Internal Control Guide

CTR Statewide Risk Management

Table of Contents

Commonwealth of Massachusetts
OFFICE OF THE COMPTROLLER
One Ashburton Place, 9th Floor
Boston, Massachusetts 02108
(617) 727-5000
macomptroller.org

William McNamara
Comptroller

To: Legislative Leadership, Judicial Branch Administrators, Elected Officials, Secretariats, Department Heads, Internal Control Officers, and Chief Fiscal Officers
From: William McNamara, Comptroller of the Commonwealth
Date: May 2022
Re: Internal Control Guide

Protection of public assets is more important than ever before. We find ourselves under the constant threat of cyber attacks and fraud attempts that will only increase in frequency and sophistication. As stewards of taxpayer resources, we must all work together to ensure that the entire Commonwealth is adapting to these ever-changing challenges. This Internal Control Guide is a framework for every department to build robust and resilient defenses against those who would seek to defraud or steal from the public.

Under Chapter 647 of the Acts of 1989, the Comptroller is responsible for developing guidelines for all Commonwealth departments to use when creating and strengthening their own internal control guidelines. The Office of the Comptroller has created this guide based on government and industry best practices. We are committed to keeping this guide fresh and insightful, so that it is useful to departments facing ever-changing risks.

Internal Controls involve everyone at all levels of each Commonwealth organization. Your department is obligated to review and update your Internal Control Plan on an annual basis, as well as whenever there is a new objective, risk, or management structure.

The Office of the Comptroller has training resources available to all Commonwealth organizations, and is always available to assist your department build, review, strengthen, your internal controls. Please contact the CTR Solution Desk to reach out at any time.

We look forward to partnering with you in protecting the assets of the Commonwealth of Massachusetts.

Sincerely,

William McNamara

Introduction

In the Commonwealth of Massachusetts, the State Auditor introduced legislation requiring the development and implementation of internal controls for Commonwealth agencies. As a result, Massachusetts became one of the first states to enact internal control legislation. This Legislation, known as Chapter 647 of the Acts of 1989, An Act Relative to Improving the Internal Controls within State Agencies, directed the Office of the Comptroller (CTR) to develop internal control guidelines for state agencies.

The purpose of The Internal Control Guide is twofold: It is designed to assist departments in designing, documenting, and implementing internal controls. In addition, it provides the format that departments must use when writing and updating their Internal Control Plans (ICPs).

This guide is based on the Committee of Sponsoring Organizations' (COSO) Enterprise Risk Management Framework (ERM) with its eight components and seventeen principles. Additionally, the guide incorporates the Standards for Internal Control in the Federal Government's (known as the Green Book) adaption of COSO's Internal Control — Integrated Framework (2013).

The guide emphasizes "Points of Focus" that are applicable to a government environment.

To be considered compliant, a department's Internal Control Plan must contain the eight components of COSO's ERM Framework:

1. Internal Environment
2. Objective Setting
3. Event Identification
4. Risk Assessment
5. Risk Response
6. Control Activities
7. Information and Communication
8. Monitoring

The subsequent pages provide an outline mapping each ERM Component and Principle(s) with corresponding Points of Focus.

Outline of Components, Principles and Points of Focus

Component	Principles	Point(s) of Focus
Section 1: Internal Environment	1. Demonstrate commitment to integrity and ethical values	1.01. Tone at the top 1.02. Mission Statement 1.03. Standards of Conduct and Adherence to these Standards
	2. Exercise oversight responsibilities	2.01. Oversight structure 2.02. Oversight for internal control system
	3. Establish structure, authority, and responsibility	3.01. Organizational structure 3.02. Assignment of responsibility and delegation of authority 3.03. Documentation of the internal control system
	4. Demonstrate commitment to competence	4.01. Expectation of competence 4.02. Recruitment, development, and retention of individuals
	5. Enforcement of accountability	5.01. Enforcement of accountability
Section 2: Objective Setting	6. Define strategic goals, objectives, risk appetite and risk tolerances	6.01. Definitions of strategic goals, and objectives 6.02. Definition of risk appetite and risk tolerance
Section 3: Event Identification	7. Identify risks	7.01. Identification of risks 7.02. Fraud risk factors and types
Section 4: Event Identification	8. Assess risks	8.01. Analyze risks
Section 5: Risk Response	9. Respond to risks	9.01. Risk response categories 9.02. Response to fraud risks

Section 6: Control Activities	10. Design control activities	10.01. Response to objectives and risks
		10.02. Design of the appropriate types of control activities
		10.03. Design of control activities at various
		10.04. Segregation of duties
	11. Design activities for the information system	11.01. Design of the entity's information system
		11.02. Design of appropriate types of control activities
		11.03. Design of information technology
		11.04. Design of security management
	12. Implement control activities	12.01. Documentation of responsibilities through policies
		12.02. Periodic review of control activities
Section 7: Information & Communication	13. Use quality information	13.01. Identification of information requirements
		13.02. Relevant data from reliable sources
		13.03. Data processed into quality information
	14. Communicate internally	14.01. Communication through the entity
		14.02. Appropriate methods of communication
	15. Communicate externally	15.01. Communication with external parties
		15.02. Appropriate methods for communication
Section 8: Monitoring	16. Perform monitoring activities	16.01. Monitor each ERM component
		16.02. Evaluation of results
	17. Evaluate issues and remediate deficiencies	17.01. Reporting of issues
		17.02. Evaluation of issues
		17.03. Corrective actions

Chapter 1 – Components, Principles, and Points of Focus

Section 1: Internal Environment Component

Overview

The internal environment is the foundation for all other components of internal control, providing discipline and structure. Moreover, management establishes the tone from the top regarding the importance of internal control and expected standards of conduct and reinforces expectations at various levels. Internal environment factors include the integrity, ethical values and competence of the entity's people; the way management assigns authority and responsibility and organizes and develops its people; and the attention and direction provided by the oversight body.

Principles and Points of Focus Relating to Internal Environment

Principles are required in supporting an effective design, implementation, and operation of the associated component. Points of focus act as additional information and may contain examples to further explain what a requirement means and what it is intended to cover.

Component	Principles	Point(s) of Focus
Section 1: Internal Environment	1. Demonstrate commitment to integrity and ethical values	1.01. Tone at the top 1.02. Mission Statement 1.03. Standards of Conduct and Adherence to these Standards
	2. Exercise oversight responsibilities	2.01. Oversight structure 2.02. Oversight for internal control system
	3. Establish structure, authority, and responsibility	3.01. Organizational structure 3.02. Assignment of responsibility and delegation of authority 3.03. Documentation of the internal control system
	4. Demonstrate commitment to competence	4.01. Expectation of competence 4.02. Recruitment, development, and retention of individuals
	5. Enforcement of accountability	5.01. Enforcement of accountability

Following is a discussion of each of the Principles and Points of Focus

Component	Principles	Point(s) of Focus
Section 1: Internal Environment	1. Demonstrate commitment to integrity and ethical values	1.01. Tone at the top 1.02. Mission Statement 1.03. Standards of Conduct and Adherence to these Standards

1. Demonstrate Commitment to Integrity and Ethical Values

1.01. Tone at the Top

Management's attitude, actions, and values set the tone of an organization, influencing the control consciousness of its people. Internal controls are likely to function well if management believes that those controls are important and communicates that view to employees at all levels. Employees are aware of the practices followed by upper management including those that circumvent internal controls. Despite policies to the contrary, employees who note that their managers frequently override controls, will also view internal controls as "red tape" to be "cut through" to get the job done. Management can show a positive attitude toward internal control by such actions as complying with their own policies and procedures, discussing internal controls at management and staff meetings, and rewarding employees for following good internal control practices.

1.02. Mission Statement

A mission statement clearly identifies an organization's purpose and how it is accomplished. It should be a brief paragraph that is easily understood by the reader, including those outside the organization or field.

An organization's mission statement may remain current for a number of years. However, it is a good idea to review it periodically – such as part of the annual internal control plan review – to ensure it up to date.

1.03. Standards of Conduct and Adherence to These Standards

Management should establish standards of conduct to communicate expectations concerning integrity and ethical values. The standards of conduct guide the directives, attitudes, and behaviors of the department in achieving its objectives. Management, with oversight from the Department head, defines the department's expectations of ethical values in the standards of conduct. Management may consider using policies, operating principles, or guidelines to communicate the standards of conduct to the department.

To ensure adherence to the standards of Conduct, management should evaluate the directives, attitudes, and behaviors of individuals and teams. These may consist of ongoing monitoring or separate evaluations. Individual personnel can also report issues through reporting lines, such as regular staff meetings, upward feedback processes, a whistle-blowing program, or an ethics hotline.

Massachusetts officials' or employees' conduct is also governed by M.G.L. c. 268A. The Conflict of Interest Law regulates the conduct of all state, county and municipal employees and volunteers, whether paid or unpaid, full or part-time, intermittent or temporary. General Law Chapter 268A governs what public officials and employees may do on the job, what they may do after hours, or on the side, and what they may do after they leave public service. Another source to consider is the NAGE Code of Conduct (https://www.mass.gov/doc/code-of-conduct-nage-unit-6/download).

