COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

This instruction implements Department of the Air Force Policy Directive (DAFPD) 65-2, *Risk Management and Internal Control Program*. It provides a structure to identify, monitor, and report on the Department of the Air Force (DAF) risks, issues, and controls in all functional areas including Special Access Programs based on recognized leading practices and in compliance with the *Federal Managers' Financial Integrity Act of 1982* (FMFIA), the Government Performance Results Act (GPRA) Modernization Act of 2010, Office of Management and Budget (OMB) Circular Number (No.) A-123 *Management's Responsibility for Enterprise Risk Management and Internal Control* and Department of Defense Instruction (DoDI) 5010.40 *Managers' Internal Control Program Procedures* requirements. This instruction applies to all civilian employees and uniformed members of the Regular Air Force, United States Space Force, Air Force Reserve, Air National Guard, Civil Air Patrol when conducting missions as the official Air Force Auxiliary, and those with a contractual obligation to abide by the terms of DAF issuances. This Department of the Air Force Instruction (DAFI) may be supplemented at any level, but all supplements that directly implement this instruction must be routed to Accounting and Financial Oversight (SAF/FMFA) for coordination prior to certification and approval. Recommended changes and questions about this publication should be sent through the appropriate channels using Department of the Air Force Form 847, *Recommendation for Change of Publications,* to the office of primary responsibility (OPR) for SAF/FM Risk Management and Internal Control (RMIC) Policy, SAF/FMFA. The authorities to waive wing, unit, or delta level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the requestor's commander for non-tiered compliance items. Waivers

will not be granted if the waiver would cause the DAF to fail to comply with OMB Circular No. A-123. Ensure all records created because of processes prescribed in this publication are maintained in accordance with Air Force Instruction 33-322, *Records Management and Information Governance Program*, and disposed of in accordance with the Air Force Records Disposition Schedule located in the Air Force Records Management System. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the **DAF.SAF.FM.A.123.Internal.Controls@us.af.mil**. This publication was produced in accordance with Department of the Air Force Manual (DAFMAN) 90-161, *Publishing Processes and Procedures*. Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System.

SUMMARY OF CHANGES

This document has been substantially revised and should be completely reviewed. Changes to address updates to OMB guidance and Department of Defense (DoD) policy include adding Enterprise Risk Management (ERM) requirements within a new chapter and throughout the instruction, including the roles and responsibilities of the Chief Risk Officer (CRO); providing guidance for internal control over operations activities; and adding a governance paragraph in **Chapter 1** identifying OMB Circular No. A-123 governing bodies and prescribing guidance and responsibilities.

Chapter 1

OVERVIEW AND RESPONSIBILITIES

1.1. Overview. The RMIC program enables the DAF to effectively identify, monitor, and report on risks and issues the DAF faces to achieving its strategic, operations, reporting, financial systems, and compliance objectives. These objectives are aligned to its mission to organize, train, and equip Airmen and Guardians, as well as the internal controls in place to mitigate identified risks. The DAF leverages its governance construct to execute the governance requirements for the Risk Management Council (RMC), Senior Management Council (SMC), and Senior Assessment Team (SAT) as defined in OMB Circular No. A-123 and DAFPD 65-2. To facilitate the field's access to more detailed internal control and risk management guidelines, SAF/FMFA has placed the A-123 RMIC Playbook on the FIAR Communication page. The A-123 RMIC Playbook builds upon previous activities, progress, and accomplishments, and defines current internal control initiatives. For questions concerning the Playbook, reach out to SAF/FMFA.

1.2. Roles and Responsibilities. The RMIC Program roles are inherently governmental; only civilian employees and/or military members of the DAF, to include direct-hire foreign national employees, are authorized to serve in its various roles. Contractors or indirect-hire foreign national employees are not authorized to serve in the RMIC Program roles. Key roles and responsibilities for internal control and risk management include:

1.2.1. The Assistant Secretary of The Air Force (Financial Management and Comptroller) (SAF/FM):

1.2.1.1. Oversees and administers the DAF's internal control monitoring program for Internal Controls over Financial Reporting, Internal Controls over Financial Systems.

1.2.1.2. Directs the associated compliance objectives and governance to satisfy the responsibilities of the SAT.

1.2.1.3. Chairs the Executive Steering Committee (ESC), which satisfies the requirements of the Senior Assessment Team (SAT).

