U.S. Immigration and Customs Enforcement

# Chapter 10: Audit Coordination

## Section 10.3 – Internal Control Testing and the Statement of Assurance

### Table of Contents


Chapter 10: Audit Coordination ....1
Section 10.3 – Internal Control Testing and the Statement of Assurance ....1
Introduction ....2
Responsibilities ....3
Policy ....6
1. Internal Control Program ....6
1. Internal Control Standards ....7
2. Internal Control Assessment ....8
3. Internal Control Assessment ....9
3-1. Internal Control Assessment ....9
3-2. Assessing Entity-Level Controls (ELC) ....10
3-3. Fraud Risk Considerations ....10
3-4. Internal Control Reporting and the Statement of Assurance ....11
4. Information Used in Controls ....12
4-1. IUC Population Identification ....12
4-2. IUC Risk Assessment ....13
4-3. IUC Risk Response ....13
5. Systems Impacting Financial Reporting ....14
6. Systems Security Assessments ....14
6-1. GAO FISCAM ....15
6-2. Assessment Timelines ....15
6-3. A-123 ITGC Assessments ....15
6-4. Remediation ....15
7. IT Commitment Letter ....16
8. System Services Received ....16
9. Annual Reporting Requirements ....16
Procedures and Internal Controls ....18
Authorities and References ....19
Glossary ....21
Summary of Changes ....23

# Introduction

This section of the Financial Management Policy Manual (FMPM) provides U.S. Immigration and Customs Enforcement (ICE) financial management policy on the establishment, evaluation and reporting on internal controls, and submission of an annual Statement of Assurance (SOA).

The policy sections in this chapter are designed to establish the framework for ICE to assess the effectiveness of internal controls and provide reasonable assurance that internal controls comply with four main objectives:

a. Effectiveness and efficiency of operations

b. Reliability of financial reporting

c. Compliance with applicable laws and regulations

d. Confidentiality, integrity, and availability of information systems

In addition to general guidance and policy on internal controls, this section of the FMPM incorporates specific policy and guidance for gaining adequate assurance of the quality of information used in controls (IUC) to support financial reporting. The Government Accountability Office (GAO) Standards for Internal Control in the Federal Government (Green Book) states management should use quality information to achieve the entity's objectives and support its internal control system. Quality information is defined by the Green Book as information that is appropriate, current, complete, accurate, accessible, and provided on a timely basis. The Department, for purposes of obtaining assurance over its IUC, has defined quality information as information that is complete and accurate.

Also, this section of the FMPM incorporates specific policy and guidance on the DHS Information Technology (IT) internal control program which supports compliance with the Office of Management and Budget (OMB) Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control. The DHS Office of the Chief Financial Officer (OCFO) Risk Management and Assurance (RM&A) Division partners with the DHS Office of the Chief Information Officer (OCIO) Office of the Chief Information Security Officer (OCISO) to manage and oversee the IT internal control program. Parties with named roles and responsibilities should coordinate those responsibilities to the extent necessary and appropriate as determined by the Chief Information Officer (CIO), with the CIO to whom statute and the Secretary have delegated authorities that complement, relate to, involve, or are concurrent with the responsibilities in this guidance.

This policy will be in effect until superseded.

## Responsibilities

The **ICE Chief Financial Officer (CFO)** is responsible for establishing, updating, and overseeing the development of overall ICE Internal Control policy. This includes:

a. Overseeing the establishment of the procedures and processes around the internal control over financial reporting program that aligns with or is more stringent than DHS policy.

b. Serving as an approving official for the IT Commitment Letter, demonstrating management's commitment to testing and passing IT system security controls over systems impacting financial reporting.

c. Assisting in the coordination and annual reporting through the Statement of Assurance process on the overall IT security control environment for systems that impact financial reporting.

d. Overseeing the establishment of ICE policy that assigns clear roles and responsibilities to entity personnel governing the assurance of quality IUC.

e. Overseeing the establishment of Component requirements for documenting, implementing, and maintaining a formal risk-based assurance and validation process for IUC.

f. Providing oversight over the remediation of deficiencies, identified through both internal assessments and audit findings, for issues related to the quality and reliability of IUC.

