RISK MANAGEMENT TOOLKIT FOR PUBLIC POWER UTILITIES

AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

VOLUME I: RISK IDENTIFICATION

SEPTEMBER 2024

This material is based upon work supported by the Department of Energy under Award Number DE-CR0000012.

The American Public Power Association is the voice of not-for-profit, community-owned utilities that power 2,000 towns and cities nationwide. We represent public power before the federal government to protect the interests of the more than 54 million customers that public power utilities serve across the United States and its territories. We advocate and advise on electricity policy, resilience, cybersecurity, grid operations, technology, trends, and training.

Table of Contents

Introduction 4
Background 4
Volume I: Risk Identification 4
Objectives 4
Importance and Benefits of ERM 5
ERM Overview 5
ERM Foundational Concepts 6
Advocating for an ERM Program 7
Key Steps to Securing Leadership Buy-In 7
Local Resources to Jumpstart ERM Program 7
ERM Stakeholder Roles and Responsibilities 8
Crafting Strategic Objectives for the ERM Program 9
The Process for Identifying Risks 9
Approach to the Risk Identification Process 10
Conducting Risk Identification Workshops 11
Developing a Risk Register 12
Risk Register Development in Excel Spreadsheet 13
Best Practices for Right-Sizing the Risk Register 13
From Risk Identification to Risk Assessment 14
Appendix A: ERM Stakeholder Roles and Responsibilities Template 15
Appendix B: Examples of Real-World Vision and Mission Statements 16
Appendix C: ERM Program Strategic Objectives Template 17
Appendix D: Sample Risks to Public Power Utilities 18
Appendix E: Sample Risk Identification Workshop Agenda 19
Appendix F: Risk Identification Form Template 20
Attachment 1: ERM Proposal PowerPoint Template
Attachment 2: Risk Identification Workshop Guide
Attachment 3: Risk Identification Workshop PowerPoint Template
Attachment 4: Risk Register Excel Template

Introduction

Background

Public power utilities operate in a complex and evolving environment, facing an array of risks that can significantly impact their operations, financial stability, and ability to deliver reliable service. These risks include but are not limited to natural disasters, cybersecurity threats, regulatory changes, and supply chain disruptions.

The Risk Management Toolkit provides essential guidance and tools for proactively identifying and assessing risks, developing tailored risk management strategies, and effectively communicating risk information to leadership and stakeholders — all of which are a part of an enterprise risk management (ERM) program. The toolkit also includes practices for continuously monitoring and adjusting risk management efforts to adapt to changing conditions. By leveraging this toolkit, utilities can build resilience, ensure sustainable operations, and make informed decisions in the face of evolving risks.

Volume I: Risk Identification

Volume I of this toolkit is designed to support public power utilities in their path to establishing an ERM program. This volume serves as the foundational step in building an ERM framework tailored specifically for the unique needs and challenges of small public power utilities.

Objectives

- Understand the fundamentals of risk and ERM, including the exploration of key concepts and benefits related to implementing an ERM program within public power utilities.
- Learn strategies to effectively present ERM benefits to leadership and secure their support.
- Learn actionable steps to kick-start ERM efforts, from setting up processes to establishing a risk management culture within the utility.
- Discover how to assemble a cross-functional team that will drive the development and execution of the utility's ERM program.
- Explore practical approaches for identifying risks and receive guidance on recognizing potential risks and understanding their impact.

Understanding the Components of Risk

For public power utilities, grasping the interplay between threat, vulnerability, and consequence is crucial for assessing risk and its elements. Risk emerges from the convergence of three aspects: the existence of a threat, the utility's susceptibility to that threat, and the potential outcomes if the threat occurs.

For example, when considering the risk of wildfires, the threat is the wildfire itself. The vulnerability might be the utility's transmission lines that are susceptible to fire damage, and the consequence could be prolonged outages and costly repairs. To manage this risk effectively within the ERM process, utilities must assess each component. They need to evaluate the likelihood of a wildfire occurring, analyze the vulnerability of their assets, and understand the potential impact on operations and customer service. This holistic assessment then informs the

development of mitigation strategies, such as maintaining clear zones around infrastructure and investing in fire-resistant materials, ultimately reducing the overall risk.