1.2.2. The Deputy Under Secretary of the Air Force, Management (SAF/MG):

1.2.2.1. Oversees and administers the DAF's ERM program and governance to satisfy the responsibilities of the RMC as the DAF's CRO.

1.2.2.1.1. Chairs the RMC; meeting will be held at least once per year or as directed by the Chairs.

1.2.2.1.2. Leads risk management efforts within the Department, advising senior leaders on the strategically aligned risk portfolio, and serving as the strategic advisor to the staff on the integration of risk management practices into day-to-day business operations and decision-making.

1.2.2.1.3. Oversees the annual review of the DAF risk profile; aggregates and manages the collection of all risks from across the DAF, including financial risks identified by SAF/FM as part of the Executive Steering Committee (ESC).

1.2.2.1.4. Reviews the outputs (ex: Air Force Strategy, Air Force Strategic Environment Assessment) of the Strategy portion of Strategy, Programming,

Budgeting, and Execution (SPPBE) in alignment with the DAF core missions to identify if updates are needed to the enterprise risks and enterprise risk statements in the enterprise Risk Profile.

1.2.2.1.5. Staffs the enterprise Risk Profile to the appropriate DAF headquarters organizations for concurrence. These organizations play an integral part in the United States Air Force's (USAF's) SPPBE process and the United States Space Force's (USSF's) Program Objective Memorandum process by overseeing specific phases and consolidating inputs from stakeholders across the DAF.

1.2.2.2. Oversees and administers the DAF's internal control monitoring program for Internal Controls over Operations and issues unrelated to financial reporting, financial systems, and associated compliance objectives and governance to satisfy the responsibilities of the SMC.

1.2.2.3. Oversees and administers the integration of the DAF's ERM and Internal Control Programs.

1.2.2.4. Manages a digital platform to record and maintain all Corrective Action Plans (CAPs) associated with Operational material weaknesses, Internal Controls, and risk.

1.2.2.4.1. The digital platform (e.g., Service Now) will be used to integrate all related functions across the DAF.

1.2.2.4. 2. All OPRs, 2-letters and advisors will use this common platform to track and manage progress towards their actions related to Operational material weaknesses, Internal Controls and risk.

1.2.3. The Auditor General of the Air Force (SAF/AG):

1.2.3.1. Oversees the CAPs for operational material weaknesses.

1.2.3.2. Serves as the subject matter experts on audit guidance, direction, and planning.

1.2.3.3. Conducts the audits necessary to validate the CAPs and milestones.

1.2.3.4. Provides executive counsel to SAF/FM and SAF/MG on audit-related actions, resolution, and closure.

1.2.4. The Deputy Assistant Secretary for Financial Operation (SAF/FMF) represents the DAF as the RMIC program's Senior Accountable Official to the Undersecretary of Defense (Comptroller) (OUSD(C)). This role may be delegated as necessary by SAF/FMF.

1.2.5. The Financial Operations Directorate (SAF/FMFA):

1.2.5.1. Represents the DAF as the RMIC Program Manager.

1.2.5.2. Compiles the DAF's annual Statement of Assurance (SoA) and supplementary templates required to be reported by OUSD(C).

1.2.5.3. Performs annual entity level control (ELC) testing.

1.2.5.4. Provides subject matter expertise to the integration of the DAF's ERM and Internal Control Programs.

1.2.5.5. Trains RMIC Program stakeholders annually on the DAF'S RMIC program.

1.2.6. Certification Statement Officials:

1.2.6.1. Confirm internal control costs do not exceed the expected benefits.

1.2.6.2. Respond to requests for information from SAF/FM and SAF/MG needed to compile the DAF annual SoA.

1.2.6.3. Actively identifies and escalates potential risks that could impede or impair the delivery of the strategic objectives specific to the organization.

1.2.7. Assessable Unit (AU) Leads:

1.2.7.1. Establish and integrate internal controls into operations in a risk-based and cost beneficial manner, to provide reasonable assurance that the DAF's internal control over operations, financial reporting, financial systems, and compliance are operating effectively.

1.2.7.2. Consider the appropriate balance between risk, controls, costs, and in their mission-support operations.

1.2.7.3. Document policies to outline proper segregation of duties and periodically review existing processes and procedures to confirm changes in internal and external environments do not increase risks related to segregation of duties.

1.2.7.4. Clearly describe personnel roles associated with a particular process to confirm measures are in place to separate responsibilities and establish appropriate oversight.