The **ICE Chief Information Officer (CIO)** is responsible for overseeing the establishment of the ICE information security program policies that align with DHS policies. This includes:

a. Serving as an approving official for the ICE IT Commitment Letter, demonstrating management's commitment to testing and passing IT system security controls over systems impacting financial reporting.

b. Assisting in the coordination and annual reporting through the Statement of Assurance process on the overall IT security control environment for systems that impact financial reporting.

The **ICE Chief Information Security Officer (CISO)** is responsible for developing, implementing, and maintaining the ICE-wide Information Security Program to ensure the security and continuity of operations of ICE information systems. This includes:

a. Serving as the Component principal advisor on information security matters.

b. Ensuring that external providers who operate information systems on behalf of the Component meet the same security requirements as required for government information and information systems.

c. Serving as an approving official for the Component IT Commitment Letter, demonstrating management's commitment to testing and passing IT system security controls over systems impacting financial reporting.

d. Providing input for the annual update of the CFO Designated Systems List.

e. Monitoring the state of the Component's IT security control environment for systems impacting financial reporting.

The **ICE System Teams** include the System Owner, Information System Security Managers, Information System Security Officers, and other team members responsible for the overall security of the information system. They are responsible for:

a. Providing input for the annual update of the CFO Designated Systems List.

b. Providing input for the internal control program IT Commitment Letter process.

c. Monitoring the state of the ICE's IT security control environment for systems impacting financial reporting.

d. Adhering to DHS and ICE policies and procedures over IT security for systems impacting financial reporting.

The **Office of Assurance and Compliance (OAC)** is responsible for establishing and maintaining internal controls in accordance with OMB A-123, DHS 4300A, and this policy and providing all required information, data calls, and deliverables. OAC accomplishes this mission through oversight of the program offices which are: Homeland Security Investigations (HSI), Enforcement and Removal Operations (ERO), the Office of the Legal Advisor (OPLA), the Office of Professional Responsibility (OPR) and the Office of Investment and Program Accountability (OIPA) who are responsible for:

a. Partnering with accountable parties and supporting the IT security assessment work performed for systems impacting financial reporting.

b. Serving as the front-line entity to identify risks and perform continuous monitoring over third-party service providers for systems impacting financial reporting related to their associated processes and/or line of business.

c. Developing policies and procedures, in accordance with DHS OCFO policies and guidance, governing the assurance of IUC to ensure quality and reliable information is used in the performance of key control activities to support financial reporting.

d. Identifying information that is used in control activities, performing a risk assessment over the population of IUC, and documenting decisions based on the assessed level of risk.

e. Providing assurance over the quality and reliability of IUC by performing validations and reviewing prior to executing any control activity that relies on the information.

f. Remediating deficiencies, identified through both internal assessments and audit findings, for issues related to the quality and reliability of IUC.

The OAC **Internal Controls Unit (ICU)** is responsible for:

a. Coordinating and providing input for the annual update of the CFO Designated Systems List.

b. Coordinating and providing input for the internal control program IT Commitment Letter process.

c. Partnering with accountable parties and supporting the IT security assessment work performed for systems impacting financial reporting.

d. Monitoring the state of the IT security control environment for systems impacting financial reporting.

e. Assisting in the development and implementation of a more structured Service Provider monitoring program for the Department.

f. Designing and implementing a risk-based approach to test the design and operating effectiveness of the key internal control over financial reporting (ICOFR) control activities to include obtaining adequate assurance over the quality of information used in those control activities.

g. Supporting program offices with the development and maintenance of the IUC population and risk assessment.

h. Coordinating with ICE program offices the identification of roles and responsibilities between parties for IUC assurance when documenting key internal controls.

i. Supporting program office remediation efforts including the development and tracking of corrective action plans, for deficiencies related to the quality and reliability of IUC.