Similarly, with cyber threats, the threat could be unauthorized access to control systems, the vulnerability might be gaps in the utility's cybersecurity infrastructure, and the consequence could be widespread outages or data breaches. By systematically addressing these elements — identifying potential cyber threats, evaluating vulnerabilities in IT systems, and assessing the consequences of a breach — public power utilities can prioritize actions within their ERM framework, such as implementing advanced firewalls, intrusion detection systems, and regular security audits.

Incorporating the risk equation into the ERM process allows public power utilities to make informed decisions about where to focus their resources and efforts, ensuring that the most critical risks are managed effectively to maintain reliability, safety, and operational efficiency.

Importance and Benefits of ERM

ERM provides public power utilities with a structured way to identify, assess, and manage risks throughout the utility. This approach ensures strategic and business objectives of providing safe and reliable electric service are met. The benefits of ERM go beyond just managing risks; it helps build a culture of informed decision-making, enhances the utility's ability to withstand various shocks, and allows the utility to seize opportunities by balancing risks and rewards.

ERM offers several benefits to public power utilities.

- Provides a clearer understanding of risks to support better decisions. For example, it helps decide on investments or new projects from a risk perspective.
- Offers insights into both current and developing risks, allowing for proactive management. For instance, spotting potential supply chain issues early can lead to securing alternative suppliers.
- Helps prioritize resources by focusing on high-impact areas.
- Prepares the utility to handle and recover from adverse events, ensuring long-term sustainability. For example, having a disaster response plan ready improves recovery from natural disasters.
- Promotes awareness of risks throughout the utility, enhancing overall strategic thinking and vigilance.
- Helps find and act on growth opportunities by analyzing risk and reward. For instance, market risk analysis might reveal new business prospects.
- Safeguards the utility's reputation and stakeholder confidence, such as by managing compliance risks to avoid legal issues.
- Enhances the ability to respond quickly and effectively in crises, like operational failures or security breaches.

ERM Overview

The goal of ERM is not to eliminate all risks but to manage them within acceptable levels while still reaching the utility's goals. **ERM is an ongoing process requiring continuous effort and engagement from all levels of the utility, not just a one-time setup**. ERM should be integrated into the overall strategy and operations, not handled as a separate or isolated function. In summary, ERM is a comprehensive approach that helps public power utilities manage risks effectively.

ERM Foundational Concepts

Public power utilities should familiarize themselves with fundamental risk concepts[1] to establish a solid understanding of ERM. This knowledge is essential before embarking on the process of building an ERM program.

Inherent risk represents the level of exposure to potential negative outcomes within a process, activity, or system *before* any controls or mitigation efforts are applied. It is the raw risk faced under normal operating conditions and serves as a baseline for understanding overall risk.

- For example, a public power utility might face inherent risks related to equipment failure or supply chain disruptions, such as a transformer breaking down or delays in receiving critical components.

Residual risk is the risk that remains after a utility has implemented controls or mitigation strategies. It reflects the exposure that persists despite efforts to manage and reduce the inherent risks, indicating the effectiveness of risk management measures.

- For instance, after installing backup generators to mitigate power outages, the residual risk might be the possibility of a generator malfunctioning during a blackout.

Public power utilities must gain a basic understanding of the various risks they may encounter. This foundational knowledge is crucial when establishing an ERM program, as it enables utilities to grasp the nuances of different risk types and their implications. Utilities might use broad categories such as strategic, operational, financial, and compliance risks; include additional categories like reputational, technology, and environmental risks; or create more detailed sub-categories.

Strategic risks affect the utility's ability to meet its long-term goals. These risks can come from changes in the industry, competitive pressures, or strategic choices made by the utility.

- For example, a major policy change in energy regulation could be a strategic risk that impacts the utility's ability to achieve its business objectives.