Chapter 2

ENTERPRISE RISK MANAGEMENT (ERM)

2.1. Overview. OMB Circular No. A-123 defines management's responsibilities for ERM and includes requirements for identifying and managing risks from a portfolio perspective, to be sourced from across the enterprise and include prioritized risks. Key requirements include the development of an enterprise Risk Profile in line with the annual strategic review process and the development of an implementation plan inclusive of integration with existing internal control programs. Together, these requirements help enable agencies to consider the full spectrum of risks to better inform decision making and enable the delivery of strategic objectives. The RMIC program provides the DAF with a proactive, top-down, and risk-based approach to reduce external audit findings, flag risks as they emerge, and manage a prioritized portfolio of risks on an on-going basis.

2.2. Risk Management Practices. Risk management practices proactively identify existing and potential risks, with an emphasis on financial reporting, financial systems, and operational business processes. ERM practices are designed to assist DAF leadership with making better decisions to manage both existing and emerging risks, as well as identify opportunities to improve the efficiency and effectiveness of operations.

2.2.1. Enterprise risks may be identified as:

2.2.1.1. Risks that are applicable across USAF, USSF and/or the DAF (e.g., enterprise-wide).

2.2.1.2. Risks that are contributing to operational, reporting or compliance material weaknesses and/or significant deficiencies in the DAF.

2.2.1.3. All risks will be considered based on risk assessments available and priority levels, with the identified DAF CRO ultimately being responsible for the DAF enterprise Risk Profile and SoA risk assessment inputs. Risks will also be considered based on their level of alignment to strategic objectives as well as the potential to adversely impact mission delivery.

2.2.1.4. Risks that are either internal or external to the SPPBE process and are deemed to have enterprise applicability. When identifying enterprise risks, management should consider the significance of the risk priority level, alignment to the DAF core missions, and what actions should be taken.

2.2.2. Fraud risk is managed within the DAF in accordance with the *Fraud Reduction and Data Analytics Act of 2015,* OMB Circular No. A-123 and DoD 70000.14-R, Volume 4, Chapter 14.

2.2.3. SAF/FM, in coordination with the CRO, will develop and maintain a comprehensive Fraud Risk Register in accordance with OMB Circular No. A-123 to identify, prioritize, and assess fraud risks. **(T-0)**

2.3. Information Technology (IT) Risk Management Framework (RMF). Refer to Air Force Instruction (AFI) 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT),* AFI 17-130*, Cybersecurity Program Management* and DoDI 8510.01, *Risk*

Management Framework (RMF) for DoD Information Technology (IT). Additional guidance is provided via the DAF RMF Knowledge Service.

Chapter 3

INTERNAL CONTROL

3.1. Overview. OMB Circular No. A-123 defines management's responsibilities for establishing, operating, and assessing an effective system of internal control. Key requirements include establishing entity and process level control, assessing internal controls at the entity and process levels, correcting internal control deficiencies, and reporting on internal controls. **Figure 3.1** identifies the DAF governance body and designated chair(s) for monitoring and oversight of each type of internal control.

Figure 3.1. OMB Circular No. A-123 Governance.

OMB Circular No. A-123 Governance	RMIC Covered	Chair(s)
Senior Management Council (SMC)	Internal controls, issues, and associated residual risks not related to financial reporting, financial systems, and associated compliance objectives.	SAF/FM SAF/MG
Risk Management Council	Regular review and approval of the DAF Enterprise Risk Profile for submission in the annual SoA package.	SAF/MG
Executive Steering Committee (ESC) / Senior Assessment Team (SAT)	Entity Level Controls (ELCs) and Process Level Controls (PLCs), issues, and associated residual risks related to financial reporting, financial systems, and associated compliance objectives.	SAF/FM

3.1.1. To maintain appropriate accountability for effective internal control, the DAF segments its internal controls into AUs that have offices of primary responsibility assigned to each. The DoD defines an AU as any organizational, functional, programmatic, or other applicable subdivision of an organization that allows for adequate internal control analysis. An AU's functions include the documentation, identification, and insertion of control activities associated with a specific sub-function to mitigate identified risk. The AU is required to have an appointed and trained AU Lead. **(T-0)**

3.1.2. AU assignments must ensure that the entire organization is covered. An AU must be large enough to allow managers to evaluate the activity being examined, but not so large that

a manager cannot document processes and controls. The DAF's AUs are determined based on OUSD(C) internal control categories as shown in **Figure 3.2**: **(T-0)**

Figure 3.2. Internal Control Categories.

