U.S. Immigration
and Customs
Enforcement

Chapter 10: Audit Coordination

Section 10.6 – Third Party Service Provider Monitoring

Table of Contents

Introduction

This section of the Financial Management Policy Manual (FMPM) provides U.S. Immigration & Customs Enforcement (ICE) policy for overseeing and monitoring third party service providers to support the Department of Homeland Security's (DHS) financial reporting.

Outsourcing certain functions and operations can be a cost-effective means by which ICE meets its needs and requirements. However, reliance on a Service Provider is always accompanied by a degree of risk and a need to perform adequate monitoring and oversight. The use of Service Providers does not diminish ICE's responsibility to ensure that the activity is performed in a safe and sound manner, in compliance with applicable laws and regulations, and accomplishes the intended objective. Understanding the risks as a result of utilizing Service Providers is critical regardless of the benefits received through their use.

A Service Provider with a financial reporting impact, is defined as an organization or segment of an organization that provides services to user entities, which are likely to be relevant with respect to the user entities' internal control over financial reporting (ICOFR). While it is important to effectively monitor all Service Providers, Service Providers with a financial reporting impact are the intended focus of this policy.

The DHS and its external auditors have identified deficiencies within the Department's monitoring and oversight of its Service Providers with an ICOFR impact. These deficiencies in Service Provider monitoring have contributed to the Department's ICOFR audit financial reporting material weakness. At ICE, this has included service provider risks not addressed by obtaining and effectively reviewing Service Organization Control (SOC) reports, or by assessing the risks when a SOC report does not exist. Adherence to this policy will assist in remediating this material weakness.

This policy supersedes ICE FMPM Chapter 10, Section 10.6, "Third Party Service Provider Monitoring" dated May 13, 2019, and is effective immediately. See the Summary of Changes in this revision.

Responsibilities

The **ICE Chief Financial Officer (OCFO)** is responsible for establishing, updating, and monitoring adherence to ICE Service Provider policy. This includes:

a) Overseeing the establishment of policy that assigns clear roles and responsibilities to ICE personnel governing the monitoring of Service Providers;

b) Developing ICE requirements for documenting decisions concerning Service Providers;

c) Supporting the development of criteria for the usage of Service Providers as well as the criteria for the acceptance and monitoring of risks related to Service Provider engagements; and,

d) Providing oversight of the remediation of deficiencies, identified through both internal assessments and audit findings, for issues related to the monitoring of Service Providers.

The **ICE Program Offices** are responsible for:

a) Developing and adhering to policies and procedures, in accordance with DHS and ICE policies and guidance, governing oversight and monitoring of Service Providers;

b) Identifying and maintaining a complete list of Service Providers;

c) Establishing Program Office roles and responsibilities for performing monitoring activities;

d) Documenting procedures that demonstrate oversight over Service Provider systems and/or business process responsibilities to include procedures to determine whether a Service Provider report (for example, a Statement on Standards for Attestation Engagement (SSAE) 18 SOC report) is available and how the report is obtained from the Service Provider;

e) Performing service provider risk assessments by developing a methodology to support an understanding of the control environment of the Service Providers, and the associated risks based on that level of understanding; and reviewing the Service Provider report(s) and addressing the risks that arise because of deficiencies identified in the report(s);

f) Establishing Standard Operating Procedures that support the identification and the formal documentation and management approval of all controls that are ICE's responsibility (i.e., the final population of controls which includes both complimentary user entity controls (CUECs) and any additional controls identified); and,

g) Remediating deficiencies identified through both internal assessments and audit findings, for issues related to Service Provider monitoring activities or key user entity controls.

The **Office of Assurance and Compliance (OAC)** is responsible for internal control reviews over implementation of Service Provider monitoring procedures executed by Program Offices. This includes:

a) Designing and implementing a risk-based approach to test the design and operating effectiveness of the Service Provider monitoring activities, key controls, and CUECs;

b) Analyzing the impact of any associated Service Provider monitoring deficiencies and reporting the impact to applicable Program Offices;

c) Supporting Programs Offices with the development and maintenance of the Service Provider population;

d) Coordinating with Programs Offices the identification of roles and responsibilities between parties when documenting key internal controls;

e) Determining the impact of the Service Providers on ICE's ICOR and Internal Controls over Financial Systems (ICOFS) and,

f) Supporting Program Office remediation efforts, including the reporting of corrective action plans, for Service Provider monitoring activities, or key controls where deficiencies are identified.

Policy

1-1 Service Provider Population Identification

U.S. Immigration and Customs Enforcement Programs are responsible for documenting and maintaining, through an annual update, a full population of Service Providers with a financial reporting impact. Programs should include any Service Provider that touches, transmits, houses, or has access to financial reporting process controls, activities, and/or data and for which ICE does not have direct, consistent involvement in and oversight of the Service Provider.