Operational risks are related to the daily functions of the utility. These might include equipment failures, supply chain, process disruptions, or human errors that impact normal operations.

- An example is failure to do normal equipment maintenance, impacting daily operations.

Financial risks concern the utility's financial stability and include market risk, credit risk, liquidity risk, and currency risk.

- For instance, the inability to obtain adequate liability insurance for wildfires is a financial risk.

Compliance risks arise from the need to adhere to laws, regulations, and industry standards. Failure to comply can result in fines, legal issues, and damage to the utility's reputation.

- An example is failing to adhere to safety standards for employees, resulting in legal penalties, fines, and increased workplace accidents.

Reputational risks relate to how stakeholders perceive the utility. Negative publicity, social media backlash, or other damaging events can harm the utility's image.

- For example, the inability to provide power for a significant length of time could lead to a loss of public trust and confidence.

[1] This toolkit employs risk concept definitions as established by the Department of Homeland Security and the Department of Energy.

Technology risks involve cybersecurity threats, data privacy issues, and failures of critical IT systems. Managing these risks is crucial for protecting sensitive information and maintaining reliable technology infrastructure.

- A reputable software provider pushes a patch that causes the software to malfunction (e.g., the July 2024 CrowdStrike incident).

Environmental risks pertain to factors like extreme climate conditions, natural disasters, and sustainability challenges. Addressing these risks is increasingly important due to the emphasis on environmental stewardship and sustainability.

- For instance, a severe weather event that damages infrastructure would be an environmental risk requiring proactive management.

Advocating for an ERM Program

Establishing and advocating for an ERM program within public power utilities is crucial, but can be challenging, particularly for smaller utilities. Successfully embedding ERM involves integrating risk management into the core operations of the utility, rather than merely introducing new procedures.

Key Steps to Securing Leadership Buy-In

- Conduct internal meetings to define the scope of work, develop a project plan, and assess whether external contract support is needed.
- Gain senior leadership support by presenting benefits of ERM to governing board, such as improved decision-making, regulatory compliance, and operational efficiency to leadership.
- Obtain support from governing board.
- Communicate objectives and goals of the ERM program to all stakeholders.
- Provide basic ERM training to all stakeholders if necessary to build understanding and support.

Implementing an ERM program can be overwhelming, especially for smaller utilities with limited resources. In such cases, reaching out to state energy offices can be beneficial. These offices often provide valuable guidance, resources, and potentially even mentorship to support the development and implementation of an ERM program. They may also offer information about funding opportunities or other local resources to assist in overcoming challenges. Below are suggestions for beginning the search for local resources to kickstart the utility's ERM program.

Local Resources to Jumpstart ERM Program

1) **Leveraging APPA's Risk Management Working Group** to join a cohort of risk managers, collaborate, and exchange information specific to risk management.[2]
2) **Engaging with other public power utilities** to exchange best practices and lessons learned, which can then be applied to improve their own ERM programs.
3) **Participating in risk management forums** and networking with other professionals at conferences and events.[3]

[2] Public power utility members can contact aserrame@PublicPower.org to request to join the Risk Management Working Group.
[3] For example, APPA's Business and Financial Conference features sessions on risk management and insurance topics.

4) **Contact state energy offices** to inquire about grants, loans, or other financial assistance programs that could support ERM efforts.
    - Example: The California Energy Commission provides funding for projects that improve energy efficiency and resilience, which can include ERM initiatives.
5) **Collaborate with state energy offices** on joint projects that align with ERM objectives.
    - Example: The Texas State Energy Conservation Office partnered with local utilities to fund projects that enhanced their risk management capabilities through training and technology upgrades.
6) **Request technical assistance, training, or access to risk management tools** provided by the state energy office.

ERM Stakeholder Roles and Responsibilities

Implementing an ERM program in a public power utility requires clear roles and responsibilities for all involved stakeholders. This ensures accountability, fosters collaboration, and maximizes the effectiveness of the ERM program. This structure will vary based on the size of the utility and the current structure of its leadership levels. As a recommendation, utilities should involve three levels of stakeholders[4] when starting their ERM program. Below is a sample structure with roles and responsibilities of each stakeholder.

