Department of the Interior
Bureau of Ocean Energy Management Manual

Effective Date: 04/02/2025
Series: Administrative
Part 340: Management Accountability and Control
Chapter 1: Enterprise Risk Management

Office of Primary Responsibility: Office of Budget and Administration

BOEMM 340.1

1.1 **Purpose**. The purpose of this manual chapter is to establish the Bureau of Ocean Energy Management (BOEM) Enterprise Risk Management (ERM) Program. ERM is an effective bureau-wide approach for addressing the full spectrum of the bureau's external and internal risks by understanding the combined impact of risks as an interrelated portfolio. By taking a portfolio (or organizational) view of risk, the bureau can better assess which risks are directly related to achieving strategic objectives and which have the highest probability of impacting the mission. This manual chapter provides guidance and sets forth requirements for the bureau to plan, budget, implement, and use results of risk identification and as an element of evidence-based decision making.

1.2 **Scope**. This manual chapter applies to all BOEM employees and offices.

1.3 **Objective**. This chapter identifies responsibilities and procedures for identifying, assessing, and mitigating BOEM strategic risks; using ERM risk for planning and evidence-based decision-making, and reporting ERM information internally and to the Department of the Interior (the Department).

1.4 **Authority**.

A. Office of Management and Budget (OMB) Circular No. A-123, “Management’s Responsibility for Enterprise Risk Management and Internal Control.”

B. OMB Circular No. A-11, “Preparation, Submission, and Execution of the Budget.”

C. Government Accountability Office (GAO-14-704G), “Standards for Internal Control in the Federal Government” also known as the “Green Book.”

D. 112 Departmental Manual (DM) 9, “Office of Planning and Performance Management.”

E. 340 DM 1, “General Policy and Responsibilities."

1.5 **Reference**.

A. International Standard (ISO) 31000:2018, "Risk Management – Guidelines."

B. ISO 31010:2019, "Risk management – Risk assessment techniques."

C. Chief Financial Officers Council (CFOC) and Performance Improvement Council (PIC)'s "Playbook: Enterprise Risk Management for the U.S. Federal Government," dated November 28, 2022.

D. Department of the Interior (DOI) ERM Framework.

E. DOI ERM Governance Charter.

1.6 **Definitions**. Please see the glossary in Appendix 1.

1.7 **Policy**. It is the policy of BOEM to monitor its risk register continuously and update it at least quarterly, implement its ERM program through appropriate BOEM governance processes, and provide timely risk information to the Department.

1.8 **Responsibilities**.

A. Director.

(1) Approves/signs BOEM's end-of-year organizational and enterprise risk assessments due to the Department.

(2) Elevates other bureau risks to the Assistant Secretary or higher through the Department's Risk Management Council (RMC) and other appropriate channels.

B. Deputy Director.

(1) Approves proposed revisions to the BOEM governance charter that covers ERM, internal controls, and audit follow-up in consultation with charter members.

(2) Chairs the BOEM governance body over ERM, internal controls, and audit follow up.

(3) Consults on, reviews, and approves BOEM's risk appetite and risk tolerance statements based on BOEM goals, objectives, and authority.

(4) Consults on, reviews, and surnames BOEM organizational and enterprise risk assessments due to the Department.

C. Associate Director, Office of Budget and Administration (OBA).

(1) Consults on, reviews, and surnames the BOEM governance charter that covers ERM, internal controls, audit follow-up, and BOEM organizational and enterprise risk assessments due to the Department.

(2) Serves as the Executive Director for the BOEM governance body that covers ERM, internal controls, and audit follow up.

(3) Consults on the BOEM's risk appetite and risk tolerance statements based on BOEM goals, objectives, and authority.

(4) Approves/signs BOEM annual ERM and Internal Control Program (ICP) Guidance.

D. Branch Supervisor, Administration and Compliance, OBA.

(1) Supervises the BOEM ERM/ICP Program Lead.

(2) Consults on, reviews, and surnames BOEM annual ERM and ICP Guidance and BOEM organizational and enterprise risk assessments due to the Department.

