for the information of the Commissioner, Bureau Chief, and management of the Tennessee Department of Transportation; however, this report is a matter of public record, and its distribution is not limited."

- An acknowledgement of audited division's effort and cooperation

9.17 Final Report Distribution List

The final audit report will be distributed to the following:

- The Commissioner of TDOT
- TDOT's Deputy Commissioner/ Chief Financial Officer
- Director or Chief of the Audited entity
- Bureau Chief of the Audited function
- The Comptroller of the Treasury
- Others parties within TDOT, as needed

9.18 Final Audit Report

The final audit report should contain all the elements required by the draft, plus the executive summary, table of contents, and management response template. If management response is in conflict with the report observations, recommendations or conclusions, the report should include a section for the auditor's evaluation of management's response. Additionally, a transmittal letter should be prepared for the Auditor's signature.

9.19 Executive Summary

The executive summary will be no more than one page. It shall be printed on the front inside cover of the report. It will provide a re-cap of why the audit was performed—as part of the audit plan or at the request of the Comptroller's office, Senior Leadership, Division Directors, or other management functions. It will state the objectives, summarize the conclusions reached by auditors and include the recommendations. It will also summarize management's concurrence with the audit conclusions and recommendations.

If management has already implemented corrective action, this should be brought to light. Outstanding accomplishments of the audit client may also be presented in this section.

9.20 Table of Contents

The table of contents lists the major sections of each audit report and the page numbers

- **Introduction**
  - Audit Initiation
  - Background
  - Other (if applicable)

- **Objectives and Conclusions**
  - Objectives and Conclusions 1
  - Objectives and Conclusions 2
  - Objectives and Conclusions 3

- **Observations and Recommendations**
  - Observation A (title)
  - Observation B (title)
  - Observation C (title)

- **General Audit Information**
  - Standards
  - Scope and Methodology
  - Criteria
  - Staff Acknowledgment

- **Appendices**
  - Appendix A, (if Needed)
  - Appendix B, Management Responses

9.21 Evaluation of Management Response

Management response should indicate: (a) accept, partially accept, or reject with each recommendation; (b) actions taken or planned / rationale for partial acceptance or rejection; (c) responsible management, and (d) targeted completion date.

The In-Charge Auditor and Principal Auditor should evaluate management comments for relevancy, timeliness, and effectiveness of the said action to resolve the issues observed. When comments are in conflict with the observations, conclusions, or recommendations, then include the comments in the audit report and explain the reasons for the disagreement in a section titled “Evaluation of Management Response”.

If management sends copies of various documents, letters, directives, etc., these items normally become part of the work paper file, but not part of the audit report. These documents normally would be incorporated into the audit report by reference only.

10 PROJECT – POST AUDIT COMPLETION TASKS

10.1 Auditor Performance Evaluations

The purpose of the Project Performance Evaluation is to provide audit staff with objective feedback on their performance that will aid in the auditor's professional growth. The Principal Auditor and In-Charge Auditor will complete an **Auditor Evaluation** of the performance of each staff auditor assigned to the project. The evaluation will be discussed with each auditor; and the auditor will have an opportunity to provide additional comments to the evaluation. The Principal Auditor will prepare an evaluation of the In-Charge Auditor's performance. These will be reviewed with the Director of Audit.

10.2 Audit Project Close-out

The Principal Auditor will perform one final check that all documentation in the electronic and hard-copy format is complete. The actual milestone dates will be recorded in the project spreadsheet. Once complete, the electronic project will be closed in the shared drive and accessed by permission from the Audit Principal or the Audit Director only. The Audit Director will selectively review files.

10.3 Office of Internal Audit Webpage Update

Whenever applicable, and after the final report is released, the Audit Director will forward the report to the Information Technology Division or other responsible party with a request to add the report to the Office of Internal Audit web page. The report will be posted within 15 days after the official release date.

11 AUDIT FOLLOW-UP

According to GAGAS, one purpose of the audit report is to facilitate follow-up to determine if corrective actions have taken place. There are no GAGAS standards for follow-up audits as they are considered to be non-audit services unless the entity decides to consider it a "full blown" audit.

Standards such as the IIA's Red Book may be followed in these cases. IIA standards require a monitoring system be set in place for follow-up of audit results.

11.1 Nature, Timing and Extent of Audit Follow-up

The Audit Director shall determine the nature, timing and extent of the follow-up of open audit observations.

If management has effectively complied with recommendations prior to the release of the audit report, there might be no need for a follow-up; however, significant issues should be monitored to determine if management has implemented the action plan as stated in the Final Management Report.

An electronic workbook will be used to monitor those audits that require a follow-up.

11.2 Follow-up Procedures

In most cases, a comprehensive audit is not necessary for follow-up of open audit observations and a report will not be issued.

The objectives of the follow-up will be limited to determining the level of achievement of significant recommendations based upon management's response to audit recommendations and a determination of the success of the recommendation to the original issue.

The Principal Auditor and In-Charge Auditor will determine the level of work necessary to ensure the recommendation has been implemented. For the sake of efficiency, minimal documentation is needed. A narrative with the objective, scope, work performed, results and conclusion will suffice. The conclusion will state if the recommendation was implemented, was not implemented, or is no longer valid. This narrative should be attached into the electronic folder system. The finding will be closed in the electronic workbook if the recommendation (or suitable alternative) was successfully implemented, or if the recommendation is no longer valid.

If the recommendation has not been implemented the finding will remain open and a memo will be sent to the appropriate director stating the facts of the issue. It will contain the date and title of original report. It will include management's response and time table for implementing the recommendations. It will also request a written response on their intentions.

Work performed on the follow-up will be recorded in the original project in the electronic folder. The project title will be "Follow-up of AU2XXX-XXX", using the original project code.

11.3 Additional Reporting Requirement

Even though no report will be issued, Audit Management will track the number of recommendations implemented and closed; therefore, it is important to close observations in the original project in the electronic working paper database when the follow-up shows they have been implemented.

12 OTHER SERVICES

12.1 General Guidelines

GAGAS describes three types of non-audit services: (1) services that will impair the independence of the audit organization, (2) services that will not impair independence, and (3) services that will not impair independence as long as supplemental safeguards are in place. It is the policy of the OIA to decline services that will impair the independence of the office or the auditors conducting the audit.

12.2 Non-Audit Services that Impair Independence

Requests for non-audit services that could potentially impair independence will be referred to the Audit Director for a decision on whether the request will or can be honored.

12.3 Non-Audit Services that Do Not Impair Independence

If a non-audit service is to be provided, the TDOT Internal Audit will consider and document the effects that such service could have on present and future audits. The engagement letter should document the objective, scope of work and deliverable of the service. The letter should also document that the responsibility for the subject matter, the work product, and any functional decisions lies with management and not with this office. Future audits of the subject matter must be designed so that an auditor is not auditing his/her own work.

