

# BPA Policy 231-1

## Enterprise Risk Management

### Compliance, Audit and Risk

#### Table of Contents

1.1 Purpose & Background .....	2
1.2 Policy Owner .....	3
1.3 Applicability.....	3
1.4 Terms & Definitions .....	3
1.5 Policy .....	3
1.6 Policy Exceptions.....	4
1.7 Responsibilities .....	4
1.8 Standards & Procedures .....	6
1.9 Performance & Monitoring.....	7
1.10 Authorities & References.....	7
1.11 Review.....	8
1.12 Revision History .....	8



## 1.1 Purpose & Background

This policy establishes the Bonneville Power Administration's (BPA) policy for managing risk systematically across the enterprise.

A. **Vision:** BPA's risks are within acceptable tolerances through the application of a robust Enterprise Risk Management (ERM) program.

B. **Philosophy for practicing ERM:** BPA considers the management of risk to be an integral part of good management and has committed to embedding risk management into existing practices and business processes so that it becomes part of BPA culture and is not viewed as an independent activity. Over time, this will allow everyone at BPA to be involved in the disciplined management of risk.

BPA has traditionally managed numerous individual risks using a variety of tools and techniques, many of which have become quite well developed. Now, BPA is integrating these widespread efforts into an enterprise-wide, disciplined approach. BPA's risks are becoming more profound, and the interactions among risks are increasingly complex. Therefore, BPA is committed to practicing ERM to:

1. Increase the likelihood of successfully delivering on its goals and objectives
2. Encounter fewer unanticipated outcomes
3. Better assess risks associated with changes in its environment
4. Better describe to customers and other stakeholders what BPA is doing to manage its risks.

C. **ERM program objectives:** This policy serves to support the following ERM objectives.

1. BPA's strategic objectives are clearly defined, measurable, and reflect the agency's risk tolerance.
2. Top tier enterprise risks to strategic objectives are identified and addressed through a consistent and disciplined process.
3. Emerging risks to agency objectives are dynamically identified and managed.
4. Decisions and policy are based on a complete and shared understanding of objectives and a robust consideration of risks to delivering on, and alternative means for achieving, those objectives.
5. Consistent and disciplined consideration and treatment of risk is part of our day-to-day processes; risk management is a visible and integral part of BPA culture.

D. **Additional guidance:** To better understand and interpret this policy, BPA maintains an ERM procedures handbook that describes the application of this policy in more detail.

Organization <b>Compliance, Audit and Risk</b>		Title/Subject <b>Enterprise Risk Management</b>		Unique ID <b>231-1</b>	
Author <b>D. Jensen</b>	Approved by <b>EVP Compliance, Audit &amp; Risk: T. McDonald</b>	Date <b>August, 26, 2015</b>	Version <b>#2</b>	Page <b>2</b>	

## 1.2 Policy Owner

The Executive Vice President of Compliance, Audit and Risk working through the Chief Risk Officer or his/her designee has overall responsibility for monitoring, reporting, deploying, evaluating, and proposing revisions to this policy.

## 1.3 Applicability

BPA employees.

## 1.4 Terms & Definitions

- A. **Risk:** The effect of uncertainty on achievement of objectives. An effect is a deviation from the expected – positive and/or negative. Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.
- B. **Risk assessment:** The overall process of risk identification, risk analysis, and risk evaluation.
- C. **Risk tolerance:** The measure of the level of risk which an individual or company is willing to accept without further treatment.
- D. **Risk-informed:** BPA uses this term to mean the following elements are present in a process, activity, project, etc.: 1) use of a logical and systematic process; 2) common understanding of objectives and context; 3) robust consideration of risks to achievement of objectives; 4) identified risks are addressed consistent with agency risk tolerance; and 5) consideration of a broad set of alternatives using a consistent set of criteria.
- E. **Enterprise Risk Management (ERM):** A strategic business discipline that supports the achievement of an organization’s objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio. ERM provides a disciplined process for managing risk and seeks to embed this discipline in existing business processes.
- F. **Corrective Action Program (CAP):** The combination of the internal policies, procedures, tools, and staff resources that support consistent investigation of significant events, identification and validation of causes, and development of corrective actions, tracking of implementation and verification of effectiveness of those corrective actions.
- G. **Root Cause Analysis (Level 1):** The first stage in determining the possible cause(s) of a particular problem through data collection and analysis.