E. ERM/ICP Program Lead.

(1) Represents BOEM at Departmental or interagency ERM meetings.

(2) Develops, maintains, and obtains leadership approval for BOEM ERM directives and delegations and the BOEM governance charter that covers ERM, internal controls, and audit follow-up.

(3) Provides staff support for the BOEM governance body that covers ERM, internal controls, and audit follow-up.

(4) Serves as a liaison to other BOEM management teams to coordinate and document special projects assigned as risk treatments.

(5) Serves as Chair of the BOEM working group that covers ERM, internal controls, and audit follow up.

(6) Develops (through coordination with the BOEM working group that covers ERM, internal controls, and audit follow-up and other functional area leads) and obtains leadership approval for BOEM's risk appetite and risk tolerance statements based on BOEM goals, objectives, and authority.

(7) Develops, signs, and issues BOEM annual ERM and ICP Guidance.

(8) Develops and delivers broad-based and role-based ERM and ICP training.

(9) Develops and obtains leadership approval for BOEM organizational and enterprise risk assessments due to the Department through coordination with the BOEM working group that covers ERM, internal controls, and audit follow-up and other functional area leads.

(10) Maintains all ERM and ICP records in a central location accessible to the governance charter and working group members.

F. Audit Liaison Officer.

(1) Consults on BOEM governance charter that covers ERM, internal controls, and audit follow up; BOEM annual ERM and ICP guidance; and broad- and role-based ERM and ICP training.

(2) Provides staff support for the BOEM governance body that covers ERM, internal controls, and audit follow up.

(3) Serves as a member of the BOEM working group that covers ERM, internal controls, and audit follow up. As a member, ensures information and recommendations from external audits and evaluations are incorporated into ERM/ICP practices.

G. Senior Leadership Team (Associate Directors, Office Directors, Regional Directors, and the Chief of Staff)

(1) Consult on revisions to the BOEM governance charter that covers ERM, internal controls, and audit follow-up in consultation with members of the BOEM governance body that covers ERM, internal controls, and audit follow up.

(2) Serve as members of the BOEM governance body that that covers ERM, internal controls, and audit follow up.

(3) Assign staff to serve on the BOEM working group that covers ERM, internal controls, and audit follow up.

(4) Serve as Risk Owners accountable for assigning resources to treat (avoid, mitigate (reduce), share or transfer, or accept) BOEM risks identified through appropriate governance and analytical processes.

H. BOEM Working Group (that covers ERM, internal controls, and audit follow up).

(1) Provide input on draft ERM, ICP, and audit follow-up directives, guidance and training materials.

(2) Attend and participate in Working Group meetings organized by the ERM/ICP Lead (Working Group Chair).

(3) Attend governance body meetings organized by the ERM/ICP Lead and the Director's Office as presenters, voting proxies, or subject matter experts (SMEs).

(4) Consult on and contribute information to BOEM's ERM Risk Register (at least quarterly) and other annual risk assessments.

(5) Consult on the scope and frequency of BOEM risk treatments (in the form of internal reviews or evaluations).

(6) Consult on and help develop, along with other SMEs, evidence to support closure requests for external audits and internal reviews.

(7) Participate in ERM, ICP, and audit follow-up training offered or promoted by DOI and BOEM. Integrate training and guidance into office work plans.

(8) Coordinate, prepare, and submit the office-level annual assurance statements on internal control to OBA and provide additional updates for the bureau's annual assurance statement on internal control.

1.9 **Procedures**.

A. The BOEM ERM Program procedures implement overarching Federal ERM policy and DOI ERM frameworks, directives, and guidance.

B. See Appendix 2 for a more detailed description of BOEM ERM procedures.

1.10 **Reporting Requirement/Forms**. The Department requires bureaus and equivalent offices to prepare, regularly update, and report enterprise and bureau or equivalent office risks on a risk register approved by leadership as defined by Departmental guidance. Other organizational risks are updated annually and reported as defined in separate Departmental guidance. BOEM issues specific instructions, forms, and templates to accomplish these requirements in its annual ERM and ICP guidance.

