Department of Veterans Affairs
Washington, DC 20420

VA Directive 0054
Transmittal Sheet
April 8, 2014

VA Enterprise Risk Management (ERM)

1. REASON FOR ISSUE: This directive provides guidelines to help VA manage enterprise risks and mitigate adverse impacts to performance. The directive sets forth policy, roles and responsibilities, and decision authority, and is aligned with the major elements of the ERM Framework.

2. SUMMARY OF CONTENTS: This policy establishes the ERM program, mission, vision, and goals. It also sets forth Department-wide ERM policies for the three major elements of the ERM program: Risk Governance, Common Risk Infrastructure, and Risk Ownership.

3. RESPONSIBLE OFFICE(S): Office of the Assistant Secretary for Management/Chief Financial Officer (004), and Office of Enterprise Risk Management are responsible for the material contained in this directive.

4. RELATED HANDBOOK: None

5. RESCISSIONS: None

CERTIFIED BY:

/s/
Stephen W. Warren
Executive in Charge and
Chief Information Officer,
Office of lnformation and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Helen Tierney
Executive-in-Charge,
Office of Management,
and Chief Financial Officer

Electronic Distribution Only:

VA ENTERPRISE RISK MANAGEMENT PROGRAM

1. PURPOSE

a. This directive establishes the policy needed to implement the Department of Veteran Affairs (VA) Enterprise Risk Management (ERM) program.

b. This directive applies to all VA offices. It sets forth Department-wide ERM policies for the three major elements of the ERM program: Risk Governance, Risk Infrastructure, and Risk Sponsorship. Risk Governance establishes how authority and decision-making over VA's enterprise risks will be exercised. Risk Infrastructure establishes the processes, human capital, and technology capabilities required to implement the ERM strategy and policy. Risk Sponsorship includes administration and staff office activities needed to carry out ERM processes and establish sponsorship of risks, including the associated risk response.

c. This directive provides guidelines to help VA manage enterprise risks and mitigate adverse impacts to performance. This directive recognizes that risk is not just focused on adverse consequences but also involves taking advantage of opportunities that can lead to positive outcomes if the attendant risks are well-managed within VA's risk appetite.

2. POLICY

a. General. This policy establishes the ERM program, mission, vision, and goals. Specific operating procedures for executing these requirements will be defined in *VA's Enterprise Risk Management Program Handbook.*

(1) ERM mission. The mission is to implement a common, enterprise wide risk management framework that provides the necessary governance, communications, training, processes, and tools to effectively identify, assess, respond to, and monitor risks – enabling VA leadership to make informed decisions, focus priorities to better serve Veterans, and make the best use of resources.

(2) ERM vision. The vision is to create a Department-wide risk-aware culture and ERM infrastructure that enables VA to better serve Veterans and make the best use of resources.

(3) ERM goals. Collectively, the goals of the ERM program aim to:

(a) Increase visibility of emerging risks and provide an opportunity to address risks before they occur.

(b) Increase leadership's confidence that they have a complete, common risk operating picture.

(c) Increase VA's ability to allocate resources to the highest priority risks.

(d) Enhance VA's ability to address risks related to non-compliant business practices, integrity, and stewardship of financial resources that impact the quality of the Veterans' experience, public trust, and compliance with applicable laws, regulations, standards, and directives.

(e) Gain efficiencies by breaking down risk management silos and redundancies, using a common taxonomy and set of tools, including sharing best practices and lessons learned.

(f) Increase risk-related information sharing to promote risk management best practices, continuous risk management, and lessons learned.

(g) Provide timely and complete risk information to leadership to help make decisions and focus priorities.

(h) Promote sponsorship and responsibility for identifying, communicating, responding to, and monitoring risk.

(i) Increase risk awareness Department-wide and expand VA's capability to manage risk using leading risk management practices and tools.

b. Risk Governance. Risk Governance is the systemic approach to exercise authority and decision-making over VA's enterprise risks. The Risk Governance Board (RGB) approves the ERM program's strategic direction, directs the applicable Department-wide risk decision-making authority, establishes VA's risk appetite and tolerance, performs oversight of the ERM program, and provides guidance to the Chief Risk Officer (CRO) and the Office of Enterprise Risk Management (OERM). The RGB is chaired by the Secretary of VA (SECVA), who is the ultimate decision authority, and is comprised of VA executive board members, who make recommendations to the SECVA. The RGB (as defined in the *RGB Charter* and further specified in Section 3) shall perform the following roles:

(1) **Policy**. The RGB shall oversee adherence to ERM policy across VA.

