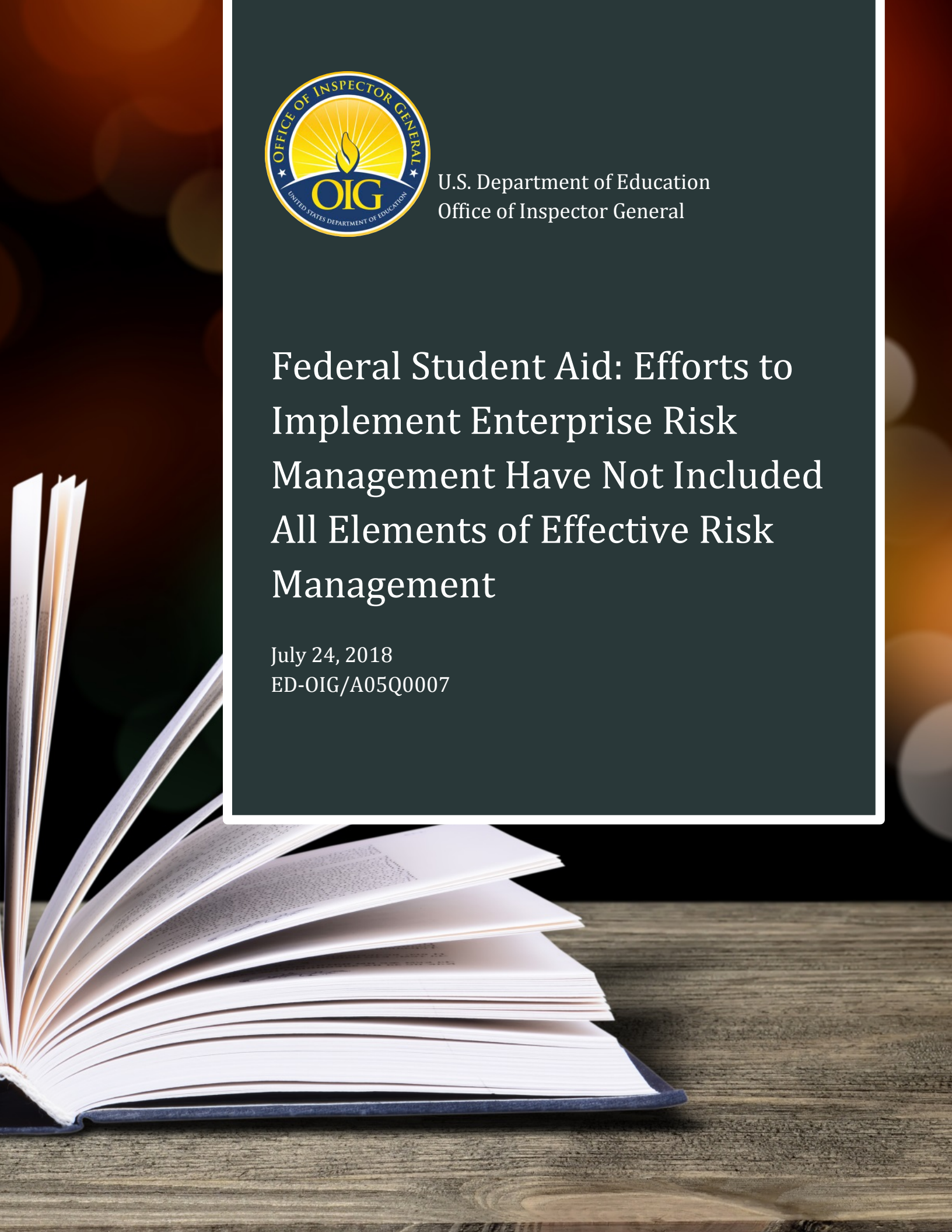


U.S. Department of Education
Office of Inspector General

Federal Student Aid: Efforts to Implement Enterprise Risk Management Have Not Included All Elements of Effective Risk Management

July 24, 2018
ED-OIG/A05Q0007

NOTICE

Statements that managerial practices need improvements, as well as other conclusions and recommendations in this report, represent the opinions of the Office of Inspector General. The appropriate U.S. Department of Education officials will determine what corrective actions should be taken.

In accordance with the Freedom of Information Act (Title 5, United States Code, Section 552), reports that the Office of Inspector General issues are available to members of the press and general public to the extent information they contain is not subject to exemptions in the Act.

July 24, 2018

TO: James F. Manning
Acting Chief Operating Officer
Federal Student Aid

FROM: Bryon S. Gordon /s/
Assistant Inspector General for Audit

SUBJECT: Final Audit Report, "Federal Student Aid: Efforts to Implement Enterprise Risk Management Have Not Included All Elements of Effective Risk Management," Control Number ED-OIG/A05Q0007

Enclosed is our final report that consolidates the results of our audit of Federal Student Aid's enterprise risk management. We have provided an electronic copy to your audit liaison officer. We received your comments disagreeing with the finding and recommendations in our draft report.

U.S. Department of Education policy requires that you develop a final corrective action plan within 30 days of the issuance of this report. The corrective action plan should set forth the specific action items and targeted completion dates necessary to implement final corrective actions on the finding and recommendations contained in this final audit report. Corrective actions that your office proposes and implements will be monitored and tracked through the Department's Audit Accountability and Resolution Tracking System.

In accordance with the Inspector General Act of 1978, as amended, the Office of Inspector General is required to report to Congress twice a year on the audits that remain unresolved after 6 months from the date of issuance.

We appreciate your cooperation during this audit. If you have any questions, please contact me at (202) 245-6900 or Bryon.Gordon@ed.gov or Gary D. Whitman at (312) 730-1620 or Gary.Whitman@ed.gov.

Table of Contents

Results in Brief 1

Introduction 6

FSA's Major ERM Implementation Activities 9

Finding. Federal Student Aid Did Not Implement All Elements Characteristic of Effective ERM 14

Appendix A. Scope and Methodology 33

Appendix B. FSA's Organizational Structure 37

Appendix C. Risk Management Frameworks 38

Appendix D. Laws and Other Requirements Affecting ERM in the Federal Government 42

Appendix E. Acronyms and Abbreviations 44

FSA Comments 45

Results in Brief

What We Did

The objective of our audit was to determine the extent to which Federal Student Aid (FSA) had implemented its enterprise risk management (ERM) framework. ERM is an organization-wide approach to addressing internal and external risks by understanding the combined impact of those risks as an interrelated set, rather than addressing the risks only within silos. ERM should be forward-looking and designed to help managers make better decisions, alleviate threats, and identify unknown opportunities to improve the efficiency and effectiveness of government operations.[1] A well-designed and implemented approach to ERM is intended to help an organization manage its risks to be within a range that management is willing to accept in pursuit of achieving organizational objectives.[2] Risk management is not a stand-alone, separate activity. Instead, it should be integrated into all of an organization's practices and processes.[3]

FSA developed its first ERM framework (2006) using the Committee of Sponsoring Organizations of the Treadway Commission (COSO) ERM framework as guidance.[4] FSA's second ERM framework (2010) was influenced by the COSO ERM framework and the International Organization for Standardization (ISO) 31000 risk management

[1] Pages 1 and 9 of OMB Circular No. A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control," updated by the Office of Management and Budget and issued on July 15, 2016.

[2] Pages 16, 17, 20, and 24 of "Enterprise Risk Management — Integrated Framework," issued by the Committee of Sponsoring Organizations of the Treadway Commission in September 2004.

[3] Sections 3(b) and 4.3.4 of ISO 31000, "Risk Management — Principles and Guidelines," issued by the International Organization for Standardization in November 2009.

[4] COSO is a joint initiative of five private sector organizations: the American Accounting Association, the American Institute of Certified Public Accountants, the Financial Executives International, the Association of Accountants and Financial Professionals in Business, and the Institute of Internal Auditors. COSO's ERM framework was developed through research, analysis, and a public review process and is used by organizations around the world (Source: COSO).

framework.[5] In 2017, FSA developed new, and updated existing, processes in response to Office of Management and Budget (OMB) Circular No. A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control."[6]

Through discussions with FSA managers and employees and reviews of FSA's documents and records relevant to ERM, we assessed whether FSA had fully implemented all elements of its ERM framework and whether FSA's implementation covered the eight elements—internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring—characteristic of effective ERM, as reflected in the COSO ERM framework, ISO risk management framework, and OMB guidance. (See Appendix C for details.) We evaluated the status of FSA's implementation of ERM as of August 2017.

What We Found

FSA did not implement all elements of its ERM framework or implement all elements characteristic of effective ERM. FSA developed an ERM framework, established a risk management office, and created a risk management committee. FSA also implemented the following elements of its ERM framework and characteristic of effective ERM.

- Risk Assessment: FSA developed processes for assessing risk, evaluating the impact of the risks, and evaluating the likelihood of the risks occurring.
- Risk Response: FSA developed a process for responding to risks.
- Control Activities: FSA developed a process for implementing internal control activities associated with the risk responses.

However, FSA did not fully implement the following elements characteristic of effective ERM.

- Internal Environment: FSA did not define and retain records of management's risk management philosophy, risk appetite, or risk tolerance.

[5] ISO is an independent, nongovernmental international organization with a membership consisting of 162 national standards bodies. ISO's risk management framework was created by a working group that included technical advisors from 18 countries and has been adopted by organizations around the world (Source: ISO).

[6] OMB Circular No. A-123 includes ERM concepts and guidelines based on COSO and ISO.

- Information and Communication: FSA did not communicate management's risk management philosophy, risk appetite, or risk tolerance; FSA's ERM framework; or information about FSA's enterprise-level risks to internal and appropriate external stakeholders.[7]
- Objective Setting: FSA did not ensure that objectives and risk responses were aligned with management's risk appetite.
- Event Identification: FSA did not identify and assess risks in a way that ensured that it had a complete risk profile (set of enterprise-level risks) to evaluate. From 2010 through 2014, FSA's risk profile described each enterprise-level risk, suggested mitigation strategies to address each risk, included assessments of risk impact and the likelihood of each risk occurring, and explained how the risk was trending from one month to the next. In response to OMB Circular No. A-123, FSA finalized (in April 2017) a process to identify and assess risks for a new risk profile. However, the process did not include all assessments of risks relevant to FSA's business units, external stakeholders, or high-risk projects.[8]
- Monitoring: FSA did not annually evaluate ERM efforts to assess whether FSA was achieving its ERM objectives or reducing risks to be within the level management was willing to accept.

Because FSA management did not ensure that all elements of FSA's ERM framework and all elements characteristic of effective ERM were fully implemented, it did not have reasonable assurance that ERM efforts helped management achieve its ERM objectives and reduced enterprise-level risks to be within the level that management was willing to accept.

What We Recommend

We recommend that the Chief Operating Officer for FSA—

1. define and retain records of management's risk management philosophy, risk appetite, and risk tolerance;
2. retain records fully describing FSA's ERM framework;

[7] Appropriate external stakeholders means those who oversee FSA (such as the Secretary and Congress), those who help FSA fulfill its risk management responsibilities (such as contractors), and others as determined by FSA management.

[8] A business unit is a part of an FSA office.

3. communicate management's risk management philosophy, risk appetite, and risk tolerance; FSA's ERM framework; and information about FSA's enterprise-level risks to internal and appropriate external stakeholders;
4. align strategic objectives and risk responses with the risk appetite that management defines;
5. ensure that the process for developing a risk profile covers all potential enterprise-level risks, including those identified through risk assessments of all business units and high-risk projects; and
6. evaluate, at least annually, whether FSA's ERM efforts have achieved management's ERM objectives and reduced enterprise-level risks to be within the level management is willing to accept. Identify and implement changes, if any, suggested by the evaluations.