Component	Principles	Point(s) of Focus
Section 1: Internal Environment	2. Exercise oversight responsibilities	2.01. Oversight structure 2.02. Oversight for internal control system

2. Exercise Oversight Responsibilities

2.01. Oversight Structure

An oversight body oversees the department's operations; provides constructive criticism to management; and where appropriate, makes oversight decisions so that the department achieves its objectives in alignment with the department's integrity and ethical values.

The term "oversight body", as used in this guide, can refer to a board of directors/ governors/regents/trustees, or an advisory/supervisory board. A board is a group of elected or appointed members who jointly oversee the activities of a company or organization.

Typical duties of an oversight body can include:

- Governing the organization by establishing broad policies and objectives;
- Selecting, appointing, supporting, and reviewing the performance of the chief executive;
- Ensuring the availability of adequate financial resources;
- Reviewing and/or approving annual budgets, policies, financial statements;
- Accountability to the stakeholders for the organization's performance;
- Setting the salaries and compensation of management

For most state agencies, "oversight body" refers to the department head and/or senior staff. Executive branch departments also get guidance from secretariats. For other agencies, like the Office of the Comptroller, there is a legislated board (in this case an "advisory board") designated to "provide advice and counsel…". Likewise, each state university and community college and has its own boards of trustees.

2.02. Oversight for the Internal Control System

The oversight body oversees management's design, implementation, and operation of the entity's internal control system with relation to the components.

Component	Principles	Point(s) of Focus
Section 1: Internal Environment	3. Establish structure, authority, and responsibility	3.01. Organizational structure 3.02. Assignment of responsibility and delegation of authority 3.03. Documentation of the internal control system

3. Establish Structure, Authority and Responsibility

3.01. Organizational Structure

An organizational structure is necessary to enable a department to plan, execute, control, and assess the achievement of its objectives. Management develops and assigns these responsibilities to groups (divisions,

offices, subunits, etc.) to enable the department to operate in an efficient and effective manner, comply with applicable laws and regulations, and reliably report quality information. Periodically, management should evaluate the organizational structure to ensure it meets its objectives (and makes changes accordingly).

3.02. Assignment of Responsibility and Delegation of Authority

As noted above, management develops and assigns responsibility. Management also evaluates the delegation for proper segregation of duties within the unit and in the organizational structure. Segregation of duties helps prevent fraud, waste, and abuse in the entity by considering the need to separate authority, custody, and accounting in the department.

3.03. Documentation of the Internal Control System

Effective documentation helps with the design an effective internal control as it communicates the who, what, when, where, and why of internal control execution to personnel. Documentation also provides a means to retain organizational knowledge and mitigate the risk of having that knowledge limited to a few personnel, as well as a means to communicate that knowledge as needed to external parties, such as auditors.

Component	Principles	Point(s) of Focus
Section 1: Internal Environment	6. Demonstrate commitment to competence	4.01. Expectation of competence 4.02. Recruitment, development, and retention of individuals

4. Demonstrate Commitment to Competence

4.01. Expectations of Competence

Competence requires relevant knowledge, skills and abilities, and is gained mainly from professional experience, training, and certifications. In establishing expectations for competence, standards of conduct, assigned responsibility, delegated authority, and policies should be considered. These competencies should be evaluated where the oversight body performs such review of both management and staff.

4.02. Recruitment, Development, and Retention of Individuals

Once management has recruited qualified personnel, the necessary training should be provided to new hires (and current personnel alike) depending on their roles, professional requirements (i.e. CPEs), and standards of conduct. Management should consider incentives to motivate and reinforce expected levels of performance and conduct.

Component	Principles	Point(s) of Focus
Section 1: Internal Environment	5. Enforcement of accountability	5.01. Enforcement of accountability

5. Enforcement of Accountability

5.01. Enforce Accountability

Management should hold personnel accountable through mechanisms such as performance appraisals and disciplinary actions. Note that accountability is driven by the tone at the top and supported by the commitment to integrity and ethical values, organizational structure, and expectations of competence – all of which influence the control culture of the department.

Section 2: Objective Setting Component

Overview

Objectives are set at the strategic level in support of the entity's mission and high level goals. The objective setting component acts as the precondition to effective event identification, risk assessment and risk response as the established objectives are aligned with the entity's risk appetite and risk tolerance levels.

Principle and Points of Focus Relating to Objective Setting

Principles are required in supporting an effective design, implementation and operation of the associated component. Points of focus act as additional information and may contain examples to further explain what a requirement means and what it is intended to cover.

Section 2**:** Objective Setting	6. Define strategic goals, objectives, risk appetite and risk tolerances	6.01. Definitions of strategic goals, and objectives 6.02. Definition of risk appetite and risk tolerance

6. Define Goals, Objectives, Risk Appetite and Risk Tolerances

6.01. Definition of Strategic Goals, and Objectives

Strategic Goals

A goal is an end result the organization wants to attain. It should be a broad, long-range concept and linked to the department's mission and/or strategic plan. Government managers set department goals and priorities based upon legislative mandates established in statutes (enabling legislation), priorities of constitutional officials and department heads, and within funding authorization set in annual appropriations. Achievement of these goals should be defined by objectives.

Objectives

An objective is an action required to achieve the long-term goal. In contrast to a goal, an objective is narrowly focused and easily measurable. It should, therefore, be an action that can be accomplished in an identified period of time, such as a fiscal year. A good objective is **SMART**:

Specific: What is the single result to be accomplished?

Measurable: How can it be measured? (Some objectives are more difficult to measure; however, they should have observable results.)

Attainable: Is it realistic given the resources currently available?

Results-focused: Does it make a difference if the objective is accomplished?

Timely: Is the timeline realistic?

Management should review the defined objectives so that they are consistent with external requirements and internal expectations. External requirements include the laws, regulations, and standards with which the department is required to comply. Internal expectations (and requirements) are set by management through standards of conduct, oversight and organizational structures, and expectations of competence as part of the internal environment.

6.02. Definition of Risk Appetite and Risk Tolerance

Risk Appetite

The COSO ERM – Understanding and Communicating Risk Appetite document states "Risk appetite is the amount of risk, on a broad level, an organization is willing to accept in pursuit of value. Each organization pursues various objectives to add value and should broadly understand the risk it is willing to undertake in doing so." Therefore, risk appetite is related to the achievement of the organizational goals and objectives; in other words risk appetite and strategy are intertwined. As such, risk appetite should be considered in setting strategies and objectives, and managing risks.

Risk Tolerance

Risk tolerance represents the application of risk appetite to specific objectives. Risk tolerance is defined as the acceptable level of variation in performance relative to the achievement of objectives. At this point, management would consider the relative importance of goals and objectives and align risk tolerances with risk appetite.

Example from COSO ERM – Understanding and Communicating Risk Appetite

Risk Appetite	Risk Tolerance
A health services organization places patient safety amongst its highest priorities. The organization also understands the need to balance the level of immediate response to all patient needs with the cost of providing such service. The organization has a low risk appetite related to patient safety but a higher appetite related to response to all patient needs.	We strive to treat all emergency room patients within two hours and critically ill patients within 15 minutes. However, management accepts that in rare situations (5% of the time) patients in need of non-life-threatening attention may not receive that attention for up to four hours.

Section 3: Event Identification Component

Overview

Management identifies events that could potentially affect the entity, and determines whether they represent opportunities or whether they might affect the entity's ability to achieve its objectives.

Events with negative impact represent risks, which require management's assessment and response. Events with positive impact represent opportunities, which management channels back into the strategy and objective-setting processes.

Though events can have both positive and negative connotations, the following section examines those involving risk.

Principle and Points of Focus Relating to Event Identification

Principles are required in supporting an effective design, implementation, and operation of the associated component. Points of focus act as additional information and may contain examples to further explain what a requirement means and what it is intended to cover.

Section 3: Event Identification	7. Identify risks	7.01. Identification of risks 7.02. Fraud risk factors and types

7. Identify Risks

7.01. Identification of Risk, including Fraud

The types of risks that impact the department should be considered. These include both inherent and residual risk. Inherent risk is the possibility that an event will occur and adversely affect the departments' achievement of its goals and objectives. Assuming management takes steps to address an event, residual risk is what remains after management's response to inherent risk. Management's lack of response to either risk could cause deficiencies in the internal control system.

Moreover, there are also internal and external factors to consider. Internal risk factors include: the internal environment, size of the organization, complexity, personnel, significant related party transactions, accounting estimates and principles that are subject to different interpretations, technological (new IT system), etc. External risk factors include new laws and/or regulations, economic instability, natural disasters, technology (new vendor commerce methods), etc.

Assess Fraud Risk

First and foremost, it is important to note that it is not failures in the systems, policies, procedures, or controls that cause fraud, it is the people (although people can take advantage of such failures). Thus, in assessing, analyzing, and responding to fraud risk, consider first understanding the motivations and rationalizations of people.

One guide to consider in assessing and identifying fraud is the Association of Government Accountant (AGA) Toolkit. As noted on their website (https://www.agacgfm.org/)

"AGA's Fraud Prevention Toolkit provides current, state-of-the-art tools for federal, state, local and tribal government financial managers to use in preventing and detecting fraud. It furthers AGA's mission of "Advancing Government Accountability."

