TN TDOT
Department of
Transportation

Tennessee Department of Transportation
Division of Internal Audit

Enterprise Risk Management Guide

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

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

The Tennessee Department of Transportation's (TDOT) Enterprise Risk Management (ERM) Guide outlines the Department's approach for implementing requirements of ***TCA §9-18-101****,* commonly referred to as ***Tennessee's Financial Integrity Act of 1983***. TDOT's ERM process adopts the framework set forth by the Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* or commonly referred to as the ***Green Book*** with additional guidance from the Department of Finance and Administration's (F&A) *Management's Guide for Enterprise Risk Management and Internal Control* for developing the Department's approach. The methodology not only focuses on the risk assessment component of an internal control system but places equal emphasis on each of the five components which comprise the department's internal control system.

An effective internal control system allows the Department to improve several factors such as (a) accountability of taxpayer resources, (b) effective achievement of the Department's mission, (c) enhancing operational efficiencies, (d) ability to handle changes to the dynamic business environment, and (d) responding to evolving risks.

Internal or management control is a process effected by **everyone** within the Department. Management controls provide reasonable assurance that managers responsible for a given departmental objective address inherent risks associated with each objective. The Green Book framework classifies objectives into three broad categories:

- **Operations** - Effectiveness and efficiency of operations
- **Reporting** - Reliability of reporting for internal and external use
- **Compliance** - Compliance with applicable laws and regulations

TDOT's ERM process must continually evolve and is both proactive and reactive. ERM must be applied continuously and systematically to facilitate the understanding, management, and communication of risks from an organization-wide perspective. TDOT's ERM process is a robust, comprehensive, flexible, and continuously evolving management control system that endeavors to provide a common risk language, standardized tools, relevant outputs, and uniform processes for managing risks at all levels within the Department.

The application of the Green Book framework provides TDOT's Senior Leadership, division directors, and middle managers with benchmarks for developing the design, implementation, and operation of an effective internal/management control system. An effective management control system helps ensure the optimum utilization of limited resources in achieving departmental and divisional objectives, goals, activities, or tasks.

Purpose

TDOT's Enterprise Risk Management Guide provides the necessary background, rationale, and procedures for developing, implementing, operating, and monitoring the adoption of the Green Book internal control framework in addressing risks necessary to facilitate the achievement of the Department's mission, goals, and objectives.

Background

Taxpayers, citizens, and other stakeholders desire and demand increasing levels of transparency and accountability on government operations; and how governmental entities utilize resources and expend taxpayer dollars. Managers of governmental operations demonstrate responsible stewardship through the prudent use of limited taxpayer resources. Consequently, the unique requirements of operational transparency, fiscal responsibility, and accountability in government create a mandatory requirement for managers to ensure efficient operations and effectiveness in service or product delivery. Efficient and effective work systems arise from understanding and responding to risks detrimental to the completion of objectives and instituting internal/management controls that mitigate the probability or severity of various risks.

In the previous iteration of TDOT's ERM, we used the bottom-up approach for completing the risk assessments. Under the old process, division directors scored a plethora of predefined risks, some of which may or may not be wholly applicable to their operational objectives. Risks acquire esoteric qualities not because directors and senior managers do not understand it, but rather because there is not a unified definition regarding what risks are. Risks mean different things to different people, but the best way to frame risks is within the context of objectives. Limiting the definition of risks relevant to the business objectives, risks become less cryptic and help management focus on the things that will inhibit the completion of objectives. Achievement of business or divisional objectives is the main reason why organizations perform risk assessments. Risk assessments provide assurance that key business processes have appropriate control activities guided by management's specific standards, policies, and procedures. Risk assessments help management identify control gaps, system limitations, efficient pathways, and process redundancies. Once identified, management develops action plans to plug control fissures, strengthen existing controls, or remove redundancies. In essence, risk assessment is a four-part process that includes:

- Determining what needs to be done, who does it, and how
- Identifying the things that would prevent the accomplishment of objectives
- Prioritizing which things pose the biggest hindrance to the objectives
- Developing an action plan to address the hindrance

2 GOVERNANCE, RISKS, and CONTROLS

The following sections discuss important foundational concepts that provide a key link between the seemingly disparate concepts of entity governance, the internal control framework, risk management, and internal/management controls.

Governance, risk, and control (**GRC**) are complementary concepts interwoven into the entity's internal infrastructure. ***Governance*** pertains to the combination of processes and structures implemented to inform, direct, manage, and monitor activities of the organization. ***Risk*** refers to the impact of uncertainties to business objectives. **Control** refers to the specific actions to manage risk and provide reasonable assurance regarding the achievement of objectives and goals.

Operationalized, GRC manifests itself in the work activity as the layered dimensions of *how we get the job done*. The **work environment** includes all those **overarching factors** that influence the way people perform their jobs. These attributes include management's philosophies and attitudes, mission and vision statements, commitment to competence, organizational structure, clarity of roles, delineation of responsibilities, risk appetite, commitment to excellence, and the human resource system. These factors affect the way all employees interpret their job duties and the importance of management controls.

The **management controls** or the **internal control system** includes all those ***tangible factors*** which management establishes to help ensure that employees perform the work, job, or task correctly. These controls include policies and procedures, standard operating guidelines, budgets, rules and regulations, job-specific training, monitoring, and supervision. Management places internal controls throughout the actual job steps to ensure that tasks are completed or performed correctly.

The **work systems** or **activity** is the actual job steps or tasks needed to perform a particular activity or job. A divisional objective could be comprised of a singular activity or several activities needed to generate a desired output.

For example, management implements internal controls at the beginning of a work system when management hires qualified workers, provides training, and develops policies and procedures to follow. Internal controls at the middle of a work system include supervision, monitoring, transaction review and approvals, access controls (to physical and electronic systems), documentation, and authorization limits. Finally, internal controls found at the end of an activity include management reviews, inventory counts, reconciliations, comparing actual to budgeted information, and performance evaluations.

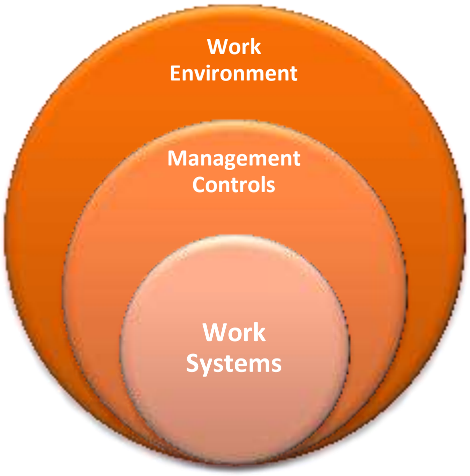


Figure 1 - Interacting Components of a Work Activity

The three interacting components provide the structure and system, which enable the successful completion of any given objective, work system, tasks, or activity. These elements provide the basis for the development of an internal control framework. The framework formalizes the guidelines on designing, implementing, operating, and monitoring the entity's internal control system.

3 What is The Green Book?

The GAO Green Book or *Framework* is an adoption of the internal control framework developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and adapted for governmental and non-profit entities. The Framework provides management with a benchmark or a guide on the relevant and critical aspects of organizational governance such as ethics, enterprise risk management, internal controls, fraud prevention, monitoring, continuous improvement, and reporting (both financial and non-financial).

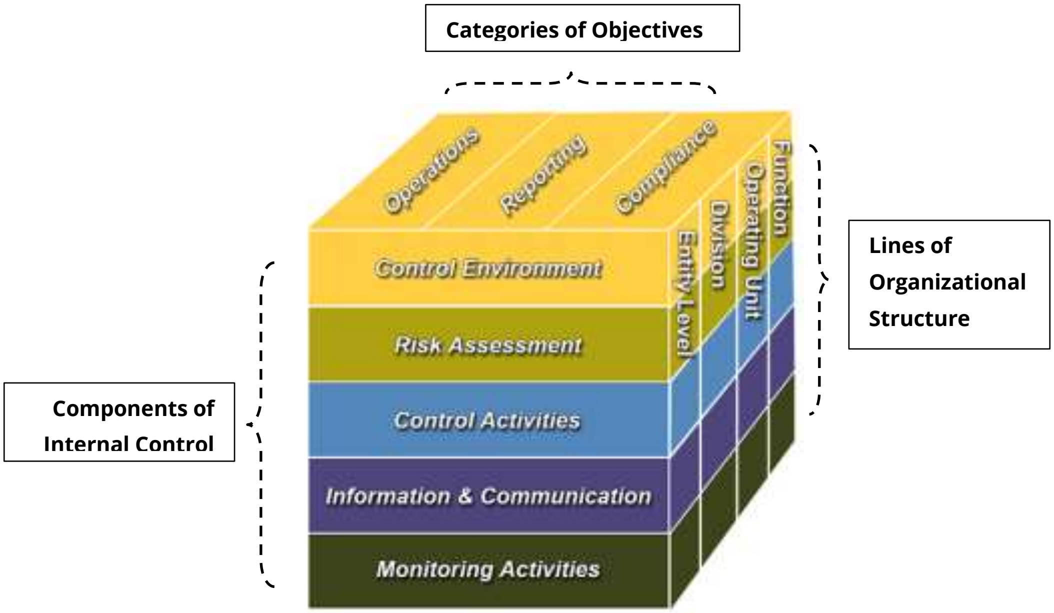


Figure 2 - The COSO Cube

The Framework distinguishes five main components and 17 principles, which set the standards and elucidates the fundamental and integral concepts associated with an entity's internal control system. We can best visualize the nature of the Green Book internal control framework by the concept of ***gestalt***; an integrated phenomena that is greater than the sum of its parts. The five components and 17 principles blend and overlap in a cascading yet cyclical manner to create a control system designed to minimize risks and enable the entity to meet its objectives.

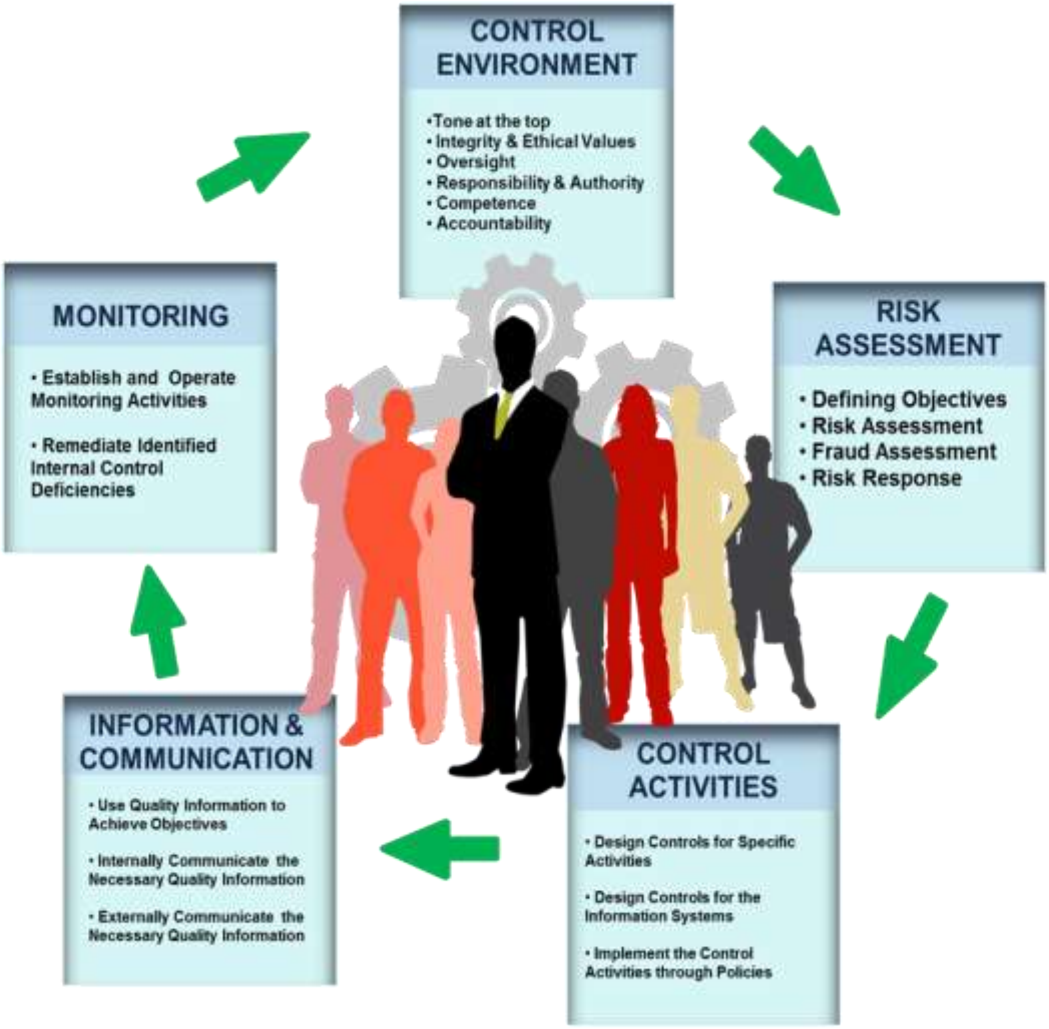

CONTROL ENVIRONMENT
•Tone at the top
• Integrity & Ethical Values
• Oversight
• Responsibility & Authority
• Competence
• Accountability
RISK ASSESSMENT
• Defining Objectives
• Risk Assessment
• Fraud Assessment
• Risk Response
CONTROL ACTIVITIES
• Design Controls for Specific Activities
• Design Controls for the Information Systems
• Implement the Control Activities through Policies
INFORMATION & COMMUNICATION
• Use Quality Information to Achieve Objectives
• Internally Communicate the Necessary Quality Information
• Externally Communicate the Necessary Quality Information
MONITORING
• Establish and Operate Monitoring Activities
• Remediate Identified Internal Control Deficiencies

Figure 3 - Summary of Requirements for Effective Internal Controls

The Control Environment

The control environment begins with the *tone at the top* and permeates throughout the organization; it is the foundation for an effective internal control system. It provides the overarching philosophy, discipline, and structure affecting the overall quality of internal control. The control environment influences how the leadership structure defines objectives and the manner in which control activities are structured. The control environment establishes and maintains a workplace setting that sets a positive attitude, throughout the entity, toward managing risks and internal controls. The control environment encompasses five key principles, which include the following requirements:

1. The oversight body and management should demonstrate a commitment to integrity and ethical values.
2. The oversight body should oversee the entity’s internal control system.

3. Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.
4. Management should demonstrate a commitment to recruit, develop, and retain competent individuals.
5. Management should evaluate performance and hold individuals accountable for their internal control responsibilities.

Risk Assessment

Risk assessment follows the establishment of an effective control environment. In this component, management considers the various internal and external risks facing the entity that may inhibit its ability to meet or achieve objectives. The risk assessment process enables management to identify, evaluate, and respond to risk events. The risk assessment component contains four principles, including:

6. Management should define objectives clearly to enable the identification of risks and define risk tolerances.
7. Management should identify, analyze, and respond to risks related to achieving the defined objectives.
8. Management should consider the potential for fraud when identifying, analyzing, and responding to risks.
9. Management should identify, analyze, and respond to significant changes that could impact the internal control system.

Control Activities

Management controls include those specific actions, which senior leadership and management establishes through policies and procedures designed to ensure the achievement of objectives and respond to risks in the internal control system. These controls include the entity's information system. Control activities have three principles, which require the following:

10. Management should design control activities to achieve objectives and respond to risks.
11. Management should design the entity's information system and related control activities to achieve objectives and respond to risks.
12. Management should implement control activities through policies.

Information and Communications

This component provides context for the importance of quality information and effective internal and external communications. Relevant and reliable information is necessary for the entity to carry out its day-to-day internal control responsibilities. Clear communications enables management to disseminate the information necessary to carry out its internal control responsibilities in achieving objectives. Three principles demonstrate management's responsibility for information and communication, these include:

13. Management should use quality information to achieve the entity's objectives.
14. Management should internally communicate the necessary quality information to achieve the entity's objectives.
15. Management should externally communicate the necessary quality information to achieve the entity's objectives.

Monitoring

Monitoring exemplifies the dynamic nature of internal controls and demonstrates that, as a process, management must continually evaluate existing controls and adapt them to the entity's changing risk profile. Through monitoring, management ascertains whether they have appropriately designed the internal control system; that the controls are properly implemented; and the controls function as intended (designed). More importantly, monitoring ensures management that internal controls remain aligned with changing organizational objectives, business environment, laws and regulations, available resources, and risks.