## Policy

Internal controls are defined by the Green Book as "… a process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved." These objectives and related risks can be broadly classified into one or more of the following three categories:

a. Operations - Effectiveness and efficiency of operations

b. Reporting - Reliability of reporting for internal and external use

c. Compliance - Compliance with applicable laws and regulations

Developing and managing an assessment process to ensure compliance with the internal control provisions of the DHS FAA and the requirements of OMB Circular A-123, Appendix A, is a function of the OCFO.

### *1. Internal Control Program*

a. ICE managers have an inherent responsibility to establish and maintain effective internal controls, assess areas of risk, identify and correct weaknesses in those controls, and keep their leadership informed.

b. ICE Managers and Supervisors are responsible for understanding and applying the OMB standards for internal control in the Federal Government and for complying with the associated internal control evaluations of key controls, conducted by the OAC team.

c. Heads of reporting organizations will give high priority to promptly correcting identified exceptions and to effectively implementing the associated internal controls.

d. Heads of reporting organizations will validate specific process flows, narratives, and internal controls to include security controls for their

operational areas.

e. No ICE activity or program is exempt from the requirements of the FMFIA, OMB Circular A-123, Appendix A, the DHS FAA, NIST SPs, or DHS 4300A.

## *1. Internal Control Standards*

a. ICE managers have a fundamental responsibility to maintain internal controls in accordance with OMB A-123. OMB A-123 specifically outlines five standards providing the basis against which internal control is to be evaluated, to include all aspects of operations whether programmatic, financial, or compliance. The five standards are:

1) Control Environment – Understanding management's attitude, awareness, and actions, clearly defined authority and responsibility, appropriate delegation of authority and responsibility, integrity and ethical standards, commitment to competence, hierarchy for reporting, proper support for human capital hiring, training, advancing, and disciplining.

2) Risk Assessment – Identifying internal and external risks, considering previous audit findings, inspections, and other assessments, and known instances of noncompliance with laws, regulations, and policies; then analyzing risk for potential effect and impact. Some significant events can affect risk; these include complexity and magnitude of programs or new operations, extent of manual processes, related party transactions, decentralized versus centralized accounting, accounting estimates, new programs, new personnel, new technology, new or amended laws, regulations, and accounting standards.

3) Control Activities – The policies, procedures, and mechanisms in place that ensure management's directives are carried out, such as proper segregation of duties, physical control over assets, proper authorization, appropriate documentation and access to documentation, analytical review and analysis, and safeguarding information.

4) Information and Communications – Information should be communicated to relevant personnel at all levels

within an organization. The information should be relevant, reliable, and timely. It is also crucial that an agency communicate with outside organizations as well, whether providing information or receiving it.

5) Monitoring – Management should conduct periodic reviews to determine the effectiveness of internal controls through self-assessment by management, direct testing or evaluations from the Inspector General (IG), auditors, or other assessment organizations. The assessment should include obtaining an understanding of major types of activities the agency uses to monitor internal control and how those activities are used to initiate corrective actions. Every step of the assessment process should be documented.

## *2. Internal Control Assessment*

a. ICE managers are responsible for continuously monitoring their internal controls.

b. Internal control assessments are performed by OAC at the direction of DHS Risk Management & Assurance (RM&A) and the ICE Chief Financial Officer (CFO) to determine whether internal controls exist, are correctly implemented, and to ensure that internal control systems are working effectively to mitigate risks. Internal control assessments are of two broad types:

1) A specific detailed examination of internal controls in a prescribed review format especially designed for that purpose, or

2) Using a variety of processes that provide adequate information regarding the effectiveness of control techniques.

c. IT internal control assessments are performed by OAC at the direction of DHS Risk Management & Assurance (RM&A), DHS OCISO, and the ICE Chief Financial Officer (CFO) to determine whether internal controls exist, are correctly implemented, and to ensure that internal control systems are working effectively to mitigate risks. IT internal control assessments are a specific detailed examination of internal controls in a prescribed review format especially designed for that purpose. Specific guidance related to review and

reporting on information systems that impact financial reporting is set forth in Sections 5 to 9 below.

d. OAC develops and communicates a yearly Internal Control plan for financial reporting and IT controls, which may include conducting necessary walkthroughs, updating process documentation, developing test plans, and reporting results.