12.4 Initiation of Non-Audit Service Projects

A project will be set up in the electronic working paper database for each non-audit project. See Section 3.6 for project initiation instructions. The project code will be assigned by the Principal Auditor or Director of Audit. If the time spent on a non-audit project is to be captured as direct hours the project code will be “SP”. If the time spent on the project is considered to be non-direct, other codes will be used.

The Principal Auditor will determine the level of documentation needed for each project. At a minimum, the correspondence containing the agreed-to procedures should be attached into the electronic working paper database system.

12.5 Time Keeping for Non-Audit Services

Time will be entered into the electronic working paper database system for all non-audit services.

12.6 Communicating Results of Non-Audit Services

Auditors performing non-audit services may not report that the services were performed according to GAGAS standards; however, they may report that the services were conducted in accordance with other standards.

12.7 Project Performance Evaluation

See Section 10.1

12.8 Office of Internal Audit Web Page

The Director of Internal Audit will determine if non-audit projects should be made available on the web page.

12.9 Integrity Services

Guidelines for investigations and investigative type activities are outlined in the ***Investigations Standards and Procedures Guide***.

13 Information Security

13.1 Foreword

The primary purpose of this section is to define the information security policies applicable to the Office of Internal Audit. It is understood that these policies augment both Departmental and State of Tennessee policies. However, because of the unique nature and the criticality of information interchange for the Internal Audit activity, additional guidance is required to enable the proper handling of data.

Information resources are assets that are critical elements needed by OIA to provide the services to its customers. Information security then is required to enable and ensure that the data is available, the data integrity is intact, and the confidentiality of the data is ensured.

13.2 Responsibilities

The Office of Internal Audit is responsible for ensuring that any information processing system attached to the State of Tennessee's enterprise network and managed by the OIA, or on behalf of the OIA, is compliant with Departmental and State of Tennessee policies. The OIA is responsible for developing and implementing procedures and operations processes that support the goals and objectives of Departmental and State of Tennessee policies. The policies developed herein are provided to meet and sometimes exceed the minimum requirements outlined by the State's Office of Information Resources Information (OIR) Security Program. The OIA is responsible for communicating this policy document throughout the staff. Auditors are responsible for adhering to statewide, departmental, and division policies, standards, procedures and guidelines pertaining to information security.

13.3 Data Classification

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the Division (and to a greater extent, the Department) should that data be disclosed, altered, or destroyed without authorization.

The classification of data helps determine what baseline security controls are suitable for safeguarding that data. All OIA data should be classified into one of three sensitivity levels, or classifications:

- **Confidential** - Data should be classified as confidential when the unauthorized disclosure, alteration or destruction of that data could cause a **significant** level of risk to OIA or the Department. Examples of confidential data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to confidential data.

Because of prevailing state statues (***Tenn. Code Ann. § 10-7-504 (22) (A)***), all working papers that arise from the Office of Internal Audit including, **but is not limited to**, auditee records, intra-agency and interagency communications, draft reports, schedules, notes, memoranda and all other records relating to an audit or investigation; and all information and records received or generated by the comptroller of the treasury containing allegations of unlawful conduct or fraud, waste or abuse.

- **Sensitive Data** - Data should be classified as sensitive when the unauthorized disclosure, alteration or destruction of that data could result in a **moderate** level of risk to OIA or the Department. By default, all Institutional Data that is not explicitly classified as Confidential or Public data should be treated as sensitive data. A reasonable level of security controls should be applied to sensitive data.

- **Public Data** - Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would results in little or no risk to the Division and its affiliates. Examples of Public data include press releases, course information and research publications. Public Information is information that TDOT must provide for access to Tennessee residents. Public Information is shared publicly to facilitate efficient and transparent government operations. Examples of public Information include information provided on the TDOT Web site and reports meant for public distribution. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

All Information obtained by TDOT Internal Audit regardless of physical form or characteristics shall be assigned a classification in accordance with the requirements set forth within this section in order to ensure that they receive an appropriate level of protection from unauthorized disclosure, use, modification, or destruction. In addition to this policy, care should be taken to ensure compliance with other applicable federal, state and local laws and authorities including but not limited to the Tennessee Public Records Act, T.C.A. § 10-7-503.

Classification of data should be performed by each auditor understanding that the default classification is confidential. Data Stewards such as the Director of Internal Audit, the Principal Auditor, and the IT Auditor should be consulted should there be issues or questions regarding the classification of data.

13.4 Personally Identifiable Information

In general, Personally Identifiable Information (PII) is information about a person that contains some unique identifier, from which the identity of the person can be determined.

PII comes in many forms and may also include any information about an individual maintained by the Department, other state agencies, or even private enterprises that conducts business with TDOT. including, but not limited to one's, education, financial

transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual."

It is the policy of this Division that any PII, obtained during the course of an audit or investigation, be afforded the security profile of CONFIDENTIAL. As such, extreme care should be exercised in safeguarding that information whether at rest or in transit. The following should be performed by each auditor:

- Inform the Principal Auditor or the Internal Audit Director for any PII obtained
- Ensure that PII will not be stored in any EWP.
- Storage of PII shall only occur within the shared drive for the OIA, under the project folder (audit of investigation).
- PII will not be retained in hardcopy format.
- PII should be redacted from working papers if possible.
- PII should not be kept in memory devices (flash drives), compact disks/DVDs, or other portable storage media,
- If retention is necessary, auditors should minimize the volume of PII retained.
- All documents or electronic files containing PII should be labeled and secured at all times.
- PII should never be transmitted by e-mail.

13.5 Privacy and Security Awareness Training and Education

Other than the oversight function, OIA auditors have a role in reducing unintentional errors and IT vulnerabilities. Auditors must:

- Understand and comply with agency security policies and procedures;
- Be appropriately trained in the rules of behavior for the systems and applications to which they have access;
- Work with audit management to meet training needs;
- Keep software/applications updated with security patches per Department requirements (or inform the proper channels); and
- Be aware of actions they can take to better protect their agency's information. These actions include, but are not limited to: proper password usage, data backup, proper antivirus protection, reporting any suspected incidents or violations of security policy, and following rules established to avoid social engineering attacks and rules to deter the spread of spam or viruses and worms.