Appendix 1

Glossary

1. **Consequence**. The outcome of an event that affects objectives. A consequence can have positive or negative, direct or indirect, effects on objectives and can be expressed qualitatively and quantitatively. Any consequence can escalate through cascading or cumulative effects.

2. **Context**. The process of defining the scope, objectives, and criteria for risk management within an organization. Context helps to align the risk management strategy with the organization's goals, culture, and external environment. Context also helps to identify and prioritize the most relevant and significant risks that may affect the organization's performance.

3. **Effect**. A deviation from the desired outcome which can be negative (weaknesses or threats) or positive (opportunities).

4. **Enterprise Risk**. A risk that significantly affects the Department's ability to achieve its mission and typically spans across multiple bureaus, offices, operations, and programs.

5. **Enterprise Risk Management Program**. An enterprise-wide, strategically aligned portfolio view of DOI risks and risk treatments that offers improved insight about how to prioritize and manage risks and better inform planning and strategies to ensure effective mission delivery.

6. **Entity**. An entity is a general term for something that exists separately from other things and has a clear identity of its own. Examples in the Department are bureaus and equivalent offices.

7. **Entity-Level Risk**. A type of risk that affects the entire organization or entity, rather than a specific process, activity, or account. Entity-level risks are usually related to the environment, culture, governance, strategy, or objectives of the organization. They can have a pervasive impact on the financial statements and the internal control system of the entity.

8. **Event**. An event (in the context of risk) is when a risk is realized (i.e., it has happened).

9. **Framework**. A set of principles and procedures that help an organization manage anticipated risks so that it can successfully achieve its objectives.

10. **Governance and Managerial Oversight**. The processes and structures that ensure the effective implementation and execution of ERM within an organization. This involves setting the risk management strategy, policies, and objectives, as well as assigning roles and responsibilities, establishing risk reporting and communication, mechanisms, and monitoring and reviewing the performance and outcomes of the ERM Program. Some of the key elements of governance and managerial oversight of an ERM Program are:

A. Risk Governance Framework. The set of principles, policies, and procedures that define the scope, objectives, and criteria for risk management within the organization. It also defines the risk appetite, risk tolerance, risk categories, risk measurement, and risk response strategies for the organization.

B. Risk Governance Board. The highest governing body that oversees the ERM Program and its framework. It consists of senior executives, board members, and other stakeholders who are responsible for setting the risk management vision, strategy, and objectives, as well as approving the risk governance framework and ensuring its alignment with the organization's goals and culture. In BOEM, this is the governance body over ERM, internal controls, and audit follow up. Additional governance body procedures are outlined in the BOEM governance charter, which is a document reviewed annually to ensure authorities, scope, membership, and organizational alignment are still relevant.

C. Risk Management Team. The team that implements and executes the ERM Program and its framework. It consists of risk managers, risk owners, risk coordinators, and other risk practitioners who are responsible for identifying, assessing, managing, monitoring, and reporting on risks within the organization. In BOEM, this is the BOEM working group that covers ERM, internal controls, and audit follow up, together with the BOEM SMEs they consult.

D. Risk Reporting and Communication. The process of providing timely and relevant information on the organization's risk profile, risk exposure, risk performance, and risk response to the risk governance board, senior management, business units, and other stakeholders. It also involves creating a culture of risk awareness and accountability within the organization. In BOEM, this includes the risk register and summary or extracted information for different target audiences.

11. **Inherent Risk**. The risk to an entity or outcome, prior to applying risk treatments.

12. **Internal Controls**. Processes and procedures used by management to achieve goals. In the context of this guidance, internal controls are a form of risk treatment to mitigate risk. Risk mitigation (or reduction) typically includes management and governance policies, procedures, requirements, checks and balances, training, and other protocols that, taken together, help management achieve outcomes and safeguard the integrity of programs.