7.02. Fraud Risk Factors and Types – The Fraud Triangle

Fraud risk factors do not necessarily indicate that fraud exists but are often present when fraud occurs. Fraud risk factors include the following:

- Incentive/pressure - Management or other personnel have an incentive or are under pressure to meet deadline or performance target, which provides a motive to commit fraud.

- Opportunity - Circumstances exist, such as the absence of controls, ineffective controls, or the ability of management to override controls, that provide an opportunity to commit fraud.
- Attitude/rationalization - Individuals involved are able to rationalize committing fraud. Some individuals possess an attitude, character, or ethical values that allow them to knowingly and intentionally commit a dishonest act.

While fraud risk may be greatest when all three risk factors are present, one or more of these factors may indicate a fraud risk. Other information provided by internal and external parties can also be used to identify fraud risks. This may include allegations of fraud or suspected fraud reported by internal auditors, personnel, or external parties (i.e. State Auditor or Inspector General) that interact with the entity.

Two general types of fraud are: those intended to benefit the individual (whether inside or outside) the department, at the department's expense, and those performed on behalf of the department.

Some of the fraud schemes that would harm the department for the benefit of the individual include: asset misappropriation, skimming, payroll fraud, expense reimbursement fraud, and disbursement fraud. On the other hand, fraud schemes on behalf of the department include information misrepresentation, tax evasion, bribery, and illegal political contributions and payoffs to government officials.

Section 4: Risk Assessment Component

Overview

Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how risks should be managed.

Its purpose is to assess how big the risks are, both individually and collectively, in order to focus management's attention on the most important threats and opportunities, and to lay the groundwork for risk response. Risk assessment is all about measuring and prioritizing risks so that risk levels are managed within defined tolerance thresholds without being over controlled or forgoing desirable opportunities.

The positive and negative impacts of potential events should be examined, individually or by category, across the entity. Once the applicable risks are identified, the assessment regarding the probability and significance of each risk is critical.

Principle and Point of Focus Relating to Risk Assessment

Principles are required in supporting an effective design, implementation, and operation of the associated component. Points of focus act as additional information and may contain examples to further explain what a requirement means and what it is intended to cover.

Section 4: Event Identification	8. Assess risks	8.01. Analyze risks

8. Assess Risks

8.01. Analyze Risks

The first activity within the risk assessment process is to develop a common set of assessment criteria to be deployed across the entity – subunits, teams, etc.

Assessment Criteria

Some form of measurement of risk is necessary. Scales are defined for rating risks in terms of likelihood and impact. These scales comprise rating levels and definitions that foster consistent interpretation and application by different units/teams in the entity. Scales should allow meaningful differentiation for ranking and prioritization purposes.

Likelihood represents the possibility that a given event will occur. Likelihood can be expressed using qualitative terms (frequent, likely, possible, unlikely, rare), as a percent probability, or as a frequency. A relevant time period should be used when expressing qualitative values (50% chance in any one month; or weekly).

Impact (or consequence) refers to the extent to which a risk event might affect the entity. Impact assessment criteria may include financial, reputational, regulatory, health, safety, security, environmental, employee, vendor/customer, and operational impacts. Entities typically define impact using a combination of these types of considerations given that certain risks may impact the entity financially while other risks may have a greater impact to reputation or health and safety. When assigning an impact rating to a risk, assign the rating for the highest consequence anticipated.

Examples

Likelihood Factors	Impact Factors
• Probability estimates based on history • Complexity of activities • Change or stability (employee turnover or new laws) • Internal Environment (integrity, ethics) • Control Process effectiveness	• Materiality (dollar loss) • Potential Reputation or brand damage • Importance of the related objective to the dept.'s mission • Velocity of occurrence, duration, and /or pervasiveness of the event • Recovery costs

Source: 201 IIA's CIA Learning System

Once the risks have been assessed, the risks should be viewed as a comprehensive portfolio to enable the next step; prioritizing for risk response. The term risk profile represents the entire portfolio of risks facing the entity. Some entities represent this portfolio as a hierarchy, some as a collection of risks plotted on a heat map.

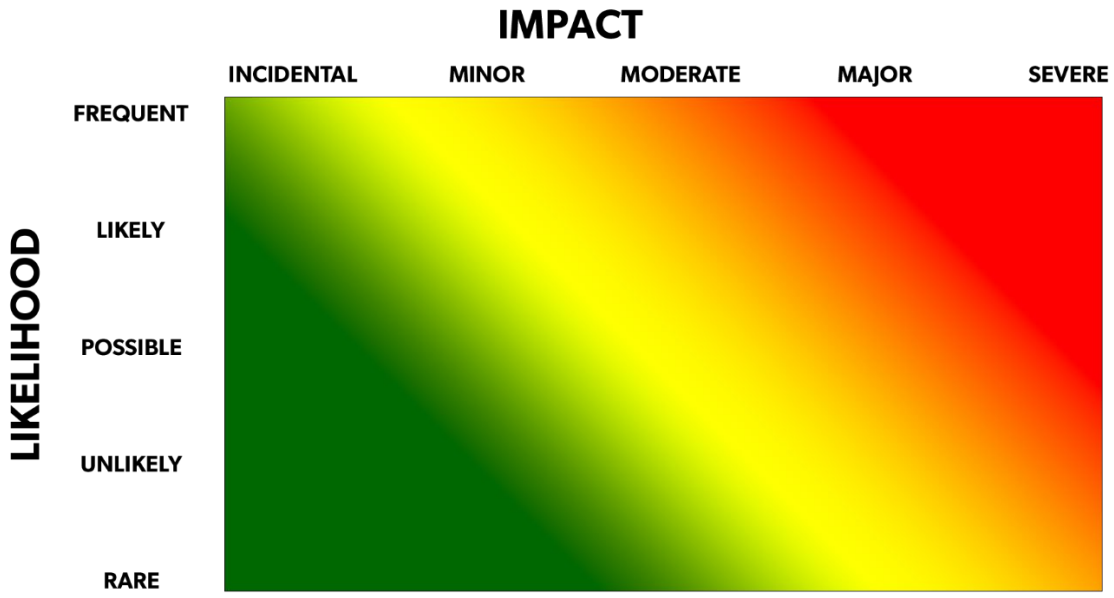
Similar to assessing risks, ranking and prioritizing is often done in a two-step process. First, the risks are ranked according to one, two, or more criteria such as impact rating multiplied by likelihood rating. Second, the ranked risk order is reviewed in light of additional considerations such as impact alone or the size of the gap between current and desired risk level (risk tolerance threshold, see Chapter 2: Objective Setting Component).

One way to view the portfolio is to create a risk map, often called a heat map. These are usually two-dimensional representations of impact plotted against likelihood.

The most common way to prioritize risks is by designating a risk level for each area of the risk map such as very high, high, medium, or low, where the higher the combined impact and likelihood ratings, the higher the overall risk level. The boundaries between levels vary from entity to entity depending on risk appetite (refer to Chapter 2: Objective Setting Component). For example, an entity with a greater risk appetite will have boundaries for its risk levels shifted toward the upper right. Also, some entities adopt asymmetric boundaries placing a somewhat greater emphasis on impact than on likelihood. For example, a risk having an impact rating of moderate and likelihood rating of frequent has an assigned risk level of high, whereas a risk having an impact rating of extreme and a likelihood rating of possible has an assigned risk level of very high.

After plotting on the risk map, risks are then ranked from highest to lowest in terms of risk level. These rankings may then be adjusted based on other considerations such as detailed knowledge of the nature of the impact. For example, within a group of risks having a designation of very high, those risks having extreme health and safety, or reputational impacts may be prioritized over risks having extreme financial impacts but lesser health and safety or reputational impacts.

Risk Map



To be effective and sustainable, the risk assessment process needs to be simple, practical, and easy to understand. Success depends upon executive commitment and resources. Furthermore, COSO's Enterprise Risk Management.

Integrated Framework emphasizes the need to assess and oversee risks from a holistic perspective. The process must sit within a larger framework that uses the information gleaned to make decisions about risk responses and monitoring, and feeds information back into the strategic planning process.

Section 5: Risk Response Component

Overview

Once risks have been assessed, management determines how it will respond. Responses should be designed so that the risks are kept within the defined risk tolerance for the related objective(s). In considering each response, management assesses the effect on risk likelihood and impact, as well as costs and benefits. Attention should be given to how much management is willing to spend in resources to address each risk.

Principle and Points of Focus Relating to Risk Response

Principles are required in supporting an effective design, implementation, and operation of the associated component. Points of focus act as additional information and may contain examples to further explain what a requirement means and what it is intended to cover.

Section 4: Event Identification	8. Assess risks	8.01. Analyze risks

9. Respond to Risks

9.01. Risk Response Categories

Risk response falls into four basic categories: Accept; Avoid; Reduce; Share.

Since government is in the business of providing critical services, whether in the areas of public health, public safety, education, transportation infrastructure, protecting the environment, social services, etc., it is not usually in a position to eliminate risk, but instead must accept risk and do its best to mitigate it. However, as shown below, there are alternatives to accepting all risks.