As part of the annual and ongoing auditor training, topics significant to information security will be emphasized in formal and informal settings with auditors. Topics may include:

- Password usage and management – including creation, frequency of changes, and protection
- Protection from viruses, worms, Trojan horses, and other malicious code – scanning, updating definitions
- Policy – implications of noncompliance
- Unknown e-mail/attachments
- Web usage – allowed versus prohibited; monitoring of user activity
- Spam
- Data backup and storage – centralized or decentralized approach
- Social engineering
- Incident response – whom to contact? "What do I do?"
- Shoulder surfing
- Changes in system environment – increases in risks to systems and data (e.g., water, fire, dust or dirt, physical access)
- Inventory and property transfer – identify responsible organization and user responsibilities (e.g., media sanitization)
- Personal use and gain issues – systems at work and home
- Handheld device security issues – address both physical and wireless security issues
- Use of encryption and the transmission of sensitive/confidential information over the Internet – address agency policy, procedures, and technical contact for assistance
- Laptop security while on travel – address both physical and information security issues
- Personally owned systems and software at work – state whether allowed or not (e.g., copyrights)
- Software license restriction issues – address when copies are allowed and not allowed
- Access control issues – address least privilege and separation of duties
- Individual accountability – explain what this means in the organization
- Use of acknowledgement statements – passwords, access to systems and data, personal use and gain
- Visitor control and physical access to spaces – discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity
- Desktop security – discuss the use of screensavers, restricting visitors' view of information on screen (preventing/limiting "shoulder surfing"), battery backup devices, allowed access to systems
- Protect information subject to confidentiality concerns – in systems, archived, on backup media, in hardcopy form, and until destroyed
- E-mail list etiquette – attached files and other rules.

14 ADMINISTRATIVE POLICIES

The policies outlined herein are provided for the benefit of auditors of the OIA. The policies are meant to support both State and Departmental policies. Additionally, in areas where the hiring authority was given explicit discretionary ability, the policies stated herein provides specific guidance to each auditor on the position of the Division regarding the policy in question. It is the responsibility of each auditor to be fully aware and cognizant of the applicable policies as stated by the Department of Human Resources and other authoritative bodies within and outside of TDOT. If any portion of this policy conflicts with applicable state or federal laws or regulations, that portion shall be considered void.

14.1 Rules of Conduct

The Division of Internal Audit and its auditors must take all necessary precautionary measures to ensure that private and personal interests do not conflict or adversely affect TDOT responsibilities. Internal Audit staff must avoid actions and activities that create an appearance of: (1) Using position for personal gain, (2) providing preferential treatment to anyone, (3) impeding TDOT efficiency of effectiveness, (4) losing objectivity and independence, and (5) making decisions outside the proper channels.

14.2 Attendance, Punctuality, and Leave

The office operating hours of the Division of Internal Audit follows the standard State of Tennessee work schedule of 8:00 A.M. to 4:30 P.M. It is the policy of the Division that during this period, the office will be staffed to meet the needs of its customers.

As an auditor of the OIA, each auditor understands that they have the responsibility to keep their supervisor informed at all times as to their work and/or leave status. The Director of Internal Audit or the Principal Auditor is responsible for approving any leave requests in advance of auditors taking leave. Each auditor understands the following:

- Annual leave, compensatory time, sick leave (when the need for leave is known prior to the date leave begins) and other types of leave must be scheduled in advance except in unusual circumstances.
- Sick leave may require a statement from the health care provider (normally a physician). Except for approved Family and Medical Leave Act leave, military leave, or other leave as allowed by policy or law.
- Leave without pay will not normally be approved.
- The Commissioner may approve special leave without pay for the good of the service.
- Abuse of attendance and leave usage is grounds for disciplinary action up to and including dismissal.

- Habitual failure to report to work at the assigned time and place is grounds for disciplinary action up to and including dismissal

Auditors may be tardy for work for up to 15 minutes without penalty. However, habitual tardiness (three consecutive days or three instances within a week) will be considered grounds for disciplinary action.

14.3 Flexible Scheduling

Under the discretion of the Director of Internal Audit, and to accommodate diverse personal responsibilities, the Director may allow flexible work schedules during the work week. Under normal circumstances, the flexible schedule shall begin no earlier than 7:00 A.M. and no later than 9:00 A.M. when working at TDOT headquarters. A formal written request for a flexible work schedule, using the standard Division form, must be initiated by the employee and approved by the Director prior to assuming a flexible schedule. Auditors are expected to abide by the flexible schedule as agreed in the approved form. Flexible scheduling is a work arrangement that is discretionary on the part of management, and voluntary on the part of the employee. Participation in flexible scheduling is NOT an employee right or entitlement.

Consideration to deviate from the flexible scheduling may be allowed for overriding situations (such as a case investigations, holidays, travel, or extreme personal circumstances) but advance notice is required.

14.4 Telework

Telework is a flexible workplace program that provides employees the opportunity to work at a place other than the regularly assigned duty station such as satellite locations or their residences. Telework is a work arrangement that is discretionary on the part of management, and voluntary on the part of the employee. Participation in Telework is NOT an employee right or entitlement.

- **Regular Telework** - Work is scheduled in advance and performed at the alternate workplace on a regular and recurring basis. The number of days scheduled at the Telework site may vary from one or more days per week depending on the approved program agreement. Regular telework is currently not implemented by the OIA.

- **Episodic Telework** – Understanding that the Internal Audit coverage extends throughout the state of Tennessee and that some of the work may require extensive travel, some assignments will be allowed to utilize this option. Episodic telework is available on an ad hoc, short-term basis to complete projects which are not regular or recurring in nature. Prior authorization with the Director of Internal Audit is required and set deliverables will be agreed upon when this option is utilized.

- **Remote work** – Occurs when an employee, with the Director of Internal Audit's approval, may take work home on occasion. This is evaluated on a case-by-case basis and greatly depends on travel requirements, financial benefit to the Division, and minimal disruption to the auditors daily work/life balance. Prior authorization with the Director of Internal Audit is required and set deliverables will be agreed upon when this option is utilized.

14.5 Professional Demeanor and Appearance

Auditors of the OIA are expected to present a professional and courteous demeanor to the public and with each other. The primary focus of each auditor should be on issues and not personalities and fostering positive relations with everyone. It is paramount that auditors of the OIA be viewed as impartial; therefore, social or personal relationships that could compromise independence and objectivity should be avoided.

One of the unwritten goals of the OIA is to create a "collegial" workplace where mutual respect and individual abilities are harnessed to achieve greater divisional objectives. OIA activities reflect the high standards expected from each auditor. However, solid efforts do not preclude enjoyment of the work or the workplace. Discrete amount of humor and fun, combined with mutual respect only serves to improve divisional operations.

Additionally, auditors of the OIA are required to dress appropriately for working conditions. Attire and appearance should reflect a professional standard of dress, good taste, and common sense. Dress and appearance should be clean, reflect a high standard of personal hygiene, and not pose a distraction or disruption to other employees or visitors in the workplace. Employees who are in contact with the public and/or persons from other State and/or government agencies shall dress in usual and accepted business attire.

Business Attire - business attire includes, but is not limited to the following:

- Suit and tie, button-down collared shirt
- Sport coat, slacks, collared dress shirt with or without a tie
- Dress shirt
- Jacket or blazer with dress, dress slacks, or jacket with skirt and shirt/blouse/shell
- Pantsuits
- Business dresses
- Dress shoes

**** *Denim is generally not considered business attire.*

14.6 Training and Education

The OIA is committed to ensuring that each auditor maintains professional growth, knowledge, proficiency, and compliance with the standards. The Director of Internal Audit will develop an annual training schedule, in collaboration with each staff member, tailored to meet the individual's CPE and proficiency needs.