Internal control monitoring also allows management to assess the quality of entity performance over a period of time and promptly resolves the findings of control self-assessments, internal audits and other reviews. Corrective actions are a necessary complement to control activities in order to achieve objectives. Monitoring completes the control cycle, and the last two principles include:

16. Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.
17. Management should remediate identified internal control deficiencies on a timely basis.

Discussion

The Framework therefore, provides us with defined practices to organize and categorize our organization's internal controls. The formalization of fundamental concepts into 17 principles adds guidance and clarity, which aids management when designing and implementing an effective system of internal controls.

The Framework, in its current form, reflects public sector considerations of good governance and fiscal responsibility. The Framework also factors the dynamic nature of the current operating and business environments including (a) high expectations for effective governance and entity oversight; (b) demands and complexities of laws, rules, regulations, and standards; (c) expectations of competent and accountable public servants; (d) the use of, reliance on, and threats arising from evolving technologies; (e) adapting to greater complexities of business; and (f) expectations relating to prevention and detection of fraud.

4 Enterprise Risk Management

Value-Creation, ERM, and the Rationale for Addressing Risks

In the concept of entity governance, management creates value through informed and inspired management decisions. For governmental units, value creation happens when taxpayers recognize fiscal responsibility, and governmental units deliver goods or services at an acceptable cost. ERM facilitates management's ability to deal effectively with events that create uncertainty. ERM provides management with the mechanisms to respond to risks in a manner that reduces the entity's exposure to the harmful effects of uncertainties. ERM enhances management's ability to communicate value creation with stakeholders through the prudent use of scarce resources, and deliver the goods or services as planned.

ERM therefore, is the coordinated set of structured activities, consistent and continuous processes, and methods that management employs to direct an organization and to control pertinent and significant opportunities and threats that can affect its ability to achieve divisional objectives. ERM includes the *architecture* that management uses to manage risk. This architecture includes the *risk management framework*, defined *risk management principles*, and a *risk management process*.

Governmental units utilize the Framework to accomplish a consistent and thorough risk management formula or architecture. The Framework therefore, becomes an evaluative criteria for audit engagements to ascertain whether management has developed the specific strategies in addressing risks relevant to the accomplishment of business objectives.

Risk(s) Defined

There are many ways to define risk(s). Some define risk as a state or condition that involves a deficiency in information. Others define risk as a level of uncertainty. For the purposes of the ERM process, we will define risks as those events, which prevent us from meeting our business objectives. Although we can define risks very broadly, it is imperative that we define it within the boundaries of the business objectives and address only those risks that we can respond to or for which we can devise controls. We must keep in mind that although risks arising from external factors are numerous, we have very limited ability, if any, in controlling them.

Why Manage Risks?

Managing risks reduces the likelihood of failing to meet divisional objectives, regardless of its category. Managing risks does not necessarily mean eliminating **all** risks prevalent to your division objectives. In practice, sound risk management practices require that management utilize ***cost-benefit*** and ***cost-efficient*** considerations when formulating management controls to address the risks. Pragmatic risk responses address the risks by applying enough controls to decrease the likelihood or the impact of a given risk event to an acceptable level.

What are the benefits of managing risks?

There are numerous benefits for managing risks. Beyond the obvious advantage of gaining assurance that, the business units will meet the business objectives, sound risk management processes result in higher success and completion rates, increases in cost efficiency, and increases in effectiveness of output delivery. Organizations that effectively manage risks are more likely to achieve stated objectives and damaging things are less likely to happen**.**

What is the ERM process?

How ERM is implemented and deployed varies from one organization to another. However, an effective ERM process has certain common elements and characteristics, which includes the following:

Objective Setting – the entity identifies key objectives. Management proceeds by defining objectives in specific and measurable terms. Specificity and measurability are important whether the objectives are qualitative or quantitative. Specificity enables everyone to understand the task. Measurability enables assessments of performance in meeting the objectives.

Organizational Structure – entity management creates the appropriate organizational structure to meet the objectives. An organizational structure defines roles, responsibilities, and authority for the accomplishment of the objectives.

Determining the Entity's Risk Appetite – requires management to gain an intimate understanding of the acceptable level of risks that can be absorbed by the entity.

Risk Identification Process – management deploys processes, which seek, recognize, and describe the uncertainties that could significantly affect the achievement of objectives.

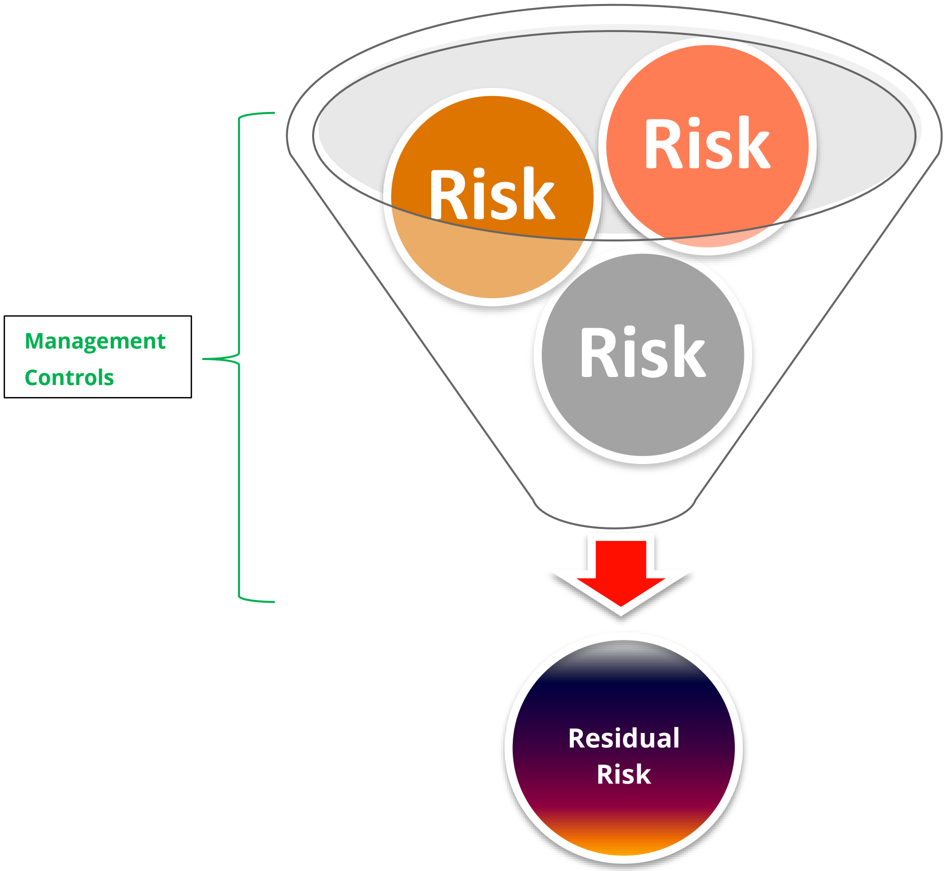
Risk Analysis and Risk Measurement – management utilizes a process to understand the nature, sources, and causes of the risks that you have identified and to estimate the level of risk. Management also uses this process to study impacts and consequences and to examine the controls that currently exist.

Risk Evaluation – management uses this process to compare the risk analysis and measurement results with the risk criteria, and determines whether a specified level of risk is within the acceptable or tolerable range.

Risk Response[1] – are those specific management strategies, which address risks significant to the objectives, and they include (a) *avoidance*, (b) *mitigation*, (c) *transference*, and (d) *acceptance*.

- ***Avoid*** strategies seek to eliminate uncertainty using direct (acquiring knowledge or skills) and/or indirect means (eliminating the source of the uncertainty).
- ***Transfer*** strategies focus on assigning the ownership and/or liability to an external party third party (buying insurance or divestiture).
- ***Mitigate*** strategies seek to reduce the size of the risk exposure below an acceptable threshold.
- ***Accept*** strategies evaluate risks or residual risks and devise methods to monitor the uncertainty. Management controls are one of many forms of risk mitigation techniques. Management designs, implements, operate, and monitor controls because TDOT has a variety of exposures, risks, and threats that can prevent it from achieving its operating, reporting, and compliance objectives.

[1] The enumerated risk responses deal with managing negative uncertainties. Opportunities, or positive uncertainties utilize *enhance*, *exploit*, *share*, and *accept* positive risk responses.



Inherent Risks − Management Controls = Residual Risks

Figure 4 - The Residual Risk Model

Residual Risk – are the risk(s) that remain after management has applied the chosen risk response or after management has instituted risk mitigation, risk acceptance, or risk elimination strategies. Alternatively, we can view residual risk as an equation. Inherent risks exist for every activity, we apply controls (hopefully based on informed decisions) to minimize the probability, size, speed, and duration of the risks. The remainder or difference between the inherent risk and management controls are the residual risks. Inherent risks and residual risks would be equivalent if management decides to accept or chooses not to apply internal controls.

5 Management or Internal Controls

The Framework delineates business objectives into three broadly defined but not mutually exclusive categories, which are (a) ***operations*** (the effectiveness and efficiency of operations), (b) ***reporting*** (reliability of financial and non-financial reporting for internal and external use), and (c) ***compliance*** (accordance with applicable laws and regulations). Management defines objectives at all levels of the organization. These objectives become more granular as it travels down the lines of responsibility and as tasks become more specific within the organizational structure.

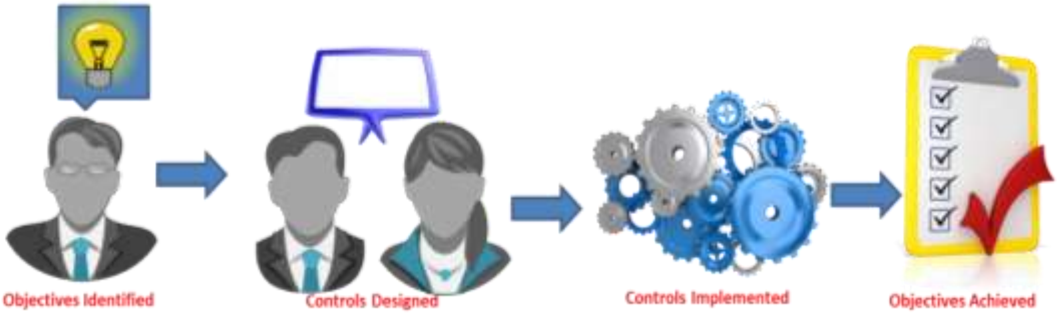


Figure 5 – Objective Setting and Controls

What are internal controls?

Internal controls are all the tools that Senior Leadership, division directors, and supervisory personnel exercise to help provide reasonable assurance that TDOT's objectives are met. Internal controls are comprised of the plans, methods, policies, and specific control activities (procedures) employed to fulfill the mission, strategic plans, goals, and various objectives of TDOT. Therefore, internal control is a system; it is not one event but rather a series of co-dependent, interacting, or fluid actions that occur throughout TDOT's operations.

What makes internal controls important?

Internal controls are important because they are TDOT's first line of defense in safeguarding assets and helping ensure the effective stewardship of public resources. It is important for a number of reasons:

- Internal controls ensure that management has accurate, timely, and complete financial records. Dependability of the information also helps management plan, monitor, and report results of business operations
- Internal controls help to ensure that TDOT is complying with the many federal, state, and local laws and regulations affecting operations

- Internal controls provide an environment in which managers and staff can maximize the efficiency and effectiveness of their operations
- An internal control system provides a mechanism for management to monitor the achievement of operational goals and objectives
- Internal controls are important because a well-designed internal control system protects TDOT's assets from misappropriation, accidental loss, theft, fraudulent activities, and corruption

The Fraud Triangle

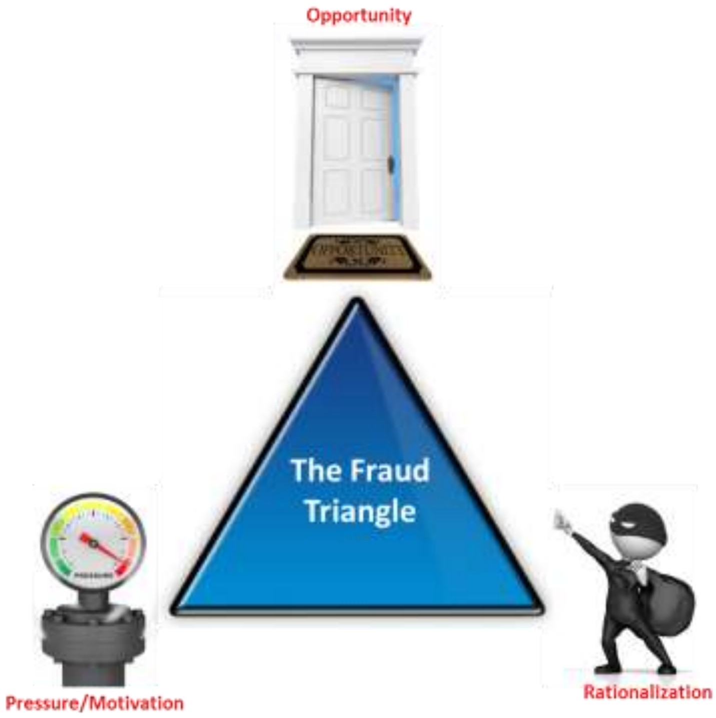


Figure 6 – Elements of Fraud: The Fraud Triangle

A discussion of management control is not complete without a discussion about the ***Fraud Triangle***. The fraud triangle is a model used to explain the mindset behind worker's decision to commit workplace fraud. The theory purports that the fraud triangle has three distinct components:

Pressure – represents the underlying motivation to commit the fraud. This may result from financial problems that the perpetrator cannot resolve legitimately. The perpetrator perceives the underlying issues as unsolvable by orthodox, legal, sanctioned routes and unshareable with others who are able to offer assistance. Financial incentives take the form of both personal interests (too much debt, living a lifestyle of excess, or avarice, to name a few), or business-related matters (the need to show company growth, increased stock value, or higher earnings, for example). Other motivators of deviant workplace behavior include (a) drug problems, (b) gambling addiction, (c) need to meet productivity or financial targets, and (d) desire for status or wealth.

Rationalization – is the cognitive stage and requires the perpetrator to justify the fraud in a way that is acceptable to his or her internal moral compass. Most fraudsters are first-time offenders who do not see themselves as criminals, but rather victims of circumstances. Fraudsters use external factors, such as (a) a medical emergency or procedure requiring a large expenditure; (b) the need to take care of a family member; (c) a dishonest or unfair employer; and (d) equitable distribution, self-promotion, or entitlement to justify, initially, the acceptability of their illicit activity. Perpetrators use rationalizations to minimize or mitigate the harm done by the fraud.

Opportunity – is the method or means by which the perpetrator will defraud the organization. Opportunity is the medium by which the perpetrator sees a clear course of action and abuses or misuses their position to solve the financial problem. Perception also plays a part in opportunity. The perpetrator must perceive that he or she is able to conceal the fraud and that the fraud will go undetected. In many documented cases, the ability to solve the financial problem in secrecy is the key to the perception of a viable opportunity.

Controlling the Opportunity Gap

Opportunity gaps represent the breach between current management controls and the methods by which a perpetrator will defraud the organization. From a managerial perspective, opportunity is the only controllable component of the fraud triangle. Management cannot limit pressures that befall an individual or how the individual can rationalize a deviant act on the organization. Management breaks the cycle of fraud by closing the opportunity gaps. Closing the opportunity gaps require instilling appropriate controls for any business objective or activity. Depending on the targeted activity and the opportunity gaps present, management has a variety of internal controls available at their disposal.

Who has responsibility for internal controls?

Everyone in TDOT has a responsibility for internal control.

Senior Leadership

The Commissioner and Bureau Chiefs are ultimately responsible and assume *ownership* of the internal control system. Collectively, they set overarching policies and procedures and establish the *tone at the top,* which affects organizational awareness, integrity, ethics, and other factors necessary for a positive control environment. Senior leadership provides the governance and broad direction for various division directors and reviews the way directors are controlling the business.

Division Directors and Managers

Directors and their managers' design, implement, maintain, and monitor objective and activity-specific internal control activities for their respective areas of responsibility.