FSA Comments

FSA stated that the draft of this report did not present a complete picture of the effectiveness of FSA's ERM program or its relative role in the Federal government's ERM systems among agencies. FSA also expressed concern about the audit objective, stating that the original objective of the audit was to determine the extent to which FSA had implemented its ERM framework. FSA asserted that the draft of this report showed that the Office of Inspector General (OIG) changed its objective and assessed whether FSA had fully implemented all elements of its ERM framework and whether FSA's implementation covered the eight elements characteristic of effective ERM.

FSA also disagreed with the finding, stating that the OIG unilaterally defined required criteria when none exist and reported about missing elements in FSA's ERM program when those cited elements are not required. FSA also disagreed with all six recommendations. About the first recommendation, FSA stated that OMB Circular No. A-123 does not require a formal risk management philosophy. FSA also stated that a formal risk appetite is not required. For the second, third, and fourth recommendations, FSA stated that it already conducts the activities OIG is recommending. About the fifth recommendation, FSA stated that its current approach for identifying and assessing ERM risks is an acceptable approach within the ERM community. Finally, for the sixth recommendation, FSA disagreed that the goal of evaluating an ERM program is to determine whether it has reduced enterprise-level risks to acceptable levels.

Within its comments on the draft of this report, FSA described enhancements it has made to its approach to ERM since August 2017. FSA stated that it began using COSO's 2017 ERM framework as guidance when modifying its ERM approach. FSA also stated that it has established a new ERM governance structure that has three levels. In

addition, the Enterprise Risk Management office (formerly the Risk Management office) is working with FSA's strategic planning team to ensure that enterprise-level risks are considered during the development of FSA's new strategic plan.

We summarized FSA's comments and provided our response at the end of the finding. We also included the full text of the comments in the FSA Comments section of this report.

OIG Response

We did not make any changes to the finding or recommendations based on FSA's comments. Contrary to FSA's comments, we did not revise our objective. Also, contrary to FSA's assertion, we did not unilaterally define ERM requirements. Our audit was intended to determine the extent to which FSA had implemented its ERM framework; nowhere in our report do we assert that specific elements of ERM are required. Rather, we state that the eight elements described in this report are characteristic of effective ERM. Specifically, our assessment was based on criteria contained in COSO, ISO, and OMB guidance—the same criteria upon which FSA's ERM framework and ERM implementation were based.

While we agree that all the criteria are not mandatory requirements established in regulation or OMB guidance, the criteria we used are necessary for the proper functioning of ERM. FSA did not provide sufficient evidence to demonstrate that its ERM has been fully implemented and is properly functioning. In fact, with its comments on the draft of this report, FSA highlighted enhancements it planned to make to its existing ERM, including areas on which we provided recommendations. Those enhancements would be responsive to some of the recommendations we made in this report.

Introduction

Background

FSA was authorized as a performance-based organization within the U.S. Department of Education (Department) by the 1998 amendments of the Higher Education Act of 1965, as amended (HEA).[9] According to the HEA, FSA was created to improve service to students and others participating in the student financial assistance programs, reduce the costs to administer those programs, increase accountability of the officials who administer the operational aspects of the programs, and develop and maintain a student financial aid system that includes complete, accurate, and timely data.

According to FSA's 2017 annual report, FSA has oversight responsibilities for almost $1.4 trillion in Federal student loans, of which it directly owns and manages about $1.2 trillion. From October 1, 2016, through September 30, 2017, FSA delivered $122.5 billion to about 13 million students attending about 6,000 postsecondary schools. FSA delivered these funds operating with an administrative budget of about $1.6 billion and almost 1,400 full-time employees whose efforts were augmented by contractors. About 12,000 contractor employees provided FSA with certain business services, such as loan servicing and information technology systems.[10]

As of July 2017, FSA consisted of 44 business units that were part of 11 offices—Administrative Services, Business Operations, Customer Experience, Enforcement, Finance, Acquisitions, Performance Management, Program Compliance, Technology, Risk Management, and the office of the Chief Operating Officer (see Appendix B). The Chief Operating Officer for FSA assigned responsibility for ERM to Risk Management. Risk Management consisted of two business units: the Risk Analysis and Reporting Group and the Internal Review Group. The Risk Analysis and Reporting Group provided enterprise risk management oversight and guidance. The Internal Review Group evaluated the effectiveness of FSA's system of internal control.

[9] A performance-based organization in the Federal government commits to achieving specific measurable goals in exchange for more flexibility in how it manages its personnel decisions, procurement, and other administrative and management functions.

[10] Source: FSA's 2016 annual report, "Letter from the Chief Operating Officer of Federal Student Aid."

Risk Management Frameworks

Two frameworks, one issued by COSO in September 2004 and one issued by ISO in November 2009, influenced the design of FSA's ERM frameworks and FSA's approach to implementing ERM. In July 2016, OMB updated OMB Circular No. A-123. The revised circular requires Federal agencies to incorporate elements of ERM into their risk management and to ensure that Federal managers effectively manage risks that an agency faces in achieving its strategic objectives and risks that arise from the agency's activities and operations. OMB, COSO, and ISO describe risk management in similar ways.

- OMB describes ERM as "an effective Agency-wide approach to addressing the full spectrum of the organization's external and internal risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos."
- COSO describes ERM as "a process, effected by an entity's board of directors, management and other 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 achievement of entity objectives." In June 2017, COSO updated its ERM framework, adding that "Enterprise risk management is not a function or department. It is the culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realizing value."
- ISO states that risk management is not a stand-alone, separate activity. Instead, risk management should be integrated into all of an organization's practices and processes.

All three describe elements (internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring) or components characteristic of effective ERM. See Appendix C for more information about these elements and components.

Laws and Other Requirements Affecting Risk Management in the Federal Government

The following Federal legislation, requirements, and guidance have had an impact on risk management in the Federal government. (See Appendix D for additional information on each item.)

- Federal Managers' Financial Integrity Act of 1982

- Government Performance and Results Act of 1993 and GPRA Modernization Act of 2010
- "Standards for Internal Control in the Federal Government" (issued by the Government Accountability Office (GAO) in November 1999 and September 2014)
- OMB Circular No. A-11, "Preparation, Submission, and Execution of the Budget," (July 2016 and updated July 2017)
- OMB Circular No. A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control," (July 2016)
- OMB Circular No. A-129, "Policies for Federal Credit Programs and Non-Tax Receivables," (January 2013)

FSA's Major ERM Implementation Activities

In 2004, FSA initiated efforts to develop an ERM framework. Since 2006 when it established its first ERM framework, FSA's major ERM implementation activities have included the following.

Table 1. ERM Activities at FSA

Year	ERM Activities
2006	Appointed its first Chief Risk Officer. Created an ERM Group under the Enterprise Performance Management Services Group. Developed an initial ERM framework.
2007	Developed and documented its process for conducting risk assessments of business units.
2010	Changed the name of the ERM Group to the Risk Management office, with a new Chief Risk Officer (the second) reporting directly to the Chief Operating Officer. Established a Risk Management Committee chaired by the new Chief Risk Officer. Revised its ERM framework. Prepared a draft of its internal control environment self-assessment. Prepared a draft risk diagnostic and draft risk dashboard (served as a risk profile).[11]
2012	Updated the draft internal control environment self-assessment. Updated the draft risk diagnostic and draft risk dashboard.
2014	Replaced the second Chief Risk Officer with an acting Chief Risk Officer (the third) but continued with the second Chief Risk Officer as the chairperson of the Risk Management Committee.
2015	Appointed a new Chief Risk Officer (the fourth) and continued with the second Chief Risk Officer as the chairperson of the Risk Management Committee.

[11] In October 2016, we requested documents relevant to FSA's ERM. FSA did not completely fulfill this request until March 2017. About 30 percent of the documents that FSA provided and we used to draw our conclusions were not finalized (for example, the documents were labeled as "draft" or "working copy").

Year	ERM Activities
2016	Updated existing and developed and documented new risk assessment processes in response to the revised OMB Circular No. A-123.
2017	Appointed an acting Chief Risk Officer (the fifth) in January. Created a risk profile in response to the revised OMB Circular No. A-123. Hired a new Chief Risk Officer (the sixth) in August. Changed the title of the position from Chief Risk Officer to Chief Enterprise Risk Officer. Changed the name of the committee from the Risk Management Committee to the Enterprise Risk Executive Committee. Appointed the Chief Enterprise Risk Officer as the chairperson of the new Enterprise Risk Executive Committee.

In 2006, the Chief Operating Officer for FSA created an ERM Group within the Enterprise Performance Management Services Group and appointed FSA's first Chief Risk Officer.[12] The ERM Group developed FSA's first ERM framework using the COSO ERM framework as guidance. That first ERM framework included all eight elements of an effective ERM framework suggested by the 2004 COSO model (see Figure 1).

Figure 1. COSO ERM Framework

[12] The Chief Risk Officer reported to the head of the Enterprise Performance Management Services Group, not directly to the Chief Operating Officer.

During 2007 and 2008, the ERM Group created documents describing a dual-step plan for implementing ERM. The first step was the identification and evaluation of the risks that could affect FSA's achievement of objectives. The second step was the ERM Group's assessment of the risks relevant to each of FSA's 26 business units. The ERM Group described processes for identifying, inventorying, and evaluating the impact and likelihood of business unit risks and then reporting on the results. From 2008 through 2010, the ERM Group completed risk assessments of 17 business units.[13]

In 2010, FSA split the Enterprise Performance Management Services Group into two offices (Performance Management and Risk Management) and established a Risk Management Committee consisting of 12 FSA managers.[14] The Chief Risk Officer was the director of Risk Management and chairperson of the Risk Management Committee, reporting directly to the Chief Operating Officer. The Risk Management Committee, through the work completed by Risk Management, was responsible for identifying, tracking, and mitigating enterprise-level risks.

All 12 Risk Management Committee members also were members of FSA's 16-member Operating Committee.[15] The Operating Committee members determined the risks specific to their respective offices that could be enterprise-level risks and reported those risks to the Risk Management Committee. In addition to the risks that Operating Committee members reported, the chairperson of the Risk Management Committee identified potential risks to discuss during meetings (after discussions with Risk Management Committee members and reviews of news reports). The Risk Management Committee determined what actions to take to address those risks.

Also in 2010, FSA revised its 2006 ERM framework. The 2010 framework was influenced by the 2004 COSO ERM framework and the 2009 ISO 31000 risk management

[13] By 2016, FSA had grown from 26 to 40 business units. As of July 2017, FSA consisted of 44 business units.

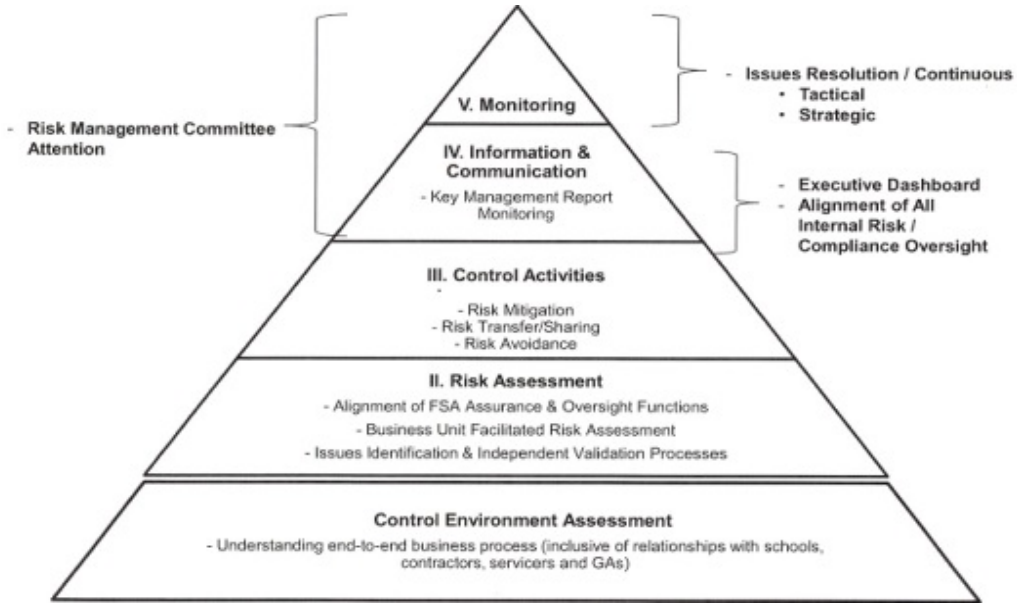
[14] Chief Operating Officer, Deputy Chief Operating Officer, Chief of Staff, Chairperson of the Risk Management Committee, Chief Business Operations Officer, Chief Compliance Officer, Chief Information Officer, Chief Risk Officer, Director of FSA Acquisitions, Chief Finance Officer, Chief Customer Experience Officer, and Chief Enforcement Officer.