13. **Likelihood**. The chance of something occurring. This is commonly used in determining the probability of an event happening.

14. **Magnitude of Impact**. Severity of deficiency that could result from a risk and is affected by factors such as the size, pace, and duration of the risk's impact.

15. **Monitoring**. Monitoring is a key activity and phase that plays a crucial role in ensuring an organization's resilience and preparedness for appropriately treating risks. Monitoring occurs across the spectrum of activities in ERM, including monitoring of internal and external drivers of risks and monitoring risk treatments to assess their effectiveness when implemented.

16. **Residual Risk**. The risk to an entity or outcome, after applying risk treatments or accepting the risk without treatments applied.

17. **Risk**. The effect of uncertainty on achieving DOI or BOEM strategic objectives, as determined by its likelihood and impact. The four specific forms of risk required in OMB Circular A-123 to be reported and assessed, include the following:

A. Strategic Risk. The risk of failing to achieve stated goals and objectives (business strategy) of the organization (e.g., risk to the Secretary's initiatives or BOEM strategic framework objectives).

B. Operational Risk. The uncertainty (threat) an organization faces while conducting its daily business activities, procedures, and (e.g., cannot hire sufficient engineers, a specific tool is out of date).

C. Reporting Risk. A lack of reliable information (internal, external, financial, non-financial reporting) which may impact decision making within DOI and/or erode confidence outside the entity.

D. Compliance Risk. The risk of failing to comply with laws, policies, or executive orders (e.g., workplace health and safety, process risk, and privacy breaches).

18. **Risk Appetite**. The broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision (and objectives). It is established by the organization's most senior level leadership and serves as the guidepost to set strategy and select objectives.

19. **Risk Assessment**. A three-step process described in the ISO 31000 standard:

A. Risk Identification. The process of finding, recognizing, describing, and recording risks to achieving the objectives of an organization.

B. Risk Analysis. The process of comprehending the nature of the risk and its characteristics, using qualitative and quantitative methods to determine:

(1) The drivers (sources) of risks and their root causes;

(2) Effectiveness of current risk treatments;

(3) Likelihood and impact of identified risks if they occur; and

(4) Risk rating and prioritization.

C. Risk Evaluation. The process of using the information developed and documented in the first two steps of risk assessment to support the organization's decisions of whether to treat or accept the risk as is.

20. **Risk Champion**. A member of leadership, management, or an employee who promotes risk management best practices in accordance with the DOI's ERM policy and guidance.

21. **Risk Drivers**. Factors or variables that influence the likelihood, impact, or timing of risks. Drivers are the root causes or sources of risks, such as market conditions, stakeholder expectations, or technical issues. Their identification is an essential aspect of formal risk management as these are the activities that lead to or trigger a risk to occur. Risk drivers play an essential role during risk analysis and the determination of root causes, the identification phase of any risk management activity.

22. **Risk Management Council**. The DOI Enterprise Risk Management Council (RMC) is a governing body that is responsible for overseeing the enterprise-wide approach to addressing department-level risks. The RMC is tasked with identifying, assessing, and preparing for the most impactful risks to DOI faces, including strategic, financial, compliance/legal, reputational, organizational, and IT risks. The RMC ensures that risks are managed in a holistic manner, considering the combined impact of various risks as an interrelated portfolio, rather than addressing them in isolation.

23. **Risk Officer**. A professional responsible for coordinating the entity's risk management program, who serves as an advisor to the governance body (risk governance board). In BOEM, this is the ERM/ICP Program Lead.

24. **Risk Owners**. The headquarters function or program or regional office manager, director, or staff members with the authority to treat (or manage) risks affecting the activities, operations, and outcomes of that organization. In BOEM, these are primarily the Associate Directors, Office Directors, and Regional Directors for accountability, while risk treatment implementation may be delegated to other managers and staff.

25. **Risk Profile**. A compilation of risks extracted from the risk register. Agencies must annually develop a risk profile coordinated with their annual strategic reviews. The risk profile differs from a risk register in that it is a prioritized inventory of the most significant risks identified and assessed through the risk assessment process versus a complete inventory of risks.

