OFFICE OF THE COMPTROLLER

ONE ASHBURTON PLACE, 9TH FLOOR
BOSTON, MASSACHUSETTS 02108
(617) 727-5000
MACOMPTROLLER.ORG

INTERNAL CONTROLS

Effective: July 1, 2004
Last Updated: February 24, 2025

Executive Summary

Internal controls are defined as a system of controls implemented by departments that provide reasonable assurances that department's mission will be achieved in compliance with applicable state and federal requirements. Internal controls are critical for or to creating an environment that enables a department to effectively achieve its mission and maintain public trust by demonstrating proper stewardship of public resources. Properly utilized, documented, and updated internal controls assist leadership and management in supporting operations while preventing fraud, waste, and abuse of Commonwealth assets and resources.

Pursuant to M.G.L. c 7A § 9, the Office of the Comptroller (CTR) is granted access to the books and papers of all departments as part its management of fiscal operations, accounting, and financial reporting. CTR does not "audit" department compliance with CTR published guidance, but performs periodic "spot checks" and due diligence reviews to review potential anomalies, incidents, fraud claims, and internal controls weaknesses. Department heads are also required to annually complete CTR's Internal Control Certification (ICC). CTR may also conduct periodic interviews and desk reviews to verify a department's compliance with this policy. Additionally, the State Auditor, independent auditors for the statewide financial and single state audit reports, federal agency auditors, and other oversight entities may audit a department's operations and system of internal controls.

Policy

Departments are responsible for implementation of the following minimum internal controls requirements which are discussed in detail below:

- Designation of an Internal Control Officer (ICO)
- System of Internal Controls, Internal Control Plan, Internal Control Guide, Technology and Information Systems
- CTR State Finance Internal Controls
- Integration of Internal Controls into daily operations
- Staff are properly trained for roles, including CTR statewide Role-Based Training
- Central Repository for Internal Controls
- Completion of Internal Control Certification (ICC) and Reviews
- Reporting of Audits, Fraud, Cyber or other Suspicious Issues

1. Designation of Internal Control Officer (ICO)

The Internal Control Officer (ICO) is one of a department's Key State Finance Compliance Roles. Department heads are responsible for designating an ICO who reports directly to the department head and is equivalent in title or rank to an assistant or deputy to the department head. The ICO is responsible for working with key department staff to ensure that all internal controls requirements, including the completion of the annual ICC, are met.

The ICO is the primary CTR contact responsible for communications related to internal controls. These communication responsibilities include ensuring that staff assigned to Key State Finance Law Compliance Roles appearing on the CTR Statewide Key Contacts listing are up-to-date and that updates are sent to CTR without delay. The ICO must also ensure that the CTR Statewide Risk Management and Compliance Team is notified of any external audit.

The ICO is also responsible for facilitating prompt responses and completion of any external audit or CTR desk review requests. Upon completion of any external audit or CTR desk review, the ICO is responsible for ensuring that audit findings or reviews are promptly evaluated, appropriate corrective action is taken, and management takes appropriate actions to align staff and budget resources to support reasonable remediation of findings, recommendations, and internal control weaknesses.

For a full list of ICO responsibilities, please refer to CTR's Key State Finance Compliance Roles and Responsibilities Guidelines.

2. System of Internal Controls, Internal Control Plan, Internal Control Guide, Technology and Information Systems

System of Internal Controls, Monitoring for Compliance, and Updates

A department must have a system of written internal controls that includes all department operations. A system of internal controls includes risk assessments, an Internal Control Plan (ICP), policies, procedures, and other operational controls including a department's Business Continuity Plan, Disaster Recovery Plan, Incident Response Plan, and asset and access management controls.

Additionally, as part of their system of internal controls, departments should document how monitoring of internal controls and mission achievement is implemented. Routine staff meetings, periodic training, report reviews, metrics, performance reviews, citizen or client feedback, internal audits, surveys, and staff check-ins are all types of monitoring controls that departments can implement. Failure to monitor internal controls creates increased risks and opportunities for fraud, waste, and abuse of Commonwealth resources.

At a minimum, a department's system of internal controls must be reviewed and updated annually. However, compliance with internal control requirements is an ongoing department responsibility, and departments must be vigilant about updating or changing their system of internal controls to account for departmental changes. Departmental changes that may impact a department's internal controls include new goals, internal structural changes, or new statutory requirements.