(2) **ERM strategy**. The RGB shall provide oversight in the development of a VA ERM strategy, including the following components.

(a) The RGB shall approve an overarching ERM program strategic plan that will be refreshed on an annual basis.

(b) The RGB shall establish Department-wide risk appetite. Risk appetite is defined as the amount of risk, on a broad level, that VA is willing to accept in pursuit of its mission and goals. The risk appetite provides criteria for deciding the appropriate levels of risk in existing VA programs and operations.

(c) The RGB shall establish risk tolerance thresholds. Risk tolerance is the acceptable level of variation relative to achievement of specific objectives. The thresholds are tactical and measurable boundaries that will be used to signal when leading indicators of a risk have reached unacceptable levels and pre-emptive actions should be taken.

(3) **Risk monitoring and oversight**. Risk monitoring and oversight responsibilities are divided between the RGB, OERM, and the administrations and staff offices.

The RGB will maintain focus on VA's top risks and ensure the Department is making the best risk management decisions. The RGB's monitoring and oversight shall include the following activities:

(a) Review and validate the content of the Top Risk Register by making decisions on which risks should be included.

(b) Make decisions on the need to develop formal risk response plans, specifying the actions needed to manage selected top risks, or conduct Risk Management Projects (RMP).

(c) Review and monitor risks and risk response plans.

(d) Provide guidance and direction to "risk sponsors" on risk response plans.

c. Risk Infrastructure. Risk Infrastructure includes the processes, human capital, and technology capabilities required to achieve the ERM mission. OERM shall maintain the VA enterprise risk infrastructure – leveraging the support and expertise of existing VA risk functions – by establishing and continually improving the tools, methodologies, and knowledge management capabilities to carry out a Department-wide ERM program. OERM shall develop policy, establish the ERM framework, report on top enterprise risks, establish ERM tools and methodologies, support analysis of specific risks, and perform other duties in support of the RGB.

(1) Policy Development. OERM shall develop and maintain ERM directives and handbooks in accordance with *VA Directive 6330: Directives Management* and *VA Handbook 6330: Directives Management Procedures*.

(2) ERM Framework. OERM shall develop and maintain the ERM framework, which encompasses the capabilities and processes for implementing Risk Governance, Risk Infrastructure, and Risk Sponsorship as described in this Directive.

(3) Risk Reporting. OERM shall be the central hub for Department-wide risk information. Guidance shall be developed to determine which VA risks are assessed through the ERM processes and ultimately reported to the RGB. OERM shall compile risk information from the administrations and staff offices into reports for dissemination to the RGB and other appropriate parties.

(4) ERM Tools and Methodologies. OERM shall develop and distribute tools, templates, and methodologies to share information, drive ERM-related analytics and reporting, promote consistent execution of ERM processes, and assist the administrations, staff offices, and RGB in performing their ERM responsibilities. Tools and methodologies include, but are not limited to, enterprise risk rating criteria; enterprise risk register; enterprise risk taxonomy; Deep Dive methodology; knowledge management technologies; communication products such as ERM frequently asked questions; risk management definitions; and ERM training materials. OERM shall also establish Department-wide standards for VA ERM software.

d. Risk Sponsorship. Risk Sponsorship includes administration and staff office activities needed to manage and establish accountability for managing risks in VA.

Activities at this level of the framework include the day-to-day aspects of on-going risk management in various VA functions, programs, services, projects, and initiatives. The RGB shall assign risk sponsors for enterprise risks. Risk sponsors shall execute enterprise risk management activities in accordance with ERM policy and procedures.

(1) Strategic Risk Assessment (SRA) Process. OERM shall facilitate, and administration and staff offices shall participate in, the SRA process. The SRA process includes the following major stages:

(a) Analyze

1. Risk identification is the process of systematically identifying, categorizing, and documenting enterprise risks in alignment with the risk taxonomy, VA mission, and VA strategic objectives.
2. Risk assessment is the process of evaluating the exposure to an identified risk by obtaining input from information sources and applying VA's risk assessment criteria for analysis and scoring.
3. Risk prioritization is the process of collaborating with key ERM stakeholders to validate VA's enterprise risks and organize them using a consistent rating and ranking methodology.

(b) Manage

1. Risk response is a process of assigning appropriate accountability, analyzing options to mitigate each risk, and selecting a risk management strategy aimed at optimizing risk and reward for VA.
2. Risk monitoring is the process of tracking the exposure of each risk over time, including the outcomes of risk responses and overall shifts in the risk profile based on internal or external changes.