26. **Risk Register**. A summary of significant risks to the entity and risk treatments designed to inform leadership of high-level risks impacting the agency. Bureau Risk Officers will establish and maintain risk registers for their bureau or equivalent office. Bureau or equivalent office risk registers are integrated into an enterprise DOI risk register and facilitate enterprise-wide analysis.

27. **Risk Tolerance**. The level of risk that an organization is willing to accept for a specific risk and is typically set by management in normal operations. Risk tolerance is related to the acceptance of the outcomes of a risk should it occur and having the right resources and controls in place to increase the given exposure to an opportunity or decrease the given exposure to a threat. Organizations typically define this risk tolerance by establishing a residual risk threshold (when the risk calculation results in a value equal to or greater than a certain numerical value, the organization determines the risk requires a risk treatment).

28. **Risk Treatment**. The process of selecting and implementing one or more treatment options to treat risks. A risk treatment system generally consists of the policies, plans, procedures, and process assessments established to provide:

A. Evidence of how risks are managed and objectives are achieved;

B. Evidence that risk treatments are appropriate, complete, and effective; and

C. Evidence that evidence related to risk can be used in decision making.

This system enables risk owners to select the appropriate risk treatment options (avoid, share or transfer, mitigate (reduce), or accept).

29. **Root Cause**. A root cause is the fundamental reason or underlying factor (highest level cause) that initiates the cause-and-effect reaction that leads to the risk event. It is the main cause that, when properly treated or addressed, can prevent the recurrence of the risk in the future. Identifying the root cause involves analyzing and understanding the various contributing factors that can lead to the risk event, enabling effective and targeted treatments.

30. **Root Cause Analysis**. The process of identifying the root cause that could result in a risk becoming an event. The analysis involves understanding the various contributing factors that can lead to the problem or issue, enabling effective and targeted treatments.

31. **Strategic Reviews**. Strategic reviews are conducted on an annual basis as required in OMB Circular No. A-11. The purpose is to report to OMB the status of meeting the goals and objectives of DOI's strategic plan. OMB Circular No. A-123 requires that a risk profile be available to support the strategic review and be utilized to identify assessed risks to the goals and objectives of DOI.

Appendix 2

ERM Risk Register Procedures

Action	Responsible Party
Update BOEM ERM Governance.	BOEM Deputy Director
Establish the BOEM risk appetite.	BOEM Deputy Director
Identify and categorize BOEM current fiscal year (FY) risks (iterative process).	BOEM ERM/ICP Lead, the BOEM working group that covers ERM, internal controls, and audit follow up, and BOEM SMEs
Analyze BOEM current FY risks (iterative and sequential Process as risks are added/modified throughout reporting period).	BOEM ERM/ICP Lead, the BOEM working group that covers ERM, internal controls, and audit follow up; and BOEM SMEs
Identify/select BOEM risk treatments for current FY risks.	BOEM governance body that that covers ERM, internal controls, and audit follow up
Analyze risk treatments.	BOEM ERM/ICP Lead, the BOEM working group that covers ERM, internal controls, and audit follow up
Document review cycle and last date for risk treatment reviews.	BOEM ERM/ICP Lead, the BOEM working group that covers ERM, internal controls, and audit follow up
Select date and name for next risk treatment reviews.	BOEM ERM/ICP Lead, the BOEM working group that covers ERM, internal controls, and audit follow up,
Scope/plan and execute planned current FY risk treatment reviews.	BOEM Deputy Director, BOEM governance body that that covers ERM, internal controls, and audit follow up; the BOEM working group that covers ERM, internal controls, and audit follow up
Document/report current FY risk treatment review results and corrective action plans.	BOEM ERM/ICP Lead, the BOEM working group that covers ERM, internal controls, audit follow up, and BOEM SMEs
Submit BOEM final current FY ERM risk register.	BOEM Director and BOEM ERM/ICP Lead