Role	Positions (may vary per utility)	Responsibilities
Governing Board	• City council • Municipal council • Utility board	• Provide guidance for ERM program • Ensure the ERM program aligns with the utility's strategic goals • Approve the ERM policy and risk strategies • Regularly review risk reports
Senior Leadership (which may make up the utility's risk committee)	• CEO • General Manager • Chief Administrative Officer • Chief Human Resources Officer • Chief Operations Officer • Chief Financial Officer • Chief Technology Officer	• Provide direction and oversight of the ERM program • Create program and strategy • Create and maintain ERM policies • Provide necessary resources for ERM • Track the progress of the ERM program
Business Units	• Utility operations • Human resources • Customer service • Accounting/payroll purchasing • Information technology	• Manage day-to-day risks • Oversee daily ERM activities • Lead risk identification and management activities • Report risks to senior leadership and the governing board

Table 1 – Sample framework of ERM roles and responsibilities aligned with utility organizational structures

[4] For smaller utilities, these three levels of stakeholders may be the same individuals or teams.

- ☐ **Action Item:** Utilize Appendix A to identify and record individuals who will be involved in the risk management committee/team.
- ☐ **Action Item:** Prepare a presentation to communicate the value proposition of establishing an ERM program within the utility. Utilize the Attachment 1: ERM Proposal PowerPoint Template to get started.
- ☐ **Action Item:** Schedule meetings with the utility's senior leadership and governing board to present ERM proposal and start the leadership buy-in process.

Crafting Strategic Objectives for the ERM Program

The ERM mission and vision statements form the core of the ERM program, outlining its purpose and future goals. The mission statement describes the ERM program's purpose and key objectives, driving daily actions and strategic decisions. The vision statement reflects the aspirational goals of the ERM program, focusing on values and long-term objectives. These statements should be regularly updated to align with the utility's values, ERM needs, and the evolving environment of its operations and community.

Utilities have two primary options for establishing the strategic objectives for their ERM program:

a) **Crafting Mission and Vision Statements** – Utilities can create mission and vision statements for their ERM program. These statements should clearly articulate the purpose and future goals of the ERM program, guiding daily actions and strategic decisions.
   - Sample Mission Statement – "To champion a proactive and systematic risk management process that safeguards our employees, customers, and the environment, ensuring the uninterrupted delivery of reliable and sustainable public power service."
   - Sample Vision Statement – "To cultivate a pervasive risk-aware culture underpinned by strategic management alignment, thereby reinforcing stakeholder trust and confidence at a scale that reflects our utility's size, complexity, and commitment to excellence."

b) **Developing an ERM Policy** – Alternatively, utilities can collaborate with senior leadership to develop an ERM policy. This policy should articulate the goals of the ERM program in relation to the strategic objectives of the utility. Once developed, the policy should be approved by the governing body to ensure formality and actionable steps.
   - Sample ERM Policy Statement – The utility is committed to proactive risk management to safeguard employees, customers, and the environment, ensuring reliable and sustainable public power service.

- ☐ **Action Item:** Review sample ERM mission and vision statements and ERM policies in Appendix B.
- ☐ **Action Item:** Utilities may utilize the template in Appendix C to accomplish this step of the initial stages of their ERM program preparation.

The Process for Identifying Risks

Once the team obtains leadership buy-in and determines the structure of the risk governance team, the next step is preparing and executing the risk identification process. It involves recognizing events or conditions that could negatively impact the utility's objectives (which could include natural and human threats and changing market conditions). By identifying risks early, utilities can develop strategies to mitigate them, safeguard operations, and maintain reliable

service. This section provides a simple approach to risk identification, including conducting risk identification workshops and developing a draft risk register.