## *3. Internal Control Assessment*

There are four key components to executing ICE's Internal Control Testing and the Statement of Assurance process:

a. Internal Control Assessment

b. Assessing Entity Level Controls

c. Fraud Risk Considerations

d. Internal Control Reporting and the Statement of Assurance

### 3-1. Internal Control Assessment

a. ICE managers are responsible for continuously monitoring their internal controls.

b. Internal control assessments are performed by OAC at the direction of DHS Risk Management & Assurance (RM&A) and the ICE Chief Financial Officer (CFO) to determine whether internal controls exist, are correctly implemented, and to ensure that internal control systems are working effectively to mitigate risks. Internal control assessments are of two broad types:

   3) A specific detailed examination of internal controls in a prescribed review format especially designed for that purpose, or

   4) Using a variety of processes that provide adequate information regarding the effectiveness of control techniques.

c. IT internal control assessments are performed by OAC at the direction of DHS Risk Management & Assurance (RM&A), DHS OCISO, and the ICE Chief Financial Officer (CFO) to determine whether internal controls exist, are correctly implemented, and to ensure that internal control systems are working effectively to mitigate risks. IT internal control assessments are a specific detailed examination of internal controls in a prescribed review format especially designed for that purpose. Specific guidance related to

review and reporting on information systems that impact financial reporting is set forth in Sections 5 to 9 below.

d. OAC develops and communicates a yearly Internal Control plan for financial reporting and IT controls, which may include conducting necessary walkthroughs, updating process documentation, developing test plans, and reporting results.

### 3-2. Assessing Entity-Level Controls (ELC)

"Entity Level Controls" are controls that have a pervasive effect on an entity's internal control system and may pertain to multiple internal control components. As required by the Green Book, Components are required to assess the design and operating effectiveness of their relevant ELC by completing the information in the ELC Assessment Template provided by DHS RM&A annually. ICE is required to apply the same rigor used in business process assessments for ELC assessments. ICE is required to maintain supporting evidence to support conclusions of Met, Partially Met, or Not Met for each Principle.

A material weakness identified in one or more principles of the Green Book indicates the system of internal control is not effective. Practically, a material weakness in a business process control activity (e.g., Property) results in a determination that the overall system of internal controls is ineffective. A control deficiency in one Green Book component often impacts other interrelated components. For example, a deficiency for lack of documented procedures may indicate deficiencies in entity governance (Control Environment), and communication of expectations to control owners (Information & Communication and Monitoring).

### 3-3. Fraud Risk Considerations

(b)(7)(E)

(b)(7)(E)

### 3-4. Internal Control Reporting and the Statement of Assurance

The DHS FAA and OMB Circular A-123, Appendix A, requires ICE to prepare an annual Statement of Assurance. All ICE Program Offices are required to provide a statement of assurance annually, specifically as it applies to their areas of responsibility.

The SOA is Management's assessment of the effectiveness of ICE's Internal Controls Over Reporting (ICOR) as of September 30th of the current fiscal year. Per OMB Circular A-123, the statement of assurance must include the following:

a. A statement of Management's responsibility for establishing and maintaining adequate ICOFR for ICE;

b. A statement identifying the OMB Circular A-123, Appendix A, as the framework used by ICE to conduct the assessment of the effectiveness of ICOFR;

c. An assessment of the effectiveness of the ICE ICOFR as of September 30, including an explicit conclusion as to whether ICOFR is effective; and

d. All material weaknesses and significant deficiencies existing as of September 30th of the current fiscal year.