[15] In addition to the 12 Risk Management Committee members, the Operating Committee included the Chief Digital Products Officer, Chief Business Optimization Officer, Director of Policy Liaison and Implementation, and Chief Administration Officer.

framework. FSA's 2010 ERM framework consolidated seven of the eight elements suggested by the 2004 COSO ERM framework under five elements (see Figure 2).

- Internal Environment (as defined in FSA's 2006 ERM framework) became Control Environment.
- Event Identification became a part of Risk Assessment rather than a separate element.
- Risk Response became part of Control Activities rather than a separate element.
- Information and Communication remained the same.
- Monitoring remained the same.

Figure 2. FSA's Revised ERM Framework



Objective setting was the one element of the COSO ERM framework that FSA did not cover in its 2010 ERM framework. FSA set goals and objectives and developed performance measures to assess its success in achieving its goals and objectives. However, setting goals and objectives was part of FSA's strategic planning process, not FSA's ERM efforts.

FSA's 2010 ERM framework included business unit risk assessments as part of the risk assessment element (see Figure 2). However, in 2010, Risk Management deviated from that framework and stopped conducting business unit risk assessments. Instead, Risk Management started assessing FSA's high-risk projects on an as-needed basis. Risk Management worked with the Chief Business Operations Officer to identify an initial list of high-risk projects. Risk Management then worked with the

Operating Committee members to add or remove high-risk projects from the list. Examples of the types of high-risk projects Risk Management might assess included a transition to a new information technology system, the implementation of new or revised regulations, or a large procurement of goods or services.

From 2010 through 2014, the Risk Management Committee used a risk diagnostic, a risk dashboard, or both, as its risk profile recording FSA's enterprise-level risks and informing the discussion of those risks during its monthly meetings. The risk diagnostic described each risk that FSA considered an enterprise-level risk, provided an assessment of inherent risk, and indicated the likelihood of each identified enterprise-level risk occurring. Risk Management updated the risk diagnostic as needed. The risk dashboard described each risk that FSA considered an enterprise-level risk, suggested mitigation strategies to address each risk, included assessments of the impact and likelihood of each identified enterprise-level risk occurring, and explained how each enterprise-level risk was trending from one month to the next (less likely, more likely, or unchanged). Risk Management updated the risk dashboard monthly. FSA stopped using the risk diagnostic in 2012 and the risk dashboard in 2014.

In 2014, the Chief Operating Officer for FSA separated the duties of the Chief Risk Officer and chairperson of the Risk Management Committee, assigning two different people to handle the duties of those two positions.

In 2015, Risk Management conducted only one business unit risk assessment. FSA had approximately 40 business units at the time.

In 2016 and 2017, FSA updated its existing and developed and documented new ERM risk assessment processes in response to the revised OMB Circular No. A-123. FSA created a document describing its processes for creating a profile of enterprise-level risks and revised and created documents describing its processes for scoring the impact and likelihood of the enterprise-level risks and how FSA planned to compile and record risk information in the profile. FSA finalized this enterprise-level risk profile in April 2017.

In August 2017, the Chief Operating Officer for FSA restored the Chief Risk Officer as the chairperson of the Risk Management Committee and changed the titles of Chief Risk Officer and Risk Management Committee to Chief Enterprise Risk Officer and Enterprise Risk Executive Committee, respectively, placing greater emphasis on FSA's enterprise-wide focus on risk management. According to FSA's fiscal year 2017 annual report (November 2017), FSA was introducing a new approach to oversight of organizations participating in or supporting Federal student aid programs and building a model that integrates proactive risk management.

Finding. Federal Student Aid Did Not Implement All Elements Characteristic of Effective ERM

FSA did not implement all elements of its ERM framework or implement all elements characteristic of effective ERM. Through discussions with FSA managers and employees and reviews of documents and records relevant to ERM, we found that FSA did not fully implement the following five elements that originally were part of its ERM framework and characteristic of effective ERM.

- Internal Environment: FSA management did not define and retain records of its risk management philosophy, risk appetite, or risk tolerance.
- Information and Communication: FSA management did not communicate its risk management philosophy, risk appetite, or risk tolerance; FSA's ERM framework; and information about FSA's enterprise-level risks to internal and appropriate external stakeholders.
- Objective Setting: FSA management did not ensure that its strategic objectives and risk responses were aligned with its risk appetite.
- Event Identification: FSA management did not identify and assess risks in a way that ensured that the Risk Management Committee had a risk profile that considered a complete set of enterprise-level risks.
- Monitoring: FSA management did not annually evaluate ERM efforts to assess whether ERM was achieving management's ERM objectives or reducing risks to be within the level management was willing to accept.

Risk Management Philosophy, Risk Appetite, and Risk Tolerance Not Defined and Communicated

FSA management did not define and retain a record of its risk management philosophy, risk appetite, or risk tolerance or communicate those concepts to internal and appropriate external stakeholders. OMB Circular No. A-123, COSO, and ISO describe risk management philosophy, risk appetite, and risk tolerance as follows.

- Risk management philosophy is the set of shared beliefs and attitudes characterizing how an organization considers risk in everything that it does, from strategy development and implementation to its day-to-day activities. It is

described in policy statements, decision making, and oral and written communications.[16]

- Risk appetite is the amount of risk an organization is willing to accept in pursuit of value, mission, and vision. It reflects the organization's risk management philosophy and influences culture and operating style. Organizations should consider the level at which risk becomes acceptable or tolerable.[17]
- Risk tolerance is measurable and is the acceptable level of variation relative to achievement of a specific objective. Operating within risk tolerances provides management greater assurance that the organization remains within its risk appetite, which, in turn, provides a higher degree of comfort that the organization will achieve its objectives.[18]

Risk Management Philosophy

FSA management did not define or ensure that management, employees, and appropriate external stakeholders (such as postsecondary schools and contractors) had at least a general understanding of FSA management's risk management philosophy.[19] When we asked a former Chief Risk Officer (the fourth) and FSA's Senior Advisor for ERM for documents or records relevant to FSA's risk management philosophy, both referenced three sections from the "Federal Student Aid Strategic Plan FY 2015–19"—"Message From the Chief Operating Officer;" "FSA Mission and Core Values;" and "Strategic Goals and Objectives." However, "FSA Mission and Core Values" does not mention risk. In "Message From the Chief Operating Officer" and "Strategic Goals and Objectives," the only mention of risk is a reference to FSA's Strategic Goal B: "Proactively manage the student aid portfolio to mitigate risks." Two of the objectives (Strategic Goal B: Objective B.1 and Objective B.2) reference risk, stating that FSA will

[16] "Enterprise Risk Management – Integrated Framework," pages 27, 28, and 71.

[17] "Enterprise Risk Management – Integrated Framework," page 19; OMB Circular No. A-123, page 10; ISO 31000, "Risk Management – Principles and Guidelines," section 5.3.5.

[18] "Enterprise Risk Management – Integrated Framework," pages 20 and 40; OMB Circular No. A-123, page 10; Attribute 6.08 of "Standards for Internal Control in the Federal Government," issued by GAO in September 2014.

[19] Participating schools must ensure that only eligible students receive student financial aid. Contractors provide services, such as servicing student loans. Both are key players in FSA's efforts to manage enterprise-level risks.

enhance analytical and research capabilities to proactively identify operational and reputational risk and develop data-driven processes to manage identified risk. However, the referenced objectives refer to risk only in the context of the student aid portfolio; they do not describe an enterprise-wide risk management philosophy.

According to the former acting Chief Operating Officer (as of May 2017), Risk Management conducted numerous educational and informational sessions during which it explained FSA management's risk management philosophy. Risk Management distributed informational handouts to employees during FSA Day,[20] created online presentations that were available to employees, and gave presentations to employees within business units as part of business unit risk assessment start-up meetings. We reviewed the informational handouts and presentations. None of them described management's risk management philosophy or reflected that management and employees shared beliefs and attitudes about risk in strategic development and day-to-day activities.

Risk Appetite and Risk Tolerance

FSA management did not define or ensure that its managers, employees, and appropriate external stakeholders had at least a general understanding of FSA management's risk appetite and risk tolerance. When we asked a former Chief Risk Officer (the fourth) and FSA's Senior Advisor for ERM for documents or records relevant to management's risk appetite and risk tolerance, they told us that both were discussed at Risk Management Committee meetings. The Senior Advisor for ERM stated that the Risk Management Committee members discussed risk appetite and risk tolerance on an individual risk basis, and Operating Committee members considered risk appetite and risk tolerance in their daily decision-making activities. The Senior Advisor for ERM also referred us to "Federal Student Aid FY 2016 Annual Report" to find FSA management's risk appetite and risk tolerance. However, the 2016 annual report stated only that FSA will work with OMB to establish an appropriate risk tolerance threshold for improper payments; it did not mention FSA management's enterprise-wide risk appetite or risk tolerance.

According to the former acting Chief Operating Officer, the Risk Management Committee discussed risk appetite and risk tolerance as part of its conversations regarding risk responses and mitigation activities. We were unable to confirm any

[20] FSA Day is an annual event in which FSA employees have the opportunity to learn about the business units within FSA and strengthen relationships with other FSA employees.

of these discussions because the Risk Management Committee did not retain any notes about the discussions that took place during its meetings.

Management is responsible for defining and communicating its risk management philosophy, risk appetite, and risk tolerance and ensuring that the organization's objectives align with management's risk appetite. A well-developed risk management philosophy that an organization's employees and business partners understand helps an organization effectively recognize and manage risks. Well-developed and understood risk appetite and risk tolerance help operational managers select a set of actions that align risks with management's risk appetite and risk tolerance.[21] According to Title 36, Code of Federal Regulations, § 1222.22, Federal agencies are required to establish policies for retaining records of such policies and procedures and corresponding actions taken. According to "Administrative Communications System, U.S. Department of Education, Departmental Directive OM: 6-103," Department offices shall create records that are sufficient to ensure adequate and proper documentation of all of the Department's policies and procedures.

Without defining and communicating its risk management philosophy, risk appetite, and risk tolerance, FSA management cannot effectively identify and then manage all enterprise-level risks. For example, until risk tolerance is defined, FSA management cannot assess the differences between its defined risk tolerance and actual risks or measure the effect of its risk mitigation activities against its defined risk tolerance. Without a risk appetite statement that is reflected in policies, procedures, decisions, training, and communication, the organization's risk appetite cannot be widely understood and used by managers, employees, and appropriate external stakeholders.

Strategic Objectives and Risk Responses Not Aligned with Risk Appetite[22]

FSA management did not ensure that its strategic objectives and risk responses were aligned with its risk appetite. FSA included strategic goals and corresponding objectives and performance measures in the strategic plans covering the 5-year periods ending 2015, 2016, and 2019. However, without first defining management's risk appetite or

[21] "Enterprise Risk Management – Integrated Framework," pages 22, 28, 39, 71, and 73; OMB Circular No. A-123, pages 10 and 13.