14.7 Outside Employment

Auditors of the OIA will not engage in any outside employment with any person or entity that has interest that may be substantially affected by the performance or nonperformance of the employee's official duties with the Department. If any employee is, or proposes to become, involved in any outside employment, the employee must submit information concerning the outside employment to the Director of Internal Audit or the Principal Auditor.

The Director of Internal Audit will advise the employee, in writing, as to whether or not a conflict exists with the outside employment and such determination will become a part of the employee's permanent personnel record.

When making a decision concerning if outside employment is or is not a conflict of interest, consideration for approval will be based on the following:

- Whether the outside employment will result in a conflict of interest, or an apparent conflict of interest, with the auditor's official duties and responsibilities;
- Whether the outside employment will interfere with the auditor's efficient performance of official duties and responsibilities; and/or
- Will the outside employment bring discredit to the Division or Department or cause unfavorable or justifiable criticism of the Division or Department.

14.8 Prohibited Activities

The State of Tennessee's Department of Human Resources delineates specific prohibited activities. It is the responsibility of each auditor of the OIA to be cognizant of those prohibitions. However, auditors of the OIA should understand that the oversight position requires a higher standard of accountability than those of "regular" employees. Auditors should be extra mindful that certain activities should be avoided, such as:

- Receiving gifts and gratuities of significant value from companies or individuals who do business with the State.
- Violence in the workplace
- Use of illicit drugs or consumption of alcohol on the job
- Theft of State property

- Misuse of state assets
- Abusive behavior to the public or other employees
- Racial discrimination
- Sexual harassment

14.9 Weekly Schedule and Time Reporting

Auditors of the OIA are required to provide the Director of Internal Audit through the Principal Auditor a weekly schedule. Every Friday, each auditor will spend 30 minutes with the Principal Auditor to provide an update on the achievement of previous week's activities and targeted outcomes and discuss the planned deliverables for the upcoming work week. It is the responsibility of the Principal Auditor to provide the Director of Internal Audit the weekly staff updates.

14.10 Travel

Auditors of the OIA specifically follow Policy 8 as delineated by the Department of Finance and Administration. Travel authorization is paramount before any auditor travel is undertaken for any OIA activity or assignment and must be approved beforehand. The OIA has developed a standardized travel request form that can be obtained directly from the Principal Auditor. It is the policy of the OIA to decline overnight travel authorization for assignments not exceeding a 60 mile radius from TDOT headquarters or the auditor's place of domicile, whichever is closer to the assignment location. Exceptions will be granted on a case-by-case basis.

14.11 Inclement Weather Policy

The OIA understands that inclement weather causes concerns for auditors. In general, however, inclement weather does not warrant the closing of state offices or functions, and it is the policy of the state to make every effort to maintain normal working hours during periods of inclement weather to continue to provide the necessary services to the citizens of the State of Tennessee.

Conditions caused by ordinary inclement weather will require each auditor to make a personal decision regarding safety in traveling to and from the workplace. As with any unexpected absence, auditors who do not feel it is safe to travel should contact the Principal Auditor or the Director of Internal Audit using approved methods. Auditors who do not report to work during periods of inclement weather may use accumulated annual or compensatory time for their absence. If the employee has no annual or compensatory time, then the time absent is charged as leave without pay. Auditors who make the effort and report to work within a reasonable period should not be required to take leave for that absence. To be eligible, the auditor must leave for work at his or her normal departure time in anticipation of regular arrival time.

Occasionally, emergency conditions caused by extreme inclement weather may warrant the closing of some state offices. When such conditions are thought to exist, the Governor or his/her designee may seek input from designated officials in the departments of Transportation and Safety, the Tennessee Emergency Management Agency, the Department of Human Resources and any other departments which may have necessary information, to determine whether state offices should be closed.

State office closures due to extreme inclement weather will be made on a county by county basis and will include all offices in each designated county. The decision to close state offices due to extreme inclement weather shall only be made by the Governor or his/her designee. Notice will be timely given to the local media for broadcast to the general public, forwarded to all appointing authorities, and communicated by other electronic media as appropriate.

14.12 Political Activity

Political activity by auditors of the OIA is regulated by the following three (3) statutes:

- The Little Hatch Act (Tennessee Code Annotated §§ 2-19-201 through 208);
- Tennessee Code Annotated § 8-30-306; and
- Title 5, United States Code Annotated §§ 1501-1508.

The Little Hatch Act (Act) applies to all state employees, except some of its provisions exempt elected officials, officials elected by the General Assembly, and auditors of the Governor's cabinet and staff. Because the Act's prohibitions are very detailed and require careful reading to determine whether particular types of activity might violate its provisions, this policy provides only a broad outline of the types of conduct that the Act regulates. For specific questions about applicability of the Act to a particular situation, consult the Director of Internal Audit.

- Intimidating or coercing public officers and employees so as to interfere with an election, nomination, or measure (Tenn. Code Ann. § 2-19-202);
- Receiving or paying any kind of assessments for political purposes or for election expenses (Tenn. Code Ann. § 2-19-202);
- Soliciting directly or indirectly contributions for political purposes or campaign expenses from persons or entities that are connected to the state or that do business with the state (Tenn. Code Ann. § 2-19-203);
- Promising state benefits, including but not limited to, employment, contracts, work, or loans as a reward for political activity (Tenn. Code Ann. § 2-19-204);
- Depriving or threatening to deprive any person of state benefits, including but not limited to, employment, compensation, contracts, work, or loans because of a person's or entity's political activity (Tenn. Code Ann. § 2-19-205);
- Using state-owned property for campaign advertising or activities (Tenn. Code Ann. § 2-19-206);

- Engaging in political activity not directly a part of that person's employment during any period when the person should be conducting business of the state (Tenn. Code Ann. § 2-19-207); and
- Promulgating any rules or issuing any policies that are more restrictive than the Act (Tenn. Code Ann. § 2-19-207)

In addition to the Little Hatch Act, Tennessee Code Annotated § 8-30-306 states, "*No person holding a position in the preferred service shall solicit, directly or indirectly, or require any other person to solicit, directly or indirectly, donations or contributions for any political party, candidate, cause or purpose in order to acquire or deny a position in state service or to materially affect the retention, promotion or demotion of any employee in state service*."

Despite the restrictions in the statutes mentioned above, auditors of the OIA retain certain rights related to political activity. Most notably, state employees' right to vote as they choose and the right to express opinions on political subjects and candidates are not affected by these statutes.