(2) Continuous Risk Assessment (CRA) Process. OERM shall facilitate, and administration and staff offices shall participate in, the CRA process. The CRA process includes the same five stages as the SRA process but operates more frequently so that emerging risks can be escalated outside the bi-annual SRA process and brought to the immediate attention of OERM, the RGB, the CRO or the SECVA. It is ERM policy to escalate emerging risks within the CRA process.

(3) RMP Process. OERM shall facilitate, and designated personnel from the administration and staff offices shall participate in, the RMP process. The RMP process is a risk response activity involving the collaboration between a risk sponsor and associated subject matter experts (SME) to conduct a more in-depth risk analysis and determine specific actions needed to better manage the risk in the future.

3. ROLES AND RESPONSIBILITIES

a. Risk Governance Board (RGB). The RGB is designated as the senior-level oversight authority for ERM. The RGB shall:

(1) Establish a centralized structure for risk management direction, accountability, and guidance, as well as govern risk management assurance and controls.

(2) Govern the VA ERM program's infrastructure, including the people, processes, and technology required to identify, measure, monitor, mitigate, report, and manage risks.

(3) Validate risks listed on VA's Top Risk Register.

(4) Require formal response plans specifying further actions on selected risks.

(5) Monitor risks through regular status updates and direct future risk management activities.

(6) Provide oversight of critical risks by monitoring risk sponsors' key findings from risk assessments and risk response plans and recommending or directing modifications to risk management strategies.

(7) Establish, communicate, and monitor VA's risk appetite in pursuing the objectives set by VA leadership to accomplish its mission.

(8) Set expectations and provide general guidance for VA management to define and comply with risk tolerance thresholds for key VA processes and operations.

(9) Collaborate with OERM to define administration and staff office risk accountability, roles, and responsibilities throughout the Department.

b. Chief Risk Officer (CRO). The CRO is the principal ERM advisor to the SECVA, RGB, Executive in Charge, Office of Management (EIC-OM) and VA Chief Financial Officer (VACFO). The CRO leads OERM in its duties to develop and facilitate all capabilities and processes in the ERM program.

c. Office of Enterprise Risk Management (OERM). OERM is the central coordinating office for the ERM program. OERM was established by the Secretary to improve VA's ability to identify and respond to a broad range of risks that could affect VA's mission to serve Veterans and preserve public trust. OERM shall:

(1) Support the development of ERM vision and policy that identifies, measures, prioritizes, reports, and mitigates Department-wide risks in an integrated manner.

(2) Develop and maintain the Department-wide ERM infrastructure.

(3) Promote a risk-aware culture and facilitate senior executive leadership commitment to ERM.

(4) Support the administrations and staff offices in aligning with ERM frameworks, tools, methodologies, learning resources, and knowledge management capabilities.

(5) Provide VA leadership and the RGB with information regarding the status of various risk management efforts.

(6) Recommend appointment of the risk sponsors to the RGB.

(7) Collaborate with risk sponsors and SMEs to perform further analysis of root causes, risk events, potential consequences, or current/recommended mitigation strategies – resulting in a risk response strategy.

(8) Establish and maintain the VA Top Risk Register and ERM dashboards.

(9) Provide regular status updates on risk response efforts to the RGB.

(10) Resolve conflicts that arise from carrying out the ERM process, such as which risks are assessed or which methodology should apply.

(11) Elevate decisions to the RGB as necessary.

d. ERM Working Group (ERMWG). The ERMWG is an advisory body that shares information and provides subject matter expertise to help shape the direction of the ERM program and communicates activities to its members' respective administration or staff office. The ERMWG does not have decision-making or tasking authority. There shall be a core team of advisors on the ERMWG, but other VA SMEs may participate on an as-needed basis. Key ERMWG responsibilities are to:

(1) Advise on ERM assessments.

(2) Act as liaison between administrations and staff offices and OERM.

(3) Support ERM communications and awareness.

(4) Review and provide advice to OERM on identified and emerging risks, risk assessment results, and risk response strategies.

e. Administrations and Staff Offices. Each administration and staff office shall participate in the ERM process and adhere to this directive. This responsibility does not need to be achieved through the establishment of a formal risk office. Administration and staff office ERM responsibilities are to:

(1) Adhere to the ERM framework, directive, and all applicable tools/methodologies referenced therein.

(2) Identify risks in accordance with VA's risk identification process and report risks that meet the criteria for escalating enterprise risk to OERM.