1. Accept the risk and monitor it: No action is taken based on the insignificance of the risk. For example, one accepts that the weather cannot be controlled, but is prepared to respond to some of its effects (power outages, floods, etc.).
2. Avoid the risk by eliminating it: For example, a budgetary reduction could mean deciding to close a program, eliminating the risks of operating that program. Yet, one must consider that ending a program could lead to another set of risks.
3. Reduce the risk by instituting controls – This is the category where most risk falls, where the response depends on the severity of the risk.
4. Share the risk by partnering with another entity: For example, an agreement with another agency to utilize its resources in an area outside of the host agency's expertise (e.g., an agency must produce coastal zone flood maps and engages the expertise of Information Technology's geographic information services.

9.02. Responses to Fraud Risks

Management should design an overall risk response and specific actions for responding to fraud risks, which can originate both inside and outside of the organization. It may be possible to reduce or eliminate certain fraud risks by making changes to the entity's activities and processes. These changes may include stopping or reorganizing certain operations and reallocating roles among personnel to enhance segregation of duties. In addition to responding to fraud risks, management may need to develop further responses to address the risk of management override of controls.

An excellent resource for learning about fraud risk is the Office of the Comptroller's Fraud Awareness and Prevention class. Contact the CTR's Statewide Learning webpage for details: CTR Statewide Learning.

Section 6: Control Activities Component

Overview

The Control Activities component consists of actions management establishes through policies and procedures to achieve objectives and respond to risks in the internal control system.

Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities including, but not limited to, approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties.

The National Association of State Comptrollers (NASC) Internal Control Self-Assessments tools can assist in determining whether the proper controls are in place for various business processes but should be evaluated for application under the user's unique circumstances. See these documents under https://www.macomptroller.org/internal-controls .

Principles and Points of Focus Relating to Control Activities

Principles are required in supporting an effective design, implementation and operation of the associated component. Points of focus act as additional information and may contain examples to further explain what a requirement means and what it is intended to cover.

Section 6: Control Activities	10. Design control activities	10.01. Response to objectives and risks
		10.02. Design of the appropriate types of control activities
		10.03. Design of control activities at various
		10.04. Segregation of duties
	11. Design activities for the information system	11.01. Design of the entity's information system
		11.02. Design of appropriate types of control activities
		11.03. Design of information technology
		11.04. Design of security management
	12. Implement control activities	12.01. Documentation of responsibilities through policies
		12.02. Periodic review of control activities

Following is a discussion of each of the Principles and Points of Focus

Section 6: Control Activities	10. Design control activities	10.01. Response to objectives and risks
		10.02. Design of the appropriate types of control activities
		10.03. Design of control activities at various
		10.04. Segregation of duties

10. Design Control Activities

10.01. Response to Objectives and Risks

Control activities are designed in response to the department's objectives and risks identified to achieve an effective internal control system. Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives and address related risks.

Policies and Procedures: Distinction

Policies and Procedures are the strategic link between the mission statement and day-to-day operations. Well-written policies and procedures allow employees to clearly understand their roles and responsibilities within predefined limits.

Policies identify the key activities and provide a general strategy to decision-makers on how to handle issues as they arise by providing the reader with limits and a choice of alternatives that can be used to 'guide' their decision making process as they attempt to overcome problems.

Procedures provide the reader with a clear and easily understood plan of action required to carry out or implement a policy. A well-written procedure will also help eliminate common misunderstandings by clearly identifying job responsibilities and establishing boundaries.

10.02. Design of Appropriate Types of Control Activities

Below are some of the control activity categories to consider, but these are not all inclusive of categories specific to a department. For further details on these categories, please refer to the Green Book.

- Top-level reviews of actual performance
- Reviews by management at the functional or activity level
- Management of human capital
- Controls over information processing
- Physical control over vulnerable assets
- Establishment and review of performance measures and indicators
- Segregation of duties (further discussed below)
- Proper execution of transactions
- Accurate and timely recording of transactions
- Access restrictions to and accountability for resources and records
- Appropriate documentation of transactions and internal control (further discussed below)

Control activities can be either preventive or detective.

- A *preventive control* activity prevents an entity from failing to achieve an objective or address a risk. Examples of preventive controls include authorization lists, segregation of duties, and prior supervisory approval.
- A *detective control activity* discovers when an entity is not achieving an objective or addressing a risk before the entity's operation has concluded and corrects the actions so that the entity achieves the objective or addresses the risk. Examples of detective controls include reconciliation, exception reports, and supervisory review.

Control activities can be implemented in either an automated or a manual manner.

- Automated control activities are either wholly or partially automated through the entity's information technology system. Automated control activities tend to be more reliable because they are less susceptible to human error and are typically more efficient.
- Manual control activities are performed by individuals with minor use of the entity's information technology.

10.03. Design of Control Activities at Various Levels

Control Activities can be designed at the entity-level, transaction-level, or both depending on the level of precision needed so that the department meets its objectives and addresses related risks.

Transaction control activities (combination of preventive and detective type controls) may include verifications, reconciliations, authorizations and approvals, physical control activities, and supervisory control activities.

10.04. Segregation of Duties

Management should divide or segregate key duties and responsibilities among different people to reduce the risk of error, misuse, or fraud. This includes separating the responsibilities for:

- authorizing transactions,
- processing and recording them,
- reviewing the transactions, and
- handling any related assets or process so that no one individual controls all key aspects of a transaction or event.

In other words, control activities related to authority, custody, and accounting of operations ought to be separated to achieve adequate segregation of duties.

If segregation of duties is not practical within an operational process because of limited personnel for example, adding closer supervision, cross-training or frequent reviews may be an alternative for this control activity.

Department Head Signature Authorization

A department head is responsible for all activities conducted by the department. Because in most departments the department head cannot personally review and certify all business transactions, the department head sets up the department's business operations with a series of checks and balances (internal controls) to balance risks and efficiencies. Department heads must directly authorize individuals within their chain of command to be their designee for incurring obligations and approving transactions on their behalf. There can be no sub-delegation by designees. See Key State Finance Law Compliance Roles and Responsibilities document. (https://public.powerdms.com/MAComptroller/documents/1861753)

Section 6: Control Activities	11. Design activities for the information system	11.01. Design of the entity's information system
		11.02. Design of appropriate types of control activities
		11.03. Design of information technology
		11.04. Design of security management

11. Design Activities for the Information System

11.01. Design of the Entity's Information System

An information system is the people, processes, data, and technology that management organizes to obtain, communicate, or dispose of information. An information system represents the life cycle of information used for the entity's operational processes that enables the entity to obtain, store, and process quality information.

An information system includes both manual and technology-enabled information processes. Technology-enabled information processes are commonly referred to as information technology.

Information processing objectives may include the following:

- Information Technology: enables information related to operational processes to become available to the department on a timelier basis. Additionally, information technology may enhance internal control over security and confidentiality of information by appropriately restricting access.
- Completeness: Transactions that occur are recorded and not understated.
- Accuracy: Transactions are recorded at the correct amount in the right account (and on a timely basis) at each stage of processing.
- Validity: Recorded transactions represent events that actually occurred and were executed according to prescribed procedures.

11.02. Design of Appropriate Types of Control Activities

For information systems, there are two main types of control activities: general and application control activities.

General controls include security management, logical and physical access, configuration management, segregation of duties, and contingency planning.

Application controls include controls over input, processing, output, master file, interface, and data management system controls.

11.03. Design of Information Technology Infrastructure

Control activities over the information technology infrastructure are designed to support the completeness, accuracy, and validity of information processing by information technology.

11.04. Design of Security Management

Objectives for security management include confidentiality, integrity, and availability. Confidentiality means that data, reports, and other outputs are safeguarded against unauthorized access. Integrity means that information is safeguarded against improper modification or destruction, which includes ensuring information's nonrepudiation and authenticity. Availability means that data, reports, and other relevant information are readily available to users when needed.

Security of Records and Assets

Management is required to protect the organization's equipment, information, documents, and other resources that could be wrongfully used, damaged, or stolen. The department head is responsible for maintaining accountability for the custody and use of resources and shall assign qualified employees for that purpose. Management can protect resources by limiting access to authorized individuals. Access may be limited by various

means such as locks, passwords, electronic firewalls, and encryption. Also, management must occasionally inventory the physical resources and the records to reduce the risk of unauthorized use or loss of resources and protect against wasteful and wrongful acts.

System Security Roles

Department management must determine each individual's enterprise system (HR/CMS, MMARS and Warehouse) security access by both business area and security level. Management can limit access to one or more specific business areas, such as Accounts Receivable, Payroll, or Fixed Assets. Within each business area, management must also select the appropriate security levels. In MMARS, the Administrator role is the most powerful since it allows the individual to validate and submit documents to final status. The User role is more restricted; it allows the processing of documents but excludes the ability to finalize documents.

Data Security – Physical Access

Data security is the means of protecting data, whether in hard media (paper, microfilm) or in computer and communications systems, against unauthorized disclosure, transfer, modifications, or destruction whether accidental or intentional. Therefore, data security helps to ensure privacy. It also helps in protecting confidential data concerning clients, consumers, and employees.