14.13 New Employee Checklist

New employees to the Office of Internal Audit (OIA) are required to complete the following items:

Introduction to the Tennessee Department of Transportation (TDOT)

- Review TDOT's division responsibilities and organizational chart
- Review the Department of Human Resources Employee Handbook
- Introduction to the Office of Internal Audit (OIA)
- Review TDOT's Internal Audit, Policies, Procedures, and Audit Guide
- Review TDOT's Internal Audit, Investigations Standards and Procedures Guide
- Read Generally Accepted Government Auditing Standards (GAGAS)
- Review audit and investigative reports
- Receive an overview with the Director of Internal Audit
- Receive an overview of TDOT's administrative procedures
    A. Edison
    B. Time reporting
    C. Leave requests
    D. Required employee handbook polices and acknowledgement forms
    E. New employee checklist
    F. Computer folders and e-mail
    G. Office keys and business cards
    H. MTA Bus card and employee parking
    I. Insurance (Health, dental, life, accident, and optional)
    J. Overnight travel policies
    K. Telephone system

L. Staff meetings

Overview on OIA's certifications, training, and continuing professional education

- Certified Internal Auditor (CIA) certifications
- Other certifications
- Staff training
- Continuing professional education requirements
- Professional memberships
- College tuition reimbursement program
- Computer classes

14.14 Departing Employee Checklist

Departing employees to the Office of Internal Audit (OIA) are required to return the following items:

- State ID Card
- Building Card Key
- Parking Tags & MTA Cards
- Credit Cards or Calling Cards
- Keys
- Home / Office Equipment
- Books and Manuals – ACL, Audit Manual, or any other office issued materials
- Cameras, Recorders, or Binoculars
- Cellular Phone and other Electronic Devices
- Laptop or Computer Devices (Tablets)
- Voice Mail Access Code
- Computer Passwords
- Database Access Codes (State Mainframe, Edison, SEIS, STARS, etc.)
- Other Passwords - any password protected files?
- Other Computer Peripherals
- Other Portable Equipment

IT Auditor or the Principal Auditor will back-up all files onto the network in one folder under terminating employee's name.

Contact all appropriate parties to have all computer accesses revoked effectively on their termination date. This included JJ, STARS, Edison, CMS, MMS, PPRM, Site Manager, etc…

Determine if Employee is willing to work 120 days in a 12 month period (Retirees Only).

Supervisor has reviewed any applicable Forms DT-1708A or DT-1709A and has completed the From DT-1713 for the employee leaving for equipment formerly assigned to the employee.

Separation Notice and copy of 201 to TDOT HR

Verify employee's leave balances between employee and Payroll.

Annual _____
Sick _____
Comp _____

APPENDICES

APPENDIX A – ENTRANCE CONFERENCE OUTLINE

Below are some of items that should be covered in the meeting:

Entrance Conference Agenda

A. Introduction of OIA staff and divisional personnel

B. Explanation of the audit process
   a. Focus on controls, compliance, and efficiency and effectiveness of operations.
   b. Will request information to assist in planning.
   c. Explanation of planning, fieldwork, reporting.
   d. Target fieldwork start and completion dates, space needs.
   e. Process surrounding audit observations, report drafting, management responses, report issuance.
   f. Report addressed to the Commissioner, the Deputy Commissioner/Chief Financial Officer, and management.

C. Discuss Audit fieldwork logistics
   a. Office hours
   b. Workspace, phones, copiers, etc.
   c. Divisional contacts

D. Establish communication with other relevant parties

E. Discussion of the divisions and sections within the bureau
   a. Discuss areas of potential audit interest.
   b. Related party transactions.
   c. Conflict of Interest.
   d. Work performed on private property.
   e. Contingent liabilities.
   f. Irregularities involving employees.
   g. Major new initiatives and projects.
   h. Specific problem areas or areas of concern.

F. Review of the Entrance Conference Request List

G. Arrange for a facility tour (if applicable)

H. Other Matters

The Opening Conference's date, key attendees and substantive items discussed which are directly related to audit scope, objectives, timing or confidentiality should be documented in the work papers.

Below are some of the items that **may be included** on the **Entrance Conference Request List**. Review the Request List with the audit client during the Entrance Conference and indicate any documents you have obtained during the Pre Planning phase. Request the audit client to provide copies of the following documents and information, as applicable.

Oversight and Management

- Copies of divisional plans, mission statements, goals and objectives
- Copies of divisional policies and procedures
- Copies of divisional organization chart and phone list
- Copies of latest Performance Measurement reports

Divisional Operations

- List of all professional associations and a brief description of each
- List of all professional journals, subscriptions, and other publications and a brief description of each
- List of all divisional locations, addresses, phone numbers, and primary contacts and a brief description of the activities at each
- List of all TDOT entities, state and federal agencies, community groups, and others that the division interacts with on a regular basis, and a brief description of each relationship
- List of other government or private sector operations of industry sources used for best practice or performance measurement comparisons

Divisional Reporting

- Listing of fiscal year end and divisional financial statements prepared for management, the board/commission, state or federal agencies, or others
- Listing of statistical and other non-financial reports prepared for management, the board/commission, state or federal agencies, or others

Legal Compliance Requirements

- List of all federal, state or other regulatory compliance requirements that the division has to monitor and/or report on, and copies of any applicable regulations, or guidelines
- Listing of all current fiscal year and open federal, state, or other grant agreements, and a list of any sub-grantees

Divisional Assets

- Copies of the most recent bank statements and reconciliation for any bank accounts under divisional control (if applicable)
- Copies of the most recent accounts receivable or other receivable listings
- Listing of supplies, materials, parts, or other inventory listings
- Listing of all divisional employees who are assigned a vehicle twenty-four hours a day, a cell phone or a procurement card

Divisional Liabilities

- Copies of the most recent customer deposit and deferred revenue listings
- Copies of any notes payable outstanding

Revenue and Cash Receipts

- For each fund and revenue object accounts, a brief description of the sources of revenue and the revenue collection procedures

Purchasing and Expenditures

- List of all current construction and other major contracts, including the vendor name, contract number, contract period, contract amount, fund/account numbers/object accounts charged, and a brief description of the goods/services under contract
- Listing of any existing lease agreements

Personnel and Payroll

- Copies of divisional job descriptions and performance standards, other than the ones prepared by the TDOT Human Resources (if applicable)
- List of all management and professional employees who have terminated employment with the division during the past two years and a brief explanation of why they terminated

Other Information

- List of all litigation the division is involved in, including a brief description of the case and any dollar amounts involved
- Copies of special studies or consulting reports
- Brief report on the implementation of the last audit

