Department of Veterans Affairs
Veterans Health Administration
Washington, DC 20420

VHA DIRECTIVE 1370
Transmittal Sheet
February 5, 2018

VHA INTERNAL AUDIT AND RISK ASSESSMENT PROGRAM OFFICE

1. REASON FOR ISSUE: This Veterans Health Administration (VHA) directive establishes the policies and assigns actions for an internal audit and risk assessment program for enterprise clinical and health care administrative operations.

2. SUMMARY OF MAJOR CONTENT: This is a new directive to address internal audit and enterprise risk management.

3. RELATED ISSUES: None.

4. RESPONSIBLE OFFICE: The Internal Audit and Risk Assessment Office (IARA) (10EC1) is responsible for the contents of this directive. Questions may be directed to IARA via Email at VHA10E1CAction@va.gov or phone at 202-266-4503.

5. RECISSIONS: None.

6. RECERTIFICATION: This directive is due to be recertified on or before the last working day of February 2023. This VHA directive will continued to serve as national VHA policy until it is recertified or rescinded.

Carolyn M. Clancy, M.D.
Executive in Charge

DISTRIBUTION: Emailed to the VHA Publication Distribution List on February 7, 2018.

CONTENTS

VHA INTERNAL AUDIT AND RISK ASSESSMENT PROGRAM OFFICE

VHA INTERNAL AUDIT AND RISK ASSESSMENT PROGRAM OFFICE

1. PURPOSE

This directive establishes the policies and assigns actions for an internal audit and risk assessment program for enterprise clinical and health care administrative operations. **AUTHORITY:** Title 38 United States Code (U.S.C.) 7301(b).

2. BACKGROUND

a. In 2015, the Under Secretary for Health consolidated essential Veterans Health Administration (VHA) program offices responsible for oversight and accountability under a single Assistant Deputy Under Secretary for Health. The Office of Integrity includes the Office of Compliance and Business Integrity (CBI), the Office of the Medical Inspector, Management Review Service, the National Center for Ethics in Health Care, and a new Office of Internal Audit and Risk Assessment (IARA).

b. To enhance the Department of Veterans Affairs' (VA) enterprise-wide oversight and accountability activities, VHA has adopted the Three Lines of Defense model for risk management and control promoted by the Institute of Internal Auditors (IIA). In this model, each of three lines play a distinct role within an organization's governance framework:

(1) 1st Line: Operational Management. A management function through which operational managers assess risk, develop controls to mitigate risk, and implement corrective actions when deficiencies are found;

(2) 2nd Line: Risk Management and Compliance. A management function through which risk, management, compliance, and controllership function conducts activities to ensure that the 1st Line of Defense is properly designed and operating as intended. As a management function, the 2nd Line of Defense may intervene directly in modifying and developing the internal control and risk systems; and

(3) 3rd Line: Internal Audit. An independent assurance function through which the government body is provided comprehensive assurance objectively and independently.

NOTE: *Appendix A describes the Three Lines of Defense in detail. IARA will serve as one element of VHA's improved 3rd Line of Defense capability.*

c. IARA's core mission is to provide independent and objective audit, assurance, and advisory services that add value and improve VHA's operations. Internal audit activities provide assurance on the effectiveness of governance, risk management, compliance, and internal controls, including how the 1st and 2nd Lines of Defense achieve their intended risk management and control objectives.

d. IARA develops independent enterprise-wide oversight policies, processes, and procedures for 3rd Line of Defense audits at the VA medical centers, Veterans Integrated Service Networks (VISN), Program Offices, and other activities as

appropriate in accordance with industry standards. These oversight policies, processes, and procedures implement the essential elements of an effective internal audit and risk assessment program.

e. External auditors, regulators, and other external bodies play a critical role in VHA's oversight and accountability efforts. VHA's external oversight agencies include the VA's Office of Inspector General (OIG), the Government Accountability Office (GAO), U.S. Office of Special Counsel (OSC), and the House and Senate Veterans Affairs Committees of the United States Congress. Additional external regulatory and accrediting bodies include The Joint Commission, the Commission on Accreditation of Rehabilitation Facilities (CARF), the Clinical Laboratory Improvement Amendments (CLIA) Act, and other accrediting bodies. Regulators sometimes set requirements intended to strengthen the controls in an organization and on other occasions perform an independent and objective function to assess the whole or some part of the 1st, 2nd, or 3rd Lines of Defense with regard to those requirements.