[22] FSA's 2006 ERM framework mentioned four types of objectives: strategic, operations, reporting, and compliance. FSA's 2010 ERM framework did not directly address any types of objectives. The scope of this audit covered only strategic objectives (not operations, reporting, or compliance objectives).

making ERM a formal part of establishing strategic goals and objectives, FSA management could not ensure that the strategic objectives were aligned with its risk appetite. Likewise, although FSA management determined how it would respond to enterprise-level risks it identified in its current risk profile (April 2017), FSA management could not ensure that those risk responses aligned with management's risk appetite.

Management is responsible for establishing an organization's risk appetite, selecting risk responses that align risks with risk appetite, and ensuring that the organization's objectives align with risk appetite. When an organization's objectives are not aligned with management's risk appetite, the organization might not accept enough risk or might accept too much risk in pursuit of achieving objectives.[23] A well-developed and understood risk appetite also is essential for determining appropriate risk responses.[24]

Without defining and communicating its risk appetite and incorporating ERM into its strategic planning, FSA management will not have reasonable assurance that its strategic objectives are within its risk appetite. Also, without defining and communicating its risk appetite, FSA management will not have reasonable assurance that its risk responses are within its risk appetite.

ERM Framework and Enterprise-Level Risks Not Communicated to Internal and Appropriate External Stakeholders

FSA management did not ensure that FSA employees and appropriate external stakeholders fully understood their roles in FSA's ERM efforts and had not ensured that business units were exchanging risk-relevant information with each other. We interviewed 41 FSA employees (33 managers and 8 nonmanagers). When we asked them to describe their roles in FSA's ERM efforts, 32 percent (13) described their roles in ERM as limited to their business unit's or offices' work and 17 percent (7) responded that they did not have any role in FSA's ERM. According to a former Chief Risk Officer (the fourth), Risk Management had not defined FSA employees' roles relevant to ERM. In 2010, FSA created a diagram of its ERM framework (see Figure 2). According to the former acting Chief Operating Officer (as of May 2017), FSA did not have any documents describing the concepts behind its ERM framework; the former acting Chief Operating Officer also informed us that the diagram listed each element of FSA's ERM framework and was self-explanatory. However, the diagram did not explain the details of FSA's ERM. Instead, it only identified the elements of FSA's ERM framework and one, two, or

[23] "Enterprise Risk Management – Integrated Framework," pages 22 and 39.

[24] OMB Circular No. A-123, page 13.

three bullet points for each element. The diagram did not include information sufficient to help management, employees, and appropriate external stakeholders better understand their ERM roles and responsibilities. It was not self-explanatory.

Additionally, the Internal Review Group and the Risk Analysis and Reporting Group were not sharing information relevant to ERM with each other. The former director of the Internal Review Group and the former Internal Review Officer both told us that the Internal Review Group generally was not sharing information about its internal reviews with the Risk Analysis and Reporting Group.

Also, after conducting 17 business unit risk assessments from 2008 through 2010 and 1 additional assessment in 2015, Risk Management provided the results of each risk assessment only to the director of the business unit that was assessed and the Operating Committee member with oversight responsibility for the assessed business unit. Risk Management did not provide results of these business unit risk assessments to all of the Risk Management Committee members.

In response to OMB Circular No. A-123, Risk Management, in collaboration with the Operating Committee and Risk Management Committee, developed and subsequently finalized (in April 2017) a risk profile documenting FSA's enterprise-level risks. According to the Senior Advisor for ERM, this risk profile was not shared with all FSA employees but was shared with the Operating Committee, Risk Management Committee, FSA employees involved in identifying activities to address the risks in the risk profile, and Department officials (external to FSA) relevant to integrating FSA's risk profile with the Department's risk profile. Although FSA communicated with its external stakeholders through mailing lists, a listserv, dear colleague letters, and electronic announcements, those communications have not been relevant to FSA's ERM.

Information relevant to risk management should be identified, captured, and communicated in a form and timeframe that helps employees carry out their responsibilities. Risk management information is needed at all levels of an organization to sufficiently identify, assess, and respond to risks. Effective communication means communication flows down, across, and up the organization. Employees receive clear communications regarding their role and responsibilities.[25]

[25] "Enterprise Risk Management – Integrated Framework," page 22.

A risk management framework ensures that information about risk is adequately reported and used for decision making and accountability at all relevant levels. Organizations should design a risk framework that includes a risk management policy. A risk management policy typically addresses accountability and responsibilities for managing risks and the way risk management performance will be measured and reported. Management should develop plans for how it will communicate with internal and external stakeholders.[26]

The concept of capturing and timely communicating information in an appropriate form has been a standard in the Federal government since at least 1999. According to "Standards for Internal Control in the Federal Government," information should be recorded and communicated to management and others who need it and be in a form and communicated within a timeframe that enables management and others to carry out their responsibilities. Effective communications should occur with information flowing down, across, and up the organization.[27] GAO refined these standards in 2014: "Management communicates quality information down and across reporting lines to enable personnel to perform key roles in achieving objectives, addressing risks, and supporting the internal control system."[28] According to Title 36, Code of Federal Regulations, § 1222.22, Federal agencies are required to establish policies for retaining records of such policies and procedures and corresponding actions taken. According to "Administrative Communications System, U.S. Department of Education, Departmental Directive OM: 6-103," Department offices shall create records that are sufficient to ensure adequate and proper documentation of all of the Department's functions, decisions, policies and procedures.

External stakeholders, including postsecondary schools and contractors, are crucial for FSA to adequately implement its ERM.

- In fiscal year 2017, about 6,000 postsecondary schools were participating in student financial assistance programs. These schools are responsible for helping FSA ensure that only eligible students receive Federal student financial aid.

[26] "Risk Management — Principles and Guidelines," sections 4.1, 4.3.2, 4.3.6, and 4.3.7.

[27] Pages 18 and 19 of "Standards for Internal Control in the Federal Government," issued by GAO in November 1999.

[28] Attribute 14.03 of "Standards for Internal Control in the Federal Government," issued by GAO in September 2014.

- As of January 2017, FSA had awarded 84 contractors a total of 120 contracts with a value of about $1.9 billion. These contractors provide FSA with goods and services, such as information technology products, call center support services, and student financial aid loan services (including loan servicing and debt collections).

External stakeholders must have quality information necessary to help them assist FSA's employees in achieving FSA's objectives and addressing risks. If information relevant to FSA's ERM and enterprise-level risks are not communicated to employees and appropriate external stakeholders, FSA management will not have reasonable assurance that management, employees, and appropriate external stakeholders have the information necessary to carry out their ERM responsibilities and help FSA achieve its objectives.

Complete View of All Enterprise-Level Risks Not Developed

Risk Management did not consolidate the results of risk assessments of business units and high-profile projects when compiling an inventory of potential enterprise-level risks. FSA established the "Enterprise Risk Management Strategic Plan" in 2008. From 2008 through 2010, Risk Management assessed risks relevant to 17 business units; it assessed risks relevant to only one more business unit in 2015. Also, from 2010 through 2015, Risk Management assessed risks relevant to at least 21 high-profile projects. In addition, Risk Management conducted one targeted risk assessment of an issue that could have had a significant impact on FSA.[29] Program Compliance conducted annual risk assessments and Technology conducted risk assessments throughout every year. Although these various risk assessments were completed, Risk Management was not consolidating the results for the purpose of identifying potential enterprise-level risks to include in the risk profile provided to the Risk Management Committee.

In April 2017, Risk Management, in collaboration with the Operating Committee and Risk Management Committee, finalized a new risk profile to retain a record of FSA's enterprise-level risks. We evaluated FSA's process for compiling enterprise-level risks for the new risk profile and concluded that it did not provide reasonable assurance that FSA compiled a complete set of enterprise-level risks. FSA identified enterprise-level risks for its 2017 risk profile through the following sources:

[29] A targeted risk assessment evaluates specific risks that could affect FSA's ability to achieve its organizational goals and objectives.

- the previous year's Federal Managers' Financial Integrity Act and OMB Circular No. A-123 self-assessments and related assurance statements,
- Inspector General Management Challenges,
- Inspector General and Government Accountability Office audits,
- financial management risks documented in FSA's annual report,
- project management risks documented in FSA's investment and project management processes,
- issues and risks identified during Congressional Hearings and Questions for the Record,
- risks indicated by media reports, and
- interviews with Operating Committee members and other personnel.

However, the document did not mention assessments of the risks associated with high-profile projects (conducted on an as-needed basis), business unit risk assessments, targeted risk assessments, or assessments of risks completed by individual FSA offices (such as those conducted by Program Compliance and Technology) as ways FSA would identify potential enterprise-level risks. The document also did not mention any external stakeholders, such as postsecondary schools and contractors, as sources of information on potential enterprise-level risks, although such entities are critical to achieving FSA's objectives and managing risks.

Effective ERM requires an organization to identify sources of risk to generate a comprehensive list of risks based on events that might create, enhance, prevent, degrade, accelerate, or delay the achievement of objectives.[30] Additionally, effective ERM ensures that the organization considers activities at all levels of the organization when identifying enterprise-level risks. Risks for individual units of the organization might be within the units' risk tolerances, but the risks for individual units when taken together might exceed the risk appetite of the organization as a whole. ERM provides insight into all areas of organizational exposure to risk, thus increasing an organization's chances of executing a better assessment of risk. An organization's risk profile must consider risks from an organizational perspective.[31]

[30] "Risk Management – Principles and Guidelines," section 5.4.2.

[31] "Enterprise Risk Management – Integrated Framework," pages 19 and 59; OMB Circular No. A-123, pages 9, 10, and 13.

Without an effective process for collecting and consolidating enterprise-level risks, FSA management will not have reasonable assurance that it has accounted for all risks that could impact FSA's ability to achieve its objectives. FSA will not be able to analyze the interrelatedness of its enterprise-level risks or consider how the nature, likelihood, and relative size of the risks might affect FSA's ability to achieve objectives. Further, FSA management will not have reasonable assurance that the identified enterprise-level risks include both threats to and opportunities for achieving objectives as well as internal and external factors that could affect achieving those objectives.

Risk Responses and Corresponding Control Activities Not Identified and Evaluated

From June 2014 until April 2017, FSA management was not identifying and evaluating possible risk responses or establishing corresponding control activities for enterprise-level risks. From 2010 through May 2014, the Risk Management Committee used a risk dashboard to facilitate discussions and document decisions made about enterprise-level risks, risk responses, and control activities.[32] The Chief Risk Officer discussed enterprise-level risks with Operating Committee members, and they suggested appropriate risk responses and control activities for addressing the enterprise-level risks. Risk Management, in collaboration with the Operating Committee, updated the risk dashboard each month. The risk dashboard included information for the current month and prior month and served as a record of (1) the enterprise-level risks; (2) the impact and likelihood of those risks; (3) how each risk was trending from one month to the next (less likely, more likely, or unchanged); and (4) strategies to mitigate the risks. The Risk Management Committee then discussed this risk dashboard during its monthly meetings, and the Operating Committee members with oversight responsibility for the risk areas would report on the actions taken (control activities) to mitigate the assigned risks. However, from June 2014 until FSA finalized a risk profile in April 2017 (in response to OMB Circular No. A-123), the Risk Management Committee did not use the risk dashboard or any similar tool to identify or evaluate risk responses or corresponding control activities to address enterprise-level risks.