Internal and External Auditors

Evaluate the effectiveness of control systems, and contribute to ongoing effectiveness by providing an independent assessment of business objectives and activities. Because of organizational position and oversight responsibilities within an entity, an internal audit function often plays a significant monitoring role.

Field Personnel: are involved in following the policies and procedures and report observed activities that are not in line with the accepted and appropriate behavior. Field personnel should report instances of fraudulent activities.

What types of Internal Controls are available?

Preventive – preventive management controls are proactive controls designed to avoid errors or irregularities from occurring. Preventive control activities aim to deter the instance of errors or fraud. Preventive activities include thorough documentation and authorization practices. Preventive control activities prevent undesirable "activities"

from happening, thus requiring a well thought out process and risk identification.

Detective - designed to identify an error or irregularity after it has occurred; they are both proactive and reactive. Detective control activities identify undesirable "occurrences" after the fact. The most obvious detective control activity is reconciliation.

Corrective - designed to correct errors or irregularities and prevent recurrence once they have been discovered; they are reactive.

What Are Examples of Internal Control Types?

Preventive	Detective	Corrective
Separation of Incompatible Duties	Exception Reports	New or Revised Policies
Multiple Authorizations	Reconciliations	Revised procedures
Sufficient Documentation	Management Reviews	Disciplinary Actions
Passwords	Compliance Audits	Continuous Improvement Programs
Input Controls	Physical Inventory Counts	Performance Improvement Plans
Concurrent Reviews	Continuous Monitoring	

Source: TDOT Internal Audit

Are there Classifications of Internal Control?

Subject matter experts agree there are two general classifications of Internal Control; they are soft and hard controls. “Soft Controls” relate to the people performing the work and are behavioral in inclination. “Hard control” relates to the processes and activities those people do.

Hard Controls	Soft Controls
Policies and Procedures	People Relations
Organizational Structure	Shared Values
User IDs and Passwords (Access Controls)	Mutual Trust and Openness (Communications)
Supervision	Clarity of Vision and Purpose
Management Reviews	Commitment to Competence
Inspections	Adherence to Professional Standards
Inventory Counts	Mentoring and Coaching
Authority Limits	Expectations for High Performance

Source: TDOT Internal Audit

Do Internal Controls have Limitations?

Absolutely, internal controls do have limitations. In considering limitations of internal controls, we must recognize two distinct ideas. The first set of limitations concedes that some events or conditions are simply beyond management's control. The second acknowledges that no system of internal control will always do what it is designed to do. No internal control, even ones that are smartly designed and implemented are foolproof. They are never perfect because of cost-benefit considerations; we can only place controls appropriate to the value of the asset we need to protect. Internal controls aim only to provide reasonable assurance and never absolute assurance. There are five main internal control limitations, namely:

Management Overrides - Personnel who have managerial responsibilities are in a position to override controls for personal gain and advantage. They are also in a position to ignore or stifle communications enabling dishonesty, misrepresentation of results, and fraud to occur. However, we must not confuse management overrides with management decisions or interventions, which are management actions that depart from prescribed policies and procedures for legitimate purposes.

Judgment – The human element of decision-making diminishes and limits the effectiveness of internal controls. This happens because, more often than not, humans make business decisions under pressure on less than perfect information.

External or Natural Events – Sometimes, peripheral events may have a significant impact on the achievement of organizational objectives and management controls cannot mitigate the impact to an acceptable level because it is beyond the organization's sphere of influence.

System Breakdowns – A well-designed internal control system can break down when employees misunderstand instructions (and perform tasks incorrectly) or simply make mistakes. Errors may also result from new technology and the complexity of computerized information systems.

Collusion – Perhaps the most difficult limitation to detect and ascertain is collusion. Collusion happens when two or more individuals conspire to circumvent existing controls. Individuals acting collectively can alter transactional information, financial data, and other management information in a manner, which existing management control systems cannot detect.

Are there Internal Control Best Practices?

Yes, several effective practices are widely adopted by various organizations. It is important to view internal control as a continuum; it begins with preventive controls that are monitored by detective controls and improved through corrective controls. Therefore, internal control is composed of proactive and reactive measures. With a good internal control system in place, other considerations to keep in mind include:

Regularly communicating updates and reminders of policies and procedures to staff through emails, staff meetings, and other communication methods

Periodic reviews by managers to see if their operations are achieving the desired results.

Reviewing security protocols for facilities and equipment

Keeping appropriate documentations to validate and support transactions and activities

Educating and training employees on proper operational procedures

Performing reconciliations on financial transactions and purchases to make sure items purchased have a valid business purpose, appropriately approved, and physically received

Devising avenues for reporting fraud, waste, and abuse

Responding to allegations of reported fraud, waste, and abuse

Consulting with the Internal Audit (IA) function to assess risks and the level of internal controls required to protect assets

What are some common misconceptions about Internal Controls?

There are many misunderstandings associated with internal controls, but here are the facts:

Internal auditors implement internal controls

Senior Leadership, division directors, and management are the owners of internal controls. Auditors only assess the presence, design, implementation, and effectiveness of those internal controls.

Internal controls are too expensive

If implementing a recommended control appears too expensive, it would be wise to consider the full cost of a fraudulent event that could occur because of absent controls. The cost considerations should include lost funds, lost productive time, investigative efforts, litigation costs, and others. Fraud is always expensive and prevention is more cost effective than any reactive measures.

Internal controls have nothing to do with operations; they are all about finance and accounting

Internal controls are fundamental to every aspect of TDOT's business operations; it spans more than just finance and accounting.

Internal controls result from policies, if a policy does not exist, we do not have to do it

This statement is just partly correct. In most organizations, common business processes are oftentimes defined and supported by written policies. An ethical management together with prudent business practices contributes greatly to a robust internal control environment. However, the lack of formal policies is not a determinant of sound or prudent business practices. This is especially true for a very mature organization that operates effectively on an "unwritten" code. The absence of written policies should not preclude the presence of good internal controls.

Internal controls inhibit us from performing daily activities and responsibilities

To the contrary, internal controls make the right thing happen the first time and prevent unwanted incidents from happening. Internal controls should be built into, not onto, business processes and help make performing daily activities better.

Management will always detect all errors and irregularities if controls are robust

Not true. Internal controls can only provide reasonable, not absolute, assurance that the organization's objectives will be achieved. Just like any system, it will have its limitations.

Controls are unnecessary, we trust our employees

Incorrect, the issue of trust is the one of the hardest to explain; especially for a mature organization whose personnel have worked together as a unit for a very long time. We understand that most TDOT employees are trustworthy and responsible. However, it is also the responsibility of management to remain objective. Thousands of fraud cases show that the most trusted employees are the ones who are involved in committing organizational frauds.

There are not enough personnel to have adequate segregation of duties

The problem of not having enough staff should be thoroughly assessed. What we would like to strive for in implementing controls is not segregating duties per se, but rather the segregation of incompatible duties. In most cases, placing compensating controls, such as supervisory review and tiered approvals, can solve observed control deficiencies.

6 IMPLEMENTATION OF THE ERM

The concept of the framework is not new to TDOT. We have used the previous version of the COSO framework in developing our risk management strategies. However, the previous iteration of the ERM did not fully address risks specific to each division's business objectives. Rather than provide each division with a deluge of predefined risks, most of which may not be wholly applicable, the revised process allows a tailored approach designed to address risks pertinent to each divisions' business objectives.

One of the more significant enhancements to the revised COSO/Green Book Framework is the formalization of fundamental concepts introduced in the original COSO framework. In the updated Framework, the concepts become *principles,* which is now directly associated with the five components and provides clarity for the user in designing and implementing systems of internal control. The *17 Principles* explain and promote a better understanding of the requirements for effective internal control. Additionally, the revised Framework now recognizes the reporting category to include not just financial reports, but other forms of reporting, such as non-financial and internal reporting, which are essential for enhanced decision-making. We have divided the rollout of TDOT's ERM into two phases.

Phase 1

In this phase, every TDOT Division management completes Form 2 and provides their respective business objectives and key business activities. Key business objectives must have defined outputs and specific deliverables to enable measurement of *key performance indicators* (KPI). Form 2 also requires each division to enumerate and define existing management controls.

The second part of Phase 1 involves a *facilitated assessment* of current controls as benchmarked through the lens of the 5 components and the 17 principles of the Framework. Internal Audit lists pre-determined risks by assessing each division for the application (presence or absence) of the elements required by the Framework's 17 principles (see Appendix A, Sample Form 3). Once we receive all responses and risk ratings, we perform a subsequent review of the responses and identify common or recurring themes. If we note any prevalent or endemic deficiencies, we will include them in the presentation packet. We then turn over the risk assessment packet to both the Comptroller of the Treasury and the Commissioner of The Department of Finance and Administration as required by statutes.

Phase 2

The second phase of the ERM involves the facilitated risk identification and risk rating of divisional-specific activities and objectives, outlined in Form 2. This process will begin in earnest at the end of the fiscal year and will employ the facilitated assessment techniques initiated in Phase 1. The process devised will seek to understand and verify specific management controls for each division-specific objectives and activities. Internal audit will not perform a test of the identified controls. We will only evaluate the process flows to ensure the incorporation of internal controls into the process or activity, the resulting evaluation is documented on Form 4 (see Appendix A, Sample Form 4). After completing Form 4, IA will evaluate management controls and determine residual risks that exist after the application of management controls. Finally, IA and division directors will complete the division's ERM through a facilitated risk rating approach by rating each residual risk(s) for impact and likelihood.

We must note that Phase 2 will also include an evaluation of each division's status concerning compliance with the 5 components and the 17 principles of the Framework; as a follow-up to the work performed in Phase 1. The results of the activity-specific risk ratings and the appropriate risk-responses will be included in the presentation packet for submission to the Comptroller of the Treasury and the Commissioner of The Department of Finance and Administration.

Addressing organizational and process-flow changes

Subsequent risk assessment activities (following the implementation of Phase 2) will begin with the reaffirmation of departmental objectives in Form 2. Any changes to departmental objectives require the division director to complete a new Form 2 and define management controls. An updated Form 2 is also required for instances where management reconfigures process-flows, even though divisional objectives remain unchanged. Instances where objectives remain unchanged would only need a reverification of Form 2. This process ensures that internal control documentation stays abreast of organizational or business changes.

7 GLOSSARY OF TERMS

Words and their varied meanings can create a barrier to mutual understanding. In order to avoid misunderstanding and confusion, we have included a list of technical terms and their definition within the context of the ERM. The following definitions provide clarification on key terms used within this guide.

Accept - in risk management, refers to a specific risk response brought about by acknowledging the existence of specific risk event but management chooses not to address

Accountability – refers to an obligation derived from public service requiring providers to keeping an accurate record of activities, documents, assets of value, property, or funds. Accountability arises from defined responsibilities and entails prudent use of limited resources, transparency on how resources are used, and reporting on outcomes from the use of public resources

Activity – an organizational process designed to convert defined inputs into defined outputs

Authorization and Approval – refers to transactional integrity and requires that the appropriate personnel authorize and approve all transactions, to help ensure the transaction has a valid business purpose and is consistent with entity objectives

Avoid - in risk management, refers to a specific risk response brought about by not participating in specific activities deemed as risk events

Baseline – refers to the difference between the criteria of the design of the internal control system and the condition of the internal control system at specific point in time

Competence – refers to an individual's skill, knowledge, and qualifications to carry out assigned responsibilities

Compliance – refers to the organization's ability to conduct business and meet organizational objectives while meeting required statutory, legal, and regulatory responsibilities

Component – refers to one of the five **required** elements of internal control. The internal control components include, (a) *Control Environment, (b) Risk Assessment,* (c) *Control Activities, (d) Information and Communication,* and *(e) Monitoring*

Contingency Plans - refers to the formalized set of management-implemented processes designed to address an entity's need to respond to sudden changes that could compromise the proper functioning of the internal control system

Control Activities – are the collective policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives and address related risks

Control Environment – the collective values, management styles, actions, and specific policies, that influence and set the tone of a firm's daily operations and activities

Control Objective - The aim or purpose of specified controls; control objectives address the risks related to achieving an entity's objectives

Control Limitations - refers to the inherent insufficiency of any internal control measure subjected to human error judgment, process and/or control breakdowns, management overrides, and conclusions

Corrective Action Plan - a defined set of management responses taken to correct a known internal control deficiency

Cost-Benefit Analysis - analysis that quantifies in monetary terms as many of the costs and benefits of a proposal as feasible, including items for which the market does not provide a satisfactory measure of economic value

Cost-Effective Analysis - are management considerations, which compare the costs of implementing controls and the alternative ways of producing the same or similar outputs

Deficiency - refers to insufficient management controls, which inhibit the achievement of organizational objectives. Control deficiencies occur when the design, implementation, and operation of a control is made ineffective due to inherent control limitations

Detective Controls - are types of control activities designed to discover undesirable events that do occur. Detective controls alert management about what has happened and enables management to take prompt corrective action. Detective controls are either manual, automated (based on predefined program logic), or both

Effectiveness – is a measure of an organization's ability to deliver actual outputs (products or services) that meets or exceeds predefined or expected outputs

Efficiency – is a measure of an organization's ability to deliver actual outputs

Entity – refers to TDOT as an organization and a distinct agency within state government

Financial Reporting – are summary records that outline the activities of a business. They include information regarding organizational inflows and outflows of resources, possession and responsibilities, retained monies, and ownership stake

Framework – see GAO Green Book

Fraud - refers to any illegal act characterized by obtaining something of value through deceit, concealment, willful misrepresentation, or a violation of trust. Individuals and groups perpetrate fraud to obtain money, property, or services; to avoid payment of a loss or services; or to secure personal or business advantage

GAO – the Government Accountability Office

Governance - are the combination of processes and structures implemented by an entity's leadership structure to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives

GRC – refers to the collective process involved in the governance, risk, and control, of any entity and its various activities

Green Book – (also called the Framework) is the commonly used name for the internal control framework developed by the Government Accountability Office (GAO), *Standards for Internal Control in the Federal Government*

Impact – in risk management, refers to the severity of deficiency, resulting from an uncertainty, to the achievement of entity objectives. Impact is affected by factors such as the duration, enormity, and speed, of the uncertainty

Information System - refers to the combination of people, processes, data, and technology which management organizes and utilizes to obtain, retain, maintain, communicate, or dispose of information

Information Technology (IT) – refers to the platform, hardware, software, communication equipment, and facilities used to input, store, process, transmit, and deliver data in whatever form necessary to meet divisional objectives

Information Technology Application Controls (ITAC) - are those controls that pertain to the scope of individual business processes or application systems, including data edits, separation of business functions, balancing of processing totals, transaction logging, and error reporting

Information Technology General Controls (ITGC) - a control, other than an application control, which relates to the environment within which computer-based application systems are developed, maintained, and operated, and is therefore applicable to all applications. The objectives of general controls are to ensure the proper development and implementation of applications and the integrity of program and data files and of computer operations

Inherent Risk (IR) - in risk management, refers to the risks intrinsic to any activity prior to the consideration of management's controls or management's chosen response to the risk

Input Controls – refers to the types of ITAC used mainly to check the integrity of data entered into a business application. Input controls work whether staff enters data directly, a business partner remotely, or through a Web-enabled application or interface. Data input is checked to ensure that it remains within specified parameters

Integrity Controls – are types of application controls that monitor data being processed (real time) and data in storage to ensure it remains consistent and correct

Internal Controls (IC) - also known as management controls, refers to any action taken, or the process by which everyone in an entity manages risks and increases the likelihood of the achievement of established objectives and goals

Internal Control System – the overall management control structure that includes people, processes, and culture

Internal Reports – are management outputs, which can be financial or non-financial in nature, and used for short and long-term planning or decision-making

Key Control Activities – are those management controls that are essential to the proper functioning of the activity that in its absence will prevent the completion of an objective

Key Performance Indicator(s) (KPI) – refers to the expected output or outcome resulting from an activity performed correctly. KPI provides management with a means for evaluating the entity's performance in achieving objectives

Likelihood - in risk management, refers to the level of probability that a risk will occur; as gauged from past incidences within the entity or industry

Management – are key entity personnel who are directly responsible for establishing all the control system activities of an entity. Management accomplishes this by designing, implementing, and monitoring the operating effectiveness of the entity's internal control system

Management Controls – see Internal Controls

Management Trails – are types of application controls pertaining to transaction logging and processing history controls. Often referred to as an audit trail, it enables management to identify the transactions and events they record by tracking transactions from their source to their output and by tracing backward. These controls also monitor the effectiveness of other controls and identify errors as close as possible to their sources