Categories of internal controls that are expected as part of a department's written system of internal controls, and which may be included in due diligence reviews by CTR include:

- Top-level reviews and monitoring of actual performance, expenditures and mission achievement
- Reviews by management at the functional or activity level
- Appropriate management, monitoring and training of human capital
- Appropriate security, privacy and system availability controls over information processing systems and data
- Physical control and protection of physical, financial and digital assets
- Access restrictions, segregation of duties and controls to support accountability for resources and records and to prevent fraud, waste and abuse of assets
- Appropriate, accurate and timely execution and recording of transactions, including supporting documentation
- Establishment and review of performance measures and indicators

Internal Control Plan (ICP)

All departments in the Commonwealth must have an ICP included in their written system of internal controls. An effective ICP is a high level, department-wide summary of goals, risks, and controls for all of a department's business processes. The ICP should reference the topics and location of more detailed policies, procedures, and

operational instructions that are provided to staff to ensure that internal controls are actively integrated into daily operations.

Internal Control Guide

Pursuant to M.G..L. c. 7A, s. 9A, in consultation with the Office of the State Auditor, CTR publishes internal control guidelines for all state departments in accordance with the Internal Control Act, Chapter 647 of the Acts of 1989. CTR publishes an Internal Control Guide which provides comprehensive instructions to assist departments with the development and implementation of a system of internal controls through a recognized Enterprise Risk Management (ERM) process. This includes the concepts of broad-based objective setting, event (risk) identification, and risk response (internal controls). The Guide outlines the most common elements of a system of internal controls and the role staff play in developing, implementing, and monitoring controls for their departments. Specifically, CTR issues the Internal Control Guide to:

- assist agencies to streamline the content of their mission-specific statutory, regulatory, and internal policies and procedures into a concise set of objectives for each fiscal year
- assist agencies in achieving those mission objectives by incorporating the principles of ERM
- provide a format that departments use when writing and updating their ICP and associated mission and fiscal policies, procedures and operational controls.

The guide also provides guidance on setting the "tone at the top" for expectations on meeting goals and objectives for all financial and programmatic activities. A department's "tone at the top" is set by management through policies, actions, and expectations. A department's "tone at the top" is important to the overall acceptance of the system of internal controls by personnel, expectations for integrity and ethics, and standards of conduct.

Technology and Information Systems

Departments must establish internal controls related to technology and information systems that maintain the security, integrity, and availability of department systems, records, data, and other assets to prevent fraud, waste and abuse of Commonwealth resources. Leadership and managers are responsible for establishing a strong "tone from the top" that identifies that information security internal controls are part of the foundation of all daily operations and are a top department priority.

An information system represents the life cycle of information used for the department's operational processes that enables the department to obtain, store, and process quality information. An information system includes the staff, processes, data, and technology that management utilizes to obtain, communicate, or dispose of information.

Departments must demonstrate that employees have completed annual and periodic information system cybersecurity awareness training. Also, guidance published by CTR at macomptroller.org/ctr-cyber may be used for periodic refreshers and integrated into internal controls and daily operations.

Technology and information systems internal controls require collaboration across the organization and extend to any contractor or third-party supporting operations. Departments remain responsible for all actions or inactions by contractors and third parties that support departmental operations.

Audits of department information systems are now routine as part of statewide financial, federal, and operational audits. Departments should expect to have internal control reviews and audits of the design, security, data reliability, operational processes, staff training, and access management to information systems.

3. CTR State Finance Internal Controls

CTR identifies specific state finance internal control standards that are considered the default minimum baseline internal controls standard for all departments of the Commonwealth. A department's system of internal controls must include these state finance internal controls standards published by CTR to properly manage, record, and account for fiscal activities. These standards are published through the following resources:

- Fiscal Year Updates and other guidance published on MAComptroller.org
- Policies, job aids/checklists, training materials and other resources published by CTR on PowerDMS,
- Enterprise system security role specific courses available at CTR Statewide Learning

The department must ensure that these standards and related internal controls are implemented, tested, included in staff training, and integrated into daily operations. Department Heads, Chief Fiscal Officers, Internal Control Officers, General Counsels, MMARS Liaisons, and other key state finance contacts are notified of updates on a weekly basis via CTR's Weekly Update email. CTR updates are also published on the CTR website.

An important part of state finance internal controls is Department Head Signature Authorization (DHSA). Each department head is required to certify, as part of the Department Head Security Certification, that the department will conduct all fiscal business in accordance with state finance law, including M.G.L. c. 29 and M.G.L. c. 7A; as well as regulations, policies, procedures, job aids and other guidance published by CTR. For more information about DHSA, please see CTR's Department Head Signature Authorization and Electronic Signatures policy.