Approach to the Risk Identification Process

To effectively manage risks, it is essential to start with a systematic identification process to uncover and document potential risks that could impact operations. Risk identification is a collaborative process that will involve the utility's governing board, senior leadership, and business units. Information will flow top-down and bottom-up[5] within the utility to inform how risks are identified based on strategic objectives.

Below are the roles and responsibilities that a utility's senior leadership, business units, and the utility's governing board will play in the risk identification process.

ERM Role	Responsibilities in Risk Identification Process
Governing Board	• Coordinate with senior leadership to set the utility's mission and strategic objectives.
Senior Leadership	• Define broad risk categories such as financial risks, regulatory compliance, operational risks, and reputational risks based on the utility's mission and strategic objectives. • Prioritize these risk categories based on potential impacts on the utility's mission and strategic objectives. • Communicate the prioritized risk categories and their importance to all levels of the organization, including the governing body, and ensure that all employees understand the strategic focus areas and the rationale behind them.
Business Units	• Identify specific risks within the broad categories set by senior leadership with a focus on managing risks in daily operations. • Leverage detailed knowledge and experience in their daily operations to analyze each of these processes/functions and provide a granular view of potential risks and identify additional risks for leadership to consider when defining and prioritizing risk categories.

Table 2 – Roles and responsibilities of the ERM team during the risk identification process

Utilities can adopt a hybrid approach to guide them through the risk identification process. This approach combines top-down strategic direction from the governing board and leadership with bottom-up operational insights. The following steps outline a comprehensive list of actions that utilities can take to prepare for their risk identification process. However, it is essential for utilities to customize their approach based on their audience, access to key stakeholders, and the desired level of granularity.

[5] The top-down approach focuses on organizational-level risk management (e.g., utility executives allocate resources for a comprehensive wildfire prevention strategy), while the bottom-up approach prioritizes operational risk management within specific business units (e.g., field crews propose targeted vegetation management near wildfire-prone zones).

Step	Details
Form a Risk Committee	• Form a committee of volunteers from each business unit to coordinate the identification process across the utility, which includes planning various workshops that are a critical part of the process.
Strategic Workshops and Departmental Engagement	• Conduct workshops with senior leadership to define strategic risk categories and priorities. These sessions should align with the utility's mission and long-term goals. • Simultaneously, engage department heads and frontline staff in workshops to identify operational risks specific to their areas. Encourage open communication and collaboration across all levels.
Establish Risk Reporting and Communication Channels	• Develop standardized risk reporting templates that capture both strategic risks and operational insights. Include fields for description, potential impact, likelihood, and proposed mitigation strategies. • Foster a culture of regular communication between departments and senior leadership to ensure alignment of identified risks with strategic priorities.
Conduct Risk Reviews and Adjustments	• Consolidate all identified risks into a list that reflects both strategic and operational perspectives. Ensure this list is regularly updated and reviewed. • Hold periodic risk review meetings involving both senior leadership and department heads to reassess priorities, adjust mitigation strategies, and address emerging risks.
Continuous Improvement and Learning	• Establish feedback loops to capture lessons learned from risk identification and mitigation efforts. Use this feedback to continuously improve risk management practices. • Provide ongoing training and development opportunities for employees at all levels to enhance their understanding of risk management principles and practices.

Table 3 – Recommended steps to adopt a hybrid risk management approach to facilitate the risk identification process

Conducting Risk Identification Workshops

Risk identification workshops are a practical and inclusive method for uncovering potential risks within a public power utility. These workshops enable diverse stakeholders to collaboratively identify, discuss, and document risks, ensuring that multiple perspectives are considered. Preparing and conducting these workshops effectively can significantly enhance a utility's ability to foresee and mitigate potential issues.

Step	Action
Define Workshop Objectives	Clearly outline what the workshop aims to achieve.
Select Participants	Choose stakeholders from different departments who can provide diverse insights.
Schedule the Workshop	Set a date and time that works for all key stakeholders.
Prepare Workshop Materials	Gather or create materials such as an agenda, risk identification forms, and a facilitator presentation.
Pre-Workshop Assignments	Assign pre-work to participants, such as reviewing background information or filling out preliminary risk identification forms.