## 1.5 Policy

- A. **Strategic direction:** BPA’s mission, vision, and core values drive its long-term strategy which in turn is realized by meeting its long-term strategic objectives. Strategic objectives set the foundation for BPA’s ERM efforts since risk management is geared

Organization <b>Compliance, Audit and Risk</b>		Title/Subject <b>Enterprise Risk Management</b>		Unique ID <b>231-1</b>	
Author <b>D. Jensen</b>	Approved by <b>EVP Compliance, Audit &amp; Risk: T. McDonald</b>	Date <b>August, 26, 2015</b>	Version <b>#2</b>	Page <b>3</b>	

towards managing the risks that could impact agency objectives. BPA sets its strategic objectives and manages risk in accordance with the following principles:

1. BPA establishes its strategic business objectives in a risk-informed manner.
2. BPA establishes measurable agency targets that define what it means to be successful in achieving its strategic business objectives.
3. BPA constantly evaluates its tolerance for failing to deliver on its strategic business objectives (i.e., BPA’s risk tolerance).

**B. Agency risk tolerance:** BPA operates the FCRPS by managing its risks within acceptable bounds so as to maintain the value of this resource for the regional stakeholders of the Northwest. An explicit discussion of risks and risk tolerance is part of BPA’s decision making process.

**C. Risk-informed decision making & operations:** Rigorous, risk-informed decision making is critical to BPA’s success. The Agency Decision Framework (ADF) and capital investment business cases, where applicable, are the principle means to integrate and document risk management in decision making. These tools reflect the application of the principles in the BPA risk management process. Please refer to the ADF and asset management policies listed in the “References” section for more information. BPA employees and contractors are expected to conduct their work and make decisions in a risk-informed manner.

Organizational units embed the principles of the risk management process into their business operations and processes so that they can effectively manage the risks that have a material impact on their objectives. Organizational units establish, in consultation with ERM staff as needed, thresholds above which formal documentation of this process is required.

**D. Best Practices:** As part of BPA’s dedication to operational excellence, BPA maintains ongoing awareness of evolving best practices connected with enterprise risk management, and invests in ERM-related governance and business processes to a degree that is fiscally and operationally prudent.

## 1.6 Policy Exceptions

None.

## 1.7 Responsibilities

Key roles and responsibilities for supporting BPA’s Enterprise Risk Management approach are:

**A. The Executive Vice President, Compliance, Audit and Risk:** Approves risk management policies and identifies top enterprise risks.

Organization <b>Compliance, Audit and Risk</b>		Title/Subject <b>Enterprise Risk Management</b>		Unique ID <b>231-1</b>	
Author <b>D. Jensen</b>	Approved by <b>EVP Compliance, Audit &amp; Risk: T. McDonald</b>	Date <b>August, 26, 2015</b>	Version <b>#2</b>	Page <b>4</b>	