3. DEFINITIONS

a. **Advisory Services.** Consulting services that focus on providing advice to senior management to improve an organization's governance, risk management, and control processes, without the internal auditor assuming management responsibility.

b. **Assessments.** Informal audits or other analyses that are designed to address concerns or provide relevant information to management in a timely manner without using the same level of resources and/or rigor necessary to fully meet Generally Accepted Government Auditing Standards (GAGAS) and IIA audit standards.

c. **Assurance.** An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, disparities for at-risk populations, system security, and due diligence engagements.

d. **Compliance.** Meaningful adherence to the requirements of any law, regulation, or standard applicable to the activity or practice in question.

e. **Clinical Risks.** A risk resulting from the potential for direct patient harm.

f. **Control.** Any action taken by VHA managers and other parties to manage risk and increase the likelihood that established goals and objectives will be achieved. Management plans, organizes, and directs the performance of sufficient actions to ensure objectives will be achieved.

g. **Enterprise Risk.** A risk that has broad or far-reaching implications for VHA.

h. **Enterprise Risk Management.** The implementation of a framework that provides governance, communications, training, processes, and tools to effectively identify, assess, respond to, and monitor risks, enabling VA leadership to make informed decisions and focus priorities to better serve Veterans. Section II of Office of

Management and Budget (OMB) Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control defines management's responsibilities for Enterprise Risk Management (ERM), and includes requirements for identifying and managing risks. Most importantly, it encourages agencies to establish a Risk Management Council (RMC), develop Risk Profiles that identify risks arising from mission and mission-support operations, and consider those risks as part of the annual strategic review process. It complements Section 270 of OMB Circular No. A-11, which discusses agency responsibilities for identifying and managing strategic and programmatic risk as part of agency strategic planning, performance management, and performance reporting practices. Together, these two Circulars constitute the ERM policy framework for the federal government, with specific ERM activities integrated and operationalized by federal agencies.

i. **GAGAS/IIA Compliant Audits.** Internal audit that meet the standards promulgated by GAO's GAGAS and the Institute of Internal Auditors (IIA) that delineate the requirements for performing a broad range of internal audit activities, and for evaluating internal audit performance.

j. **Health Care Administrative Risks.** A risk resulting from organizational or operational problems that may indirectly threaten effective patient care.

k. **Independence.** The freedom from conditions that threaten the ability of the internal audit entity to carry out internal audit activities in an unbiased manner.

l. **Internal Audits.** A systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management and control processes.

m. **Objectivity.** An unbiased and impartial mental attitude, approach, and operating environment that allows internal auditors to perform engagements in such a manner that they believe in the opinions and recommendations delineated by their work products and that no compromises on quality are made. Objectivity requires that internal auditors be aware of their own unconscious biases and do not subordinate their judgment on audit matters to others.

n. **Risk.** The potential for loss, harm, or missed opportunities in relation to achievement of the organization's mission and strategic objectives.

o. **Risk Assessment**. A systematic process of evaluating the potential risks that may be involved in a projected activity or undertaking.

p. **Risk Governance.** A systematic approach to decision making associated with natural and technological risks based on principles of cooperation, participation, mitigation, and sustainability, adopted to achieve more effective risk management convergent with other public and private policies.

q. **Risk Rating.** The rating resulting from the application of the entity's risk assessment criteria; represents a quantitative or qualitative risk assessment value used for comparing risks.

r. **Risk Sponsor.** An individual that has responsibility for managing and monitoring a risk, or for overseeing the management/monitoring of risk by specialists.

4. POLICY

It is VHA policy that IARA will provide independent and objective audit, assurance, and advisory services to improve VHA's operations, and advise and inform VHA leadership by assessing enterprise risks. IARA will conduct outreach to VHA program offices that perform or oversee 1st and 2nd Lines of Defense activities to enhance clarity regarding risk and controls and improve the effectiveness of VHA's risk management system(s).

5. RESPONSIBILITIES

a. **Under Secretary for Health.** The Under Secretary for Health is responsible for:

(1) Promoting and encouraging an ethical organizational culture that upholds internal audits, compliance, and risk assessment activities, among others, to the laws, regulations, and standards that govern VHA operations, and to the highest standards of integrity and oversight.

(2) Integrating internal audit, risk assessment, and compliance into the structure of VHA leadership and operations.