Internal Control Category	Assessing Organization	AU Segmentation
Entity Level Controls (ELCs)	SAF/FMFA	OPRs for policies in place to comply with Government Accountability Office (GAO) internal control standards
Financial Reporting	SAF/FMFA	Business processes that impact the DAF's financial statements
Financial Systems	Systems Integration and Innovation (SAF/FMFS)	Systems that are used in business processes that impact the DAF's financial statements
Operations	SAF/MG	DAF Organizations that report directly to the Secretary of the Air Force, Chief of Staff of the Air Force, or Chief of Space Operations.

3.2. Entity Level Controls (ELCs). ELCs are defined by GAO-14-704-G, *Standards for Internal Control in the Federal Government* (also referred to as the "GAO Green Book") as controls that have a pervasive effect on an entity's internal control system and pertain to multiple components. ELCs also include controls related to the entity's use of service organizations or management override of internal control and fraud. The GAO Green Book identifies five components and 17 principles, each principle aligned to one of the five components which provide the basis for evaluating the system of internal controls at the entity level as described below:

3.2.1. Component 1: Control Environment. The foundation for an internal control system. It provides the discipline and structure to help an entity achieve its objectives.

3.2.1.1. Principle 1: Demonstrate Commitment to Integrity and Ethical Values

3.2.1.2. Principle 2: Exercise Oversight Responsibility

3.2.1.3. Principle 3: Establish Structure, Responsibility, and Authority

3.2.1.4. Principle 4: Demonstrate Commitment to Competence

3.2.1.5. Principle 5: Enforce Accountability

3.2.2. Component 2: Risk Assessment. Assesses the risks facing the entity as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses.

3.2.2.1. Principle 6: Define Objectives and Risk Tolerances

3.2.2.2. Principle 7: Identify, Analyze, and Respond to Risks

3.2.2.3. Principle 8: Assess Fraud Risk

3.2.2.4. Principle 9: Identify, Analyze, and Respond to Change

3.2.3. Component 3: Control Activities. The actions management establishes through policies and procedures to achieve objectives and respond to risks in the internal control system, which includes the entity's information system.

3.2.3.1. Principle 10: Design Control Activities

3.2.3.2. Principle 11: Design Activities for the Information System

3.2.3.3. Principle 12: Implement Control Activities

3.2.4. Component 4: Information and Communication. The actions management establishes through policies and procedures to achieve objectives and respond to risks in the internal control system, which includes the entity's information system.

3.2.4.1. Principle 13: Use Quality Information

3.2.4.2. Principle 14: Communicate Internally

3.2.4.3. Principle 15: Communicate Externally

3.2.5. Component 5: Monitoring. Activities management establishes and operates to assess the quality of performance over time and promptly resolve the findings of audits and other reviews.

3.2.5.1. Principle 16: Perform Monitoring Activities

3.2.5.2. Principle 17: Evaluate Issues and Remediate Deficiencies

3.3. Process Level Controls (PLCs). PLCs are control activities embedded within business processes that do not meet the criteria of ELCs. DAF AU Leads are responsible for determining which PLCs are necessary to achieve reasonable assurance that business processes will achieve their operations, financial reporting, financial systems, and compliance objectives. The DAF leverages three categories to monitor and report on PLCs: operations, financial reporting, and financial systems. Operations, financial reporting, and financial systems align with OMB Circular No. A-123's internal control over reporting category, and compliance is considered within each category.

3.3.1. Operations. DAF Commanders are responsible for oversight of Internal Controls over Operations. They certify internal controls are developed and maintained to mitigate risks relating to the effective and efficient use of their organizations' resources related to administrative and major program operations.

3.3.2. Financial Reporting. DAF AU Leads execute business processes that impact the DAF's financial statements. AU Leads will develop and maintain internal controls, over these business processes, to mitigate risks of material misstatements in the DAF's financial statements. **(T-0)**

3.3.3. Financial Systems. DAF financial systems AU Leads who develop, deploy, or sustain information systems that produce information that is presented in the DAF's financial statements will develop and maintain internal controls over those financial systems in accordance with the Federal Financial Management Improvement Act of 1996 (FFMIA). OMB Circular No. A-123 Appendix D, *Compliance with the Federal Financial Management*

Improvement Act of 1996, provides goals and compliance indicators that must be satisfied for financial management systems to comply with FFMIA. The IT Complimentary User Entity Controls will be evaluated in the areas of security management, access control, segregation of duties and configuration management. **(T-0)**

3.4. Monitoring and Oversight. The DAF has multiple internal control monitoring and oversight programs, including, but not limited to, the Air Force Inspection System, Internal Audit Services, Quality Assurance Program, and RMF. Each program has its own assessing organizations and standards. The procedures below should be followed by assessing organizations unless it conflicts with the internal control assessment programs already in place at the DAF level.