According to OMB Circular A-123, Appendix A, in its statement of assurance on ICOFR, Management is required to state a direct conclusion about whether the ICE ICOFR is effective. The statement must take one of the following forms:

a. Unmodified statement of assurance (no material weaknesses or lack of compliance reported);

b. Modified statement of assurance, considering the exceptions explicitly noted (one or more material weaknesses reported); or

c. Statement of no assurance (no processes in place or pervasive material weaknesses).

The SOA provides the Secretary a level of reasonable assurance that ICE's internal controls are in place and operating effectively in three distinct areas:

d. Operational and administrative controls assessment relevant to all mission essential functions throughout ICE.

e. Financial reporting assessment relevant to ICE's financial statements.

f. Financial systems assessment relevant to the financial management system's conformance with Federal requirements, (See Sections 5 to 9 below.)

## *4. Information Used in Controls*

IUC can be defined as any information used by the Department, to include information produced by the entity (IPE) as well as information produced by third party service providers, in the performance of control activities. IUC is commonly in the form of financial or non-financial information presented in reports and is commonly used by management in the operation of control activities to support business processes and mission operations that have a financial reporting impact. IUC can include, but is not limited to, information from a standard/canned generated source; information from a custom generated source; information from a query generated source; information from a manually generated source; or information from a third-party provided source.

### 4-1. IUC Population Identification

Programs must obtain an understanding of the information, both internally and externally produced, that the program utilizes in its internal control environment. To assist in this effort, ICE is required to develop and maintain, through an annual update, a complete and accurate population of its IUC. The IUC population should include a full inventory of information utilized in controls that have an ICOFR impact. Programs must obtain an understanding of the reports and data sources that are critical to their control activities and processes based on the activities performed during the IUC inventory.

Along with an IUC population, programs should also develop a comprehensive understanding of where and how the information is being used, the critical data attributes within the IUC, identification of the Data Owner, and how the IUC is produced and provided. Appropriate categories for the identified IUC should be defined and documented and captured in its population. Delineations between IUC categories will assist in implementing a risk-based program response that clearly defines risks to be mitigated by information type and production approach.

U.S. Immigration and Customs Enforcement is required to document the IUC Population and provide to the DHS OCFO Risk Management and Assurance (RM&A) Division in accordance with the deliverables and timelines established in the annual Component Commitment Letter. For detailed information on the identification of an IUC population, including recommended IUC categorizations, refer to the DHS OCFO RM&A ICOFR Process Guide – Information Used in Controls Guidebook.

### 4-2. IUC Risk Assessment

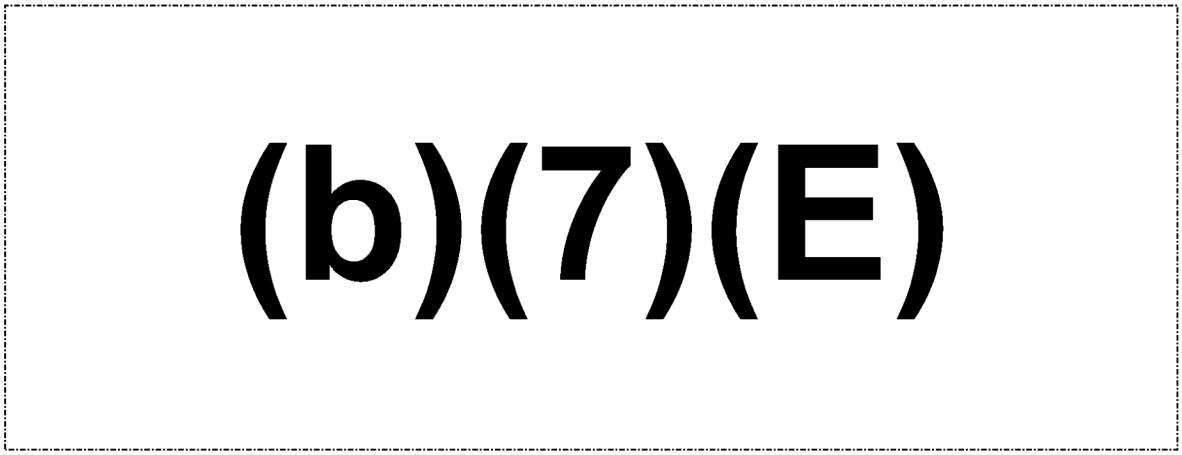
Program offices must perform a risk assessment over the full population of identified IUC to determine which are most critical to monitor and assess. An IUC risk assessment will help prioritize limited resources and determine additional risk response activities, to include IUC validations, as needed. Assessments should be performed of both impact and likelihood to determine overall IUC risk levels.