Risk response requires management to identify and evaluate possible responses to risks. Possible risk responses include acceptance, reduction, sharing, and avoidance. Management can then establish control activities—the policies and procedures applied to ensure that risk responses are effectively carried out. Management should select

[32] FSA used a risk diagnostic, a risk dashboard, or both, as its risk profile. However, only the risk dashboard included information on risk responses or control activities.

a set of actions (risk response) to align risks with the organization's risk tolerances and risk appetite. Management then should identify control activities needed to help ensure that the risk responses are implemented properly and timely.[33] Most ERM approaches include steps to (1) identify and assess a range of risk response options (developing alternatives), (2) decide on the best options among the alternatives, and (3) prepare and execute the selected response strategy.[34]

Risk response should fit with the organization's culture, management structure, and processes so that ERM becomes an essential part of regular management functions. We could not determine whether FSA managed risks to bring them within its risk appetite because FSA management has never defined its risk appetite (see Risk Appetite and Risk Tolerance). Additionally, FSA could not provide us with records (like the risk dashboard) covering June 2014 until April 2017 and showing that FSA management was developing appropriate risk responses and control activities to address enterprise-level risks. Therefore, we could not assess whether FSA management identified all potentially enterprise-level risks, such as the failure of a large school or a major data breach, and proactively developed appropriate risk responses and control activities for such risks.

FSA's April 2017 risk profile describes enterprise-level risks, responses to address risks and the corresponding control activities, and proposed actions to further reduce any exposure remaining after implementing the risk responses and control activities. According to the document showing how FSA developed its April 2017 risk profile, every 6 months FSA will determine whether the risk responses and control activities for its enterprise-level risk profile are managing risks as intended.

Performance of ERM Efforts Not Monitored

FSA management did not develop and implement processes for evaluating its ERM efforts, determining whether ERM was achieving management's objectives, or measuring whether ERM was bringing enterprise-level risks within management's risk appetite. The former Chief Risk Officer (fourth) and former Deputy Chief Operating Officer stated that the Risk Management Committee monitored FSA's ERM. However, the Risk Management Committee did not retain any records about the discussions that took place or decisions that were made during its meetings. According to Title 36, Code of Federal Regulations, § 1222.22, Federal agencies are required to establish

[33] "Enterprise Risk Management – Integrated Framework," pages 22, 55, and 61.

[34] OMB Circular No. A-123, pages 10 and 11.

policies for retaining records of decisions made, including substantive decisions reached in person, by telecommunications, or electronically, and records of important board, committee, or staff meetings. According to "Administrative Communications System, U.S. Department of Education, Departmental Directive OM: 6-103," Department offices shall create records that are sufficient to ensure adequate and proper documentation of all of the Department's functions, policies, decisions, procedures, and essential transactions.

Because we did not have records of discussions that took place or decisions that were made during its meetings, we could not confirm whether the Risk Management Committee monitored FSA's ERM efforts. Even if the Risk Management Committee were monitoring FSA's ERM efforts (and just did not retain records), it would not have been able to assess whether ERM was bringing enterprise-level risks within managements' risk appetite or achieving ERM objectives because FSA management has never defined its risk appetite and has not defined its ERM objectives since it developed the "Enterprise Risk Management Strategic Plan" in 2008.

FSA monitored performance metrics associated with strategic goals and completed assessments of internal control in response to OMB Circular No. A-123. However, those activities were not designed to evaluate whether all elements of its ERM framework were present and functioning as intended. Rather, FSA used the performance metrics to evaluate progress toward achieving strategic goals. "Federal Student Aid Strategic Plan Fiscal Years 2015–2019" listed five strategic goals. Only one mentioned risk: Strategic Goal B, "Proactively manage the student aid portfolio to mitigate risk." According to the strategic plan for 2015 through 2019, FSA planned to use two metrics to measure progress in mitigating student aid portfolio risk. The first metric focused on progress in reducing the improper payment rate on programs identified as susceptible to the risk of improper payments. The second metric focused on progress in reducing the percentage of borrowers more than 90 days delinquent on their loans. FSA did not specifically design either metric to be used in evaluating the effectiveness of ERM.

FSA annually completed assessments of internal control in response to OMB Circular No. A-123. Several operational and programmatic controls (such as assessments of contractor performance, business process control design and operating effectiveness, and information technology control design and operating effectiveness) were evaluated during those assessments. However, those assessments primarily focused on internal control over financial reporting. Assessments that primarily focus on internal control over financial reporting are not sufficient to evaluate the effectiveness of an organization's ERM efforts, because ERM impacts more than an organization's financial reporting.

ERM should include a monitoring element. An organization, guided by its risk appetite, should identify and assess a range of risk responses to address the enterprise-level risks it has identified and decide which risk options to implement.[35] Because an organization can experience new risks, changing risks, or risks that disappear, it should periodically evaluate whether the risk management framework and policy are still appropriate and report on how well the risk management policy is being followed.[36] In addition, the organization should evaluate the performance of its ERM to determine whether the implemented options achieved the stated objectives.[37] Based on the results of these evaluations, management should make decisions about how the risk management framework and policy can be improved.[38] All aspects of the risk management process should be reviewed at least once a year.[39] Monitoring of ERM can be conducted through ongoing activities or separate evaluations and can include evaluating the entirety of ERM or just individual elements of ERM. Elements of ERM are present and functioning properly when there are no material weaknesses and the managed risks have been brought within the organization's risk appetite.[40]

Without defining management's risk appetite and ERM objectives, FSA management cannot design an effective process for monitoring ERM. Also, FSA management will not be able to measure or report on the results of ERM, evaluate whether FSA's ERM framework and risk management policies are still appropriate, or evaluate whether ERM policies are being followed. Finally, FSA management will not have reasonable assurance that the policies, procedures, and activities associated with its ERM are effective in addressing risks and helping FSA achieve its ERM objectives.

Challenges FSA Faced in Implementing ERM

FSA faced challenges that negatively affected its ability to implement ERM. Possibly the biggest challenge has been consistent turnover in the Chief Risk Officer position. From October 2010 until August 2017, the Risk Management office had five different chief risk

[35] OMB Circular No. A-123, pages 10–11.

[36] "Risk Management – Principles and Guidelines," sections 3(j) and 4.5.

[37] OMB Circular No. A-123, pages 10–11.

[38] "Risk Management – Principles and Guidelines," sections 3(j), 4.5, and 4.6.

[39] OMB Circular No. A-123, pages 19–20.

[40] "Enterprise Risk Management – Integrated Framework," pages 22, 24, 75, and 77.

officers responsible for FSA's ERM efforts; two of the five were only acting in that capacity while continuing with their regularly assigned duties.

Another challenge: Since 2010, FSA management has not clearly communicated the details of its ERM framework. Instead, FSA primarily has used a diagram of the ERM framework and bullet points for each element. The diagram does not provide detailed descriptions of each element or explain how FSA plans to implement each of the elements. The diagram is not sufficient to help management, employees, and appropriate external stakeholders better understand their ERM roles and responsibilities.

Impact of Not Fully Implementing ERM

Though it started pursuing ERM in 2004, as of August 2017, FSA still had not implemented all elements characteristic of effective ERM. FSA management had not

- defined and retained records of its risk management philosophy, risk appetite, and risk tolerance;
- communicated its risk management philosophy, risk appetite, and risk tolerance to internal and appropriate external stakeholders;
- fully described FSA's ERM and communicated information about FSA's ERM framework and enterprise-level risks to internal and appropriate external stakeholders;
- ensured that FSA's objectives and risk responses were aligned with management's risk appetite;
- identified and assessed risks in a way that ensured a complete view of all enterprise-level risks; and
- annually evaluated ERM efforts to assess whether FSA was achieving management's ERM objectives or reducing risks to be within the level management was willing to accept.

Until it implements ERM in a way that incorporates all elements characteristic of effective ERM, FSA management will not have reasonable assurance that all enterprise-level risks have been identified, the combined impact of enterprise-level risks on the organization are fully understood, or managers, employees, and appropriate external stakeholders have the information necessary to effectively carry out their risk management responsibilities. In addition, FSA management will not have reasonable assurance that enterprise-level risks are being proactively managed to be within the level management is willing to accept.

If FSA does not openly communicate with appropriate external stakeholders about FSA management's risk appetite and risk tolerance and consider how they align with its external stakeholders, FSA management could unintentionally accept too much risk through those external stakeholders. Also, FSA cannot create a comprehensive risk profile without everyone having a strong understanding of management's risk appetite and risk tolerance. In addition, until FSA's employees and appropriate external stakeholders understand FSA's ERM approach and their involvement in FSA's ERM efforts, FSA management cannot successfully implement and sustain ERM.

Recommendations

We recommend that the Chief Operating Officer for FSA—

1.1 Define and retain records of management's risk management philosophy, risk appetite, and risk tolerance.

1.2 Retain records fully describing FSA's ERM framework.

1.3 Communicate management's risk management philosophy, risk appetite, and risk tolerance; FSA's ERM framework; and information about FSA's enterprise-level risks to internal and appropriate external stakeholders.

1.4 Align FSA's strategic objectives and risk responses with the risk appetite that management defines.

1.5 Ensure that the process for developing a risk profile considers all potential enterprise-level risks, including those identified through risk assessments of all business units and high-risk projects.

1.6 Evaluate, at least annually, whether FSA's ERM efforts have achieved management's ERM objectives and reduced enterprise-level risks to be within the level management is willing to accept. Identify and implement changes, if any, suggested by the evaluations.

FSA Comments and OIG Response

FSA disagreed with the finding and all six of the recommendations (see FSA Comments section of this report). However, it did not provide any additional documents or records to support its position. Therefore, we did not make any changes to the finding or any of the six recommendations. The following sections summarize FSA's comments on the finding and each of the six recommendations and our responses to FSA's comments.

FSA Comments on Finding

FSA stated that the OIG unilaterally defined required criteria where none exists and reported its assumptions about missing elements in FSA's ERM when those cited

elements are not required. FSA stated that, although COSO's 2004 ERM framework, ISO 31000, and OMB guidance provide a framework for an effective ERM program, those frameworks are not requirements and are specifically not prescriptive to allow an organization's management flexibility to create an ERM program appropriate to the organization.

OIG Response

The purpose of our audit was to determine the extent to which FSA had implemented its ERM framework as of August 2017. FSA's argument against this finding is that the elements that the OIG identified as missing from FSA's ERM are not required. This report does not assert that these specific eight elements of ERM are required. Rather, we state that the eight elements described in this report are characteristic of effective ERM. According to COSO, to be considered an effective ERM program, all eight elements we describe in this report need to be implemented. After considering the guidance (COSO, ISO, and OMB) FSA used to develop its ERM program, interviews with FSA employees, and the documents and records that FSA provided as evidence of its implementation of ERM, we concluded that FSA did not fully implement five elements—internal environment, information and communication, objective setting, event identification, and monitoring.

FSA Comments on Recommendation 1.1

FSA disagreed with this recommendation. FSA stated that neither OMB Circular No. A-123 nor any of the other frameworks the OIG cited require a formal risk management philosophy. FSA stated that a formal risk appetite is not required, and that, rather than "tolerating risk," emerging practices within the ERM industry point out that risk tolerance relates to organizations managing risks within acceptable variations of performance that the organization has defined. Although not required, FSA recognizes that a formal risk appetite statement helps decision-makers at multiple levels of the organization. FSA plans to develop a formal risk appetite statement in the summer of 2018. FSA also agrees that the wider distribution and understanding of key risk concepts is important and has developed an ERM program communication plan that extends to a broad range of stakeholders, including all FSA employees.

OIG Response

We recognize the fact that organizations are not required to have a formal risk management philosophy or formal risk appetite and that risk tolerance is the acceptable variation of performance in achieving objectives. Nevertheless, as part of any ERM program employees and external stakeholders of an organization should have an understanding of an organization's risk management philosophy, risk appetite, and risk tolerance. Without such understanding, management cannot effectively identify

and manage enterprise-level risks. FSA stated that it developed an ERM program communication plan; however, FSA did not provide that communication plan to us. In addition, FSA did not indicate whether that communication plan would include communicating FSA's risk management philosophy, risk appetite, or risk tolerance to various stakeholders.