(3) Appointing a Chief Audit Executive (CAE) to provide oversight, guidance, and direction to the Office of IARA.

(4) Delegating authority to the Audit, Risk, and Compliance Committee (ARCC) to prioritize VHA clinical and health care administrative risks and to develop VHA's annual audit and compliance plan.

(5) Reviewing and approving the ARCC charter and any amendments.

(6) Approving formal recommendations received from the ARCC.

b. **Audit, Risk, and Compliance Committee**. The ARCC shall serve as the governance body that provides strategic guidance and direction for all VHA internal audit, compliance, and risk assessment activities.

(1) The Principal Deputy Under Secretary for Health shall serve as the ARCC chairperson.

(2) The ARCC membership shall consist of:

(a) VHA Principal Deputy Under Secretary for Health (Chairperson);

(b) VHA Deputy Under Secretaries for Health;

(c) VHA Chief of Staff;

(d) Two Network Directors

(e) Two Medical Center Directors;

(f) Office of General Counsel;

(g) Assistant Deputy Under Secretary for Health for Integrity;

(h) Healthcare Improvement Center (HIC) Director;

(i) CAE (ex officio); and

(j) Executive Director/Chief Officer, CBI (ex officio).

(3) Voting and other operational requirements shall be articulated in an approved ARCC Charter.

(4) The ARCC is responsible for:

(a) Ensuring IARA's comprehensive and proactive oversight drives continuous improvement in the quality, efficiency, and consistency of VHA's operations and enhances Veteran trust in VHA health care services;

(b) Adhering to the ARCC Charter that governs its operations, to include meeting at least quarterly;

(c) Providing executive guidance and decision-making on the strategic direction of CBI operational planning in accordance with VHA Directive 1030, Compliance and Business Integrity Oversight Program, dated February 26, 2016, or subsequent policy;

(d) Establishing procedures to address enterprise-wide risks that will require an urgent risk response;

(e) Selecting VHA clinical and health care administrative risks subject to IARA audits, reviews, or assessments;

(f) Providing formal recommendations to the Under Secretary for Health based on the findings, conclusions, causes, and recommendations in IARA's audit reports.

c. **Office of Internal Audit and Risk Assessment.** IARA serves as the primary staff support for the ARCC and is responsible for:

(1) Leading all audit and ERM activities under the direction of the ARCC chairperson as authorized by this directive. ***NOTE:*** CBI will lead all nonclinical compliance activities under the direction of the ARCC chairperson and in accordance with VHA Directive 1030. VHA Directive 1030 is currently in revision to address a critical gap around clinical compliance activities;

(2) Providing independent assurance through its internal audit and risk assessment operations, which enhance and strengthen a culture of accountability and integrity in service of Veterans;

(3) Implementing VHA's internal audit and risk assessment program;

(4) Completing all ARCC directed audits in a timely manner and according to industry standards and/or best practices;

(5) Developing and issuing internal audit and risk assessment guidance;

(6) Promoting and cultivating an integrated framework of audit partnerships and associations to strengthen the integrity and transparency of clinical and health care management systems to build trust and ensure accountability;

(7) Submitting an Enterprise Risk Assessment to the ARCC that identifies and prioritizes VHA's enterprise-wide risk, at least annually;

(8) Providing a quarterly update of all internal audit activity to the ARCC;

(9) Proposing the annual VHA internal audit plan for ARCC consideration and approval, which directs and prioritizes IARA in-process, recurring, and new audit activities for the upcoming fiscal year; and

(10) Serving as VHA's central coordinating office for the Department's ERM program to include:

(a) Develop and maintain the Administration-wide ERM infrastructure.

(b) Promote a risk-aware culture and appoint VHA Enterprise Risk Management Working Group (ERMWG) members, risk sponsors, and other appropriate representatives to work within the ERM framework.

(c) Support the Department in aligning ERM frameworks, tools, methodologies, learning resources, and knowledge management capabilities.

d. **Chief Audit Executive.** The CAE serves as the executive director of the Office of IARA ensuring program standards and day-to-day operations are aligned with VA, VHA and industry standards for an effective internal audit and ERM program. These include:

(1) **Written Policies and Procedures**. Written policies and procedures, developed under the direction and supervision of the CAE, will guide IARA's audit, enterprise risk, and execution activities, in addition to identifying specific areas in which internal audits and risk assessments are needed.