Monitoring – an activity performed by internal managers and external oversight body designed to ensure the completion of objectives

Must – a specific term used within the Green Book framework to denote a requirement that management must comply with in all cases; these requirements are the components of internal control

Non-Financial Reporting – are reports related to performance goals or measures, which provide a comparative baseline for ascertaining the achievement of organizational objectives

Objectives – are the defined purposes, activities, and core functions of any work group within an organization. Management defines business objectives through structure, business requirements, and/or lines of responsibility

Objective Setting – involves the development goals and the specific action plans to achieve the goals relevant to the business purpose of an organization

Operations – refers to the day-to-day activities of an organization, which enables it to meet and complete business objectives

Opportunity Gap – represents the inverse relationship (gap) between actual controls and the likelihood a person (or persons) to perpetrate fraud; robust controls means a very narrow opportunity gap

Organizational Structure - The operating units, operational processes, and other structures management uses to achieve objectives

Output Controls – are types of ITAC that address what is done with the data after processing. Output controls help ensure quality information by comparing actual output results with the intended results

Oversight body – are those entity functions with the responsibility for overseeing management's design, implementation, operation, and monitoring of an internal control system

Physical Security – are the combination of control activities that involve safeguarding entity assets (equipment, inventories, cash, and checks). Physical security may involve, armed and unarmed security personnel, physical locks, gates, access limitations (ingress and egress), videographic monitoring, inventory control procedures, periodic inventory counts, and reconciliations. Physical security is also a primary component of ITGC

Policies - statements of responsibility for an operational process's objectives and related risks, and control activity design, implementation and operating effectiveness

Pressure – defined as the prime motivator for committing workplace fraud and may include: financial need, drug addiction, gambling habits, desire for status, and the need to meet external expectations

Preventive Control – are types of control activities designed to deter the occurrence of an undesirable event, inhibit an entity from achieving an objective, or addressing a risk. Preventive controls require proactive risk identification in determining potential undesirable events before they happen and implementing control procedures to prevent them

Principle - Fundamental concept that is integral to the design implementation, and operating effectiveness of the associated component

Process - describes the combination of business activities undertaken to complete an entity objective

Processing Controls – are types of ITAC that provide an automated means to ensure processing is complete, accurate, and authorized. Management evaluates processing controls

Qualitative Objectives - are types of objective(s) where management decides, defines, and designs key performance indicators that indicate a level or degree of conformance to a goal such as milestones

Quality Information – refers to information derived relevant and reliable data sources that is appropriate, current, complete, accurate, accessible, and provided on a timely basis. Quality information meets the identified information requirements for a given activity or objective

Quantitative Objective – are types of objective(s) where the key performance indicators or measures may be a targeted percentage or a numerical value

Rationalization – refers to the internal justification a fraudster makes to provide an excuse or make sense of why he or she committed the fraud

Reasonable Assurance - refers to the degree of confidence that acknowledges the existence and elements of human judgment in providing some assurance relevant to control objective; reasonable assurance provides a high degree of confidence, but never absolute confidence

Reconciliation and Review - performance reviews of specific functions or activities may focus on compliance, financial, or operational issues. Reconciliation involves crosschecking transactions or records of activity to ensure that the information reported is accurate. For example, revenue and expense activity recorded on accounting reports should be reconciled or compared to supporting documents to ensure that the transactions are recorded in the correct account and for the right amount

Reporting Lines - communication lines, both internal and external, at all levels of the organization that provide methods of communication that can flow down, across, up, and around the organizational structure

Residual Risk (RR) - in risk management, refers to the risk that remains after management's response to an inherent risk. Residual risk is calculated as the difference between the inherent risk less the controls. Residual risk may also represent the acceptable level of risk (risk tolerance) after the application of controls

Responsibility – refers to an obligation derived from public service, which require individuals to carry forward an assigned task to a successful conclusion. Responsibilities arise from empowerment or authority to take the necessary actions, within acceptable conduct and standards, to ensure success. Responsibility is concerned with due diligence in performing the tasks; proper custody of valued assets; and the care and safekeeping of documents, property, or funds entrusted to the possession or supervision of an individual

Risk – in risk management, refers to an uncertainty that exists or an event that presents an adverse effect on the achievement of objectives

Risk Appetite - in risk management, refers to the amount of uncertainty (or uncertainties) the entity managers are willing to accept in its pursuit of its mission, vision, goals, and objectives

Risk Assessment - in risk management, refers to figuring out what needs to be done, how to decrease the chance of failure and increase the chance of successfully achieving desired goals

Risk Ranking - in risk management, refers to prioritizing obstacles that have the potential to prevent achievement of goals; efforts should be focused on the most critical risks, which if they went wrong, could potentially disrupt or derail the entire process

Risk Tolerance – in risk management, refers to the acceptable level of variation in performance relative to the achievement of objectives. Additionally, risk tolerance refers to the concept that costs of avoiding risks beyond the risk appetite do not surpass the cost-benefit consideration

Security Management – refers to the collective information processes and control activities related to access rights in an entity's information systems

Segregation of Incompatible Duties – is a particular control activity, which ensures division of duties among different employees to reduce the risk of error or inappropriate actions. Segregation ensures that authorizing, performing, reviewing, and recording of a transaction does not rest on one individual

Service Organization – refers to contractors, vendors, service providers, or other external parties performing operational tasks or processes for an entity

Services - a service is the output by which an agency or organization fulfills its objectives or goals. Most agencies are responsible for a collection of services. The delivery of each service is made possible by several processes, and each process is a collection of employee-level functions

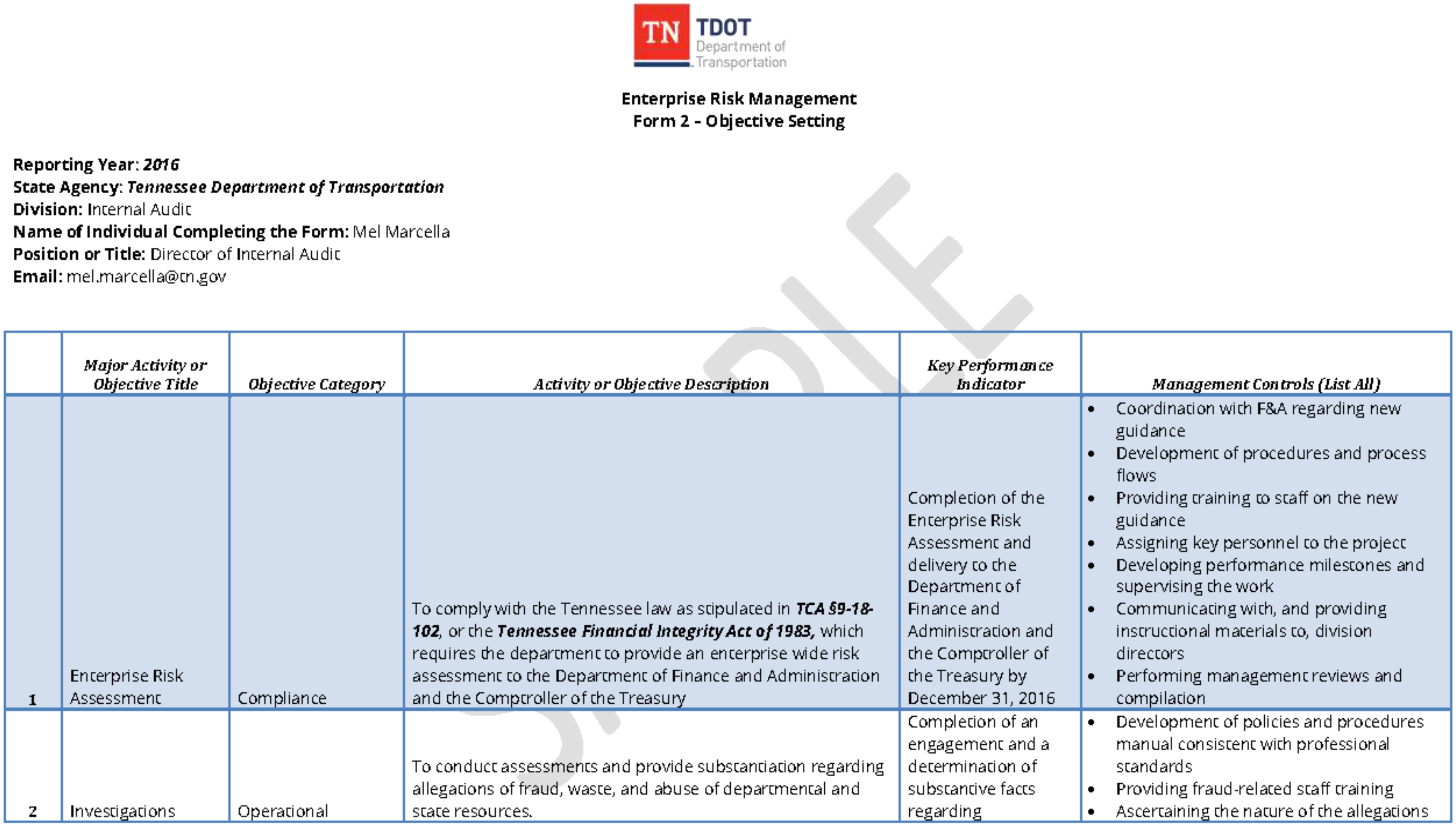
Should - denotes a principle requirement management must comply with except in rare circumstances where the requirement is not relevant for the entity

Succession Plans - the processes that address an entity's need to replace competent personnel over the long term

Transaction - an occurrence in which goods, services, records, or money passes from one entity, account, or person to another. Transactions may occur within operational, compliance, or financial processes

APPENDIX A – ERM FORMS

Sample Form 2 – Objective Setting



Enterprise Risk Management
Form 2 - Objective Setting

Reporting Year: ***2016***
State Agency: ***Tennessee Department of Transportation***
Division: Internal Audit
Name of Individual Completing the Form: Mel Marcella
Position or Title: Director of Internal Audit
Email: mel.marcella@tn.gov

	Major Activity or Objective Title	*Objective Category*	*Activity or Objective Description*	*Key Performance Indicator*	*Management Controls (List All)*
1	Enterprise Risk Assessment	Compliance	To comply with the Tennessee law as stipulated in ***TCA §9-18-102***, or the ***Tennessee Financial Integrity Act of 1983,*** which requires the department to provide an enterprise wide risk assessment to the Department of Finance and Administration and the Comptroller of the Treasury	Completion of the Enterprise Risk Assessment and delivery to the Department of Finance and Administration and the Comptroller of the Treasury by December 31, 2016	• Coordination with F&A regarding new guidance • Development of procedures and process flows • Providing training to staff on the new guidance • Assigning key personnel to the project • Developing performance milestones and supervising the work • Communicating with, and providing instructional materials to, division directors • Performing management reviews and compilation
2	Investigations	Operational	To conduct assessments and provide substantiation regarding allegations of fraud, waste, and abuse of departmental and state resources.	Completion of an engagement and a determination of substantive facts regarding	• Development of policies and procedures manual consistent with professional standards • Providing fraud-related staff training • Ascertaining the nature of the allegations

				allegation(s) of fraud, waste, and abuse of departmental and state resources	received • Assigning key personnel to the project • Developing performance milestones and supervising the work • Performing management reviews prior to releasing reports • Reporting and communicating engagement outcome to division directors, senior leadership, the Comptroller of the Treasury, and, as appropriate, federal or local law enforcement agencies
3		Choose an item.			
4		Choose an item.			
5		Choose an item.			
6		Choose an item.			
7		Choose an item.			
8		Choose an item.			
9		Choose an item.			
10		Choose an item.			
11		Choose an item.			
12		Choose an item.			
13		Choose an item.			
14		Choose an item.			
15		Choose an item.			
16		Choose an item.			
17		Choose an item.			
18		Choose an item.			

Instructions for Completing Form 2

This section provides guidance on how to complete the objective setting form. We strongly advise division directors to include key operating personnel in completing the form, especially when identifying management controls within each major activity. Bear in mind that as we review your responses, we will further evaluate residual risks, relevant to the activity, and meet with you on an individual basis to complete and finalize the risk assessment.

Major Activity or Objective Title

This data field is one of the more important values within the form. We ask that you enumerate the major or core functions of your division. Use questions like, "*What are my division's responsibilities and primary objectives?*", "*What output do we provide for other divisions, the department, or external customers*?", "*What are the key activities that I must do to comply with federal or state regulations*?", and "*What are my division's core functions?*"

Objective Category

In this data field, we ask that you classify the purpose of each major activity into three categories: ***compliance***, ***reporting***, or ***operational***.

- **Compliance** - this activity exists in order to comply with federal or state laws and regulations

- **Reporting** - this activity applies to some objective that meets a reporting requirement. Keep in mind that reporting may include reporting for internal and external purposes as well as financial and nonfinancial category. For example, your division may be required to provide a quarterly report of performance metrics to the Commissioner's office. We classify that activity as reporting nonfinancial information for internal purposes.

- **Operational** - this activity is one of the division's core operating responsibilities.

Activity or Objective Description

Provide a brief description and purpose for each of the major activities in the division.

Key Performance Indicator

Briefly describe the expected result from this activity if performed correctly. You may use the question, "*what is the output/outcome if this objective was completed successfully?*"

Management Controls (List All)

Enumerate all existing management controls that you have implemented for each major activity. Please list, or select from the examples provided, all management controls that you utilize.

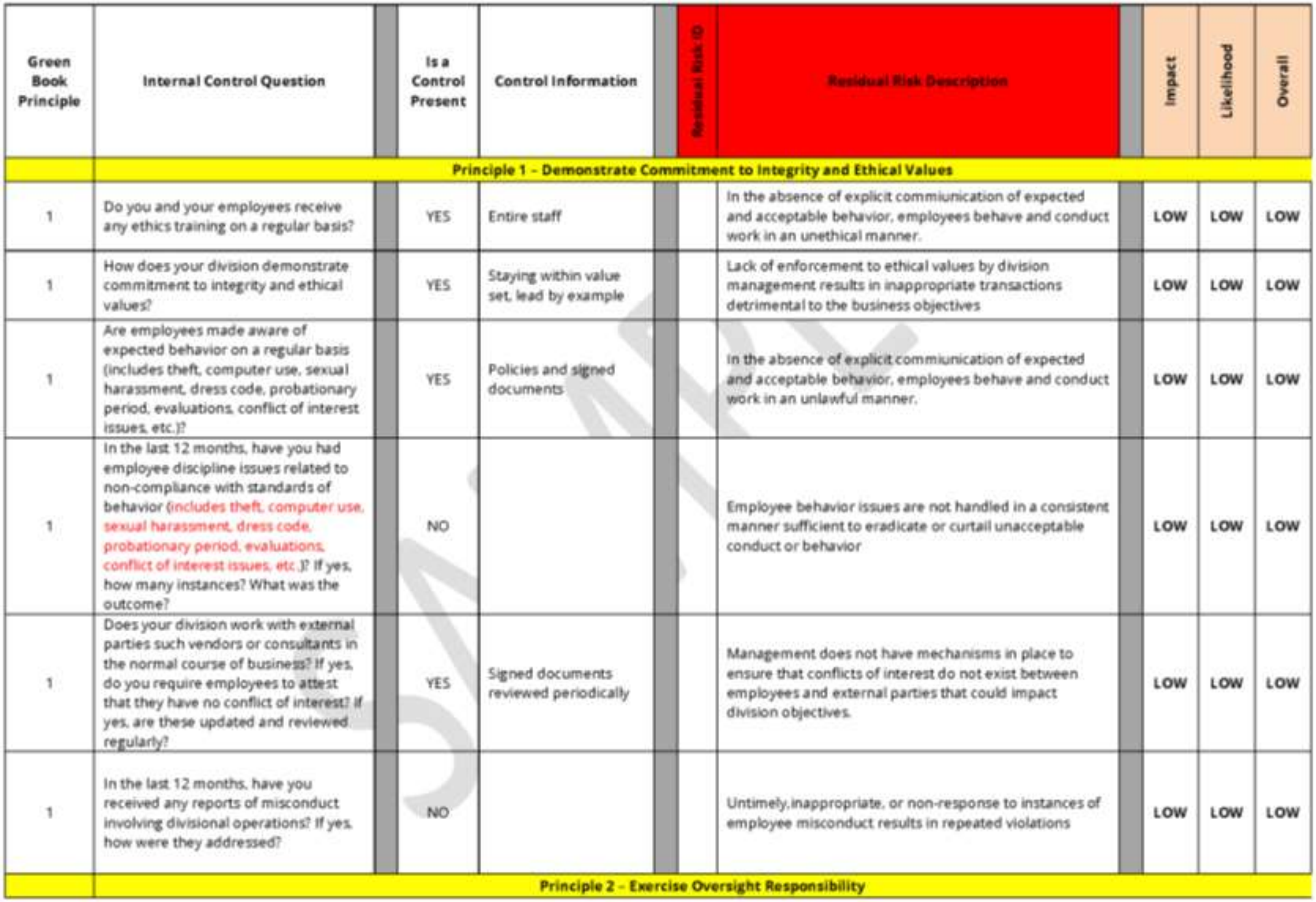
Bear in mind that management or internal controls consist of both tangible and intangible practices, which you and your management structure embeds into each activity to ensure that you achieve your divisional objectives.