FSA Comments on Recommendation 1.2

FSA disagreed with this recommendation, stating that it already retains records fully describing FSA's ERM framework and program. FSA stated that it provided a variety of documents to the OIG to support its ERM program and continues to retain records fully describing its ERM program. Although it disagrees with the recommendation, FSA is enhancing its ERM program and has created or updated a glossary of risk terms, risk categories, its process to assess risk, a risk register user guide, and a risk register template. In addition, FSA is developing an operationalization guide that will coordinate many of the trainings, tools, and templates into a single document that fully describes the execution of the ERM program and is developing a formal communication plan.

OIG Response

During our audit, FSA provided us with various records relevant to its ERM. However, those records did not fully describe FSA's ERM framework or demonstrate that FSA retained records showing full implementation of its ERM program. Although FSA indicated that it was developing an operationalization guide and formal communication plan for its ERM program, it did not provide us with additional documentation.

FSA Comments on Recommendation 1.3

FSA disagreed with this recommendation, stating that it already has provided various communications within the organization related to its ERM program and has conducted internal training. FSA stated that it holds kickoff meetings with business unit employees when it conducts a business unit risk assessment. The kickoff meetings provide employees with an overview of ERM concepts and methodologies. Despite the communication that has taken place, FSA agrees that it could improve the communication and is developing a comprehensive ERM program communication plan.

OIG Response

Our reason for making this recommendation was that FSA's information and communication relevant to ERM at the time of our audit needed improvement. Although FSA disagreed with the recommendation, FSA agreed that it could improve its ERM communication.

FSA Comments on Recommendation 1.4

FSA disagreed with this recommendation, stating that it continually evaluates risk appetite as part of its ongoing discussions surrounding strategic objectives and risk responses. FSA stated that risk appetite is often considered through risk discussions, and the discussions around risk responses necessarily include an indication of the amount of risk FSA was willing to accept in pursuit of achieving its strategic goals and objectives. Regardless, FSA is including risk in the development of its 2019–2024 strategic plan, with the goal of the ERM program being to integrate risk with strategy and performance.

OIG Response

FSA has not provided any evidence that it considered risk appetite during its risk discussions or that its discussions about risk response included an indication of the amount of risk FSA is willing to accept in pursuit of strategic goals and objectives. As of August 2017, FSA's Risk Management Committee was not retaining any records about the discussions that took place or decisions that were made during its meetings. FSA did not provide any such records in response to the draft of this report.

FSA stated that it seeks to integrate risk with strategy. Integrating enterprise-level risks identified through FSA's ERM efforts into the development of a strategic plan would partially address this recommendation. However, FSA still would need to maintain evidence that it defines its risk appetite and aligns the objectives in its strategic plan and its risk responses with that risk appetite.

FSA Comments on Recommendation 1.5

FSA disagreed with this recommendation, stating that its approach for identifying and assessing enterprise-level risk is a "top-down" approach that is an accepted approach within the ERM community. Managers often have insight into the most significant risks their organization faces and it is incorrect to assume that this approach could not uncover the most significant risks to the organization. FSA's projects with the highest risks were represented on FSA's risk profile. However, FSA acknowledges that a "bottom-up" approach is better at providing insight into risks throughout the organization, and FSA will use that approach moving forward.

OIG Response

We understand the benefits of having management involved in identifying and assessing enterprise-level risks. However, to ensure that FSA has vetted all potential enterprise-level risks, FSA should not ignore business unit risk assessments and other risk assessments conducted within the organization. Ignoring such "bottom-up" approaches to risk assessment could keep valuable information from management.

FSA Comments on Recommendation 1.6

FSA disagreed with the recommendation, stating that monitoring the effectiveness of the ERM program and its corresponding objectives is different than reducing risk to acceptable levels. FSA disagreed that ERM efforts will reduce enterprise-level risks to be within the level management is willing to accept. Bringing risks within an organization's risk appetite will not always occur for many reasons. FSA does agree that it should annually review the effectiveness of its ERM program and acknowledges that it historically has not done so. FSA assessed the ERM program in 2010, and the Enterprise Risk Management Office is currently assessing FSA's ERM program.

OIG Response

Contrary to FSA's statement, we did not confuse the purpose of monitoring ERM efforts. The goal of the recommendation is two-fold. One, annual evaluations can determine whether ERM efforts have achieved management's ERM objectives. Two, the evaluations can determine whether ERM efforts have reduced enterprise-level risks to be within the level management is willing to accept and, if not, FSA can decide what modifications to ERM are necessary.

We included in the recommendation to identify and implement changes, if any, suggested by the evaluations because we agree that ERM will not always result in reducing risk to an acceptable level. However, without periodic monitoring, FSA management cannot determine whether its ERM efforts are reducing risks to an acceptable level and cannot determine whether changes to its efforts might be necessary.

Appendix A. Scope and Methodology

We evaluated the extent of FSA's implementation of its ERM framework as of August 2017. We gained an understanding of how FSA implemented ERM through discussions with 33 FSA managers and 8 Risk Management employees (who were not managers) and a review of the following documents and records that they provided us:

- Organization charts and list of key personnel.
- Performance plans for Operating Committee members.
- Position descriptions and other information describing the responsibilities of Risk Management employees.
- FSA's strategic plans for fiscal years 2006 through 2010, 2011 through 2015, 2012 through 2016, and 2015 through 2019.
- FSA's initial (2006) and revised (2010) ERM frameworks.
- Risk categories, risk ratings, and heat maps.[41]
- FSA's processes for assessing business unit risks, conducting targeted risk assessments, and completing a risk profile.
- Examples of reports on an assessment of the risks associated with a specific business unit, a targeted risk assessment, and a completed risk profile.
- Overviews of the Risk Management Committee, the Risk Management Committee charter, and agendas of the Risk Management Committee meetings.
- A list of the risk management activities completed from 2006 through March 2017.
- Reports on risk assessments completed by three of FSA's offices (Program Compliance, Finance, and Technology).

[41] Heat maps are tools that help calculate risk scores based on the significance and likelihood of the risks.

We also reviewed the following information relevant to risk management and ERM:

- "Enterprise Risk Management – Integrated Framework," issued by COSO in September 2004 and updated as "Enterprise Risk Management—Aligning Risk with Strategy and Performance" in June 2016.
- "Risk Management – Principles and Guidelines," issued as standard 31000 by ISO in November 2009.
- "Preparation, Submission, and Execution of the Budget," issued by OMB through Circular No. A-11 in July 2016 and updated in July 2017.
- "Management's Responsibility for Enterprise Risk Management and Internal Control," issued by OMB through Circular No. A-123 in July 2016.
- "Policies for Federal Credit Programs and Non-Tax Receivables," issued by OMB through Circular No. A-129 in January 2013.
- "Standards for Internal Control in the Federal Government," issued by GAO in November 1999 and updated in September 2014.
- The Federal Managers' Financial Integrity Act of 1982 (Public Law 97-255).
- The Government Performance and Results Act of 1993 (Public Law 103-62).
- The GPRA Modernization Act of 2010 (Public Law 111-352).
- "Review of Federal Student Aid's Enterprise Risk Management Program" (control number I13I0005), issued by the OIG in May 2009.
- "Enterprise Risk Management—Selected Agencies' Experiences Illustrate Good Practices in Managing Risk" (GAO-17-63), issued by GAO in December 2016.

Internal Control

We did not assess the effectiveness of FSA's internal control over ERM because such an assessment was not significant within the context of our audit objective (determine the extent to which FSA had implemented its ERM framework).

Sampling Methodology

To gain an understanding of FSA's ERM efforts and evaluate the extent to which FSA had implemented ERM, we obtained testimonial evidence from a judgmentally selected sample of 41 employees. We judgmentally selected our sample from a population of 1,369 employees who worked in 10 FSA offices (as of September 2016). Because ERM affects the entire organization, we ensured our sample included representation from each of FSA's 10 offices. We selected 33 (of 50) managers who were assigned primary responsibility for managing risks relevant to their respective offices or business units

and we selected 8 (of 16) nonmanagers from Risk Management because Risk Management had responsibility for development and implementation of FSA's risk management strategy.

We used the information gathered from each interview to understand qualitative aspects, such as the ERM role of each employee, the level of understanding of FSA's ERM framework that each employee demonstrated, and the different ERM activities each employee conducted. We did not make any projections using the sample results.

Analysis Techniques

To evaluate whether FSA implemented its ERM framework and developed and implemented an ERM framework that included elements characteristic of effective ERM, we compared the elements included in FSA's ERM framework and descriptions of FSA's efforts to implement them to elements and indicators of efforts characteristic of effective ERM described by COSO, ISO, and OMB. Through interviews and reviews of available documents and records, we looked for evidence indicative of eight elements characteristic of effective ERM: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring. We looked for evidence of the following.

- Managers required to complete annual ethics training, risk management competence included as part of managers' performance plans, ERM clearly defined, and employees operating within their roles (internal environment).
- All strategic objectives included corresponding performance measures, ERM woven into strategic planning, and ERM considered a formal part of objective setting (objective setting).
- Viable opportunities evaluated at Risk Management Committee meetings, operational and programmatic processes clearly defined, operational and programmatic process-specific risks identified, and front-line risk owners understood how their mitigation activities related to ERM (event identification).
- Operational risk priorities reported to the Risk Management Committee, risk tolerance defined for each aspect of risk, actual risk compared against assessed risk, and standardized evaluation criteria consistently used to prioritize risk across the organization (risk assessment).
- Risks and opportunities within managers' areas of authority consistently managed, risk issues communicated and acted upon, and the effect of risk mitigation measured against risk tolerance (risk response).

- Sequential and repeatable steps for risk identification, assessment, mitigation, and monitoring used to improve decision-making and performance (control activities).
- Operational risk priorities reported to the Risk Management Committee; ERM issues clearly understood; risk ownership clearly defined; information needed for effective ERM required to be dynamic, available, and shared across departments; and periodic reports measuring ERM progress and activities provided to the Risk Management Committee and other stakeholders (information and communication).
- Management regularly reviewed enterprise-level risks and results of managing enterprise-level risk measured and reported. Measuring the results of managing enterprise-level risks, reviewing enterprise-level risks, and reporting on the results of managing enterprise-level risks helps management evaluate the effectiveness of its ERM efforts (monitoring).

Compliance with Auditing Standards

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our finding and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objective.

We conducted our audit at FSA's offices in Washington, DC, and our offices. We started our audit on October 25, 2016, and we discussed the results of our audit with FSA officials on December 14, 2017.