Along with a Service Provider population, Programs should also develop a comprehensive understanding of their Service Providers to include the services or functions they are performing and the Programs level of reliance on the Service Providers. Programs should also define and document appropriate categories for the identified Service Providers in its population. The Department has identified five primary categories of Service Provider: (1) Within DHS; (2) Federal Agency Outside DHS; (3) FEDRAMP Authorized; (4) Private Vendor; and (5) State/Local Entity. Delineations between Service Provider categories are designed to assist in implementing risk-based monitoring and oversight that addresses risks to be mitigated for each Provider type.

The U.S. Immigration and Customs Enforcement is required by DHS to document the Service Provider population and provide this information to the DHS OCFO RM&A

Division in accordance with the deliverables and timelines established in the annual Component Commitment Letter. Detailed information on the identification of a Service Provider population, including recommended Service Provider categories, can be found in the DHS OCFO Risk Management and Assurance (RM&A) *Internal Control over Financial Reporting (ICOFR) Process Guide – Service Provider Monitoring Guidebook.*

1-2 Service Provider Risk Assessment

Programs must perform a risk assessment over their population of identified Service Providers to determine which are most critical to monitor and assess. The Service Provider risk assessment provides the basis for developing appropriate response actions to address identified risks. Completing a risk assessment for identified Service Providers provides insight into the inherent risk associated with the Service Provider and assists in prioritizing resources to perform oversight and monitoring to mitigate any potential vulnerabilities that may arise.

Programs are responsible for performing risk assessments and documenting decisions based on level of risk, including justification that supports the risk level assessments. For Service Providers that impact internal control over financial reporting, sufficient information must be obtained to determine which Service Providers are being used and their potential impact to financial reporting.

Programs should perform assessments of both impact and likelihood to determine overall Service Provider risk levels. An assessment of Service Provider impact will assist in determining which are most critical to monitor. When performing an assessment of impact for Service Providers, consideration should be given to the business processes supported, systems support provided, potential dollar value impact, materiality to ICE, level of reliance, and level of direct oversight performed by the Program. It is also important to consider the total exposure that can potentially be mitigated by adequate controls, monitoring, and oversight.

An assessment of likelihood considers the probability or likeliness that deficiencies within the Service Provider internal control system will occur and impact the Program. The following areas may be considered for inclusion in the likelihood assessment structure when performing a likelihood assessment: known issues with the Service Provider; the current status of remediation for identified deficiencies in the Service Provider internal control system; and whether the Service Provider provides an internal control assessment or Service Organization Control (SOC) 1 report.

Programs must document and maintain their Service Provider risk assessments for all identified Service Providers and are required to provide to DHS RM&A in accordance with the deliverables and timelines established in the annual Component Commitment Letter. Service Provider risk assessments must be reviewed at least annually but should reflect risk updates in a timely manner, as identified. For additional information on conducting a risk assessment of

Service Providers, to include both impact and likelihood assessments, refer to the DHS OCFO RM&A *ICOFR Process Guide – Service Provider Monitoring Guidebook.*

1-3 Service Provider Risk Response

The risk assessment should be used to prioritize, and rank identified Service Providers based on the overall ICOFR risk level and a response should start with those determined to be the highest risk. Responses should start once a risk level has been determined and the overall risk used to determine if additional monitoring and oversight actions are needed.

All steps within the risk management lifecycle should be full documented to include the initial risks, appetite, and tolerances; the due diligence performed in Service Provider selection and agreement construction; and the ongoing monitoring and justification for risk response activities. Proper documentation and reporting facilitate the accountability, monitoring, and risk management associated with Service Providers. Note that risk response for ICOFR should consider and leverage other risk response activities, as possible, that may be performed under alternate authorities and requirements. For additional information on making risk-based decisions and determining appropriate Service Provider risk responses, refer to the DHS OCFO RM&A *ICOFR Process Guide – Service Provider Monitoring Guidebook.*

Service Provider Risk Management Lifecycle

2-1. Planning and Due Diligence in Service Provider Selection

Service Provider reliance and the associated risk related to a Service Provider relationship should be assessed during the initial evaluation period prior to entering into a formal agreement with the Service Provider. All procurement reviews should be completed, and risk assessment structure and template can be used to gain a better understanding of where the Service Provider risk may align depending on contractual language and requirements that are under proposal or negotiation.

2-2. Service Provider Ongoing Monitoring Based on Risk

Service Providers should be continuously monitored and evaluated to ensure that both parties are performing in accordance with the requirements of the signed agreement or contract, and that the intended objectives are being satisfied. The timing, extent, and frequency of Service Provider monitoring activities should be determined in accordance with ICE and DHS policies, based on the assessed Service Provider risk level. The performance of monitoring activities must be sufficiently documented to demonstrate effective Service Provider oversight. Risk assessments should be updated at least annually, and the risk response reprioritized and adjusted as necessary.