In general, management controls can be **preventive, detective,** or **corrective**. We can also classify management controls as **manual** or **automated**, as well as **soft** or **hard**. Whatever the distinction or classification, you use a variety of management controls to ensure that employees perform the jobs correctly.

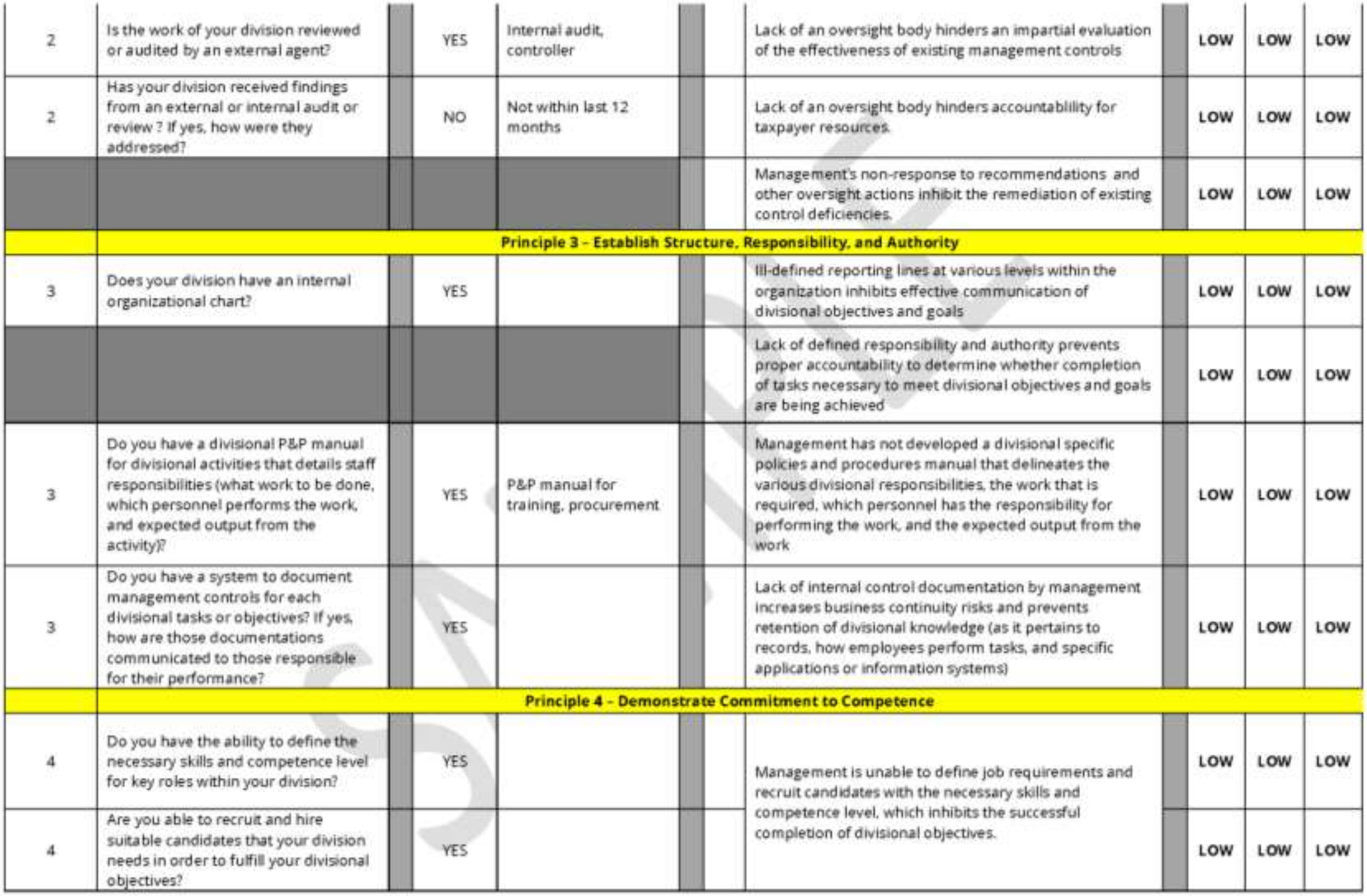
Some examples of management controls are:

Policies and Procedures, Standard Operating Manuals, and Desk Guides
Job Training
Supervision, Supervisory Review
Inspections
Checklists and Activity Reports
Separation of Incompatible Duties
Requiring Multiple Authorizations (for transactions)
Sufficient Documentation
User IDs Passwords, Input Controls, Physical Access Controls (locks and barriers), Output Controls (Quality checks)
Management Reviews
Reconciliations
Inventory Counts
Periodic Audits
Clarity of Vision and Purpose
Commitment to Competence
Adherence to Professional Standards
Honest and Open Communications
High Expectations for High Performance

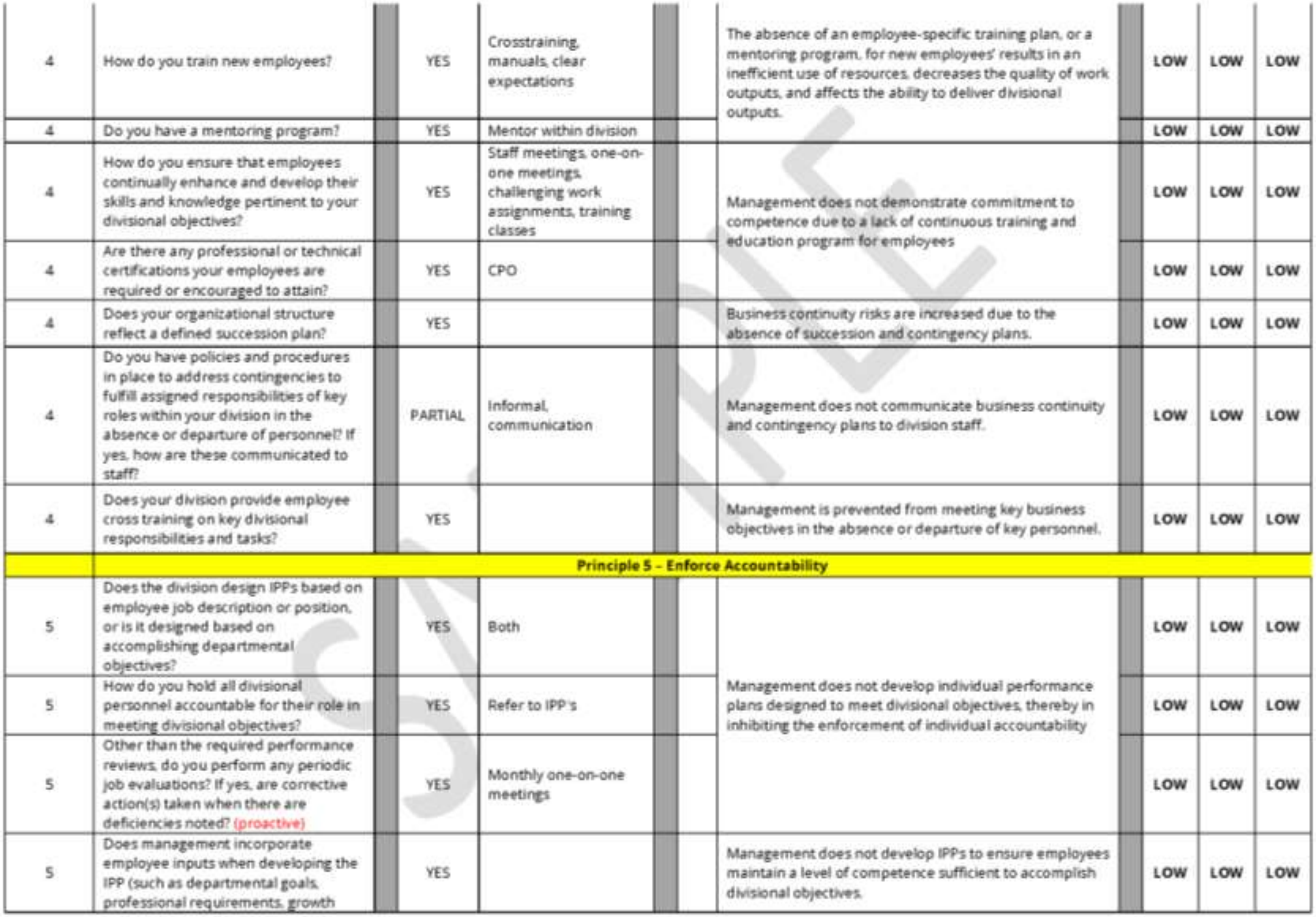
Sample Form 3 – Green Book Principles Assessment



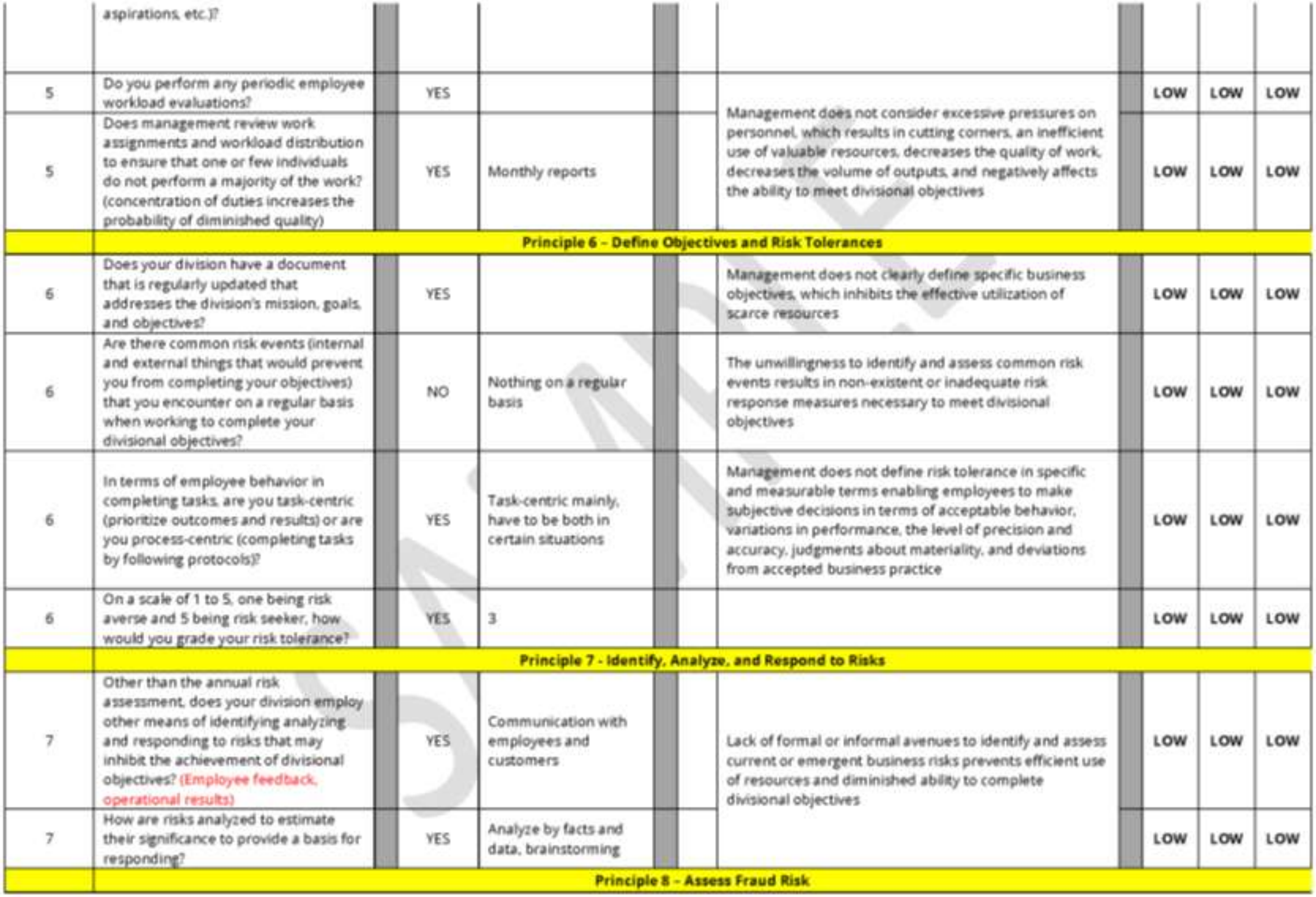
Green Book Principle	Internal Control Question	Is a Control Present	Control Information	Residual Risk ID	Residual Risk Description	Impact	Likelihood	Overall
Principle 1 - Demonstrate Commitment to Integrity and Ethical Values								
1	Do you and your employees receive any ethics training on a regular basis?	YES	Entire staff		In the absence of explicit commiunication of expected and acceptable behavior, employees behave and conduct work in an unethical manner.	LOW	LOW	LOW
1	How does your division demonstrate commitment to integrity and ethical values?	YES	Staying within value set, lead by example		Lack of enforcement to ethical values by division management results in inappropriate transactions detrimental to the business objectives	LOW	LOW	LOW
1	Are employees made aware of expected behavior on a regular basis (includes theft, computer use, sexual harassment, dress code, probationary period, evaluations, conflict of interest issues, etc.)?	YES	Policies and signed documents		In the absence of explicit commiunication of expected and acceptable behavior, employees behave and conduct work in an unlawful manner.	LOW	LOW	LOW
1	In the last 12 months, have you had employee discipline issues related to non-compliance with standards of behavior (includes theft, computer use, sexual harassment, dress code, probationary period, evaluations, conflict of interest issues, etc.)? If yes, how many instances? What was the outcome?	NO			Employee behavior issues are not handled in a consistent manner sufficient to eradicate or curtail unacceptable conduct or behavior	LOW	LOW	LOW
1	Does your division work with external parties such vendors or consultants in the normal course of business? If yes, do you require employees to attest that they have no conflict of interest? If yes, are these updated and reviewed regularly?	YES	Signed documents reviewed periodically		Management does not have mechanisms in place to ensure that conflicts of interest do not exist between employees and external parties that could impact division objectives.	LOW	LOW	LOW
1	In the last 12 months, have you received any reports of misconduct involving divisional operations? If yes, how were they addressed?	NO			Untimely,inappropriate, or non-response to instances of employee misconduct results in repeated violations	LOW	LOW	LOW
Principle 2 - Exercise Oversight Responsibility								