Appendix B. FSA's Organizational Structure

Figure 3. FSA's Organizational Structure as of September 28, 2016[42]

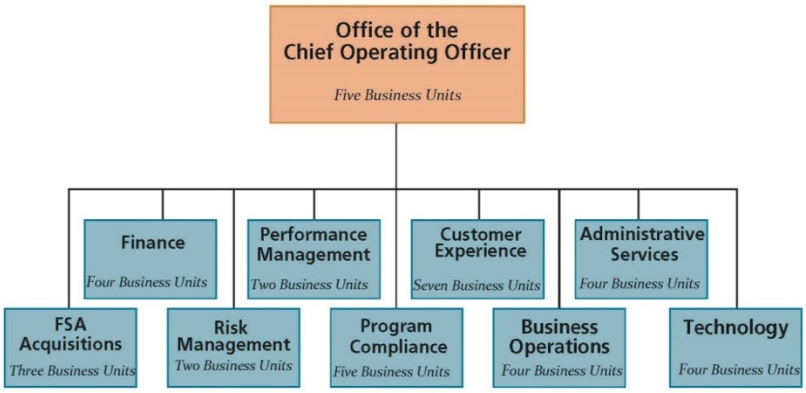
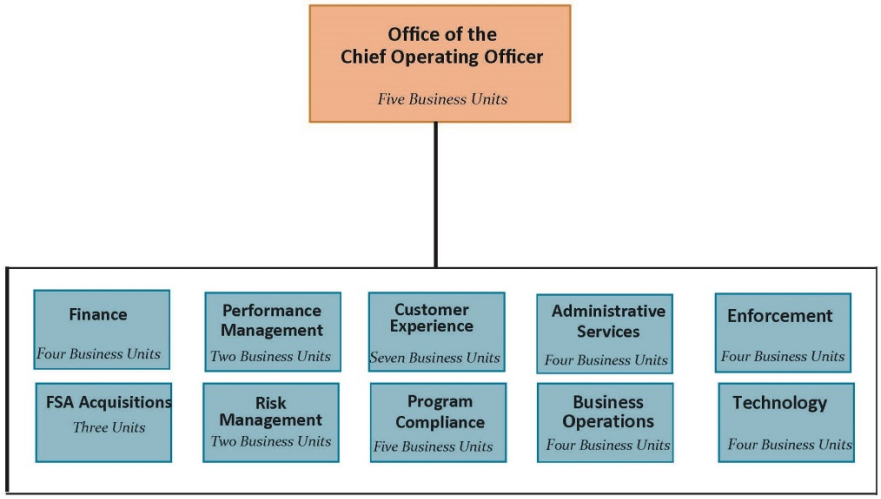


Figure 4. FSA's Organizational Structure as of July 17, 2017



[42] As of September 28, 2016, the Chief Enforcement Officer worked within the office of the Chief Operating Officer. Effective July 17, 2017, FSA revised its structure, creating the Enforcement office.

Appendix C. Risk Management Frameworks

All eight elements characteristic of effective ERM described in this report are reflected in all three frameworks (COSO ERM framework, ISO 31000 risk management framework, and OMB ERM guidance) that had an impact on FSA's implementation of ERM.

Table 2. Comparison of Elements of Three Frameworks

Element	COSO	ISO 31000	OMB
Internal Environment	Internal Environment	Establish the Context	Establish the Context
Objective Setting	Objective Setting	Reflected in Framework But Not a Specific Element[43]	Reflected in Framework But Not a Specific Element[44]
Event Identification	Event Identification	Risk Assessment	Identify Initial Risks
Risk Assessment	Risk Assessment	Risk Assessment	Analyze and Evaluate Risks
Risk Response	Risk Response	Risk Treatment	Develop Alternatives
Control Activities	Control Activities	Risk Treatment	Respond to Risks

[43] ISO 31000 states that risk management occurs within the context of the organization's objectives, and management should align risk management objectives with the objectives and strategies of the organization.

[44] OMB states that identifying objectives is part of developing a risk profile. Also, risk must be analyzed in relation to the achievement of strategic objectives established in the organization's strategic plan and appropriate operational objectives.

Element	COSO	ISO 31000	OMB
Information and Communication	Information and Communication	Communication and Consultation	Reflected in Framework But Not a Specific Element[45]
Monitoring	Monitoring	Monitoring and Review	Monitor and Review; Ongoing Risk Identification

COSO Integrated Framework

COSO issued "Enterprise Risk Management – Integrated Framework" in September 2004 to provide principles-based guidance to help entities design and implement effective enterprise-wide approaches to risk management. According to COSO, a well-designed and implemented approach to ERM is intended to help an organization manage its risks to be within a range that management is willing to accept in pursuit of achieving organizational objectives. "Enterprise Risk Management – Integrated Framework" defined ERM components, discussed key ERM principles and concepts, suggested a common ERM language, and provided direction and guidance for ERM. This framework consisted of the following eight, interrelated components.[46]

- Internal Environment: The tone of an organization. Sets the basis for how risk is viewed and addressed by an organization's people. Includes risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
- Objective Setting: What the organization wants to accomplish. The established objectives should support and align with the organization's mission and should be consistent with the organization's risk appetite.

[45] The diagram for this framework indicates that "Communicate and Learn" is central to the overall framework.

[46] COSO used the term "components," ISO used the term "steps," and OMB used the term "elements." In this report, we used "elements."

- Event Identification: Identification of internal and external events affecting achievement of an organization's objectives. Makes a distinction between risks (negative impact) and opportunities (positive impact).
- Risk Assessment: An analysis of the identified risks to determine how risks should be managed. Should consider the likelihood and impact of the identified risks.
- Risk Response: The selection of appropriate risk responses—avoiding, accepting, reducing, or sharing risk—and the development of a set of actions to align risks with the organization's risk tolerances and risk appetite.
- Control Activities: The policies and procedures of an organization created to help ensure risk responses are effectively carried out.
- Information and Communication: The identification, capture, and communication of relevant information. Should be in a form and timeframe that enable people to carry out their responsibilities.
- Monitoring: The monitoring and modifying of the entirety of ERM, as necessary. May be completed through ongoing management activities, separate evaluations, or both.

ISO 31000

ISO published ISO 31000, "Risk Management — Principles and Guidelines," in November 2009 to be used by a wide range of organizations, both public and private. According to ISO 31000, risk management is not a stand-alone, separate activity. Instead, it should be integrated into all of an organization's practices and processes. ISO 31000 described the following five steps as necessary for effectively implementing a risk management process.

- Establish Context: Set the goals, objectives, and scope for risk management, and understand the internal and external environments in which the organization seeks to achieve its objectives.
- Risk Assessment: Identify, analyze, and evaluate risks.
- Risk Treatment: Select and implement one or more options for addressing risks.
- Communication and Consultation: Communicate and consult with both internal and external stakeholders (takes place throughout the risk management process).
- Monitoring and Review: Assure that controls are effective and risks are appropriately addressed.

OMB Circular No. A-123

OMB published a revised Circular No. A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control," in July 2016. The revised circular required Federal agencies to implement an ERM capability. According to OMB, ERM is an organization-wide approach to addressing the full spectrum of internal and external risks by understanding the combined impact of such risks as an interrelated set, rather than addressing risks only within silos.[47] It should be forward-looking and designed to help managers make better decisions, alleviate threats, and identify unknown opportunities to improve the efficiency and effectiveness of government operations. An organization may take many approaches to implement ERM but most approaches include the following seven elements.

- Establish Context: Understand and articulate the internal and external environments of the organization.
- Identify Initial Risks: Use a structured and systematic approach to recognize whether the potential for undesired outcomes or opportunities can arise.
- Analyze and Evaluate Risks: Consider the causes and sources of risks, the probability of the risks occurring, the potential positive or negative outcomes, and then prioritize the results of the analysis.
- Develop Alternatives: Systematically identify and assess a range of risk response options as guided by risk appetite.
- Respond to Risks: Make decisions about the best options among a number of alternatives and then prepare and execute the selected response strategy.
- Monitor and Review: Evaluate and monitor performance to determine whether the implemented risk management options achieved the stated goals and objectives.
- Ongoing Risk Identification: Identify risks throughout the year, including leading indicators of future risks from internal and external environments.

[47] OMB Circular No. A-123 references the COSO ERM framework as including the concepts of risk appetite, risk tolerance, and an organizational view of risk.

Appendix D. Laws and Other Requirements Affecting ERM in the Federal Government

Federal Managers' Financial Integrity Act of 1982

The Federal Managers' Financial Integrity Act of 1982 requires the Comptroller General to issue standards for internal control in the Federal government. The law also requires agencies to establish internal accounting and administrative controls in accordance with the standards prescribed by the Comptroller General. In addition, the law requires agencies to provide an annual report on whether their accounting systems conform to the Comptroller General's standards. This law is relevant to ERM because it provides the statutory basis for management's responsibility for and assessment of internal control.

GPRA Modernization Act of 2010

The GPRA Modernization Act of 2010 retained and amplified some aspects of the Government Performance and Results Act of 1993. The 1993 law required strategic plans that covered a period of at least 5 years. The 2010 law changed this requirement, requiring strategic plans that covered a period of at least 4 years. The required strategic plans should include mission statements, general goals and objectives for the organization's major functions and operations, and a description of how the organization will achieve the goals and objectives. These two laws serve as a foundation for engaging leaders in performance improvement and creating a culture where data and other evidence plays a greater role in policy, budget, and management decisions.

Standards for Internal Control in the Federal Government

In accordance with the Federal Managers' Financial Integrity Act of 1982, GAO issued "Standards for Internal Control in the Federal Government" in November 1999 (revised in September 2014). In 1999, GAO identified five standards: control environment, risk assessment, control activities, information and communications, and monitoring. These five standards represented the minimum level of quality acceptable for internal control in the Federal government. In September 2014, GAO expanded the 5 standards (now referred to as components) for internal control by establishing 17 principles describing the requirements for each component and providing attributes to explain each principle in greater detail. For an internal control system to be effective, the five components must be effectively designed, implemented, operating as management intended, and operating together in an integrated manner. An effective internal control system increases the likelihood that an organization will achieve its objectives.

Office of Management and Budget Circular No. A-11

OMB published a revised Circular No. A-11, "Preparation, Submission, and Execution of the Budget," in July 2016 (updated in July 2017). This circular describes ERM and the characteristics of effective ERM. It also describes how ERM is relevant to strategic reviews and the key roles of risk managers at an organization.

Office of Management and Budget Circular No. A-123

OMB published a revised Circular No. A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control," in July 2016. The revised circular defines management's responsibility for ERM and internal control and requires Federal agencies to implement an ERM capability. See Appendix C for more details.

Office of Management and Budget Circular No. A-129

OMB published Circular No. A-129, "Policies for Federal Credit Programs and Non-Tax Receivables," in January 2013. This circular prescribes policies and procedures for managing Federal credit programs and collecting non-tax receivables. It also provides guidance on integrating risk management into the management and oversight of Federal credit programs. Finally, this circular describes the characteristics of risk management functions.

Appendix E. Acronyms and Abbreviations

COSO	The Committee of Sponsoring Organizations of the Treadway Commission
Department	U.S. Department of Education
ERM	Enterprise Risk Management
FSA	Federal Student Aid
GAO	Government Accountability Office
HEA	Higher Education Act of 1965, as amended
ISO	International Organization for Standardization
OIG	Office of Inspector General
OMB	Office of Management and Budget

FSA Comments

May 1, 2018

TO: Bryon S. Gordon
Assistant Inspector General for Audit

FROM: James F. Manning /s/
Acting Chief Operating Officer
Federal Student Aid

SUBJECT Draft Audit Report, "Federal Student Aid: Efforts to Implement Enterprise Risk Management Have Not Included All Elements of Effective Risk Management," Control Number: ED-OIG/A0SQ0007

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) draft audit report "Federal Student Aid: Efforts to Implement Enterprise Risk Management Have Not Included All Elements of Effective Risk Management," dated March 23, 2018. The purpose of the audit was to determine the extent to which Federal Student Aid (FSA) had implemented its enterprise risk management (ERM) framework. We appreciate the work done by the OIG and have taken a number of steps to continue to improve our ERM program.

Enterprise Risk Management in Federal Student Aid

While the OIG draft audit is helpful for continuing to improve our ERM program, it does not present a complete picture of the effectiveness of the program, or its relative role in the Federal government's ERM systems among agencies. FSA's Enterprise Risk Management (ERM) program was the first enterprise-wide ERM implementation in the federal government that spanned all key business processes. FSA's decision in 2004 to hire a Chief Risk Officer and begin an ERM program exemplified the agency's commitment to proactively managing strategic and enterprise-level risks and collectively resolving high-risk issues. FSA's ERM was developed to reflect the risk challenges faced by FSA, and was among the pioneers in recognizing the importance and value of ERM. During the early implementation, it became clear that the implementation of an off-the-shelf model designed for the private sector would not properly identify FSA's unique risks. FSA needed to design and develop a risk mitigation strategy best suited to its business processes. FSA's ERM program has been a model for other Federal agencies and has progressed in its development for well over a decade. FSA pioneering efforts and continued good practice in ERM was recognized in the Government Accountability Office's October 2016 report, *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk* "as exemplifying best practices in ERM implementation."