(2) **Training and Education**. A multifaceted training and education program that focuses on the elements of internal audit and enterprise risk assessment to ensure

IARA staff are well-trained and educated on internal audit and ERM standards, requirements, best practices and expectations.

(3) **Open Lines of Communication**. Open lines of communication between auditors and stakeholders are equally important to successfully implementing an internal audit and risk assessment program and enhancing VHA's oversight and accountability activities. Additionally, extensive outreach across the VHA enterprise will ensure a common understanding of the Three Lines of Defense, reduce deficiencies in oversight activities, and promote a collaborative culture across the enterprise.

(4) **External Review/Audits**. IARA should have periodic peer reviews and external audits to assess the effectiveness of its internal audit and risk assessment activities.

(5) **Performance Measures**. IARA will establish a performance measures plan and conduct routine periodic reviews to assess the effectiveness of its risk assessment and internal audit programs. Analysis of program metrics will be used to identify areas for improvement and to determine the effects of the organization's quality assurance efforts.

e. **VHA Program Officers, VISN Directors, and Medical Facility Directors.** Each VHA Program Officer, VISN Director, and Medical Facility Director is responsible for:

(1) Responding to requests from IARA promptly and completely. IARA, as a component of VHA, has legal authority under applicable federal privacy laws and regulations to access and use any information, including health information, maintained in VHA records for the purposes of health care operations and oversight.

(2) Providing, as requested, subject matter experts to augment the teams IARA assembles to perform internal audit activities.

(3) Cooperating fully with internal auditors. Maximum support and assistance shall be provided to an internal audit team.

(4) Submitting a corrective action plan to address findings and recommendations resulting from audit reports to the CAE within 30 calendar days of receiving a final audit report.

(5) Implementing corrective actions until all are completed and verified by the appropriate/assigned Deputy Under Secretary for Health.

(6) Ensuring the CAE is contacted directly when issues arise that might lead to questions or difficulties regarding provision of information to or support for the audit team.

6. TRAINING

There are no formal training requirements associated with this directive.

7. RECORDS MANAGEMENT

All records regardless of format (paper, electronic, electronic systems) created by this directive shall be managed per the National Archives and Records Administration (NARA) approved records schedules found in VA Records Control Schedule (RCS) 101. If you have any question to the regarding any aspect of records management you should contact your facility Records Manager or your Records Liaison. See also VHA Directive 6300, Records Management, or subsequent policy issue.

8. REFERENCES

a. Title 38 U.S.C. 7301(b).

b. VHA Directive 1030, Compliance and Business Integrity Oversight Program, dated February 26, 2016, or subsequent policy.

c. The Executive Office of The President, Office of Management and Budget (OMB) Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control (M-16-17): https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m-16-17.pdf. ***NOTE:*** *This linked document is outside of VA control and may or may not be conformant with Section 508 of the Rehabilitation Act of 1974.*

d. Generally Accepted Government Auditing Standards, available at: http://www.gao.gov/yellowbook/overview. ***NOTE:*** *This linked document is outside of VA control and may or may not be conformant with Section 508 of the Rehabilitation Act of 1974.*

e. The Institute of Internal Auditors Position Paper: The Three Lines of Defense in Effective Risk Management and Control, available at: https://www.theiia.org/3-Lines-Defense. ***NOTE:*** *This linked document is outside of VA control and may or may not be conformant with Section 508 of the Rehabilitation Act of 1974.*

THE THREE LINES OF DEFENSE

(1) In the Institute of Internal Auditors (IAA) position paper IIA Position Paper: *The Three Lines of Defense in Effective Risk Management and Control*, the IAA explains: *…management control is the first line of defense in risk management, the various risk control and compliance oversight functions established by management are the second line of defense, and independent assurance is the third. Each of these three lines plays a distinct role within the organization's wider governance framework.*

(2) It is important to note that the third line of defense must be independent and objective of the first and second line of defense functions. Additionally, while independence and objectivity are not required characteristics of the 2nd line of defense, independence does help avoid potential conflict of interests in which the same organization or staff conducting first and second line of defense functions are not objective evaluators of their own systems and controls.

The IAA Position Paper can be found at https://www.theiia.org/3-Lines-Defense.
NOTE: *This linked document is outside of VA control and may or may not be conformant with Section 508 of the Rehabilitation Act of 1974.*