An assessment of IUC impact will consider the criticality of the IUC as well as ramifications to the entity if the IUC is not quality information. When performing an assessment of impact for IUC, it is important to consider the materiality of the information, the severity and criticality of the ICOFR controls utilizing the IUC, audience of the IUC, and the usage of the IUC to include whether management is utilizing the IUC to make financial or operational decisions.

An assessment of likelihood considers the probability or likeliness that the information within the IUC is not quality information. The likelihood of bad data within the IUC can be reduced by designing and implementing IUC assurance and validation activities prior to usage of the information in control activities.

After considering both impact and likelihood factors, programs must calculate and document the overall risk levels for the IUC to quantify and compare the population of risks. The IUC risk assessments must be documented and maintained for all identified IUC and are required to be provided to the DHS RM&A in accordance with the deliverables and timelines established in the annual Component Commitment Letter. Information Used in Controls risk assessments must be reviewed at least annually but should reflect risk updates in a timely manner, as identified. For additional information on conducting an IUC risk assessment, to include both impact and likelihood assessments, refer to the DHS OCFO RM&A ICOFR Process Guide – Information Used in Controls Guidebook.

### 4-3. IUC Risk Response



(b)(7)(E)

### 5. Systems Impacting Financial Reporting

The DHS OCFO's internal control program includes the responsibility to identify information systems that have an impact on financial reporting. Annually, RM&A initiates and coordinates requesting inputs and updating the CFO Systems Lists to formally document the information systems and applications that are key to processes supporting financial reporting requirements, the flow of financial data, etc. U.S, Immigration and Customs Enforcement must provide current and accurate inputs on information systems potentially impacting financial reporting to RM&A through annual or more frequent data call requests.

The CFO Designated Systems List is annually reviewed and approved by the DHS CFO and CIO. Once finalized, the CFO Designated Systems List is disseminated to relevant stakeholders by the DHS OCFO and the DHS Office of the Chief Information Security Office (OCISO).

For more information on this process, refer to the RM&A *ICOFR Process Guide – IT Supplement.*

### 6. Systems Security Assessments

(b)(7)(E)

## 6-1. (b)(7)(E)

U.S. Immigration and Customs Enforcement evaluates ITGCs in accordance with the GAO FISCAM to assess and provide assurance for ICOFR. During a financial statement audit, the Independent Public Accountant (IPA) uses the (b)(7)(E) (b)(7)(E) to evaluate ITGCs and application controls. The (b)(7)(E) "provides a methodology for performing information system control audits in accordance with 'generally accepted- government auditing standards' (GAGAS), as presented in Government Auditing Standards (also known as the 'Yellow Book')." The (b)(7)(E) defines general controls as "the policies and procedures that apply to all or a large segment of an entity's information systems and help ensure their proper operation." General controls are the structure, policies, and procedures that apply to an entity's overall IT operations. This includes controls over account management, configuration management, segregation of duties, contingency planning, interfaces, security management, etc. In line with this, ICE uses ITGCs to manage and control IT security across information systems.