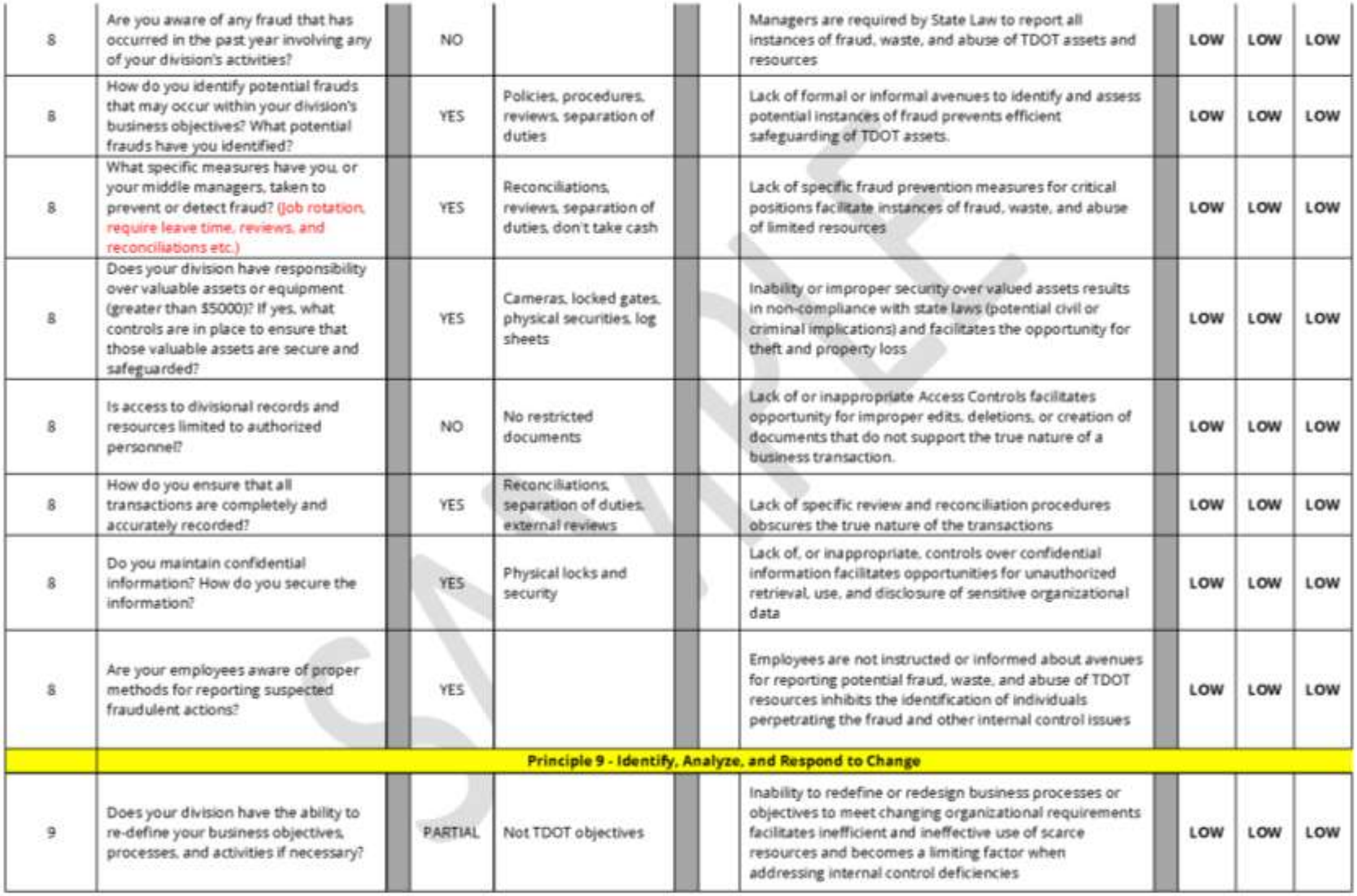
2	Is the work of your division reviewed or audited by an external agent?	YES	Internal audit, controller	Lack of an oversight body hinders an impartial evaluation of the effectiveness of existing management controls	LOW	LOW	LOW
2	Has your division received findings from an external or internal audit or review ? If yes, how were they addressed?	NO	Not within last 12 months	Lack of an oversight body hinders accountablility for taxpayer resources.	LOW	LOW	LOW
				Management's non-response to recommendations and other oversight actions inhibit the remediation of existing control deficiencies.	LOW	LOW	LOW
	Principle 3 – Establish Structure, Responsibility, and Authority						
3	Does your division have an internal organizational chart?	YES		Ill-defined reporting lines at various levels within the organization inhibits effective communication of divisional objectives and goals	LOW	LOW	LOW
				Lack of defined responsibility and authority prevents proper accountability to determine whether completion of tasks necessary to meet divisional objectives and goals are being achieved	LOW	LOW	LOW
3	Do you have a divisional P&P manual for divisional activities that details staff responsibilities (what work to be done, which personnel performs the work, and expected output from the activity)?	YES	P&P manual for training, procurement	Management has not developed a divisional specific policies and procedures manual that delineates the various divisional responsibilities, the work that is required, which personnel has the responsibility for performing the work, and the expected output from the work	LOW	LOW	LOW
3	Do you have a system to document management controls for each divisional tasks or objectives? If yes, how are those documentations communicated to those responsible for their performance?	YES		Lack of internal control documentation by management increases business continuity risks and prevents retention of divisional knowledge (as it pertains to records, how employees perform tasks, and specific applications or information systems)	LOW	LOW	LOW
	Principle 4 – Demonstrate Commitment to Competence						
4	Do you have the ability to define the necessary skills and competence level for key roles within your division?	YES		Management is unable to define job requirements and recruit candidates with the necessary skills and competence level, which inhibits the successful completion of divisional objectives.	LOW	LOW	LOW
4	Are you able to recruit and hire suitable candidates that your division needs in order to fulfill your divisional objectives?	YES			LOW	LOW	LOW



4	How do you train new employees?		YES	Crosstraining, manuals, clear expectations			The absence of an employee-specific training plan, or a mentoring program, for new employees' results in an inefficient use of resources, decreases the quality of work outputs, and affects the ability to deliver divisional outputs.		LOW	LOW	LOW
4	Do you have a mentoring program?		YES	Mentor within division					LOW	LOW	LOW
4	How do you ensure that employees continually enhance and develop their skills and knowledge pertinent to your divisional objectives?		YES	Staff meetings, one-on-one meetings, challenging work assignments, training classes			Management does not demonstrate commitment to competence due to a lack of continuous training and education program for employees		LOW	LOW	LOW
4	Are there any professional or technical certifications your employees are required or encouraged to attain?		YES	CPO					LOW	LOW	LOW
4	Does your organizational structure reflect a defined succession plan?		YES				Business continuity risks are increased due to the absence of succession and contingency plans.		LOW	LOW	LOW
4	Do you have policies and procedures in place to address contingencies to fulfill assigned responsibilities of key roles within your division in the absence or departure of personnel? If yes, how are these communicated to staff?		PARTIAL	Informal, communication			Management does not communicate business continuity and contingency plans to division staff.		LOW	LOW	LOW
4	Does your division provide employee cross training on key divisional responsibilities and tasks?		YES				Management is prevented from meeting key business objectives in the absence or departure of key personnel.		LOW	LOW	LOW
	Principle 5 – Enforce Accountability										
5	Does the division design IPPs based on employee job description or position, or is it designed based on accomplishing departmental objectives?		YES	Both			Management does not develop individual performance plans designed to meet divisional objectives, thereby in inhibiting the enforcement of individual accountability		LOW	LOW	LOW
5	How do you hold all divisional personnel accountable for their role in meeting divisional objectives?		YES	Refer to IPP's					LOW	LOW	LOW
5	Other than the required performance reviews, do you perform any periodic job evaluations? If yes, are corrective action(s) taken when there are deficiencies noted? (proactive)		YES	Monthly one-on-one meetings					LOW	LOW	LOW
5	Does management incorporate employee inputs when developing the IPP (such as departmental goals, professional requirements, growth		YES				Management does not develop IPPs to ensure employees maintain a level of competence sufficient to accomplish divisional objectives.		LOW	LOW	LOW

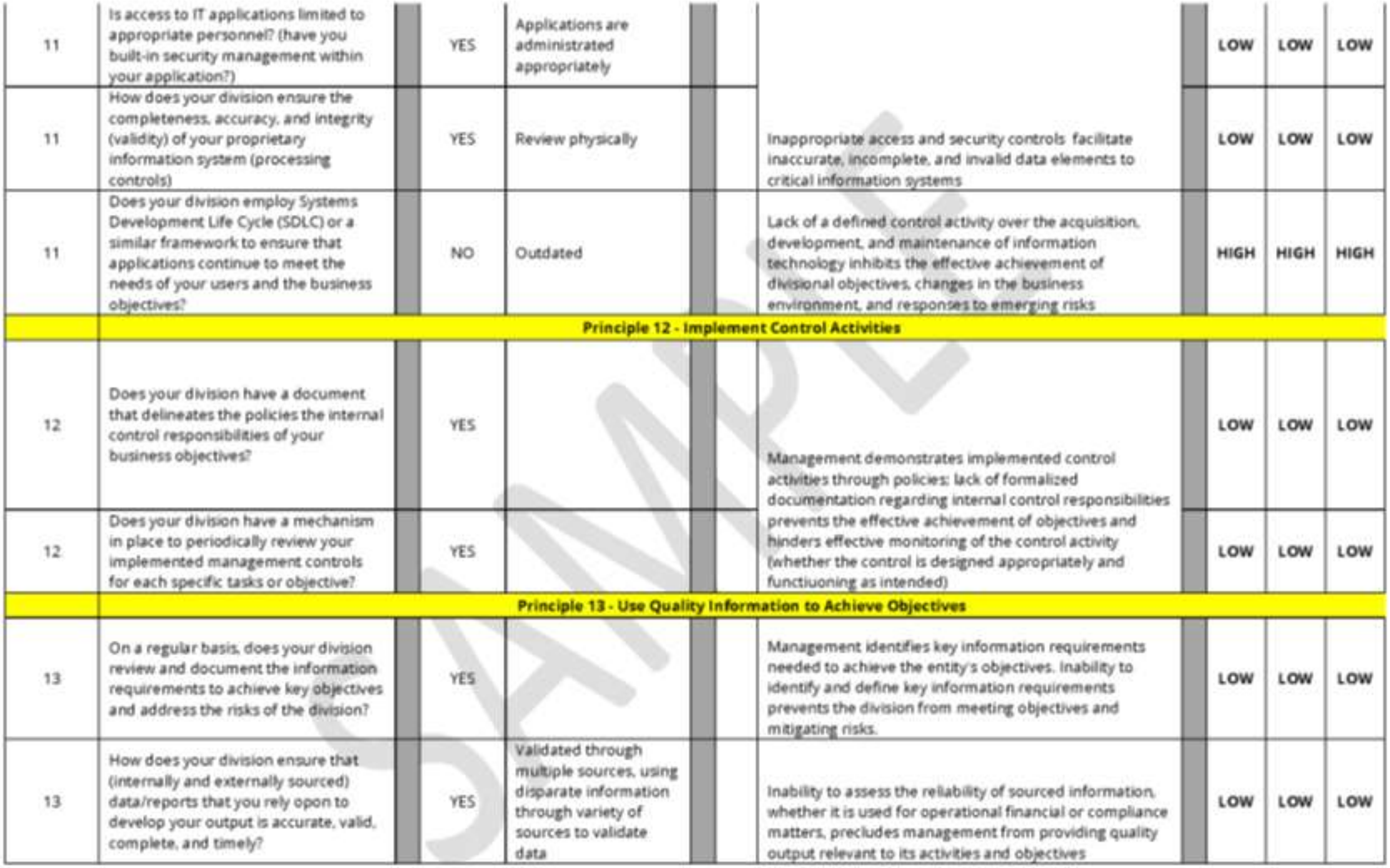


	aspirations, etc.)?						
5	Do you perform any periodic employee workload evaluations?	YES		Management does not consider excessive pressures on personnel, which results in cutting corners, an inefficient use of valuable resources, decreases the quality of work, decreases the volume of outputs, and negatively affects the ability to meet divisional objectives	LOW	LOW	LOW
5	Does management review work assignments and workload distribution to ensure that one or few individuals do not perform a majority of the work? (concentration of duties increases the probability of diminished quality)	YES	Monthly reports		LOW	LOW	LOW
	Principle 6 – Define Objectives and Risk Tolerances						
6	Does your division have a document that is regularly updated that addresses the division's mission, goals, and objectives?	YES		Management does not clearly define specific business objectives, which inhibits the effective utilization of scarce resources	LOW	LOW	LOW
6	Are there common risk events (internal and external things that would prevent you from completing your objectives) that you encounter on a regular basis when working to complete your divisional objectives?	NO	Nothing on a regular basis	The unwillingness to identify and assess common risk events results in non-existent or inadequate risk response measures necessary to meet divisional objectives	LOW	LOW	LOW
6	In terms of employee behavior in completing tasks, are you task-centric (prioritize outcomes and results) or are you process-centric (completing tasks by following protocols)?	YES	Task-centric mainly, have to be both in certain situations	Management does not define risk tolerance in specific and measurable terms enabling employees to make subjective decisions in terms of acceptable behavior, variations in performance, the level of precision and accuracy, judgments about materiality, and deviations from accepted business practice	LOW	LOW	LOW
6	On a scale of 1 to 5, one being risk averse and 5 being risk seeker, how would you grade your risk tolerance?	YES	3		LOW	LOW	LOW
	Principle 7 - Identify, Analyze, and Respond to Risks						
7	Other than the annual risk assessment, does your division employ other means of identifying analyzing and responding to risks that may inhibit the achievement of divisional objectives? (Employee feedback, operational results)	YES	Communication with employees and customers	Lack of formal or informal avenues to identify and assess current or emergent business risks prevents efficient use of resources and diminished ability to complete divisional objectives	LOW	LOW	LOW
7	How are risks analyzed to estimate their significance to provide a basis for responding?	YES	Analyze by facts and data, brainstorming		LOW	LOW	LOW
	Principle 8 – Assess Fraud Risk						