- B. The Enterprise Risk Management Committee (ERMC):** Is the lead risk management committee that oversees a rigorous and coordinated approach to assessing and responding to risks that affect the achievement of BPA’s objectives. The ERMC provides a dedicated forum for advancing ERM and for monitoring the overall effectiveness of BPA’s risk management efforts. The ERMC approves all risk management policies and then recommends them to the Administrator for final approval. Specific duties of the ERMC are outlined in the ERMC charter.
- C. Management Committees:** BPA’s other decision making bodies such as the Executive Board, Capital Allocation Board (CAB), Business Operation Board (BOB), Audit and Internal Controls Committee (AICC), and Business Unit Management Committees (MCs), Business Continuity Steering Committee (BCSC), and Agency Strategy Forum (ASF). Executives ensure that decisions made in these forums are risk-informed and that staff uses accepted agency methodologies for assessing risks.
- D. The Transacting Risk Management Committee (TRMC):** Serves as a subcommittee of the ERMC. The purpose of the TRMC is to oversee BPA’s commodity transacting risks by implementing ERMC approved transacting risk policies. Specific TRMC duties are outlined in the TRMC charter.
- E. The Business Continuity Steering Committee (BCSC):** Serves at the behest of the ERMC and is accountable for agency-wide resilience, response, and recoverability.
- F. Executive Board:** Promotes and assures effective risk management within BPA. Board members set the tone at the top by providing constructive feedback on ADFs, capital investment business cases, and other applications of the risk management process.
- G. Corrective Action Review Board (CARB):** Ensures that a Level 1 causal analysis and corresponding corrective actions meet BPA’s guidelines. The CARB is the ultimate committee to review and approve Level 1 corrective action plans. The CARB provides support and direction for the Corrective Action Program. Specific duties of the CARB are outlined in the CAP guide.
- H. The Chief Risk Officer (CRO):** Leads the Risk Management group which is comprised of Enterprise Risk Management and Transacting and Credit Risk Management. The CRO is responsible for a comprehensive risk management program, which entails proposing risk vision, strategy, policies, and philosophy regarding risk tolerance to executive management. Specific duties of the CRO are outlined in the ERM Procedures Handbook.
- I. The Enterprise Risk Manager (ERM Manager):** Reports to the CRO and is responsible for ensuring the consistent implementation of BPA’s ERM program throughout BPA. The ERM Manager develops, administers, and helps interpret the ERM policy. Specific duties of the ERM Manager are outlined in the ERM Procedures Handbook. The ERM Manager is responsible for the development, maintenance and implementation of the Corrective Action Program at BPA.

Organization <b>Compliance, Audit and Risk</b>		Title/Subject <b>Enterprise Risk Management</b>		Unique ID <b>231-1</b>	
Author <b>D. Jensen</b>	Approved by <b>EVP Compliance, Audit &amp; Risk: T. McDonald</b>	Date <b>August, 26, 2015</b>	Version <b>#2</b>	Page <b>5</b>	

- J. **The ERM staff:** Conduct/facilitate risk assessments on key strategies, major projects, and initiatives. The staff assists employees and managers through risk management training and consultation. The staff also develops, administers, and helps interpret the ERM policy. Specific duties of the ERM staff are outlined in the ERM Procedures Handbook. An ERM staff member with training in root cause analysis will be the team lead for all Level 1 root cause analyses and corrective action plan development.
- K. **Internal Audit:** Coordinates with the ERM function to design and perform assurance audits to verify the level of compliance of BPA with this policy and associated risk management-related processes and procedures. Internal Audit provides other audit services that support ERM, including periodically determining the effectiveness of risk management education across BPA and generally promoting greater risk management awareness.
- L. **All employees:** Responsible for risk management at BPA and reporting events that may require corrective actions. All executives, managers, staff, and contractors have an important role in managing risk across the enterprise. They are expected to make and support risk-informed decisions and remain vigilant in watching for emerging risk issues that could jeopardize BPA’s success. To the extent that any employee or contract staff becomes aware of what appears to be a significant risk-related issue or an event that may require a corrective action, the employee should notify his or her supervisor or contracting officer’s technical representative so that action may be taken as appropriate.

## 1.8 Standards & Procedures

**BPA risk management process:** BPA’s disciplined approach to risk management is iterative, scalable, and includes the steps below. Consistent application of this process enables continuous improvement in decision making and performance. Please refer to the “References” section for a more detailed explanation of the risk management process.

- A. **Communication and dialog:** Communication and dialog with internal and, as appropriate, external stakeholders as far as necessary takes place at each stage of the risk management process.
- B. **Establishing the context:** This defines the internal, external, and risk parameters to be taken into account when managing risk, and setting the scope and risk criteria for the remaining process.
- C. **Risk identification:** The purpose of this step is to generate a comprehensive list of risks based on those events that might enhance, prevent, degrade, or delay the achievement of the objectives.
- D. **Risk analysis:** Risk analysis is about developing an understanding of the risk by considering the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur. Existing risk controls and their effectiveness should be taken into account.