### 6-2. Assessment Timelines

Stakeholders, to include but not limited to program offices, system teams, and internal control teams, should plan to complete assessments and deliver results in accordance with due dates defined within ICE's internal control program IT Commitment Letter.

### 6-3. A-123 ITGC Assessments

(b)(7)(E)

### 6-4. Remediation

Remediation is the process of correcting identified deficiencies whether the deficiencies are identified through A-123 ITGC assessment testing, external

audits, or other internal processes and assessments. When deficiencies are identified, ICE and system teams must perform a root cause analysis, create a Plan of Action and Milestones (POA&M), and begin remediation in accordance with DHS 4300A requirements to address the deficiency. For more information on this process, refer to Attachment H of the DHS 4300A Sensitive Systems Handbook and the FY20 Plan of Action and Milestones Policy Updates Memorandum.

### *7. IT Commitment Letter*

(b)(7)(E)

### *8. System Services Received*

(b)(7)(E)

### *9. Annual Reporting Requirements*

Final results of the annual IT security assessments performed over systems impacting financial reporting support the consolidated Department-wide Annual Financial Report (AFR), Federal Managers' Financial Integrity Act (FMFIA), and the annual Statement of Assurance (SOA) reporting process. The Department of Homeland Security Financial Accountability Act (DHS FAA), Public Law 108-330, requires DHS to report an annual statement of assurance for ICOFR, material weaknesses identified, and the independent auditor's opinion over ICOFR in the AFR. The annual SOA for ICOFR is a subset of the overall SOA, an attestation from the Department's senior leadership that provides reasonable assurance that the entity's objectives will be met, required under Section 2 of the FMFIA. DHS and ICE Management must assess and report on the effectiveness of their

internal controls as of September 30th each fiscal year.

## Procedures and Internal Controls

The U.S. Immigration and Customs Enforcement has developed and implemented procedures and internal controls to comply with this policy.

# Authorities and References

## Authorities

Public Law 97-255, *Federal Managers' Financial Integrity Act of 1982 (FMFIA)*

Public Law 101-576, *Chief Financial Officers Act of 1990*

OMB Circular A-123, Appendix A, *Management's Responsibility for Enterprise Risk Management and Internal Control*

Pub. L. 108-330, *Department of Homeland Security Financial Accountability Act of 2004 (DHS FAA)*

Pub. L. 104-208, *Federal Financial Management Improvement Act of 1996 (FMFIA)*

Pub. L. 107-296, *Federal Information Security Management Act of 2002 (FISMA)*

Pub. L. 113-291, *Federal Information Technology Acquisition Reform Act (FITARA)*

Title 40, U.S. Code, Section 1401 (3), "Clinger-Cohen Act of 1996"

Office of Management and Budget Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*

Government Accountability Office (GAO), *Standards for Internal Control in the Federal Government* (Green Book)

## References

National Institute of Standards and Technology, Special Publication 800-53

GAO, *Federal Information Systems Controls Audit Manual* (FISCAM)

DHS Policy Directive 4300A, *DHS Sensitive Systems*

DHS 4300A, *Sensitive Systems Handbook*, relevant attachment, and update memorandums

DHS Office of the Chief Financial Officer (OCFO) Risk Management and Assurance (RM&A), *Internal Controls Over Financial Reporting (ICOFR) Process Guide – Information Technology (IT) Supplement*

DHS OCFO RM&A, *ICOFR Process Guide – Service Provider Monitoring Guidebook*

DHS OCFO RM&A, *ICOFR Process Guide- - Information Used in Controls Guidebook*

DHS Financial Management Policy Manual (FMPM), Section 10.1, "Information Technology Guidance"

DHS FMPM Section 10.3, "Information Used in Controls"

GAO, *Assessing Data Reliability* (GAO-20-283G) (Grey Book)

# Glossary

The following tables contain definitions of the acronyms and terms used in this policy.