Data Security - Logical Access

Data security consists of procedures that prevent unauthorized access to computer resources. Security procedures protect data from unintentional acts, as well as intentional ones. Examples of data security include:

- Select appropriate password safeguards
- Require periodic password changes
- Alphanumeric characters per password
- Keeping passwords confidential
- Require screen-saver passwords
- Assign each user a unique user ID
- Limit user access to system software
- Control access to specific applications and data files
- Limit access to what is required to perform a person's job function and to allow for appropriate segregation of duties
- Review security logs and user activity reports
- Limit concurrent logins
- Activate intruder detection and prevention mechanisms
- Implement adequate virus protection procedures

Access to enterprise systems should be reviewed quarterly, as well as when significant turnover occurs in sensitive positions or in realignment of duties.

Physical Security

Physical security is the protection of facilities that house data, personnel, clients, records, and other assets. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism. Security engineering involves three elements of physical security: (1) obstacles to frustrate trivial attackers and delay serious ones, such as locks and swipe card access; (2) detection devices such as alarms, security lighting, and security guards to

make it likely that attacks will be noticed; and (3) security response to repel, catch or frustrate attackers when an attack is detected.

Section 6: Control Activities	12. Implement control activities	12.01. Documentation of responsibilities through policies 12.02. Periodic review of control activities

12. Implement Control Activities

12.01. Documentation of Responsibilities through Policies

Managers and other staff in key roles should document internal control, all transactions and other significant events in a manner that allows the documentation to be readily available for examination. The documentation may appear in management directives, administrative policies, or operating manuals, in either paper or electronic form.

Documentation may include responsibilities by divisions and/or staff by position title for responsibility for an operational process's objectives and related risks, and control activity design, implementation, and operating effectiveness.

Managers should communicate to appropriate personnel the policies and procedures so they can implement the control activities for their assigned responsibilities. Each division/group may document policies in the appropriate level of detail to allow management to effectively monitor the control activity. Procedures may include the timing of when a control activity occurs and any follow-up corrective actions to be performed by competent personnel if deficiencies are identified.

12.02. Periodic Review of Control Activities

Management should periodically review policies, procedures, and related control activities for continued relevance and effectiveness in achieving the department's objectives or addressing related risks. If there is a significant change in a process, management should review the process in a timely manner after the change to confirm that the control activities are designed and implemented appropriately. Changes may occur in personnel, operational processes, or information technology. Regulators and legislators may also change either an entity's objectives or how an entity is to achieve an objective.

Section 7: Information and Communication Component

Overview

Information systems use data generated from both internal and external sources to provide information for managing risks and making decisions. Effective communication occurs dimensionally, flowing up, down and across the organization. Each employee understands their own role in relation to the work of others. They must have a means of communicating significant information upstream. There is also effective communication with external parties, such as taxpayers, vendors and regulators.

Principles and Points of Focus Relating to Information and Communication

Principles are required in supporting an effective design, implementation and operation of the associated component. Points of focus act as additional information and may contain examples to further explain what a requirement means and what it is intended to cover.

Section 7: Information & Communication	13. Use quality information	13.01. Identification of information requirements 13.02. Relevant data from reliable sources 13.03. Data processed into quality information
	14. Communicate internally	14.01. Communication through the entity 14.02. Appropriate methods of communication
	15. Communicate externally	15.01. Communication with external parties 15.02. Appropriate methods for communication

Following is a discussion of each of the Principles and Points of Focus

Section 7: Information & Communication	13. Use quality information	13.01. Identification of information requirements 13.02. Relevant data from reliable sources 13.03. Data processed into quality information

13. Use Quality Information

13.01. Identification of Information Requirements

Information requirements consider the expectations of both internal and external users. Management should define the identified information requirements at the relevant level and requisite specificity for appropriate personnel.

13.02. Relevant Data from Reliable Sources

Reliable internal/external sources provide data that are reasonably free from error and bias and faithfully represent what they purport to represent. Management should evaluate both internal and external sources of data for reliability. Sources of data can be operational, financial, performance or compliance related.

Examples of external sources can be profit and non-profit organizations, industry publications, professional association memberships and websites. Examples of internal sources can be financial reports, performance metrics, transaction analyses and incident management systems.

13.03. Data Processed into Quality Information

Quality information meets the identified information requirements when relevant data from reliable sources are used. Quality information is information that is appropriate, current, complete, accurate, accessible, and provided on a timely basis.

Management processes relevant data from reliable sources into quality information within the entity's information system. An information system is the people, processes, data, and technology that management organizes to obtain, communicate, or dispose of information.

Section 7: Information & Communication	14. Communicate internally	14.01. Communication through the entity 14.02. Appropriate methods of communication

14. Communicate Internally

Communication is the exchange of useful information between and among people and organizations to support decisions and coordinate activities. Information should be communicated to management and other employees who need it in a form, and within a timeframe, that helps them to carry out their responsibilities.

14.01. Communication throughout the Entity

Communication is multi-dimensional – from the top down, bottom up and across the organization. Effective communication informs all levels of the organization and must be ongoing. Communication systems can be formal or informal. Formal communication systems, from sophisticated computer technologies to staff meetings, provide input and feedback relative to an organization's activities, including the achievement of goals and objectives. Informal conversations with employees, contractors, vendors and regulators often provide some of the most critical information needed to identify risks and opportunities.

In some circumstances separate lines of communication are needed to serve as a fail-safe mechanism in case normal channels are inoperative. In the event regular communications channels are not effective or appropriate, many organizations have set up supplemental employee communications channels. These channels, which may be called "whistle-blower" programs or "ethics hotlines," may be voluntary or legally mandated. Their purpose is to provide a ready means whereby employees at any organizational level can confidentially discuss or report perceived or actual illegal, unethical, or otherwise inappropriate behavior.

A desirable goal is, over time, to embed communications on enterprise risk management into an entity's broad-based, ongoing communications programs, consistent with the concept of building enterprise risk management into the fabric of the organization.

14.02. Appropriate Methods of Communication

Communication is multi-faceted – verbal, non-verbal and written. It is important to remember that effective verbal communication is two way, requiring that management welcome, and listen to, suggestions and feedback. Staff must be comfortable enough to share their awareness of problems with managers who can act on this information. Verbal communication should be in support of, not in place of, written documentation of policies and procedures. All written documentation, whether it is official policy/procedure, memo, or e-mail, must be distributed to anyone who requires the information in order to perform his or her responsibilities.

Section 7: Information & Communication	15. Communicate externally	15.01. Communication with external parties 15.02. Appropriate methods for communication

15. Communicate Externally

15.01. Communication with External Parties

External communication can take a variety of forms, including statutorily mandated annual reports and financial reports, web sites, press releases, newsletters, and informational brochures. Other methods of communication include focus groups, presentations at conferences, budget hearings and oral updates. Regardless of the methods used, maintaining open lines of communication with outside parties will enhance a department's internal control. For example:

- Vendors, service providers, and consultants can provide significant input on the quality and design of agency products and services.
- Auditors, advocacy groups, and other outside reviewers can alert management to minor problems before they become major difficulties.
- Suppliers and contractors who are made aware of the agency's ethical standards can help deter or detect inappropriate purchasing or bidding practices.
- Complaints or inquires can point out control problems, or the department's ability to supply accurate information to the media or concerned citizens.

15.02. Appropriate Methods of Communication

As noted above, communication is multi-faceted – verbal, non-verbal and written. Effective verbal communication is two way, requiring that management welcome, and listen to, suggestions and feedback. Management should consider the following factors in selecting the appropriate method of communication:

- Audience - The intended recipients of the communication
- Nature of information - The purpose and type of information being communicated
- Availability - Information readily available to the audience when needed
- Cost - The resources used to communicate the information
- Legal or regulatory requirements - Requirements in laws and regulations that may impact communication

Section 8: Monitoring Component

Overview

Enterprise risk management must be continually monitored – ensuring that all components are relevant and functioning– in order to be effective. Ongoing monitoring occurs in the normal course of management activities and can lead to more detailed individual component evaluations. Enterprise risk management deficiencies are reported upstream, with serious matters reported to top management and the board.

Principles and Points of Focus Relating to Monitoring

Principles are required in supporting an effective design, implementation, and operation of the associated component. Points of focus act as additional information and may contain examples to further explain what a requirement means and what it is intended to cover.

Section 8: Monitoring	16. Perform monitoring activities	16.01. Monitor each ERM component 16.02. Evaluation of results
	17. Evaluate issues and remediate deficiencies	17.01. Reporting of issues 17.02. Evaluation of issues 17.03. Corrective actions

Following is a discussion of each of the Principles and Points of Focus

Section 8: Monitoring	16. Perform monitoring activities	16.01. Monitor each ERM component 16.02. Evaluation of results

16. Perform Monitoring Activities

16.01. Monitoring each ERM Component

Monitoring the ERM framework is essential for determining whether your Internal Control Plan needs updating. Evaluation of the framework should be done in a way that provides an objective perspective on any or all elements of enterprise risk management, from the internal environment through the monitoring component itself. In some cases, external events can mean that your department must consider new goals and objectives. In other cases, particular attention is given to analysis, response and mitigating controls when new risks are identified.