2-3 Termination of the Service Provider Relationship

There should be a full understanding of the contractual terms and the termination process as well as any contractual loopholes or practices that may affect migration plans to an alternate Service Provider or in reintroducing the functions within ICE responsibilities. If a Service Provider introduces an unacceptable amount of risk that cannot be mitigated, then an appropriate risk response may be to terminate the relationship. Programs should consider developing a contingency plan where the activities can be transitioned to another Service Provider, bring the activities in-house, or discontinue the activities when an agreement expires or has been satisfied. The contingency plan should include the capabilities, resources, and timeframe required to transition the activity.

Service Organization Control Reports

If a Service Provider outside DHS is being used a SOC 1 Report should be obtained when possible. A- SOC 1 Report, performed in accordance with Statement on Standards for Attestation Engagement (SSAE) No 18. A SOC 1 Report is specifically intended to meet the needs of user entities that use Service Providers in evaluating the effect of the controls at the service organization on the user entities' financial statements. Obtaining and reviewing SOC 1 Reports is an effective and valuable monitoring activity that provides for more effective oversight and assists in managing the risks of Service Provider activities.

A SOC 1 Report includes any deficiencies identified in the Service Provider's system of internal control. If Service Provider control deficiencies are identified in the report, deficiencies must be evaluated and a conclusion reached as to the impact on financial reporting. A SOC 1 Report also outlines the controls that are the responsibility of the user entity. The CUECs are controls that the Service Provider states should be in place within the user entity's control environment and are necessary to support the Service Provider's stated control objectives. The CUECs can be either IT or business process focused. U.S, Immigrations and Enforcement Programs must be aware of CUECs documented within the applicable SOC 1 Reports and have proper policies, procedures, and processes in place to address the CUECs.

Review of Service Provider SOC 1 Reports must be documented, including an impact assessment of any identified Service Provider control deficiencies. Internal controls that address the Service Provider CUEC objectives must be assessed and be consistent with the timelines and scoping requirements established in the annual Component Commitment Letter. Corrective action plans should also be established to remediate identified control deficiencies. For additional information on the assessment of Service Provider CUECs, refer to the DHS OCFO RM&A *ICOFR Process Guide –Information Technology (IT) Supplement.*

SOC 1 Reports are a valuable monitoring and oversight tool and should be obtained and reviewed, when possible. If a SOC 1 Report cannot be obtained from the Service

Provider, alternative monitoring and oversight procedures should be performed that are consistent with the assessed risk level of the Service Provider. For specific monitoring procedures based on the Service Provider category and determined risk level refer to the DHS OCFO RM&A *ICOFR Process Guide – Service Provider Monitoring Guidebook.*

Authorities and References

Authorities

Public Law 101-576, Chief Financial Officer (CFO) Act of 1978

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 (FFMIA)

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

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

Pub L. 97-255, Federal Managers' Financial Integrity Act of 1982 (FMFIA)

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, Standards for Internal Control in the Federal Government (Green Book)

References

DHS Office of the Chief Financial Officer (OCFO) Risk Management and Assurance (RM&A), Internal Controls over Financial Reporting (ICOFR) Process Guide

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

DHS OCFO RM&A, ICOFR Process Guide – Information Technology (IT) Supplement

Glossary

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

Acronym	Definition
CFO	Chief Financial Officer
CUEC	Complimentary User Entity Control
DHS	Department of Homeland Security
FMPM	Financial Management Policy Manual
ICE	U.S. Immigration & Customs Enforcement
RM&A	Risk Management and Assurance
SOC	Service Organization Control
SP	Service Provider
SSAE	Statement on Standards for Attestation Engagement

Term	Definition
Complimentary User Entity Control	Controls that the service organization assumes, in the design of its service, will be implemented by user entities, and which, if necessary to achieve control objectives, are identified in the description of its system.
Service Provider	An individual, group, or organization that has been assigned responsibility for providing specified services and/or deliverables to the user entity but does not fall within the chain of command or direct supervision/oversight of the user entity: as such, the user entity has a level of reliance on the provided services and/or deliverables without direct, consistent involvement in and oversight of the process. The services provided by individual, group, or organization are likely to be relevant to the user entity's internal control over financial reporting.
Statement on Standards for Attestation Engagements 18	SOC 1 reports are based on the SSAE 18 standard developed by the American Institute of Certified Public Accountants (AICPA) and report on the effectiveness of internal controls at a service organization that may be

(SSAE 18) Service Organization Controls (SOC) 1 report:	relevant to the user entity's agency internal control over financial reporting.
User Entity	An entity that uses a service organization and whose financial statements are being audited.

Summary of Changes

Revision Type: Technical

Changes:

- Updated introduction section with clarifying language to be in alignment with DHS FMPM. [Introduction; Page 2].
- Removed DHS Management Responsibilities and added clarifying language. [Responsibilities; Page 3].
- Updated language for responsible parties on the responsibilities section. [Responsibilities; Page 3].
- Added clarifying language on the Policy section to ensure alignment with DHS FMPM [Policies; Page 5].
- Updated Authorities and References [Authorities and References; Page 11].
- Made formatting changes and added clarifying language throughout policy to align with FMPM Style Guide.