4. Integration of Internal Controls as Part of Daily Operations

A department's system of written internal controls, along with CTR published fiscal guidance, should be actively integrated as part of daily operations and communicated to all staff required to implement these internal controls. It is insufficient to maintain updated written internal controls without being able to demonstrate that these controls are embedded into daily operations and actively in use by staff. In response to CTR desk reviews and external audits, departments should be prepared to identify how written internal controls are integrated into daily operations, how staff are assured of ready access to written controls, policies and procedures, and how internal controls are communicated to staff.

5. Staff Are Properly Trained for Roles, Including CTR Statewide Trainings Role Based Training

It is expected that all staff are properly trained on the department's system of internal controls, as well as the specific internal controls that apply to staff roles and their related responsibilities. It is insufficient to merely provide access to internal controls documentation. For audit and CTR desk review purposes, departments should be prepared to identify how staff are trained on the internal controls that apply to specific fiscal roles.

To ensure users are properly trained for the type of access and responsibilities of access, CTR may, at any time, prescribe mandatory security access role-based training for users for initial and ongoing access to the enterprise accounting and payroll systems and other identified systems.

In addition to specific fiscal role training, CTR provides additional statewide training that all staff should attend to ensure that they understand their obligations to protect Commonwealth resources, protect confidential data, systems, and prevent fraud, waste, and abuse. CTR provides statewide training and resources on fraud management and mitigation, risk management and internal controls. CTR also provides cybersecurity internal controls at macomptroller.org/ctr-cyber.

6. Central Repository of Internal Controls

Departments must ensure that internal controls documentation is maintained for audit and CTR quality assurance purposes in a central repository, with appropriate backups that will not be lost due to staff, management, or system changes. Central repositories may include a central electronic folder, SharePoint site, or other paper or electronic filing repository where the department's written system of internal controls is maintained. Departments must ensure that staff have access to the internal controls for their specific roles in order to ensure these controls are integrated into daily operations.

7. Completion of Internal Control Certification (ICC) and Reviews

Department heads are required to annually certify, as part of the ICC, that the department has a system of written internal controls, training and monitoring actively in place as part of daily operations to achieve the department's mission, ensure compliance with CTR's published guidance (PowerDMS, MAComptroller.org, Fiscal Year Memos, CTR Statewide Trainings), and prevent fraud, waste, and abuse of Commonwealth resources.

8. Reporting of Audits, Fraud, Cyber or other Suspicious Issues

Reporting to CTR

After internal notification to appropriate staff, departments must also immediately report to CTR any incident of suspected, suspicious, attempted or successful fraud, cyber, phishing, ransomware or other technology disruption, compromise or intrusion. See https://www.macomptroller.org/ctr-cyber/cyber-incidents/.

Reporting to CTR is in addition to any other mandated reporting to local law enforcement or other oversight entity. While a department may immediately remediate an incident, compromise or other disruption, these events are considered internal controls weaknesses and, if not properly mitigated, may create incidents or disruption outside of the department.

The primary purpose of reporting is to ensure that CTR can take appropriate actions to protect the Commonwealth enterprise accounting and payroll systems from disruption or compromise. Departments have an obligation to prevent fraud, waste and abuse of Commonwealth resources, and this extends to the enterprise systems that the department is provided with access to for financial operations.

CTR assists other technology and law enforcement entities to ensure a disruption is properly contained and mitigated and other Commonwealth departments, vendors, municipalities or citizens are not negatively impacted. CTR will not publicize any information related to any incident or suspected incident and will not intervene in the management of the incident for the department. CTR provides support and recommendations for remediation and support for continued fiscal operations if operations are impacted.

CTR reserves the right to suspend access to enterprise accounting and payroll systems by any department or staff if an incident or compromise has occurred, the threat of an incident or compromise is suspected or imminent, or it is necessary to protect the Commonwealth's enterprise financial systems, or other Commonwealth departments or systems from harm. Such suspension may last until the incident or compromise is remediated. See Statewide Enterprise Systems Security Access Management.

Reporting to the Office of the State Auditor

In addition to reporting to CTR, departments must immediately report all unaccounted-for variances, losses, shortages, or thefts of funds or property to the Office of the State Auditor. (See Report Unaccounted For State Property or Funds)

Reporting by Individuals

Staff should be encouraged to safely report issues through reporting lines, such as regular staff meetings, upward feedback processes, a whistle-blowing program, or an ethics hotline. Departments can set up their own resources or refer to the resources at macomptroller.org/internal-controls.