New goals or objectives require an assessment of the risks you will encounter in trying to achieving them. When new risks are identified a review of internal control activities is necessary.

Even your monitoring process can undergo changes, for example, if there is an audit finding involving a process or control that was missing or had not been tested.

Any changes that impact your ICP require you to gather the necessary information for proper analysis, and to communicate the changes to all responsible parties.

Ongoing monitoring occurs during normal operations and includes regular management and supervisory activities, comparisons, reconciliations, and other actions people take in performance of their duties.

Monitoring may include automated tools, which can increase objectivity and efficiency by electronically compiling evaluations of each ERM component.

Separate evaluations are a way to take a fresh look at each component by focusing directly on the component's relevance and/or effectiveness at a given time. These provide greater objectivity when performed by reviewers who do not have responsibility for the activities being evaluated, internal auditors for example. If there are no internal auditors available, consider the option of periodically hiring an outside vendor.

Everyone within an organization has some responsibility for monitoring. The position a person holds in the organization helps to determine the focus and extent of these responsibilities. Therefore, the monitoring performed by managers, supervisors and staff will not have the same focus. For example:

- Executive management should focus their monitoring activities on the major divisions within the organization. With this broad focus, they emphasize the organization's internal environment, mission, and goals.
- Managers must be watchful for new risks that might impact business processes and assess how well internal controls function in multiple units within the organization.
- Supervisors monitor all activities within their respective units to ensure staffs are performing their assigned responsibilities, internal control activities are functioning properly, and the unit is accomplishing its goals and objectives.
- Staffs monitor their own work to ensure it is being done properly. They should be trained by supervisors and management regarding internal controls and be encouraged to report any irregularities.
- Access to systems and sensitive data should be reviewed periodically to ensure employees have adequate access, but not more than what is needed to complete their responsibilities.

16.02. Evaluation of Results

Results of the ongoing monitoring and component evaluations should be documented and reviewed to identify issues that could compromise the effectiveness of the internal control plan.

Section 8: Monitoring	17. Evaluate issues and remediate deficiencies	17.01. Reporting of issues
		17.02. Evaluation of issues
		17.03. Corrective actions

17. Evaluate Issues and Remediate Deficiencies

17.01. Reporting of Issues

Personnel should report issues through established reporting lines to the appropriate internal parties on a timely basis to enable the department to promptly evaluate those issues.

Depending on the entity's regulatory or compliance requirements, it may also be required to report issues to the appropriate external parties, such as the legislators, regulators, and standard-setting bodies that establish the laws, regulations, and standards to which the department is subject.

17.02. Evaluation of Issues

We primarily think of a deficiency when discussing internal controls. A deficiency can be in the design, implementation, or operating effectiveness of an internal control and its related process. But it is important to note that all of the ERM components are interrelated and, a shortcoming in any one of them can lead to control deficiencies. All control deficiencies and ERM component issues require further evaluation and remediation by management.

17.03. Corrective Actions

When deficiencies in compliance or internal control lead to formal audit findings, corrective actions must be taken to remediate the finding in a timely manner. The audit resolution process begins when audit or other review results are reported to management and is completed only after action has been taken that (1) corrects identified deficiencies, (2) produces improvements, or (3) demonstrates that the findings and recommendations do not warrant management action.

Non-audit related recommendations must be evaluated for their potential to cause changes in the ERM components and Internal Control Plan.

Chapter 2: Internal Control Plan Checklist

An internal control plan should have a statement of awareness and compliance with Chapter 647 guidelines in addition to the eight ERM components.

A. Statement of Compliance with Chapter 647

B. Evidence of ERM Components – does it include all principles related to each Component?*

1. Internal Environment – Leadership demonstrates a commitment to integrity, ethical values and competence

    a. Tone at the Top, Mission Statement, Ethical Expectations, Standards and Adherence to Conduct

    b. Department Head statement of support of the Internal Control Plan

    c. Is the ICP readily available, distributed and communicated throughout the organization?

2. Objective Setting – measurable targets or purpose of the organization's efforts

    a. Goals and Objectives are defined, and aligned to the Mission Statement

3. Event Identification – occurrences that could prohibit the accomplishment of objectives

    a. Have risks that may impede the achievement of each objective been identified?

    b. Are risks linked to objectives?

4. Risk Assessment – Impact and likelihood of occurrence for each potential risk identified.

    a. Assessment of risks is performed in determining how risks should be managed

    b. Potential for Fraud is considered in assessing risks

    A risk assessment can be a significant undertaking and result in a large volume of information. For purposes of the ICP, the Risk Assessment component need only be a short summary of how and when the assessment was conducted. The summary should include who was involved, the programs and activities considered, how risks were rated (what was the scale/methodology used and was it used applied consistently throughout the process), how they were prioritized and by whom? The existence and location of the risk assessment documentation should be referenced here.

5. Risk Response –how the organization will respond to an event

    a. Are responses appropriate for significance of risks?

    b. Necessary changes and management of risks is determined in order to achieve objectives

6. Control Activities – mitigation steps that are linked to risk events

    a. Policies and procedures

    b. Preventive and Detective controls

    c. Segregation of duties

d. Are control activities linked to risks?

Goals, objectives, risk events and control activities should be linked as follows:

1. Goal #1

    a. Objective #1 for Goal #1

        i. Risk #1 for Objective #1 for Goal #1

            a. Internal Control #1 for Risk #1 for Objective #1 for Goal #1

            b. Internal Control #2 for Risk #1 for Objective #1 for Goal #1

        ii. Risk #2 for Objective #1 for Goal #1

            a. Internal Control #1 for Risk #2 for Objective #1 for Goal #1

            b. Internal Control #2 for Risk #2 for Objective #1 for Goal #1

7. Information and Communication – internal and external

    a. Information –quality information is generated for and/or from both external and internal sources

    b. Communication – internal communication is disseminated throughout the organization, and information to external parties is appropriately communicated

8. Monitoring –each component is evaluated to keep the Internal Control Plan up to date

    a. Ongoing and separate evaluations are used to ascertain whether each of the components of ERM is present and functioning.

*Refer to Chapters 1 through 8 of the Internal Control Guide for further discussion on each component and subsequent principles.

Following are a set of questions (following the ERM Framework and discussion in Section 1) to assist in developing a plan:

Your Outline

- What is your mission statement?
- Would an Organizational Chart help to convey your department's various activities?
- What is your "Tone at the Top"?
- Have the other Principles under the ERM Component Internal Environment been considered?
- What are the long term goals that support your mission?
    1. Goal #1
    2. Goal #2
    3. Goal #3
- What are the short term objectives that support each of your long term goals?
    1. Goal #1
        a. Objective #1 for Goal #1
        b. Objective #2 for Goal #1

- Have the types of risks been identified, and specific events considered?
- What are the risks associated with each objective?
  1. Goal #1
     a. Objective #1 for Goal #1
        i. Risk #1 for Objective #1 for Goal #1
        ii. Risk #2 for Objective #1 for Goal #1
     b. Objective #2 for Goal #1
        i. Risk #1 for Objective #2 for Goal #1
        ii. Risk #2 for Objective #2 for Goal #1
- Has a Risk Assessment been completed?
- Has Fraud Risk been considered?
- Have risk responses been documented for the risks identified?
- What Control Activities (policies and procedures) are employed to mitigate risk?

2. Goal #1

a. Objective #1 for Goal #1

i. Risk #1 for Objective #1 for Goal #1

a. Internal Control #1 for Risk #1 for Objective #1 for Goal #1

b. Internal Control #2 for Risk #1 for Objective #1 for Goal #1

ii. Risk #2 for Objective #1 for Goal #1

a. Internal Control #1 for Risk #2 for Objective #1 for Goal #1

b. Internal Control #2 for Risk #2 for Objective #1 for Goal #1

b. Objective #2 for Goal #1

i. Risk #1 for Objective #2 for Goal #1

a. Internal Control #1 for Risk #1 for Objective #2 for Goal #1

b. Internal Control #2 for Risk #1 for Objective #2 for Goal #1

ii. Risk #2 for Objective #2 for Goal #1

a. Internal Control #1 for Risk #2 for Objective #2 for Goal #1
b. Internal Control #2 for Risk #2 for Objective #2 for Goal #1

- Have all the Principles under the ERM Component Information and Communication been considered?
- Have all the Principles under the ERM Component Monitoring been considered?

Additional evaluation points to consider in developing the initial control plan, during their Internal Control Plan review or to further refine major programs, bureaus, institutions, or other department subdivisions are:

1. Does the department have an internal control plan written in the correct format? If so, when was it last updated?

2. Is the internal control plan a high-level summarization, on a department-wide basis, of the department's goals, objectives, risks, and of the controls used by the department to mitigate those risks?
3. Is the internal control plan supported by lower-level detail such as departmental policies and procedures (details of the policies and procedures do not need to be included in the internal control plan)?
4. Were the department head and senior management instrumental in developing the plan?
5. Does the internal control plan include a department-wide risk assessment? Or, does the risk assessment include only fiscal? Are any business areas missing from the risk assessment?
6. Does the risk assessment identify the most significant areas that could keep the department from attaining its mission, goals and objectives?
7. Are the stated risks cross-referenced to internal controls?
8. Does the internal control plan include programs and controls to prevent, deter, and detect fraud?
9. Do the policies, procedures and organizational structure (control activities) attempt to control the risks that were identified in the risk assessment?
10. Does the internal control plan include information explaining how and when management monitors each ERM component in the plan?
11. Does the internal control plan describe the method that should be used by staff to report internal control issues such as unresolved reconciling items and policy violations; the process to report unaccounted for variances, losses, shortages or theft of funds or property to the Office of the State Auditor?
12. Is the internal control plan shared with all employees?
13. Has the department trained employees in internal controls within the past year? Have employees attended the internal control training provided by the Office of the Comptroller?