| Acronym | Definition |
|---|---|
| AFR | Annual Financial Report |
| CFO | Chief Financial Officer |
| CEM | Control Evaluation Matrix |
| CISO | Chief Information Security Officer |
| CUEC | Complementary User Entity Control |
| DHS | Department of Homeland Security |
| COSO | Committee of Sponsoring Organizations of the Treadway Commission |
| ELC | Entity Level Controls |
| FAA | Financial Accountability Act |
| FISCAM | Federal Information Controls Audit Manual |
| FISMA | Federal Information Security Act of 2002 |
| FITARA | Federal Information Technology Acquisition Reform Act |
| FMFIA | Federal Managers' Financial Integrity Act |
| FMPM | Financial Management Policy Manual |
| GAGAS | Generally Accepted Government Auditing Standards |
| GAO | Government Accountability Office |
| ICE | US Immigration & Customs Enforcement |
| ICOFR | Internal Controls Over Financial Reporting |
| IPE | Information Produced by the Entity |
| ITGC | Information Technology General Controls |
| IUC | Information Used in Controls |
| NIST SP | National Institute of Standards and Technology Special Publications |
| OAC | Office of Assurance and Compliance |
| OCIO | Office of the Chief Information Officer |
| OMB | Office of Management and Budget |
| POA&M | Plan of Action and Milestones |
| RM&A | Risk Management and Assurance |
| SOA | Statement of Assurance |

| Term | Definition |
|---|---|
| Designated Systems List | An annually reviewed and approved list that is comprised of systems that support or have an impact on financial processing and financial reporting. It is approved by the DHS CFO and CIO. |
| Fraud Risk | Events or conditions that indicate an incentive or pressure to commit fraud or provide an opportunity to commit fraud. |

| (b)(7)(E) | |
|---|---|
| Green Book | Standards for effective internal controls for federal agencies, which guide federal agencies to comply with applicable laws and regulations. |
| Heads of Reporting Organizations | ICE Program Office leadership responsible for establishing and maintaining internal controls, i.e., ERO, HSI, OPR, and M&A. |
| Information Technology General Controls | Controls that apply to all systems, components, processes, and data for a given organization or information technology (IT) environment. |
| IT Commitment Letter | Results of assessments – The assessments are a formally documented strategy of testing and remediation efforts that, when implemented, will enable DHS and Components to gain an overall understanding of whether the controls in place over information systems are designed and operating effectively. |
| IT Security Controls | A particular safeguard of countermeasure to protect the confidentiality, integrity, and availability of a system and its information. |
| IUC Population | Complete and accurate population of a components IUC. This includes a full inventory of information utilized in controls that have an ICOFR impact. |

## Summary of Changes

**Revision Type:** Substantial

**Revision Date:** April 19, 2023

**Changes:**

- Added paragraphs on Information Used in Controls (IUC) and Information Technology (IT) [Introduction; Page 2]
- Updated Superseded Statement [Introduction; Page 3]
- Added responsibilities relating to IUC and IT to CFO [Responsibilities; Page 3]
- Added ICE CIO [Responsibilities; Page 4]
- Added responsibilities relating to IT to ICE CISO [Responsibilities; Page 4]
- Added ICE Systems Teams [Responsibilities; Page 4]
- Added Internal Control Teams [Responsibilities; Page 5]
- Added Section 4 [Information Used in Controls; Page 12]
- Added Section 5 [Systems Impacting Financial Reporting; Page 14]
- Added Section 6 [System Security Assessments; Page 14]
- Added Section 7 [IT Commitment Letter; Page 16]
- Added Section 8 [System Services Received; Page 16]
- Added Section 9 [Annual Reporting Requirements; Page 16]
- Added Authorities and References related to IUC and IT [Page 17]
- Added IT and IUC related acronyms to Glossary [Page 19]
- Added terms and definitions related to IT and IUC to Glossary [Page 20]
- Made formatting and other changes throughout the policy to align with the DHS FPFM Style Guide.