APPENDIX B – ACRONYMS and ABBREVIATIONS

SPECIFIC ACRONYMS AND ABBREVIATIONS USED IN THE AUDIT MANUAL	
American Association of State Highway and Transportation Officials	AASHTO
Association of Certified Fraud Examiner	ACFE
Audit Command Language	ACL
American Institute of Certified Public Accountants	AICPA
Association of Local Government Auditors	ALGA
Audit Risk (Detection Risk)	AR
Computer Aided Audit Tools	CAATs
Committee of Sponsoring Organizations of the Treadway Commission	COSO
Control Objectives for Information and Related Technology	COBIT
Control Risk	CR
Enterprise Risk Assessment	ERA
Enterprise Risk Management	ERM
Generally Accepted Government Auditing Standards	GAGAS
Governance, Risk, and Compliance	GRC
Government Accountability Office	GAO
Government Accounting Standards Board	GASB
Government Auditing Standards	GAS
Individual Performance Plan	IPP
Information Systems Audit and Control Association	ISACA
Institute of Internal Auditors	IIA
Institute of Management Accountants	IMA
Internal Control	IC
Internal Control Questionnaire	ICQ
International Professional Practices Framework	IPPF
Office of Internal Audit	OIA
Personally Identifiable Information	PII
Process Risk Assessment	PRA
Quality Assurance	QA
Quality Control	QC
Risk Assessment	RA
Risk Management	RM
Standard Operating Procedure	SOP
Statement on Auditing Standards	SAS
Statement on Standards for Attestation Engagements	SSAE
Tennessee Department of Transportation	TDOT
Financial Accounting Standards Board	FASB

APPENDIX C – RISK BASED AUDIT GUIDELINES

Risk Management

Risk management is defined as a coordinated set of activities and methods that is used to direct an organization and to control the many risks that can affect its ability to achieve objectives. It includes the architecture that is used to manage risk. This architecture includes risk management principles, a risk management framework, and a risk management process. Risk assessment itself is a three pronged approach which includes the process of risk identification, risk analysis, and risk evaluation.

Purpose of the Risk Identification Process

- To identify the threats facing the program or contract under audit; identify the controls or procedures the function has in place to prevent, eliminate, or mitigate the threats.
- To identify the threats facing the program or contract under audit; identify the controls or procedures the function has in place to prevent, eliminate or minimize the threats.

Purpose of the Risk Analysis and Evaluation

- To determine the probability that noncompliance and abuse, which is determined individually or in the aggregate, could occur and not be prevented or detected in a timely manner by the internal controls in place.
- To determine the impact of such noncompliance, abuse, or inadequacy of internal controls on the achievement of objectives.

The purpose of a risk-based auditing is to develop audit procedures to see if the controls or procedures the function has in place to prevent, eliminate, or minimize identified threats are designed properly and working as intended and to determine if additional audit procedures are necessary to document threats actually occurring.

The rationale for conducting a risk assessment is that auditors can limit testing and focus on those areas most vulnerable to noncompliance, lack of internal controls, insufficient or excessive controls, and abuse. This produces a more cost-effective and timely audit.

In conducting a risk assessment, the auditor:

- Identifies the threats associated with the area or activity under review;
- Determines the inherent risk associated with the identified threats; and
- Assesses whether the existing internal controls will prevent, detect, or correct instances when perceived risks actually occur.

The extent of audit testing is directly related to an assessment of the activity's degree of vulnerability. The higher the vulnerability, the more extensive the audit testing needs to be

and vice versa. Thus, even though an activity may have a high degree of inherent risk, a strong system of internal controls can reduce the entity's exposure to a low or moderate level. Accordingly, the need to conduct detailed audit tests could be reduced to an appropriate level

The risk assessment work should be documented in the audit working papers. This assessment should serve as the foundation for the developing the detailed audit steps and tests to be performed in the Audit Program portion of the Planning Memorandum. The risk assessment should be documented in a completed risk matrix and relevant to the audit objectives.

Risk Assessment Audit Steps

1. Based on information gathered during the Preliminary Survey, prepare a tentative list of business processes relevant to the general audit objectives. Secondly, enumerate the risks related with each business process. If computer processed data is an important or integral part of the audit and the reliability of the data is crucial to accomplishing audit objectives, the auditor should include threats to computer processed data in this list. Auditors must consider the following factors.

    - Assess the risk that abuse or illegal acts could occur and materially impact the auditee's compliance with laws, rules, or regulations or have a material effect on the auditee's operations. Consider whether the auditee has controls that are effective in preventing or detecting illegal acts.
    - If computer systems or computer-processed data are included as threats or as controls above, consult with the Principal Auditor to determine the need for IT auditor assistance.
    - Identify material and significant findings and recommendations from previous reports issued by the office on the agency or program that may require follow-up in the current project. An auditee's failure to rectify outstanding issues and implement previous recommendations are considered threat

2. Meet with audit management to review the list of potential threats and include any additional threats to the list. Auditors may send this information to the auditee prior to the meeting. At the same meeting, auditors must document management's internal controls (actual or potential controls) to mitigate the identified threats.

3. Complete the risk matrix with the business activity, the identified risks and corresponding identified controls. Use the rating guides to assess each threat's inherent risk, rate each internal control, and assess the vulnerability of each internal control given the threat risk and internal control rating. The Principal Auditor reviews the final risk matrix and the Director of Internal Audit approves the document. A meeting may be held to discuss the matrix and assessment.

Rating Guidelines for Risk Assessment

The Threat's Inherent Risk is	If	The Internal Control is	If
HIGH	▪ Noncompliance or abuse may result in significant losses to TDOT assets (e.g., monies, funds, equipment, tools, and supplies) ▪ Noncompliance or abuse will likely expose TDOT to adverse criticism in the eyes of its citizens ▪ Incentives of noncompliance or abuse outweigh the potential penalties.	**WEAK**	▪ Management and/or staff demonstrate an uncooperative or uncaring attitude with regard to compliance, recordkeeping, or external review. ▪ Prior audits or the preliminary survey has disclosed significant problems. ▪ The Risk Matrix reveals that adequate and/or sufficient internal control techniques are not in place. ▪ Documentation of procedures is lacking or of little use.
MEDIUM	▪ Noncompliance or abuse may result in significant losses to TDOT assets (e.g., monies, funds, equipment, tools, and supplies) ▪ Noncompliance or abuse will result in inefficient operations or substandard service to the citizens of Tennessee ▪ Incentives of noncompliance or abuse are approximately equal to the potential penalties.	**ADEQUATE**	▪ Management and staff demonstrate a cooperative attitude with regard to compliance, recordkeeping, and external review. ▪ Prior audits or the preliminary survey has disclosed some problems but management has implemented remedial action and has satisfactorily responded to audit recommendations. ▪ The Risk Matrix reveals that adequate and/or sufficient internal control techniques are in place.

			▪ Although deficient or outdated, documentation of procedures is still useful or can easily be updated.
LOW	▪ Noncompliance or abuse may result in significant losses to TDOT of assets (e.g., monies, funds, equipment, tools, and supplies). ▪ Noncompliance or abuse will result in a disregard of an administrative procedure or authoritative standard. ▪ The potential penalties outweigh the incentives of noncompliance or abuse.	**STRONG**	▪ Management and staff demonstrate a constructive attitude, including an eagerness to anticipate and forestall problems. ▪ Prior audits and the preliminary survey have not disclosed any problems. ▪ The Risk Matrix reveals that numerous and effective internal control techniques are in place. ▪ Procedures are well documented.