Table 4 – Recommended steps to preparing risk identification workshops

After all workshop preparation is completed, the risk management team should move on to orchestrating the workshops. Below are steps to follow in executing risk identification workshops.

Step	Action
Welcome and Introduction	Start with a brief overview of the workshop objectives, agenda, and ground rules.
Review of Risk Management	Provide a short introduction to risk management principles and the role of risk identification.
Overview of Utility Strategic Objectives	Provide overview of the utility's strategic objectives and goals to stakeholders.
Brainstorming Session	Facilitate a brainstorming session where participants identify potential risks.
Categorize Identified Risks	Group the identified risks into categories such as operational, financial, and regulatory.
Document Risks	Record all identified risks in a risk register, noting the potential impact and likelihood of each.
Preliminary Assessment	Collaboratively perform preliminary assessment for the identified risks based on their potential impact and likelihood. At this stage, this will not have a numerical scoring however, the team should document narrative and anecdotal details shared by participants.
Next Steps and Action Items	Discuss and assign next steps for further analysis or mitigation planning.
Wrap-Up and Feedback	Summarize the key points discussed, confirm action items, and gather feedback on the workshop.

Table 5 – Recommended steps to executing risk identification workshops

- ☐ **Action Item:** Refer to the following supplementary materials to assist with workshop planning, development, and execution.
  - Appendix E – Sample workshop agenda
  - Appendix F – Pre-workshop material for participant preparation for risk identification
  - Attachment 2: Risk Identification Workshop Guide – Workshop planning guide
  - Attachment 3: Risk Identification Workshop PowerPoint Template
- ☐ **Action Item:** Plan and execute the risk identification workshop, take detailed notes, and compile all notes and data collected.

Developing a Risk Register

A risk register is a document that records identified risks, their severity, and the actions steps to manage them.[6] It centralizes and documents all identified risks, their impacts, and mitigation strategies to enhance visibility and support informed decision-making.

Once risks are identified through interviews with the governing board and engaging personnel via risk identification workshops or other methods,[7] the next crucial step is to document the risks in a risk register. This process helps utilities compile and categorize the identified risks effectively. Below are tactical steps to guide utilities in this process.

[6] *"DHS Risk Lexicon" Department of Homeland Security. September 2010. https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf Accessed September 2024.*

[7] Other methods could be one-on-one interviews with specific personnel or departments of the utility if workshops are not feasible due to factors such as expense, difficulty in workshop planning, or lack of participation.

Step	Description
Compile Identified Risks	Gather all identified risks from various sources such as interviews with governing board, stakeholder workshops, additional interviews, etc.
Categorize Risks	Group risks into categories (e.g., operational, financial, regulatory) for clarity and utility.
Create a Risk Register	Develop a structured and simple risk register with essential details for each risk.
Document Risk Details	Include preliminary information such as risk description, category, potential impact, likelihood, risk owner, and mitigation strategies based on initial conversations from the workshops, interviews, and meetings.

Table 6 – Recommended steps to documenting identified risks

- ☐ **Action Item:** Compile and summarize the notes from the workshop(s), interviews, and other stakeholder engagement activities.
- ☐ ***Action Item:*** Transcribe relevant details into the risk register. Utilize Attachment 4: Risk Register Excel Template to begin this process.

Risk Register Development in Excel Spreadsheet

For many small utilities, using Microsoft Excel is a practical and cost-effective solution for developing a risk register. Excel offers significant flexibility with custom fields, formulas, and sorting filters, making it a versatile tool for developing and managing a risk register without incurring additional costs associated with ERM software. While Excel does not support real-time collaboration and requires manual updates, its familiar interface and extensive capabilities make it a suitable choice for utilities seeking an accessible and efficient way to manage their risk registers.

- ☐ **Action Item:** Review the initial risk register and ensure that all details are included and accurate.
- ☐ **Action Item:** Follow-up with stakeholders if information from the risk register is incomplete or requires addition of further details.