Chapter 3: Commonwealth Reliance on Department Internal Controls

The Commonwealth manages its finances based on a series of reliances:

- The Governor submits a warrant to the Governor's Council for approval relying upon the "certification" by the Comptroller;
- The Comptroller relies on certification by a Department Head evidenced by electronic signature within the accounting system,
- A Department Head relies on their Chief Fiscal Officer (CFO) that manages the day to day activity within the Department evidenced by electronic signature within the accounting system;
- The CFO relies on Department employees to make purchases and confirm receipt, delivery and acceptance of commodities and services (including payroll) in accordance with prescribed laws, regulations, policies, and procedures.

Department Head delegation of signature authority is captured based upon "Security roles" established as part of the state accounting system (Massachusetts Management Accounting and Reporting System – MMARS). In addition, Department Heads may choose to implement further restrictions with use of Department Head signature authority which will be implemented through Department policy, not by system security. These restrictions must also be documented and referenced in the Department's internal control plan

The Single Audit Act, as amended in 1996, and the Office of Management and Budget (OMB) require single audits to provide the federal government with reasonable assurance on the accuracy of financial statements and on major programs' compliance with federal laws and regulations. Other audits must, by law, build on the work of the single audit rather than duplicate it. OMB released new uniform administrative requirements, cost principles, and audit requirements for federal awards (Title 2 CFR Subtitle A, Chapter II, Part 200 - also referred to as the "Super Circular") effective 12/27/2014. This guidance is meant to strengthen internal control over federal programs and reduce administrative burden for non-Federal entities receiving Federal awards while reducing the risk of waste, fraud and abuse.

At the beginning of each Single Audit, auditors perform a preliminary evaluation of the Commonwealth's internal controls. They then review the internal controls of some departments in more depth. The auditors use departments' internal control plans and Internal Control Questionnaire responses, along with other criteria, to render an opinion on the internal controls of the Commonwealth as a whole.

Internal Control Questionnaire

The Internal Control Questionnaire (ICQ) is one component of the Single Audit. Each spring, at the beginning of the audit cycle, the Office of the Comptroller distributes the questionnaire to all departments. This web-based survey is designed to provide insight into departmental internal control procedures. Because of its length, questions are divided by topic into multiple sections; however, because not all questions are applicable to all departments, most departments are able to skip one or more of these sections. The Comptroller recommends that the internal control officer, the single audit liaison, and the chief fiscal officer work closely with senior management in responding to these questions. In most departments, several individuals will need to be involved. Auditors and the Quality Assurance Bureau review the ICQ responses as part of the annual planning process and may contact department staff to follow up on some of the questions.

Representations

The last piece of the Questionnaire is the Representations section. In this section, the department head, the chief fiscal officer, and the internal control officer must read and approve the statements, confirming that the information entered into the questionnaire is accurate. (The responsibilities of these key personnel are defined in the Comptroller's Key Contact Lists (https://www.macomptroller.org/statewide-key-contact-lists). Enter names and official titles in the Representations section of the form. Staff should plan to provide a copy of the ICQ to any auditors who come to your agency as part of the Single Audit.

Conclusion

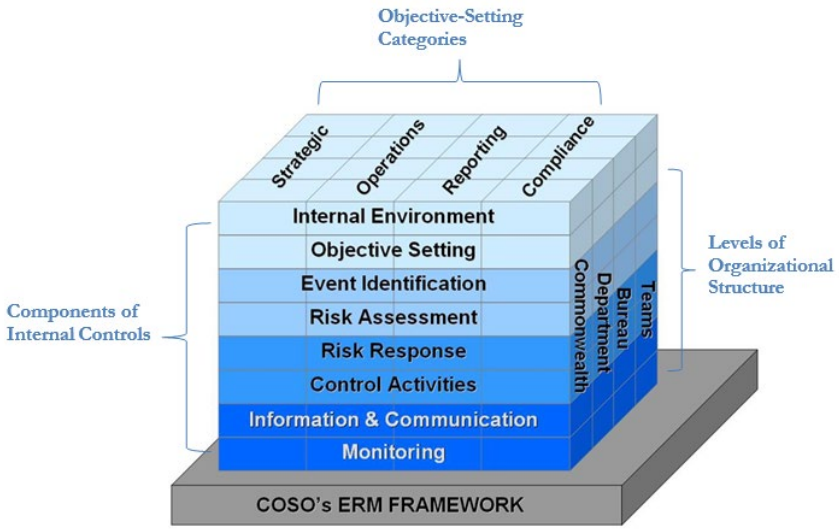
Each of us plays a vital role in creating an environment that is accountable to the public while being responsive to the needs and direction of senior management. Internal controls are a critical element of this environment.

APPENDIX I

After COSO issued its first report in 1992, various accounting organizations and the U.S. General Accounting Office (GAO) also began developing internal control guidance. In 2004, COSO issued its framework for enterprise-wide risk management, Enterprise Risk Management – Integrated Framework also known as COSO II or ERM. The ERM framework expands and elaborates on the risk assessment and internal environment components of the previous guidance Internal Control – Integrated Framework. For example, it breaks out internal environment into two components (internal environment and objective setting) and risk assessment into three components (event identification, risk assessment and risk response).

Guide Structure in Preparing the Internal Control Plan

Per the **COSO ERM Executive Summary** document, ERM is defined as "a process, effected by an entity's board of directors, management and (all) personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the Objective-Setting Categories Levels of Organizational Structure achievement of entity objectives."



A direct relationship exists between objectives, which are what the entity strives to achieve, the components, which represent what is needed to achieve the objectives, and subunits/teams of the entity.

ERM is geared to achieving an entity's objectives, set forth in four categories:

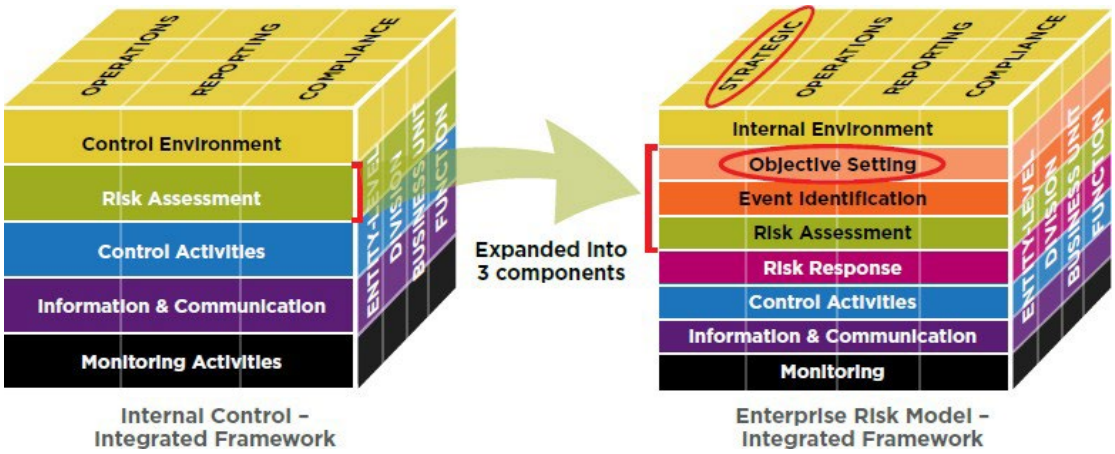
1. Strategic – specific goals that are aligned with and supporting the organization's mission
2. Operational - Effective and efficient use of its resources
3. Reporting- Reliability of reporting
4. Compliance - Adherence to applicable laws and regulations

Within each of these four objective-setting categories, there are eight interrelated components. Each of these has been discussed above, taking into consideration the Green Book's adaptation of the principles and points of focus.