3.4.1. During the annual scoping process SAF/MG and SAF/FM, working in coordination with SAF/AG, will recommend AUs to be assessed each fiscal year taking a risk-based approach that depends on the nature of the internal controls and importance of the AUs' objectives to the DAF achieving its objectives as described in **Figure 3.3**. **(T-0)** SAF/MG, in coordination with SAF/AG is responsible for oversight and monitoring operational internal control reporting. SAF/FM is responsible for oversight and monitoring of internal controls over financial reporting, financial systems, and associated compliance objectives. Each assessing organization considers the following when determining the scope of internal control assessments:

3.4.1.1. Internal controls to be assessed are being executed in the current fiscal year

3.4.1.2. Results of internal and external audits are considered in the scoping process

3.4.1.3. Internal controls that have known deficiencies or are already being assessed in the same fiscal year by another assessing organizations are not in-scope.

Figure 3.3. Scoping Approach.

Internal Control Category	Scoping Approach
ELCs	Policies in place to comply with GAO internal control standards.
Financial Reporting	Business processes that have a material impact on the DAF's General Fund (GF) and Working Capital Fund (WCF) financial statements as defined by Generally Accepted Government Auditing Standards and the GAO Financial Audit Manual.
Financial Systems	Systems that are used significantly in material business processes that impact the DAF's GF and WCF financial statements, in accordance with the *Federal Information Security Modernization Act of 2014*.
Operations	Programs in place for the DAF to achieve its core missions and mitigate enterprise risks.

3.4.2. Internal control assessments will be conducted annually and assessing organizations assesses compliance with the internal controls identified in the GAO Green Book. **(T-0)** This

process includes assessments of ELCs and PLCs. Assessments are performed through the following activities:

3.4.2.1. Identify objectives for in-scope AUs.

3.4.2.2. Assess inherent risks to achieving AU objectives.

3.4.2.3. Identify existing DAF policies, procedures, and internal controls that address objectives and mitigate risks.

3.4.2.4. Perform walkthroughs to confirm the accuracy of identified policies, procedures, and internal controls. If policies, procedures, or internal controls do not exist to address a principle, the assessing organization identifies an internal control deficiency.

3.4.2.5. Assess the design, implementation, and operating effectiveness of identified internal controls. If policies, procedures, or internal controls are not designed, implemented, or operating effectively, the assessing organization identifies an internal control deficiency.

3.4.2.6. Evaluate the severity of internal control deficiencies, individually and in the aggregate, identified from the assessment and recommend significant deficiencies and/or material weaknesses to the ESC or SMC to report in the SoA.

3.4.2.7. Share results of testing and material weakness and significant deficiency determinations with the Certification Statement Official.

3.4.2.8. Report the status and results of the assessment, as required, to the ESC and SMC.

3.4.3. Deficiency management and corrective actions for internal control deficiencies are an integral part of management accountability and are considered a priority. Material weaknesses should be prioritized by SAF/MG, SAF/FM, and deficiency OPRs should prioritize material weaknesses over significant deficiencies and prioritize significant deficiencies over all other control deficiencies.

3.4.3.1. SAF/FM and SAF/MG, with advice from SAF/AG, determine the severity of deficiencies identified by assessing organizations and approve material weaknesses and significant deficiencies to be reported in the DAF's annual SoA via the SMC and ESC. See OMB Circular No. A-123 for definitions and guidance for determining significant deficiencies and material weaknesses related to operations, financial reporting, and financial systems.

3.4.3.2. The deficiency owner must prepare, implement, and validate a Corrective Action Plan (CAP) for all internal control deficiencies as they are identified. **(T-0)** A CAP identifies specific actions and estimated completion dates for correcting the material weakness. The plan lists detailed tasks, called milestones, together with interim target dates for accomplishment. Milestones for CAPs related to material weaknesses and/or significant deficiencies may be revised, but the SMC and ESC are required to approve these changes, to include granting extensions from original completion dates. **(T-0)** Refer to the Air Force Deficiency Acceptance and CAP Process Guide for guidance on accepting and documenting the remediation process associated with external and self-identified deficiencies.