Vulnerability Assessment and Testing Extent Matrix

Inherent Risk	Internal Control	Vulnerability and Testing Extent
High	**Weak** **Adequate** **Strong**	**High** **Moderate to High** **Low to Moderate**
Medium	**Weak** **Adequate** **Strong**	**High** **Moderate to High** **Low to Moderate**
Low	**Weak** **Adequate** **Strong**	**High** **Moderate to High** **Low to Moderate**

APPENDIX D – GUIDELINES FOR AUDIT TESTING PROCEDURES

There are many types of audit procedures which can be used to test transactions or processes. The audit objective determines the type of procedure to be used. The auditor must judge the evidence obtained through the audit procedures to make conclusions for each audit objective. The evaluation process requires professional judgment in determining the adequacy, efficiency, economy and effectiveness of what has been audited. Care must be taken in selecting the correct procedure to achieve the audit objective.

The audit risks include:

- Selection of an improper audit procedure
- Executing the procedure incorrectly
- Incorrectly evaluating results of the test work
- Faulty conclusions

The following general types of audit procedures are discussed below: Verification, Observation, Inquiry, and Analysis.

Verification

Verification is the confirmation of things such as: Assets; Records; Statements; Documents; Compliance with laws and regulations; effectiveness of internal controls; transactions; and processes. The purpose of verification is to establish the accuracy, reliability, or validity of something. Below are types of verification techniques:

- ***Count:*** An auditor will use this technique to verify the accounting records of a physical asset by physically counting the assets.
- ***Compare:*** An auditor will identify similar and/or different characteristics of information from two or more sources. Types of comparison include:

    - Comparison with prescribed standards
    - Comparison of current operations with past or similar operations.
    - Comparison with written policies and procedures
    - Comparison with laws or regulations
    - Comparison with other reasonable criteria.

    Specific examples are:

    - To compare a law requiring that a percentage of taxes will be used for a particular program with the accounting records showing the amount of taxes and how much was spent on the program.

    - To compare the documentation of a transaction with the procedure for the transaction.

- ***Examinations:*** To look something over carefully, such as a document, especially for the purpose of detecting flaws or irregularities. For example, an auditor may examine a document to verify that it has been executed by authorized persons***.***
- ***Inspections:*** To look something over carefully, such as a physical asset, especially for the purpose of detecting flaws or irregularities. For example, an auditor may inspect inventory to verify quality***.***
- ***Footing:*** To recompute the mathematical result of addition or subtraction of columns or rows of numbers in documents or records.
- ***Recompute:*** To check mathematical computations performed by others.
- ***Reconciliations:*** The process of matching two independent sets of records and to show mathematically, with supporting documentation, the difference between the two records. For example, the beginning and ending balances in an account could be reconciled to document the transactions that account for the changes between the beginning and the end.
- ***Confirmation:*** To obtain information from an independent source (third party) for the purpose of verifying information.
- ***Vouching:*** To verify recorded transactions or amounts by examining supporting documents. In vouching, the direction of testing is from the recorded item to supporting documentation. The purpose for vouching is to verify that recorded transactions represent actual transactions.
- ***Tracing:*** Tracing procedures begin with the original documents and are followed through the processing cycles into summary accounting records. In tracing, the direction of testing is from supporting documentation to the recorded item. The purpose of tracing is to verify that all actual transactions have been recorded.

Observation

Observation is auditors seeing with a purpose, making mental notes and using judgment to measure what they see against standards in their minds. Experienced auditors may be better able to observe deviations from the norm. Observed deviations usually require confirmation through analysis or corroboration.

Types of deficient conditions which can be observed include:

- Idle personnel, equipment, or facilities
- Security violations
- Dangerous conditions or safety violations
- Backlogs
- Current practices vs. Prescribed practice

Inquiry

Auditors perform interviews with the auditee and related parties throughout the audit. Good oral communication skills on the part of the auditor assist in getting accurate and meaningful information from the interviewee. Auditors should use open-ended questions

when possible. Depending on the type of information received in an interview, it may need to be confirmed through documentation.

Analysis

Analysis is the separation of an entity for the purpose of studying the individual parts of data. The elements of the entity can be isolated, identified, quantified, and measured. The quantification may require the auditor to perform detailed calculations and computations. Furthermore, the auditor can document ratios and trends, make comparisons and isolate unusual transactions or conditions.

APPENDIX E – Risk Register Elements

OBJECTIVE TYPE	DEFINITION	EXPLANATION
For every objective, indicate whether it is Financial Reporting, Operational, or Compliance.		
Financial Reporting	Objective relates to preparation of reliable published financial statements.	We do this to make sure that financial reporting is timely and accurate.
Operational	Objective relates to effective and efficient use of the company's resources to achieve corporate objectives.	We do this to make sure we achieve our mission, improve and maintain profitability, or reduce and avoid costs.
Compliance	Objective relates to the company's compliance with laws and regulations.	We do this because a local, state, or federal law requires it.
RISK IMPACT RATING		
For every risk, indicate High, Medium, or Low.		
High	A significant barrier that if realized would materially impair the ability to meet the stated objective.	For risks to financial reporting objectives, a lack of control or inadequate control here would result in material errors in the financial statements.
Medium	A moderate barrier to meeting the stated objective that if realized could be material if aggregated with other moderate to significant risks.	For risks to financial reporting objectives, a lack of control or inadequate control here would create errors that are not clearly immaterial, the aggregation of which could be significant.
Low	A minor barrier that if realized is clearly not material to meeting the stated objective.	For risks to financial reporting objectives, a lack of control or inadequate control here would cause errors that are clearly immaterial.
RISK LIKELIHOOD RATING		
For every risk, indicate High Medium, or Low.		
High	Is highly likely and expected to occur.	

Medium	Is reasonably possible and could occur several times.	
Low	Is conceivable, but is highly unlikely to occur.	
COMPOSITE OR OVERALL RISK RATING		
For every risk, indicate High, Medium, or Low based on the combination of risk frequency and severity.		
High	In the absence of controls for this risk, there is a high risk of not achieving the stated objective.	High-High, High-medium, or Medium-High all map to an overall rating of High.
Medium	In the absence of controls for this risk, there is a medium risk of not achieving the stated objective.	Medium-Medium, High-Low, or Low-High all map to an overall rating of Medium.
Low	In the absence of controls for this risk, there is a low risk of not achieving the stated objective.	Low-Low, Medium-Low, and Low-medium all map to an overall rating of Low.
COSO CONTROL COMPONENTS		
For every risk, indicate which component(s) apply.		
Control Environment	*Establishes the tone of the organization *Influences the control consciousness of its people *Provides discipline and structure	*Integrity, ethical values & competence of the entity's people *Management's control consciousness & operating style *Commitment to competence *The attention provided by the Board of Directors