Organization <b>Compliance, Audit and Risk</b>		Title/Subject <b>Enterprise Risk Management</b>		Unique ID <b>231-1</b>	
Author <b>D. Jensen</b>	Approved by <b>EVP Compliance, Audit &amp; Risk: T. McDonald</b>	Date <b>August, 26, 2015</b>	Version <b>#2</b>	Page <b>6</b>	

- E. **Risk evaluation:** The purpose of risk evaluation is to assist in making decisions based on the outcomes of risk analysis about which risks need treatment and to prioritize treatment implementation for those unacceptable risks (i.e. those that exceed risk tolerance.)
- F. **Risk treatment:** This involves selecting one or more options for modifying unacceptable risks and implementing those options. Risk treatment options include: avoiding the risk, seeking out an opportunity, removing the source of risk, changing the likelihood, changing the consequence, sharing the risk with another party, and retaining the risk by choice.
- G. **Corrective Action Program:** This program ensures that responsible agency organizations effectively analyze root causes and implement corrective actions for events having the most significant impacts on BPA’s mission, vision, or core values. The Corrective Action Program is an agency resource that provides guidance, training and assistance to groups within BPA that are addressing significant events. The implementation of the Corrective Action Program supports BPA’s risk management philosophy by treating significant risks through the reduction of the consequences and/or likelihood of those events happening again.

## 1.9 Performance & Monitoring

- A. **Monitoring and review:** Encompasses all aspects of the risk management process to:
  1. Analyze and learn lessons from events, changes, and trends.
  2. Detect changes in the external and internal context including changes to the risk itself.
  3. Ensure that the risk controls and treatment measures are effective in both design and operation.
  4. Identify emerging risks.
- B. **Governance and Compliance:** The BPA Internal Audit department designs and conducts, or arranges for outside specialists to conduct, audits and assessments of BPA’s compliance with this policy and associated procedures. Internal Audit coordinates with the ERMC to determine the focus of each audit or assessment. The results of the audit or assessment are presented to the ERMC and reported to the Administrator.

The ERMC assures that BPA’s ERM competency is assessed via a structured ERM maturity model. The purpose of this review is to ascertain the overall level of quality and implementation effectiveness of BPA’s ERM program. The results of the assessment are presented to the ERMC and reported to the Administrator.

## 1.10 Authorities & References

- A. BPA ERM Procedures Handbook (pending)

Organization <b>Compliance, Audit and Risk</b>		Title/Subject <b>Enterprise Risk Management</b>		Unique ID <b>231-1</b>	
Author <b>D. Jensen</b>	Approved by <b>EVP Compliance, Audit &amp; Risk: T. McDonald</b>	Date <b>August, 26, 2015</b>	Version <b>#2</b>	Page <b>7</b>	

- B. ISO 31000 Risk Management Standard
- C. BPA Likelihood and Impact Scales
- D. BPA Business Risk Framework
- E. BPA Business Risk Inventory
- F. Transacting Risk and Credit Policies
- G. Business Continuity Policy
- H. Asset Management Policy
- I. ERM Charter
- J. TRM Charter
- K. AICC Charter
- L. BCSC Charter
- M. BPA Manual Chapter 21.5 – Decision Making using Agency Decision Framework
- N. OMB Circular A-123: Appendix A
- O. CAP Guide
- P. CAP Handbook

### 1.11 Review

This policy is scheduled for review in 2020.

### 1.12 Revision History

Version	Issue Date	Description of Change
2	08-26-2015	Migration of content to new policy format.

Organization <b>Compliance, Audit and Risk</b>		Title/Subject <b>Enterprise Risk Management</b>		Unique ID <b>231-1</b>	
Author <b>D. Jensen</b>	Approved by <b>EVP Compliance, Audit &amp; Risk: T. McDonald</b>	Date <b>August, 26, 2015</b>	Version <b>#2</b>	Page <b>8</b>	