(3) Provide OERM with points of contact to participate in the SRA, CRA, and RMP processes.

(4) Work with risk sponsors to implement risk response plans and provide regular updates on risk response effectiveness.

(5) Appoint ERMWG members, risk sponsors, and other appropriate representatives to work within the ERM framework.

(6) Review and approve risk information escalated to OERM.

(7) Collaborate with OERM, senior leaders, and supporting staff that administer other VA management processes.

f. Risk Sponsor. The risk sponsor is designated as the person responsible for participating in the risk identification, assessment, prioritization, response, monitoring and reporting of a particular enterprise risk that becomes part of VA's Top Risk Register. The Risk Sponsor shall:

(1) Participate in risk management training designed by OERM.

(2) Conduct or participate in risk assessments. After identifying potential top risks and prioritizing which ones will go forward for full assessment, risk owners will participate in risk assessments to inform whether they qualify as a top risk that will go forward for reporting to the RGB.

(3) Develop risk response strategies and action plans. As part of the assessment, risk owners will either document current risk response strategies or propose new ones; secondly, after a top risk has been presented to the RGB and the RGB direct. -So that risk owners will work with OERM to conduct deep dive analysis and develop more robust risk response strategies.

(4) Monitor risks within established thresholds. For the top risks that have been approved by the RGB, risk owners will establish risk tolerance thresholds for monitoring acceptable risk levels.

(5) Report on risks according to standards. For top risks or emerging top risks, risk owners will monitor and report on status of risk profiles in preparation for updating the RGB at least semi-annually.

4. DECISION AUTHORITY

a. The decision authority describes the ability of key VA ERM roles to approve, ratify, and recommend certain actions. SECVA is the ultimate decision authority of the RGB and VA's ERM program.

(1) Approval. The RGB shall have Department-wide authority to review and either adopt, accept, appoint, amend, modify, disapprove, or return for further consideration an action recommended or approved by OERM or the risk sponsor.

(2) Ratification. The RGB shall have the authority to accept or reject, without imposing an alternative, an action recommended by OERM or the administrations or staff offices.

(3) Recommend. OERM with counsel from administrations and staff offices, shall have the authority to initiate an action for consideration and approval or ratification. OERM, with counsel from administrations and staff offices, shall have the authority to provide information or guidance aimed at resolving a problem or difficulty.

5. REFERENCES

a. VA Strategic Plan Refresh Fiscal Year 2011 – 2015

b. VA Enterprise Risk Management Memo (VAIQ 7318792**)**

c. OMB Circular A-123, Management's Responsibility for Internal Control

d. COSO Enterprise Risk Enterprise Management— Understanding and Communicating Risk Appetite, January 2012

e. OMB Memo: Updated Principles for Risk Analysis, September 2007

6. DEFINITIONS

a. Emerging Risk. A risk that is either not widely known, not currently recognized at an actionable level within the organization, or known within the organization but has not been elevated to leadership. Emerging risks can also be enterprise risks.

b. Enterprise Risk. A risk that has broad or far-reaching implications for VA as a whole and includes risks to: healthcare, cemeteries, benefits, mission support, planning and management, regulatory and compliance issues, and external factors.

c. 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.

d. Issue. An existing event or condition that an organization must address to achieve its mission.

e. Mitigation. An action to reduce, transfer or eliminate risk, which affects the likelihood or the impact of a risk.

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

g. Risk Appetite. The amount of risk an entity is willing to accept in pursuit of its mission. Risk appetite reflects the risk management philosophy and in turn influences the entity's culture, operating style, and decisions. Risk appetite is directly related to strategy, and stakeholder expectations.

h. Risk Assessment. The process of evaluating and estimating risk in comparison to an acceptable level of exposure; used for the purpose of informing priorities, developing or comparing courses of action, and informing decision making.

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

j. Risk Prioritization. Ranking a set of risks on a highest-to-lowest scale according to their respective value and the organization's vulnerability to them. This helps determine which risks need to be considered for management attention, response, and/or monitoring.

k. 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.

l. Risk Register. A central repository of information and associated data elements related to all identified risks; includes sub-sections for the TRR and risks identified during the CRA process.

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

n. Risk Taxonomy. Grouping of risks into categories/subcategories to establish a structure for consistent classification of risks to identify, measure, monitor, report risk management activity and communicate risk information.

o. Risk Tolerance. The acceptable variation in outcomes linked to objectives the organization seeks to achieve.

p. Root Cause. The conditions or events, which, if eliminated or corrected, would prevent a risk from turning into an issue or crisis.