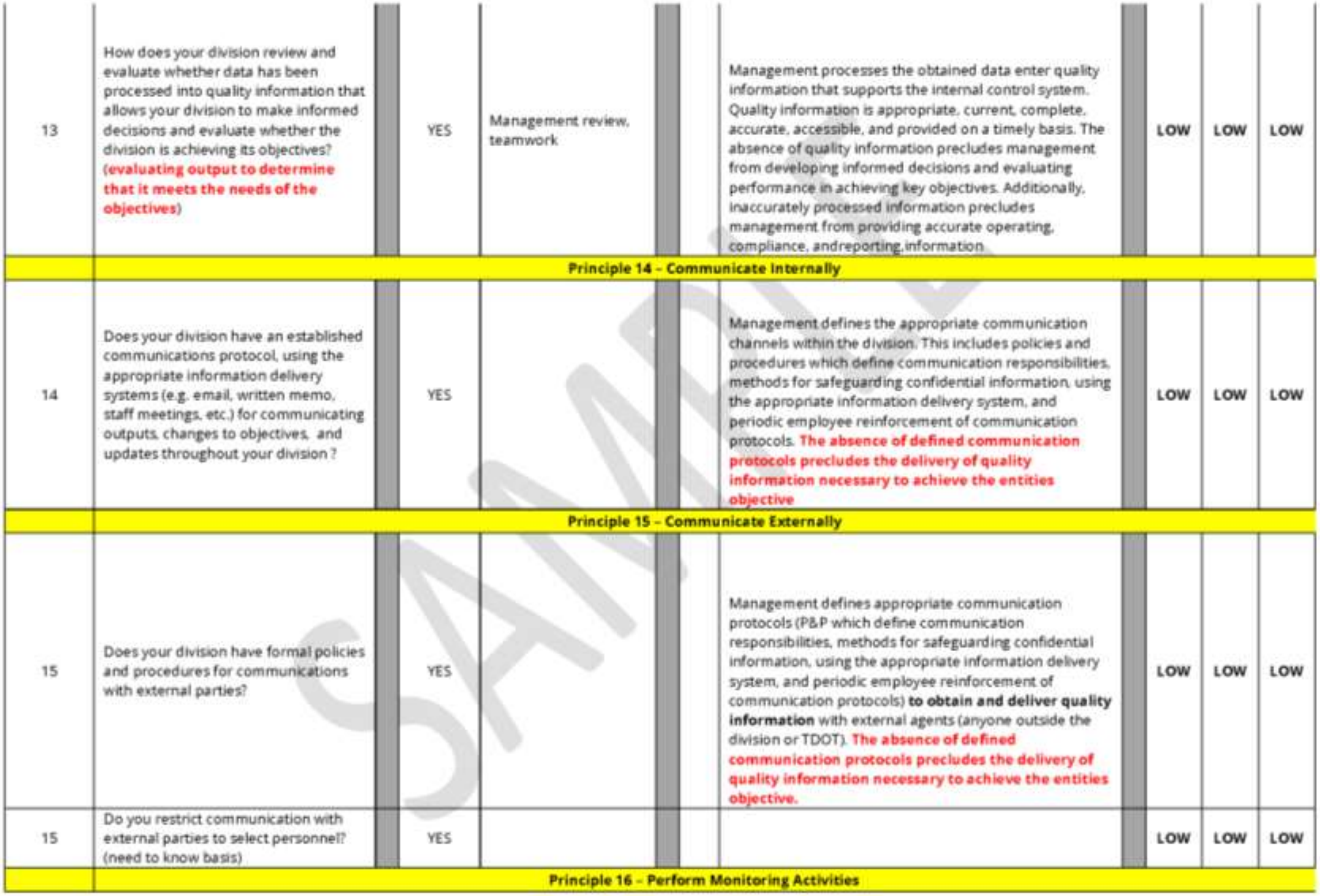


8	Are you aware of any fraud that has occurred in the past year involving any of your division's activities?	NO			Managers are required by State Law to report all instances of fraud, waste, and abuse of TDOT assets and resources	LOW	LOW	LOW
8	How do you identify potential frauds that may occur within your division's business objectives? What potential frauds have you identified?	YES	Policies, procedures, reviews, separation of duties		Lack of formal or informal avenues to identify and assess potential instances of fraud prevents efficient safeguarding of TDOT assets.	LOW	LOW	LOW
8	What specific measures have you, or your middle managers, taken to prevent or detect fraud? (Job rotation, require leave time, reviews, and reconciliations etc.)	YES	Reconciliations, reviews, separation of duties, don't take cash		Lack of specific fraud prevention measures for critical positions facilitate instances of fraud, waste, and abuse of limited resources	LOW	LOW	LOW
8	Does your division have responsibility over valuable assets or equipment (greater than $5000)? If yes, what controls are in place to ensure that those valuable assets are secure and safeguarded?	YES	Cameras, locked gates, physical securities, log sheets		Inability or improper security over valued assets results in non-compliance with state laws (potential civil or criminal implications) and facilitates the opportunity for theft and property loss	LOW	LOW	LOW
8	Is access to divisional records and resources limited to authorized personnel?	NO	No restricted documents		Lack of or inappropriate Access Controls facilitates opportunity for improper edits, deletions, or creation of documents that do not support the true nature of a business transaction.	LOW	LOW	LOW
8	How do you ensure that all transactions are completely and accurately recorded?	YES	Reconciliations, separation of duties, external reviews		Lack of specific review and reconciliation procedures obscures the true nature of the transactions	LOW	LOW	LOW
8	Do you maintain confidential information? How do you secure the information?	YES	Physical locks and security		Lack of, or inappropriate, controls over confidential information facilitates opportunities for unauthorized retrieval, use, and disclosure of sensitive organizational data	LOW	LOW	LOW
8	Are your employees aware of proper methods for reporting suspected fraudulent actions?	YES			Employees are not instructed or informed about avenues for reporting potential fraud, waste, and abuse of TDOT resources inhibits the identification of individuals perpetrating the fraud and other internal control issues	LOW	LOW	LOW
	Principle 9 - Identify, Analyze, and Respond to Change							
9	Does your division have the ability to re-define your business objectives, processes, and activities if necessary?	PARTIAL	Not TDOT objectives		Inability to redefine or redesign business processes or objectives to meet changing organizational requirements facilitates inefficient and ineffective use of scarce resources and becomes a limiting factor when addressing internal control deficiencies	LOW	LOW	LOW

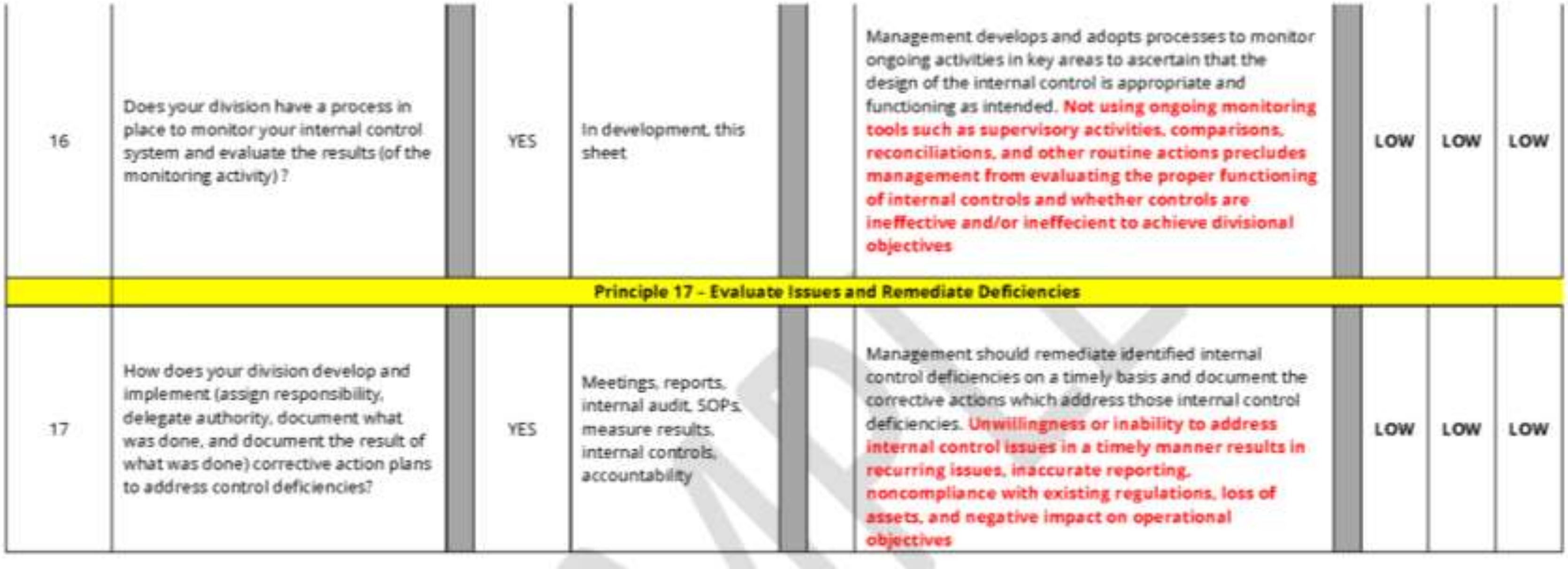
9	How do you identify, respond, and ensure compliance to changes in federal and state regulations.	YES	Receive updates from TDOT legal and feds	Ineffective internal risk identification and risk assessment procedures hinder effective change management especially when external factors necessitate prompt response	LOW	LOW	LOW
9	How do you communicate changes to staff?	YES	Meetings as needed, verbal communication, e-mail	Ineffective communication channels throughout the organization inhibit management's ability to respond to identified changes and related risks in order to maintain an effective internal control system	LOW	LOW	LOW
	Principle 10 – Design Control Activities						
10	Is there supervisory or independent review of work products?	YES	Supervisory	Lack of supervisory or management reviews diminishes the preventive and detective value of internal controls; Lack of supervisory or management reviews facilitates inconsistent performance, decreased output quality, inaccurate records and transactions, diminished physical control over valued assets, inappropriate information flow, and lack of individual accountability	LOW	LOW	LOW
10	Is the quality of staff work inspected?	YES			LOW	LOW	LOW
10	Do you generate an internal report that summarizes the work of the division for the year that is compared to the plans, goals, and objectives?	YES	3 major things accomplished	Lack of top-Level reviews of actual vs. expected performance hinders the evaluation of management's effectiveness and efficiency in deploying taxpayer resources	LOW	LOW	LOW
10	Does your division hire external consultants and contractors? If yes, how does your division monitor the quality of their contracted work?	NO		Inability to properly supervise consultants facilitates inconsistent performance, decreased output quality, inaccurate records and transactions, diminished physical control over valued assets, inappropriate information flow, and lack of individual accountability	LOW	LOW	LOW
10	Are key duties and responsibilities separated among employees? (separation of incompatible duties require that the same person must not be able to authorize, perform, record, or review the same transaction)	YES	Separation of duties	Lack of separation of incompatible duties increases opportunities for errors, misuse of resources, misappropriation, and fraud	LOW	LOW	LOW
	Principle 11 – Design Activities for the Information System						
11	Does your division utilize proprietary IT applications? If yes, who within your division has the responsibility for ensuring the proper functioning of those IT applications?	YES	Utilized, not managed	Lack of defined responsibilities limits management's ability to ensure the proper functioning of business unit specific IT applications and processes	LOW	LOW	LOW



11	Is access to IT applications limited to appropriate personnel? (have you built-in security management within your application?)		YES	Applications are administrated appropriately			Inappropriate access and security controls facilitate inaccurate, incomplete, and invalid data elements to critical information systems		LOW	LOW	LOW
11	How does your division ensure the completeness, accuracy, and integrity (validity) of your proprietary information system (processing controls)		YES	Review physically					LOW	LOW	LOW
11	Does your division employ Systems Development Life Cycle (SDLC) or a similar framework to ensure that applications continue to meet the needs of your users and the business objectives?		NO	Outdated			Lack of a defined control activity over the acquisition, development, and maintenance of information technology inhibits the effective achievement of divisional objectives, changes in the business environment, and responses to emerging risks		HIGH	HIGH	HIGH
	Principle 12 - Implement Control Activities										
12	Does your division have a document that delineates the policies the internal control responsibilities of your business objectives?		YES				Management demonstrates implemented control activities through policies; lack of formalized documentation regarding internal control responsibilities prevents the effective achievement of objectives and hinders effective monitoring of the control activity (whether the control is designed appropriately and functiuoning as intended)		LOW	LOW	LOW
12	Does your division have a mechanism in place to periodically review your implemented management controls for each specific tasks or objective?		YES						LOW	LOW	LOW
	Principle 13 - Use Quality Information to Achieve Objectives										
13	On a regular basis, does your division review and document the information requirements to achieve key objectives and address the risks of the division?		YES				Management identifies key information requirements needed to achieve the entity's objectives. Inability to identify and define key information requirements prevents the division from meeting objectives and mitigating risks.		LOW	LOW	LOW
13	How does your division ensure that (internally and externally sourced) data/reports that you rely opon to develop your output is accurate, valid, complete, and timely?		YES	Validated through multiple sources, using disparate information through variety of sources to validate data			Inability to assess the reliability of sourced information, whether it is used for operational financial or compliance matters, precludes management from providing quality output relevant to its activities and objectives		LOW	LOW	LOW

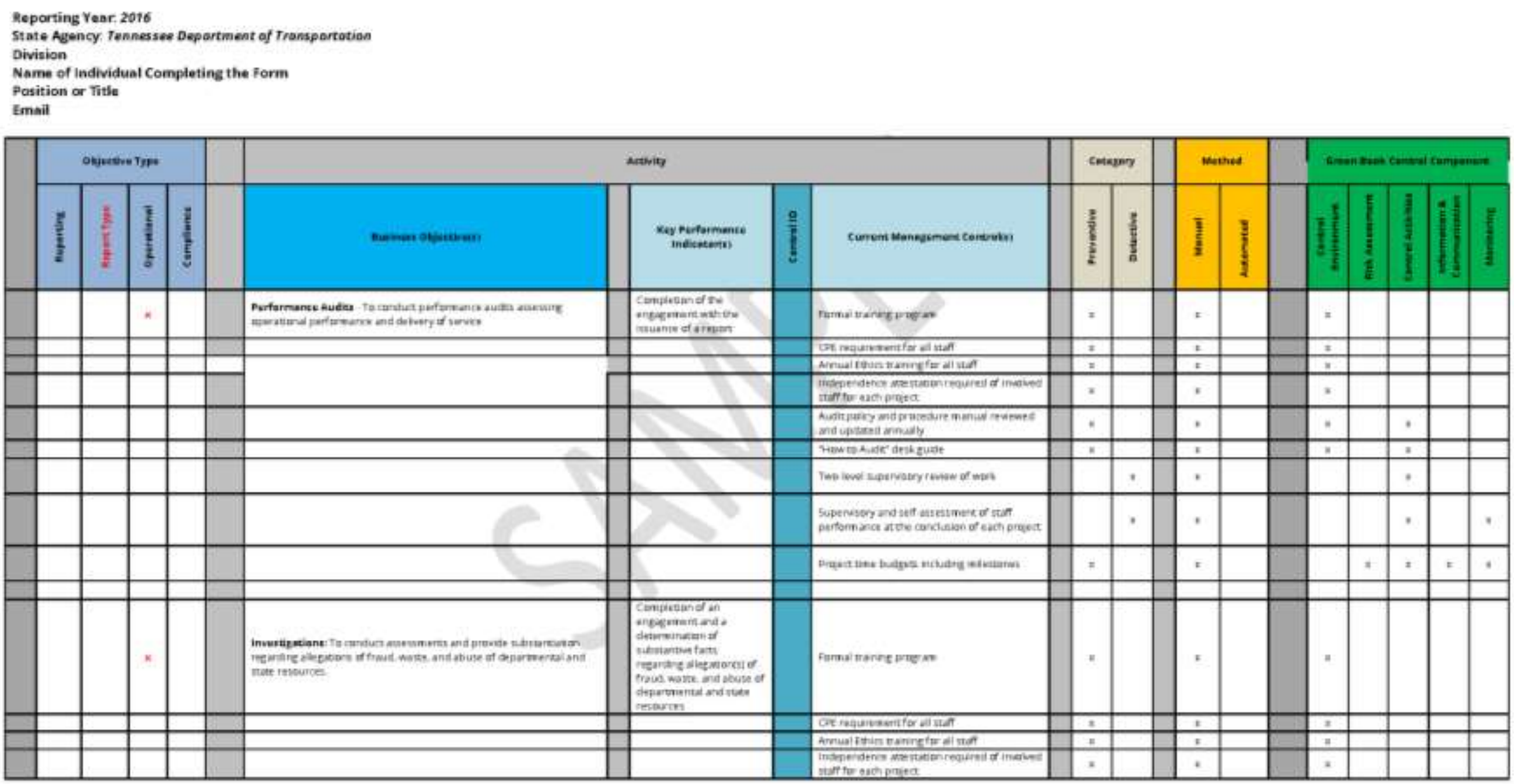


13	How does your division review and evaluate whether data has been processed into quality information that allows your division to make informed decisions and evaluate whether the division is achieving its objectives? **(evaluating output to determine that it meets the needs of the objectives)**		YES	Management review, teamwork			Management processes the obtained data enter quality information that supports the internal control system. Quality information is appropriate, current, complete, accurate, accessible, and provided on a timely basis. The absence of quality information precludes management from developing informed decisions and evaluating performance in achieving key objectives. Additionally, inaccurately processed information precludes management from providing accurate operating, compliance, andreporting information		LOW	LOW	LOW
	Principle 14 – Communicate Internally										
14	Does your division have an established communications protocol, using the appropriate information delivery systems (e.g. email, written memo, staff meetings, etc.) for communicating outputs, changes to objectives, and updates throughout your division ?		YES				Management defines the appropriate communication channels within the division. This includes policies and procedures which define communication responsibilities, methods for safeguarding confidential information, using the appropriate information delivery system, and periodic employee reinforcement of communication protocols. **The absence of defined communication protocols precludes the delivery of quality information necessary to achieve the entities objective**		LOW	LOW	LOW
	Principle 15 – Communicate Externally										
15	Does your division have formal policies and procedures for communications with external parties?		YES				Management defines appropriate communication protocols (P&P which define communication responsibilities, methods for safeguarding confidential information, using the appropriate information delivery system, and periodic employee reinforcement of communication protocols) **to obtain and deliver quality information** with external agents (anyone outside the division or TDOT). **The absence of defined communication protocols precludes the delivery of quality information necessary to achieve the entities objective.**		LOW	LOW	LOW
15	Do you restrict communication with external parties to select personnel? (need to know basis)		YES						LOW	LOW	LOW
	Principle 16 – Perform Monitoring Activities										



16	Does your division have a process in place to monitor your internal control system and evaluate the results (of the monitoring activity) ?		YES	In development, this sheet		Management develops and adopts processes to monitor ongoing activities in key areas to ascertain that the design of the internal control is appropriate and functioning as intended. **Not using ongoing monitoring tools such as supervisory activities, comparisons, reconciliations, and other routine actions precludes management from evaluating the proper functioning of internal controls and whether controls are ineffective and/or ineffecient to achieve divisional objectives**		LOW	LOW	LOW
	Principle 17 - Evaluate Issues and Remediate Deficiencies									
17	How does your division develop and implement (assign responsibility, delegate authority, document what was done, and document the result of what was done) corrective action plans to address control deficiencies?		YES	Meetings, reports, internal audit, SOPs, measure results, internal controls, accountability		Management should remediate identified internal control deficiencies on a timely basis and document the corrective actions which address those internal control deficiencies. **Unwillingness or inability to address internal control issues in a timely manner results in recurring issues, inaccurate reporting, noncompliance with existing regulations, loss of assets, and negative impact on operational objectives**		LOW	LOW	LOW