Risk Assessment	The process of identifying and evaluating risks based on their relative significance and probability of occurrence. *Includes the establishment of objectives. *Forms the basis for how the risks should be managed. *Helps to manage change. *Provides all associates with critical means of communicating significant information upstream. *Requires that effective communication with external parties (customers, suppliers, regulators, shareholders) takes place.	Special areas of focus: *Changes to operating environments *Changes in personnel *New or modified system/process *Rapid growth *New technology *New products/markets *Restructuring
Control Activities	Ensure necessary actions taken to address risks for the achievement of the entity's objectives. *Include policies and procedures that help ensure management's directives are carried out. *Occur throughout the organization; throughout all levels & in all functions.	Include a range of activities as diverse as: *Approvals *Authorizations *Verifications *Reviews of operating performance *Security of assets *Segregation of duties *Management reports *Access reports
Information & Communication	*Identifies, captures, and communicates information in a form and timeframe that enables people to carry out their responsibilities.	*Information systems produce reports containing, operational, financial, and compliance-related information that make it possible to run and control the business. They deal not only with internally generated data but also with information about external events, activities and conditions. *Effective communication must occur in a broad sense, flowing down, and throughout the organization. *All personnel must receive a clear message from top management that control responsibility must be taken seriously. *All associates must understand their role in the internal control system, as well as how their activities relate to the role of others.

Monitoring	*The on-going and periodic activities that track the relevance and effectiveness of control activities in terms of their abilities to identify and address new and existing business risks.	*Internal control systems need to be monitored. *It is a process through on-going monitoring oversight, separate evaluation, or a combination of the two. *Includes regular management and supervisory activities, and other action personnel takes in performing their duties. *Defining the scope and frequency of separate evaluations which depend primarily on assessment of risk and on-going monitoring procedures. *Requests those internal deficiencies are reported upstream with serious matters reported to senior management or the Comptroller of the Treasury.
CONTROL CATEGORY		
For every control, indicate Preventive or Detective.		
Preventive	These controls keep risks from occurring.	Examples include locking unauthorized people out of systems, restricting certain combinations of accounts in journal entries, and segregation of duties.
Detective	These controls alert management that risks have already occurred.	Many controls are detective, because they are designed to find an error that may have already occurred--these include reconciliations and re-calculations.
CONTROL METHOD		
For every control, indicate Manual or Automated.		
Manual	Some user input or action is required for this control to function effectively.	Example of manual controls are reconciliations between two reports, reviews and approval of data entry, or running a query that highlights exceptions to be researched by an associate.
Automatic	The control functions automatically, whenever needed, without any user input.	For example, blocking certain combination of chart fields during journal entry input is an automated control.
KEY CONTROL?		

For risks with an overall rating of High or Medium, there must be at least one key control. Low risks will have none.		
Key	Key controls are critical to achieving the stated objective. For example, reconciliations, authorizations, and restricted access are critical to ensuring the accuracy of financial reporting.	If the overall risk rating is High or Medium, there should be at least one key control. There may be more than one key control where controls complement, rather than overlap, each other.
INITIAL CONTROL ASSESSMENT		
For every risk, indicate (on that row only) if the group of controls, as described, is adequate--prior to walk through or testing.		
Inadequate	The controls described do not provide reasonable assurance that the risk will be mitigated.	The controls are not appropriate for the risk or no controls are in place at all.
Adequate	The controls described provide reasonable assurance that the risk will be mitigated.	The controls seem appropriate to the risk.
Excessive	The controls described for this risk seem excessive.	Too much time, effort, or resources are spent controlling this risk.
TEST STEP (Planning Memo Only)		
For key controls only, indicate in which Test Step the control will be tested, or "None."		
Specific Audit Test Step	This reference should correspond to the Audit Program in the Planning Memorandum	
ISSUES (Planning Memo Only)		
For every rating of Inadequate, indicate the control gap.		
Issues Description	These are gaps for inadequate controls.	

APPENDIX F – Data Analytics

Data Analytics

Data analytics (DA) is the science of examining raw data with the purpose of drawing conclusions about that information. Data analytics is used in auditing to: (1) verify or disprove existing models or theories, (2) sort through data sets to identify undiscovered patterns, and (3) establish hidden relationships within the data set. Data analytics focuses on inference, or the process of deriving a conclusion based solely on interpretation, using informed judgment.

The science of data analytics is generally divided into:

- Exploratory data analysis (EDA) – is a type of data analysis where new features in the data are discovered.
- Confirmatory data analysis (CDA) - is a type of data analysis where existing hypotheses are proven true or false.
- Qualitative data analysis (QDA) - is used in the social sciences to draw conclusions from non-numerical data.

The Office of internal Audit may use several tools for performing data analytics such as MS Excel, MS Access, or the preferred software Audit Command Language (ACL).

Initiating Analytics

As part of an audit engagement, data analytics can be a vital tool to identify and assess disparate data sets and reveal information regarding a function, process or transactions that would otherwise be obscured from the auditor. However, to optimize and harness data the power of data analytics the auditor or data analyst should follow a set protocol to help ensure that the work performed is efficient, accurate, and thorough.

The Five Stages of Data Analysis:

- Planning – As with any endeavor, planning the activity is critical to success. In this phase the audit team defines the objectives for analysis and subsequently develops strategies that will enable the team to meet the stated objectives.
- Data Access – in this phase the data requirements are defined, data is located, requested from the proper channels, and transferred to a usable file before handled by ACL.
- Data Integrity Verification – in this phase of the analysis, the auditor tests the integrity of the data for accuracy and completeness to ensure that subsequent results are reliable and correct.
- Data Analysis – In this phase the auditor performs the tests to achieve the stated planning objectives using a combination of ACL commands, filters, and computed fields to generate the targeted outcome.

- Data Reporting – see documenting analytics

Documenting Analytics

One of the most critical elements of conducting data analytics is not only documenting the results but also in documenting the steps or procedures performed to arrive at the results.

Because of quality assurance standards, it is imperative that the auditor/data analyst performing the analysis provide sufficient detailed documentation to enable an experienced auditor, having no previous connection to the audit, to understand from the audit documentation the nature, timing, extent, and results of audit procedures performed, the audit evidence obtained and its source and the conclusions reached, including evidence that supports the auditors' significant judgments and conclusions.

Auditors/data analysts can perform analytic documentation using the standard narrative format in the record of work performed section of the audit work papers augmented by screenshots, print out of ACL scripts, log information (if applicable), or other traceable element needed for verification during the quality assurance process.

Storing Analytic Activities and Results

When creating new projects in ACL, the auditor must utilize the shared drive. New projects must be placed on a folder titled "ACL" under the specific project folder for the audit or investigation that is being performed. The folder should contain the project and all relevant files associated with it.

When utilizing MS Excel for data analytics, the auditor must place the file in the appropriate section of the audit phase (Planning or Fieldwork folder) and follow the work paper labeling conventions outlined in this manual.