3.4.3.3. Assessing organizations will provide deficiency owners with the templates' necessary design and provide status updates on corrective actions. **(T-0)**

3.4.4. The SMC and ESC, who serve as the DAF's RMIC governance bodies, must approve material weaknesses and significant deficiencies in internal control and monitor CAP progress. **(T-0)**

3.4.4.1. The SMC approves material weakness and significant deficiency additions, changes, and recommended closures not related to financial reporting, financial systems, and associated compliance objectives.

3.4.4.2. The ESC approves material weakness and significant deficiency additions, changes, and recommended closures related to financial reporting, financial systems, and associated compliance objectives.

3.4.4.3. The RMC, SMC, and ESC will utilize the governance package outlined below to record their meetings. **(T-0)** The governance package will include, at a minimum, the following:

3.4.4.3.1. All products presented during the meeting or discussed as key references.

3.4.4.3.2. Meeting minutes will be recorded in the Governance Meeting Minutes Template provided by SAF/FMFA and include the following information. **(T-1)**

3.4.4.3.2.1. Date, time, and location of the meeting.

3.4.4.3.2.2. General overview of the RMC, SMC, or ESC purpose.

3.4.4.3.2.3. An executive summary of the meeting.

3.4.4.3.2.4. Meeting attendees broken down by Chair(s), Presenters, and Office Representation.

3.4.4.3.2.5. Action items, listed by office, from the previous meeting.

3.4.4.3.2.6. The meeting agenda.

3.4.4.3.2.7. The meeting summary (by slide), recording votes or decisions on any action items.

3.4.4.3.2.8. Outstanding action items, listed by office, and captured for the next meeting.

3.4.4.3.3. Governance packages will be completed within 30 business days of each RMC, SMC, and ESC meeting. **(T-1)**

Chapter 4

STATEMENT OF ASSURANCE (SOA) REPORTING

4.1. Overview. The DAF reports its SoA annually to OUSD(C). OUSD(C), in turn, consolidates the DAF's SoA with those received from all other DoD Departments and Components into a single, comprehensive DoD's annual SoA for submission to Congress.

4.2. Department of the Air Force SoA.

4.2.1. SAF/FMFA prepares the DAF SoA according to instructions received from OUSD(C) to satisfy the requirement outlined in the FMFIA. The SoA provides the Secretary of Air Force's (SecAF's) assertion as to whether the SecAF can provide reasonable assurance as to the effectiveness of DAF's system of internal control and the number significant deficiencies and material weaknesses existing as of 30 September of each fiscal year.

4.2.2. SAF/FMFA compiles the information to complete SoA templates required by OUSD(C) annually. Reporting elements are required to submit a Certification Statement. The Certification Statement process is outlined below.

4.2.2.1. Reporting elements confirm points of contact on an annual basis.

4.2.2.2. Reporting elements attend annual Certification Statement training hosted by SAF/FM. 4.2.2.3. Reporting elements complete a Certification Statement by early June. An exact date will be provided at the beginning of each fiscal year.

4.2.2.4. SAF/FM consolidates Certification Statement inputs for review and approval by the appropriate governance body.

4.2.2.5. SAF/FM consolidates approved material weaknesses and significant deficiencies for inclusion in the final DAF SoA.

4.2.2.6. For questions about the Certification Statement process or the reporting element points   of   contact,   reach   out   to   SAF/FMFA   at **SAF.FM.A.123.Internal.Controls@us.af.mil**.

Chapter 5

SPECIAL CONSIDERATIONS

5.1. Special Access Programs. DAF Special Access Programs are established and maintained when it is necessary to protect the most sensitive capabilities, information, technologies, and operations or when otherwise mandated by statute. The DAF must establish controls, infrastructure, and processes to manage, execute and protect the Special Access Programs. **(T-0)** Special Access Programs are required to align their RMIC efforts to comply with the guidance outlined in this instruction, where possible. **(T-0)** Key roles and responsibilities for establishing a Special Access Program are identified in AFI 16-701, *Management, Administration and Oversight of Special Access Programs*.

5.2. Freedom of Information Act Implications . The DAF's SoA may be made available, upon request, to the public, except in the case of any statement containing restricted information. The FMFIA specifies that information in the following categories be deleted from the Statement before it is made available to the public:

5.2.1. Information specifically prohibited from disclosure by any provision of law.

5.2.2. Information specifically required by Executive Order to be kept secret in the interest of national defense or the conduct of foreign affairs.