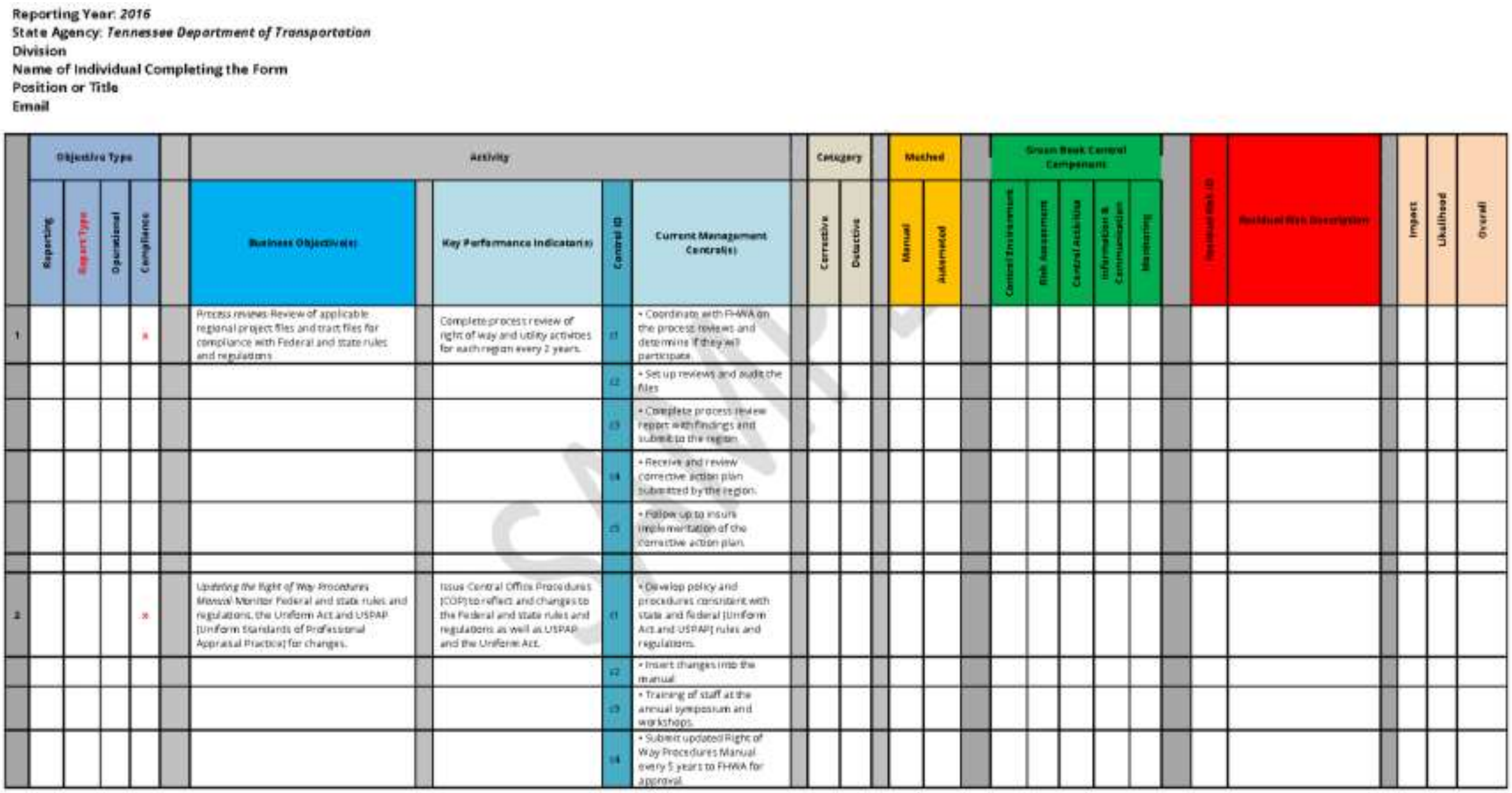
Sample Form 4 – Activity-Specific Controls



Reporting Year: *2016*
State Agency: *Tennessee Department of Transportation*
Division
Name of Individual Completing the Form
Position or Title
Email

Objective Type				Activity				Category		Method		Green Book Control Component				
Reporting	Report Type	Operational	Compliance	Business Objective(s)	Key Performance Indicator(s)	Control ID	Current Management Control(s)	Preventive	Detective	Manual	Automated	Control Environment	Risk Assessment	Control Activities	Information & Communication	Monitoring
		x		**Performance Audits** - To conduct performance audits assessing operational performance and delivery of service	Completion of the engagement with the issuance of a report		Formal training program	x		x		x				
							CPE requirement for all staff	x		x		x				
							Annual Ethics training for all staff	x		x		x				
							Independence attestation required of involved staff for each project	x		x		x				
							Audit policy and procedure manual reviewed and updated annually	x		x		x		x		
							"How to Audit" desk guide	x		x		x		x		
							Two level supervisory review of work		x	x				x		
							Supervisory and self assessment of staff performance at the conclusion of each project		x	x				x		x
							Project time budgets including milestones	x		x			x	x	x	x
		x		**Investigations**: To conduct assessments and provide substantiation regarding allegations of fraud, waste, and abuse of departmental and state resources.	Completion of an engagement and a determination of substantive facts regarding allegation(s) of fraud, waste, and abuse of departmental and state resources		Formal training program	x		x		x				
							CPE requirement for all staff	x		x		x				
							Annual Ethics training for all staff	x		x		x				
							Independence attestation required of involved staff for each project	x		x		x				

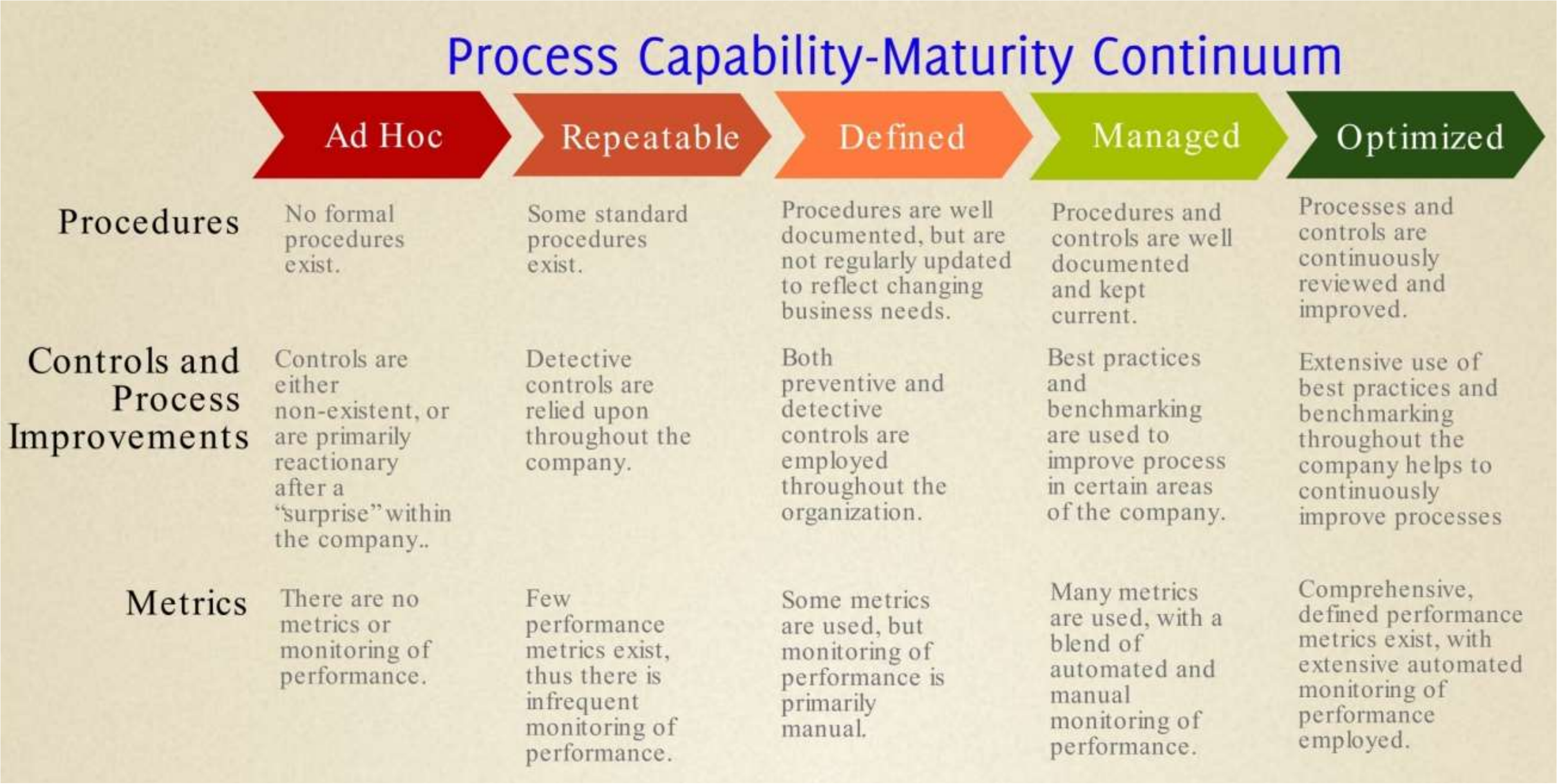
Sample Form 4 – Activity-Specific Residual Risk Assessment



Reporting Year: *2016*
State Agency: ***Tennessee Department of Transportation***
Division
Name of Individual Completing the Form
Position or Title
Email

	Objective Type				Activity				Category		Method		Green Book Control Component					Residual Risk ID	Residual Risk Description	Impact	Likelihood	Overall
	Reporting	Report Type	Operational	Compliance	Business Objective(s)	Key Performance Indicator(s)	Control ID	Current Management Control(s)	Corrective	Detective	Manual	Automated	Control Environment	Risk Assessment	Control Activities	Information & Communication	Monitoring					
1				x	*Process reviews*: Review of applicable regional project files and tract files for compliance with Federal and state rules and regulations	Complete process review of right of way and utility activities for each region every 2 years.	c1	• Coordinate with FHWA on the process reviews and determine if they will participate.														
							c2	• Set up reviews and audit the files														
							c3	• Complete process review report with findings and submit to the region.														
							c4	• Receive and review corrective action plan submitted by the region.														
							c5	• Follow up to insure implementation of the corrective action plan.														
2				x	*Updating the Right of Way Procedures Manual*: Monitor Federal and state rules and regulations, the Uniform Act and USPAP (Uniform Standards of Professional Appraisal Practice) for changes.	Issue Central Office Procedures (COP) to reflect and changes to the Federal and state rules and regulations as well as USPAP and the Uniform Act.	c1	• Develop policy and procedures consistent with state and federal (Uniform Act and USPAP) rules and regulations.														
							c2	• Insert changes into the manual														
							c3	• Training of staff at the annual symposium and workshops.														
							c4	• Submit updated Right of Way Procedures Manual every 5 years to FHWA for approval.														

APPENDIX B – MATURITY MATRIX



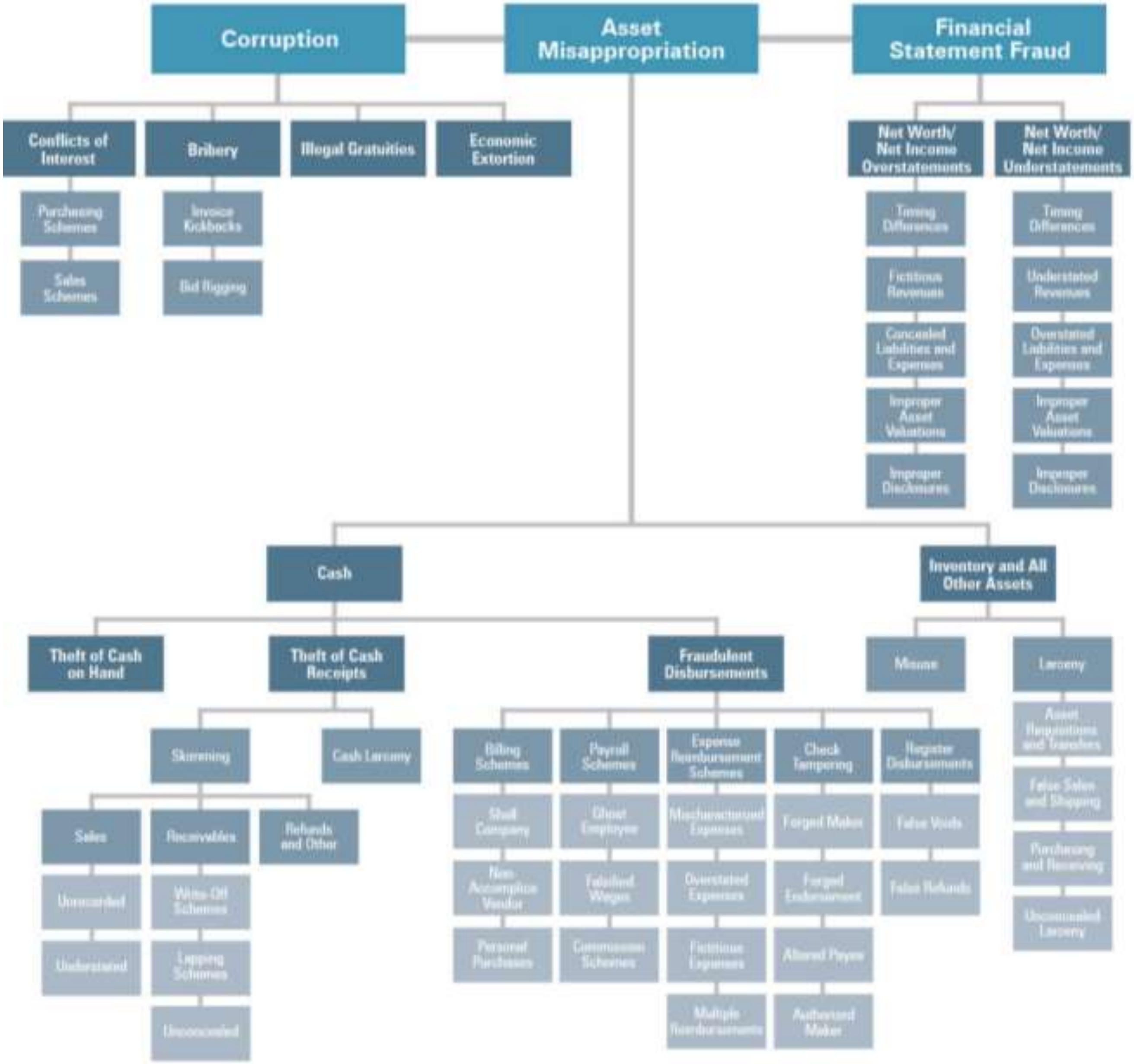
Process Capability-Maturity Continuum

	Ad Hoc	Repeatable	Defined	Managed	Optimized
Procedures	No formal procedures exist.	Some standard procedures exist.	Procedures are well documented, but are not regularly updated to reflect changing business needs.	Procedures and controls are well documented and kept current.	Processes and controls are continuously reviewed and improved.
Controls and Process Improvements	Controls are either non-existent, or are primarily reactionary after a “surprise” within the company..	Detective controls are relied upon throughout the company.	Both preventive and detective controls are employed throughout the organization.	Best practices and benchmarking are used to improve process in certain areas of the company.	Extensive use of best practices and benchmarking throughout the company helps to continuously improve processes
Metrics	There are no metrics or monitoring of performance.	Few performance metrics exist, thus there is infrequent monitoring of performance.	Some metrics are used, but monitoring of performance is primarily manual.	Many metrics are used, with a blend of automated and manual monitoring of performance.	Comprehensive, defined performance metrics exist, with extensive automated monitoring of performance employed.

Source: Carnegie Mellon University

APPENDIX C – THE FRAUD TREE

OCCUPATIONAL FRAUD AND ABUSE CLASSIFICATION SYSTEM



Source: Association of Certified Fraud Examiners