Evolving into a modernized ERM approach in 2017, FSA's ERM program includes re-engineered and documented ERM system and a new tiered governance structure which includes executive level, cross business-unit level, and enterprise cyber risk components. The ERM implementation effort is supported

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION
830 First St. N.E., Washington, DC 20202

by a dedicated and formally recognized Risk Management Office led by a Chief Risk Officer, who reports directly to the Chief Operating Officer, and has continued its evolution. The draft audit does not give enough credit to this model ERM program, and it also does not recognize the challenges that such a pioneering effort overcame.

Audit Objective Concerns
We acknowledge that the OIG's original audit objective was to determine the extent to which FSA had implemented its enterprise risk management (ERM) framework. However, several instances within the Draft Audit Report show that the OIG revised its objective from its originally stated intent. Rather than addressing its original stated objective, the OIG stated that it assessed whether "FSA had fully implemented all elements of its ERM framework and whether FSA's implementation covered the eight elements-internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring-characteristic of effective ERM, as reflected in the Committee of Sponsoring Organizations of the Treadway Organization (COSO) ERM framework, International Organization for Standardization (ISO) risk management framework, and Office of Management and Budget (0MB) guidance." None of the elements in the revised OIG objective are specifically required.

FSA Response to Finding
Finding No. 1: FSA did not implement all elements characteristic of effective ERM.

FSA disagrees with this finding. The OIG appears to have unilaterally defined required criteria where none exists. Throughout the audit, OIG reports its assumptions about missing elements when in fact the elements cited as missing are not required. While COSO's 2004 framework, ISO 31000, and OMB guidance provide a framework on an effective ERM program, they are not requirements and specifically not prescriptive and allow flexibility for an organization's management to create an ERM program that is appropriate for the organization's size, scope, scale, and complexity. The OIG presented no evidence in the report that FSA's ERM program is not effective, and not appropriate for addressing FSA functions. Instead, OIG presented only elements it assumes should be in FSA's program. OIG stated that it did not assess the effectiveness of FSA's internal control over ERM because such an assessment was not significant within the context of the audit objective.

FSA Response to Recommendations
Recommendation 1.1: Define and retain records of management's risk management philosophy, risk appetite, and risk tolerance.

FSA disagrees with this recommendation. A formal risk management philosophy is not required by OMB Circular A-123, nor is it specifically required by any of the ERM frameworks cited by the OIG. Additionally, a formal risk appetite is not required. Risk appetite can be implied through the risk responses chosen from previous enterprise risk lists. Risk tolerance is a common risk term, which was also referenced throughout the audit report. Emerging practice within the ERM industry relating to risk tolerance points out that organizations do not "tolerate" risk, rather an organization identifies specific levels of performance it would like to achieve. That is, different risks are associated with different levels of performance, and we manage those risks within acceptable variations of performance. As part of its enhanced ERM program, FSA plans to develop a formal risk appetite statement in the summer of 2018. While FSA recognizes that a formal risk appetite statement clarifying the amount of risk FSA is willing to

accept helps decision-makers at multiple levels of the organization, it is not required.

FSA also agrees that wider distribution and understanding of key risk concepts is important. Further, FSA has developed an ERM program communication plan that extends to a broad range of stakeholders, including all FSA employees.

Recommendation 1.2: Retain records fully describing FSA's ERM framework.

FSA disagrees with this recommendation. FSA does not think that this recommendation is needed since FSA already retains records fully describing FSA's framework and program. FSA provided a variety of documentation to the OIG to support its ERM program, including but not limited to, methodologies, rating scales and definitions, training decks, risk templates, and various reports. FSA continues to retain records fully describing its ERM program.

In pursuit of an enhanced ERM program, the Enterprise Risk Management Office {ERMO) has created and/or updated training decks, tools and templates to include: a glossary of risk terms, the risk taxonomy, assessment methodology, risk register users guide and a risk register template. These are housed on a SharePoint site with access available to all FSA employees. An operationalization guide is also in progress, which coordinates many of the training, tools, and templates into a single document that fully describes the execution of the program in addition to a formal communication plan.

Recommendation 1.3: Communicate management's risk management philosophy, risk appetite, and risk tolerance; FSA's ERM framework; and information about FSA's enterprise-level risks to internal and appropriate external stakeholders.

FSA disagrees with this recommendation. FSA does agree that the organization could improve communication as it relates to its ERM program and a comprehensive ERM program communication plan is in development. That said, FSA conducted internal training which was available to all FSA regional and headquarters employees, as well as contractors. This internal training provided an overview of the ERMO, as well as FSA's ERM program. It also provided attendees with a look at how their business units aligned with the ERM program. The training materials remain available on the ERMO's website. Additionally, the Risk Analysis & Reporting Group within ERMO conducted a kickoff meeting with each business unit ahead of risk assessments. At the meeting an overview of the ERM program and information relating to ERM concepts and methodologies was provided.

Business unit-level risk information was provided to the appropriate executive who had responsibility and decision-making authority to share results with staff as they deemed appropriate. All personnel involved in the risk profile activities were afforded an opportunity to review and revise information. The final risk profile was provided to the Operating Committee, the Risk Management Committee and the Enterprise Risk Management Council at the Department, each having the authority to share the information, as appropriate.

Recommendation 1.4: Align FSA's strategic objectives and risk responses with the risk appetite that management defines.

FSA disagrees with this recommendation. Discussions around risk responses necessarily included an

indication of the amount of risk FSA was willing to accept in pursuit of achieving its strategic goals and objectives. While understanding specifically the levels of risk an organization is willing to accept is best, risk appetite is often contemplated through risk discussions. Risks on FSA's risk profile are aligned with FSA's strategic objectives as outlined in its most recent strategic plan. FSA continually evaluates risk appetite as part of its ongoing discussions surrounding strategic objectives and risk responses.

As an additional point, FSA is including risk in its development of its 2019- 2024 Strategic Plan. Risk should inform strategy as well as being informed by strategy. FSA's ERM program seeks to integrate risk and strategy with more clarity. In addition, FSA's ERM program will include the identification and monitoring of key performance activities generated in response to its risk profile. The goal of the ERM program is to integrate risk with strategy and performance; making risk an integral part of decision-making and not a one-off exercise.

Recommendation 1.5: Ensure that the process for developing a risk profile considers all potential enterprise-level risks, including those identified through risk assessments of all business units and high-risk projects.

FSA disagrees with this recommendation. A top-down approach for risk identification and assessment is an accepted approach within the ERM community for identifying enterprise level risks. Executives often have insight into the most significant risks their organization faces. While a bottom-up approach is better at propagating risk throughout the organization (and is the approach FSA will use moving forward), the assumption that the top-down approach could not uncover the most significant risks to the organization is incorrect. FSA's top-down approach had a line of sight into high risk/high profile projects. While some projects made it into the Risk Portfolio (formerly known as the Watch List), the projects with the highest risk were represented on the Risk Profile.

Recommendation 1.6: At least annually, evaluate whether FSA's ERM efforts have achieved management's ERM objectives and reduced enterprise-level risks to be within the level management is willing to accept. Identify and implement changes, if any, suggested by the evaluations.

FSA disagrees with this recommendation. FSA agrees with evaluating its ERM program annually. However, FSA disagrees with the goals of that evaluation as stated in the recommendation. While FSA acknowledges that it historically has not annually reviewed the effectiveness of its ERM program, it did assess the program in 2010, and significant changes were made to best meet the needs of the organization at that time. In addition, the ERMO is currently assessing its program internally and has pivoted its operationalization approach to better reflect the size, scope, scale and complexity of the organization. In the audit report, "monitoring" conflated "efforts to assess whether FSA was achieving its ERM objectives" with "reducing risks to be within the level management was willing to accept." Monitoring the effectiveness of the ERM program and its corresponding objectives is different than reducing risk to acceptable levels. For FSA, monitoring will be a set of monitoring activities: regularly considering business context and adjusting assessment scores; monitoring key activities and providing transparency on the influence of key activities on FSA's overall risk profile; developing and monitoring key risk indicators; analyzing trends across business units; and providing second line of defense challenges to business self-assessments. FSA is institutionalizing its annual evaluation methodology into its operationalization guide.

Additionally, as part of its governance structure, FSA has included the conduct of annual self-assessments by each governing body in their respective charters - The Enterprise Risk Executive Committee (made up of key executives within the organization), the ERMC (made up of key business unit personnel from all business units serving as risk champions), and the Enterprise Cyber Risk Committee (made up of cyber subject matter experts from across FSA and the Department) - to ascertain the effectiveness of their roles and responsibilities relating to FSA's ERM program.

Further, FSA disagrees with the statement that ERM efforts will "reduce[d] enterprise-level risks to be within the level management is willing to accept." As previously discussed, bringing risks within the organization's risk appetite will not always occur for many reasons, including the existence of a dynamic business environment and limited resources. ERM is about making deliberative choices and understanding the impact on the overall risk profile of FSA. ERM is also about improving transparency into risks the organization is taking in pursuit of its mission, considering risk in decision-making, being forward-looking and proactive in managing risk, and enhancing agility and resilience in the face of change and challenge.

FSA's Enhanced ERM Approach Going Forward

FSA's ERM program moving forward builds on the framework of the pioneering ERM program already in place but should also improve it significantly and it should be markedly different than the ERM program that the OIG audited.

FSA is in the process of enhancing its program, which leverages COSO's new 2017 framework, Enterprise Risk Management: Integrating with Strategy and Performance, as its starting framework and continues to mature its program to best meet the needs of the organization. FSA has established a new three level governance structure which includes an Enterprise Risk Executive Committee (consisting of business unit heads), Enterprise Risk Management Committee (comprised of key leaders within and across business units), and an Enterprise Cyber Risk Committee (consisting of cyber subject matter experts). The Office of the Chief Operating Officer sits at the top of the governance structure. This enhanced structure allows penetration across FSA to several layers of leadership, while leveraging the knowledge of business unit subject matter experts, and also better utilizing limited resources. It also fosters a more risk-aware culture and propagates risk conversations among multiple layers of decision-makers.

FSA's ERM program uses FSA's mission and strategic goals to define its risks, integrating risk with strategy and objective setting. The ERMO is working in tandem with the strategic planning team to ensure that risk is considered during the development of the new strategic plan. The enhanced ERM program emphasizes business context to ensure that the program is forward-looking. Working sessions, within the governance structure, include discussions of business context- both external and internal- to ensure that the program is dynamic and able to be responsive to the constantly-changing business environment. FSA is also working to incorporate risk into its investment decision modelling, which is also supportive of an overall view of risk in the strategic deployment of its financial resources.

FSA's operationalization approach includes the development of both business unit-level and enterprise-level objectives using the risk lens. For enterprise-level risks, executive sponsors will be assigned for enterprise risks in the Risk Profile. Key potential mitigating activities will be developed, and risks associated with each potential option will be considered. Once key mitigating activities have been determined, performance objectives will be created, defined and monitored. This approach will also be

rolled out to the business units for development at the business unit-level. The ERMO has developed and delivered training, tools, and templates that support this self-assessment methodology and has strengthened its role as a second line of defense. A regular cadence of reporting will continue to reinforce accountability for risk across FSA.

FSA's ERM program will help to generate greater value to the organization by increasing positive outcomes, while reducing negative surprises, identifying and managing enterprise-wide risks, reducing performance variability and improving the effectiveness of resource deployment. By integrating risk with strategy and performance, FSA is creating the connectivity needed to be able to see the influence of risk and performance in the achievement of its strategic objectives as it pursues its mission.

We appreciate the opportunity to discuss the draft findings and recommendations, and we hope that, with these comments, the OIG will further recognize the very positive contributions of FSA's pioneering ERM efforts, and see the promise of the advancements that FSA is planning to take. Please let us know if you have questions or need further information.