Background: COSO Issuances

Internal Control Framework (Issued 1992)

ERM Framework

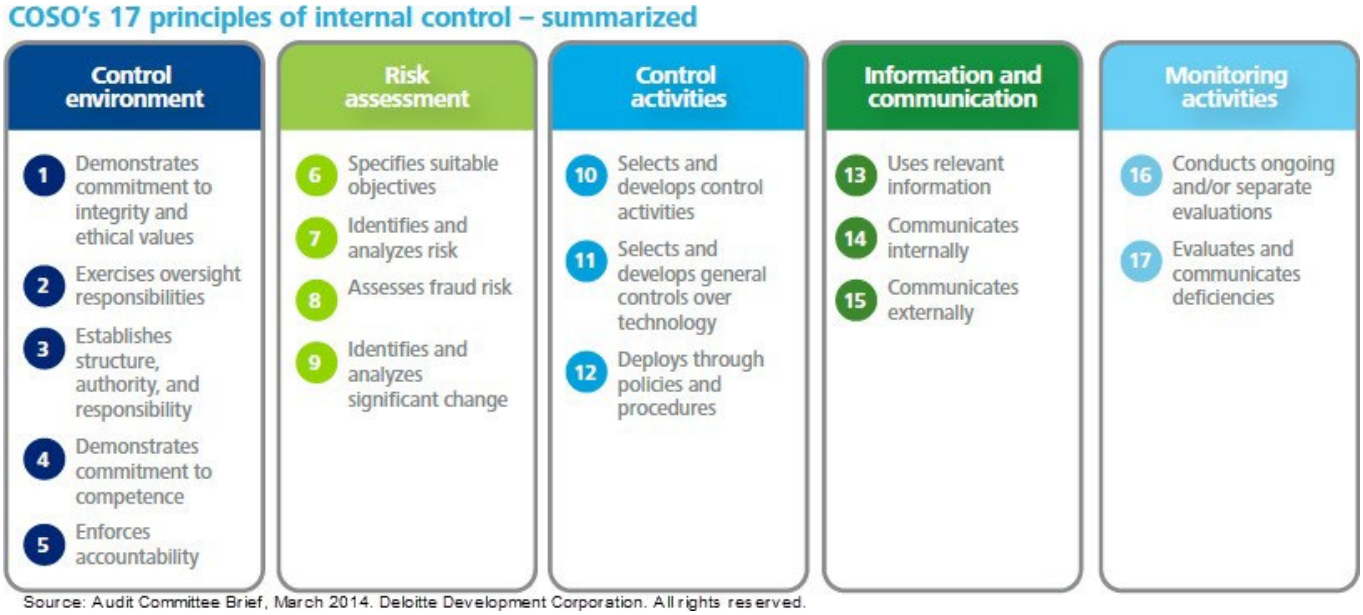


Internal Control – Integrated Framework

Enterprise Risk Model – Integrated Framework

COSO updated its internal control guidance in 2013 with the issuance of a revised Internal Control – Integrated Framework. The new COSO Framework explicitly articulates on the 17 principles that the 1992 COSO Framework conceptually introduced in narrative only. Note the 2013 COSO Framework is based on the internal Control Framework (5 components), not the ERM Framework (8 components).

Internal Control – Integrated Framework (Issued 2013)



Source: Audit Committee Brief, March 2014. Deloitte Development Corporation. All rights reserved.

The Government Accountability Office's Standards for Internal Control in the Federal Government (also known as The Green Book) adapts the 2013 COSO Framework for a government environment in its most recent issuance as of September 2014.

Regulations and Guidance

Chapter 647 of the Acts of 1989

In accordance with M.G.L. c. 7A, s. 9A and Chapter 647 of the Acts of 1989, An Act Relative to Improving the Internal Controls within State Agencies, the Office of the Comptroller (CTR) is directed to work with the Office of the State Auditor (OSA) to publish minimum standards for internal control systems at state departments for administrative and financial operations. The Internal Control Laws require that departmental internal control structure be developed in accordance with the internal control guideline established by the CTR.

The law also requires that all unaccounted for variances, losses, shortages or thefts of funds or property, are immediately reported to the OSA. The OSA has the responsibility to determine the internal control weaknesses that contributed to the condition, identify the internal control policies and procedures that need modifications, identify the amount of funds involved, make recommendations that address the correction of the condition found, and report the matter to appropriate management and law enforcement officials.

The Internal Control Laws are an integral part of State Government to provide reasonable assurance that departments' financial and programmatic operations are effective, efficient, and reliable and are in compliance with applicable laws, rules and regulations.

Yellow Book

The Comptroller General of the United States issues Government Auditing Standards (known as the Yellow Book, December 2011 Revision), through the U.S. Government Accountability Office (GAO). These standards, also referred to as generally accepted government auditing standards (GAGAS), explain the rules that auditors must follow during audits of governmental entities, programs, activities, and functions. Audit organizations must also use Government Auditing Standards during reviews of governmental assistance that is administered by contractors and nonprofit organizations, when required by statute or other mandates, or when auditors hold themselves out as following government auditing standards. The Yellow Book establishes requirements for auditors' professional qualifications, the quality of audit effort, and the characteristics of professional and meaningful audit reports. It includes requirements and guidance for the following types of reviews: financial audits, attestation engagements, and performance audits.

Title 2 CFR Subtitle A, Chapter II, Part 200

The U.S. Office of Management and Budget (OMB) released new uniform administrative requirements, cost principles, and audit requirements for federal awards (also referred to as the "Super Circular"). The new uniform guidance supersedes and streamlines requirements from eight OMB Circulars A–21, A–87, A–110, and A–122 (which have been placed in OMB guidance); Circulars A–89, A–102, and A–133; and the guidance in Circular A–50 on Single Audit Act follow-up. This guidance will help strengthen internal control over federal programs and reduce administrative burden for non-Federal entities (states, local governments, Indian tribes, institutions of higher education (IHE), and nonprofit organizations) receiving Federal awards while reducing the risk of waste, fraud and abuse. These new rules went into effect on December 27, 2014. Per audit requirements, a non-Federal entity that expends $750,000 or more during the fiscal year in Federal awards must have a single or program-specific audit conducted in accordance with

§200.514 Scope of audit and must do the following:

1. Maintain internal control for federal programs,
2. Comply with the laws, regulations, and the provisions of contracts or grant agreements,

3. Prepare appropriate financial statements, including the schedule of expenditures of federal awards,
4. Ensure that the required single audits are properly performed and submitted when due, and
5. Follow up and take corrective actions on audit findings.

Audit Committee

Within the public sector, an audit committee is an extension of the governing body. Committees are formed to fulfill the governing body's responsibilities, not expand them. Officials are able to increase their oversight of specific issues by assigning various matters to committees.

In this light, the audit committee is an integral element of public accountability and governance. It plays a key role for the governing body in carrying out its legal and fiduciary responsibilities, especially with respect to the integrity of the government's financial information, system of internal control, and legal and ethical conduct of management and employees.

The roles of the audit committee may vary from entity to entity depending on the complexity and size, as well as the requirement of the governing body. However, the one common responsibility for all audit committees, among all their potential roles, is risk management oversight.

An audit committee has three fundamental goals. First, it must satisfy itself that management is maintaining a comprehensive framework of internal control.

Second, the audit committee must ensure that management's financial reporting practices are assessed objectively. Third, the committee needs to determine to its own satisfaction that the financial statements are properly audited and that any problems disclosed in the course of the audit are satisfactorily resolved.

Every organization faces a variety of potential risks, such as:

- Loss of key staff
- Loss of funding or reduction of revenue sources
- Regulatory non-compliance
- Conflicts of interest
- Fraudulent activities resulting from weaknesses in internal controls

Internal Audit

As defined by the Institute of Internal Auditors, "Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an

organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes."

Management is responsible for establishing and maintaining an adequate system of internal controls. An internal audit office is charged by management with "… assessing the effectiveness of the design and execution of the system of internal controls and risk management processes."

Internal auditors continuously evaluate risk exposures in relation to:

- Effectiveness and efficiency of operations
- Reliability and integrity of financial and operational information
- Safeguarding of assets
- Compliance with laws, regulations and contracts

- Accomplishment of established operational goals and objectives

Internal auditors are responsible for making recommendations for improvement in internal controls to top management and, if applicable, a governing board of directors. To maintain independence, and to perform in an objective capacity, internal auditors should not engage in any operational or programmatic responsibilities.

Appendix II

Works Cited

Auditing – An Integrated Approach by Alvin A. Arens, Randal J. Elder and Mark S. Beasley.

Audit Committees by Stephen J. Gauthier, Government Finance Officers Association, Chicago, IL 2006.

Title 2 CFR Subtitle A, Chapter II, Part 200 (Uniform Guidance)
https://www.ecfr.gov/current/title-2/subtitle-A/chapter-II/part-200?toc=1

COSO ERM –Integrated Framework Executive Summary:
https://www.coso.org/Shared%20Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

COSO ERM – Understanding and Communicating Risk Appetite
https://www.coso.org/Shared Documents/ERM-Understanding-and-Communicating-Risk-Appetite.pdf

COSO ERM Integrated Framework- Application Techniques
http://www.macs.hw.ac.uk/~andrewc/erm2/reading/ERM%20-%20COSO%20Application%20Techniques.pdf

Standards for Internal Control in the Federal Government (The Green Book) - GAO (U.S. Government Accountability Office)
https://www.gao.gov/greenbook

Government Auditing Standards (The Yellow Book) - GAO
https://www.gao.gov/yellowbook

Single Audit Information Service. Thompson Publishing Group State of Connecticut Accountability Directive Number 1.
https://www.osc.ct.gov/manuals/InternalCntl/index.html

OFFICE OF THE COMPTROLLER
COMMONWEALTH OF MASSACHUSETTS

One Ashburton Place, 9th Floor

Boston, MA, 02108

617-727-5000

MAComptroller.org