5.2.3. All other requests for information are to be handled in accordance with procedures for release of information established by DoDM 5400.07_AFMAN 33-302, *Freedom of Information Act Program*.

5.3. Performing RMIC Activities for External Agencies. Some DAF organizations perform RMIC activities for both the DAF and other federal agencies with shared missions. Examples include Air Force Special Operations Command for United States Special Operations Command, Surgeon General, U.S. Air Force and U.S. Space Force (AF/SG) for Defense Health Agency, and Air Mobility Command for United States Transportation Command. In these instances, the DAF organization should not duplicate activities and should report their program's completed activities on behalf of the external program to SAF/FM if those activities are relevant to DAF objectives.

Kristyn E. Jones
Assistant Secretary of the Air Force
(Financial Management and Comptroller)

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Public Law 114-186, *Fraud Reduction and Data Analytics Act of 2015*, 30 June 2016

Public Law 97-255, *Federal Managers' Financial Integrity Act of 1982*, 08 September 1982

Public Law 104-208, *Federal Financial Management Improvement Act of 1996*, 30 September 1996

Public Law 113-283, *Federal Information Security Modernization Act of 2014 (FISMA)*, 18 December 2014

Public Law 111-352, *GPRA Modernization Act of 2010*, 04 January 2011

OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, 15 July 2016

OMB Circular No. A-123, *Appendix D, Compliance with the Federal Financial Management Improvement Act of 1996*, 20 September 2013

GAO-14-704G, *Standards for Internal Control in the Federal Government*, 10 September 2014

GAO-21-368G, *Government Auditing Standards 2018 Revision Technical Update April 2021*, April 2021

GAO-22-105894, *Financial Audit Manual*, 30 June 2022

DoD 7000.14-R, Volume 4, *Accounting Policy*, current edition

DoDI 5010.40, *Managers' Internal Control Program Procedures*, 30 May 2013

DoDI 8510.01, *Risk Management Framework for DoD Systems*, 19 July 2022

DoDM 5400.07_AFMAN 33-302, *Freedom of Information Act Program*, 27 April 2018

DAFPD 65-2, *Enterprise Risk Management and Managers' Internal Control Program*, XX Dec 2022

AFI 16-701, *Management, Administration and Oversight of Special Access Programs*, 18 February 2014

AFI 65-301, *Internal Audit Services*, 31 August 2018

AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*, 06 February 2020

AFI 17-130, *Cybersecurity Program Management,* 13 February 2020

AFI 33-322, *Records Management and Information Governance Program*, 23 March 2020

DAFMAN 90-161, *Publishing Processes and Procedures*, 15 April 2022

Prescribed Forms

None

Adopted Forms

DAF Form 847, Recommendation for Change of Publication

Abbreviations and Acronyms

AFI—Air Force Instruction

AFMAN—Air Force Manual

AU—Assessable Unit

CAP—Corrective Action Plan

CRO—Chief Risk Officer

DAF—Department of the Air Force

DAFI—Department of the Air Force Instruction

DAFMAN—Department of the Air Force Manual

DAFPD—Department of the Air Force Policy Directive

DoD—Department of Defense

DoDI—Department of Defense Instruction

ELC—Entity level control

ERM—Enterprise Risk Management

ESC—Executive Steering Committee

FFMIA—Federal Financial Management Improvement Act of 1996

FMFIA—Federal Managers' Financial Integrity Act of 1982

GAO—Government Accountability Office

GF—General Fund

GPRA—Government Performance and Results Act

IT—Information Technology

MICP—Managers' Internal Control Program

No.—Number

OMB—Office of Management and Budget

OPR—Office of primary responsibility

PLC—Process level control

RMC—Risk Management Council

RMF—Risk Management Framework

RMIC—Risk Management and Internal Control

SAF—Secretary of the Air Force

SAT—Senior Assessment Team

SecAF—Secretary of Air Force

SMC—Senior Management Council

SoA—Statement of Assurance

SPPBE—Strategy, Planning, Programming, Budgeting, and Execution

USAF—United States Air Force

USSF—United States Space Force

WCF—Working Capital Fund

Office Symbols

AF/SG—Surgeon General, U.S. Air Force and U.S. Space Force

OUSD(C)—Office of the Undersecretary of Defense (Comptroller)

SAF/FM—Assistant Secretary of The Air Force (Financial Management and Comptroller)

SAF/FMF—Deputy Assistant Secretary for Financial Operation

SAF/FMFA—Accounting and Financial Oversight

SAF/FMFS—Systems Integration and Innovation

SAF/MG—Deputy Under Secretary of the Air Force, Management

Terms

Statement of Assurance (SoA)—An annual statement, in memorandum format, that provides the SecAF's explicit level of assurance on whether internal controls are effective. The SoA is based on self-assessments and testing of internal controls developed for mission-essential functions relative to risk and identifies any material weaknesses found during the analysis.