Best Practices for Right-Sizing the Risk Register

When developing a risk register, it is important to maintain practicality and manageability based on the utility's size and complexity. Consider the following suggestions:

- Categorize risks based on impact and likelihood. Focus on key risks affecting operations or objectives rather than minor uncertainties.
    - Example: Prioritize risks such as transmission line failures over minor supply chain disruptions due to their potential impact on service reliability and customer satisfaction.
- Combine similar risks to reduce redundancies and simplify management.
    - Example**:** Combine risks related to regulatory changes from different state or federal agencies into a single category to streamline compliance efforts and reduce administrative overhead.
- Periodically assess the risk register, removing risks that are no longer relevant or impactful, and updating it with evolving risks.
    - Example**:** Conduct quarterly reviews of the risk register to remove risks that have been adequately mitigated or are no longer relevant due to policy changes or improvements in operational procedures.

- Use consistent criteria for including risks in the register, such as financial impact thresholds or strategic significance.
    - Example**:** Use a financial impact threshold of $50,000 for including risks related to infrastructure maintenance projects in the risk register to ensure focus on significant budgetary impacts.
- Create both a high-level overview and a detailed register for critical and specific risks, ensuring that management attention is appropriately distributed.
    - Example**:** Maintain a high-level risk register that includes overarching risks affecting power distribution, like severe weather events, and a detailed register for specific risks, such as cybersecurity vulnerabilities in smart grid technologies, to address varying levels of operational and security concerns.

From Risk Identification to Risk Assessment

Having established a foundational knowledge in risk identification through Volume I, utilities will move forward to understanding the next steps in the risk management cycle. Volume II will delve into the risk assessment process, where essential tools and methodologies are provided to evaluate and prioritize identified risks effectively.

Volume II will guide utilities through a systematic approach to assessing risks, ensuring that each potential threat is analyzed for its likelihood and impact. By understanding these assessment techniques, utilities can make informed decisions, allocate resources efficiently, and enhance their overall resilience.

Appendix A: ERM Stakeholder Roles and Responsibilities Template

Instructions

- **Name**: Enter the name of the individual assigned to the role.
- **Position**: Enter the actual position of the individual within the utility.
- **Role**: Identify the ERM role assigned to the individual.
- **Responsibilities**: Define the key responsibilities for each role related to ERM.
- ***Actions (Optional)***: Specify the actions that each role needs to take to fulfill their responsibilities.

Name	Position	Role	Responsibilities	Actions

See sample below on how to complete the ERM Team Roles table.

Name	Position	Role	Responsibilities	Actions
Jane Doe	Board Member	Board of Directors	- Provide strategic oversight - Approve ERM policy and strategies - Review risk reports	- Attend ERM training - Review and approve ERM framework
John Smith	CEO	Executive Management	- Champion ERM program - Allocate necessary resources - Monitor ERM progress	- Assign an ERM leader - Include risk management in meetings
Sarah Brown	Risk Manager	ERM Leader	- Coordinate ERM activities - Develop ERM policies - Lead risk identification and management - Report to management and board	- Conduct risk assessments - Facilitate risk workshops
Mark Johnson	Department Head	Department Heads / Managers	- Identify and assess risks - Develop risk mitigation plans - Monitor and report risks	- Participate in risk assessments - Create action plans for identified risks
Emily White	Committee Member	Risk Management Committee	- Review risk reports - Advise on risk issues - Ensure communication on risk matters	- Meet regularly to discuss risks - Provide feedback on ERM activities
Various Staff	Various Positions	All Employees	- Understand the basics of ERM - Participate in ERM training and workshops - Report risks or incidents	- Attend ERM training - Follow the utility's risk policies

Appendix B: Real-World Vision and Mission Statements

Below are examples of public power utility mission and vision statements and ERM policy statements.