Assessable Unit (AU)—Any organizational, functional, programmatic, or other applicable subdivision of an organization that allows for adequate internal control analysis. An AU's functions include the documentation, identification, and insertion of controls associated with a specific sub-function to mitigate identified risk.

Control Deficiency—A control deficiency exists when the design, implementation, or operation of a control does not allow management or personnel, in the normal course of performing their assigned functions, to achieve control objectives and address related risks.

Enterprise Risk Management (ERM)—An enterprise-wide framework and governance structure that provides a strategically aligned portfolio view of organizational risks, issues, challenges, and potential opportunities to provide insight into how to proactively address performance issues and most effectively prioritize resource allocations to ensure successful mission delivery.

Entity level control (ELC)—Controls that have a pervasive effect on an entity's internal control system; ELCs may include controls related to the entity's risk assessment process, control environment, service organizations, management override, and monitoring.

Executive Steering Committee—Governance body that provides high-level guidance and direction to ensure the timely implementation of corrective actions related to material weaknesses and significant deficiencies in reporting, financial systems, and compliance. The committee will also monitor the ongoing execution of financial audit improvement, internal control requirements, and risk management. The ESC will serve as the Department of the Air Force Senior Assessment Team (SAT) when performing SAT responsibilities and is comprised of senior level executives, chaired by the Assistant Secretary for Financial Management and Comptroller and the Deputy Chief Management Officer.

Internal Control—A process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved.

Material Weakness—A deficiency, or a combination of deficiencies, in internal control, important enough to merit attention by those charged with governance. A material weakness in internal control over reporting is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the DAF's financial statements will not be prevented, or detected and corrected, on a timely basis. A material weakness in internal control over operations might significantly weaken established safeguards against fraud, waste, loss, unauthorized use, or misappropriation of funds, property, other assets, or conflicts of interest.

Process Level Control—Controls that address material risk areas within AUs and help organizations meet objectives related to operations, financial reporting, financial systems, and compliance.

Risk Management and Internal Control (RMIC) Program—The Managers' Internal Control Program (MICP) was established by Public Law 97-255, FMFIA and was enacted to ensure efficient and effective management of government resources to protect against fraud, waste, and abuse. It requires all federal agencies to establish management controls that provide reasonable assurance that: obligations and costs follow applicable laws; funds, property, and other assets are safeguarded against waste, loss, unauthorized use or misappropriation; revenues and expenditures are properly recorded and accounted for; and programs are efficiently and effectively carried out according to applicable law and management policy. The law also requires the head of each agency report annually to the President and Congress through a SoA on whether they are in compliance with the FMFIA. These requirements are further codified in references DoD Instruction (DoDI) 5010.40, *Managers' Internal Control Program (MICP) Procedures* and OMB Circular No. A-123 provide authoritative guidance on implementing these laws.

Risk Management Council (RMC)—Governance body that oversees the establishment of the Agency's enterprise Risk Profile, regular assessment of risk, and development of appropriate risk response. RMC structures will vary by Agency, and in some cases may be integrated with existing management structures. An effective RMC will include senior officials for program operations and mission-support functions to help ensure those risks are identified, which have the most significant impact on the mission outcomes of the DAF. The DAF's RMC is chaired by SAF/MG, as the DAF's CRO.

Senior Assessment Team (SAT)—A team of senior level executives that provide oversight of assessing and documenting the effectiveness of internal controls for financial reporting and financial systems. The DAF executes the responsibilities of the SAT through the DAF's ESC, and this meeting is chaired by SAF/FM.

Senior Management Council (SMC)—A committee or board of senior level executives that convene to advise DAF senior leaders on internal control matters related to operations, to include the identification of internal control material weaknesses that merit reporting as material weaknesses. The DAF executes the responsibilities of the SMC through the DAF's governance construct, and these meetings are co-chaired by SAF/MG and SAF/FM.

Significant Deficiency—A deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness yet important enough to merit attention by those charged with governance.