Sample Public Power Utility ERM Mission Statement

- *Grant County Public Utility District*[8]
  "The Enterprise Risk Management (ERM) group promotes greater efficiency and alignment across Grant County Public Utility District by forming resilient financial outcomes and enhancing the organization's access to capital through identifying, measuring, and recommending the disposition of beneficial and harmful risks throughout the district's operations."

Sample Public Power Utility ERM Vision Statements

- *Grant County Public Utility District*
  "Grant County Public Utility District endeavors to develop peer-leading risk management by integrating the principles of Enterprise Risk Management (ERM) into the culture and decision making of its business functions. ERM promotes the success and enhance the accountability of Grant County Public Utility District by incorporating risk assessment into its strategic objectives."
- *Long Island Power Authority*[9]
  "The vision for Enterprise Risk Management (ERM) is to maintain an industry-leading program that identifies, assesses, and monitors significant risks to achieving LIPA's purpose and vision and the Board's objectives as stated in each policy."

Sample Public Power ERM Policy Statements

- *Florida Municipal Power Agency*[10]
  "... FMPA is hereby authorized to put mechanisms in place, such as those more fully described in this Policy, that will control, transfer or mitigate these risks so that, to the extent possible, there will not be an adverse effect on FMPA's ability to protect its employees and material assets from damage or loss."
- *Omaha Public Power District*[11]
  "OPPD shall maintain an enterprise risk management (ERM) program to perform an independent oversight function of the District's risk management activities to ensure significant risks are identified, assessed, managed, and reported through organizational policies, procedures, and processes to maintain risk exposures within agreed upon risk tolerance levels."
- *Lincoln Electric System*
  "To provide a framework and guidance to the Administrative Board, Executive Management, and LES employees to effectively identify, communicate and manage enterprise-level risks that could jeopardize the achievement of LES' Strategic Plan."
- *Sacramento Municipal Utility District*[12]
  "SMUD will implement and maintain an integrated enterprise risk management process that identifies, assesses, prudently manages and mitigates a variety of risks facing SMUD, including financial, supply, operational, physical and cyber security, climate change, legal, legislative and regulatory, and reputational risk."

---

[8] *Grant County PUD. "Enterprise Risk Management Update" April 13, 2021. Begins on page 37 of: https://www.grantpud.org/block/documents/606f67d691f31-2021-04-13-presentation-packet.pdf Accessed September 2024.*

[9] *Dehnert, J. "Enterprise Risk Management – F&A Committee Training" Long Island Power Authority. June 26, 2024. https://www.lipower.org/wp-content/uploads/2024/06/4._Enterprise_Risk_Management_Update.pdf Accessed September 2024.*

[10] *Florida Municipal Power Agency. "Insurance Program Risk Management Policy for Florida Municipal Power Agency". February 17, 2021. Page 17-23 of https://portal.fmpa.com/wp-content/uploads/2022/01/Finance-Committee-Agenda-Package-2022-01-19.pdf Accessed September 2024.*

[11] *Focht, S. and Laskowsky, D. "Enterprise Risk Management Monitoring Report" Omaha Public Power District. June 15, 2021. https://www.oppd.com/media/317707/2021-6-jun-sd15-erm-monitoring-rpt.pdf Accessed September 2024.*

[12] *Sacramento Municipal Utility District. "SMUD Board Policy: Enterprise Risk Management" September 21, 2023. https://www.smud.org/-/media/Documents/Corporate/About-Us/Company-Information/Strategic-Direction/SD-17.ashx# Accessed September 2024.*

Appendix C: ERM Program Strategic Objectives Template

Mission and Vision Statement

Purpose: Define the core purpose of your ERM program. Why does it exist? What fundamental needs does it address for your public power utility? Articulate the long-term aspirations and desired future state of your ERM program. What ultimate impact or transformation do you envision for your public power utility?
Template: *Our mission is to [describe the primary goal of the ERM program] by [briefly outline the key activities or approaches]. Through our efforts, we aim to [describe the desired impact or outcome for the utility].*
Your Mission and Vision Statement: *Our mission and vision are to [insert your mission statement here].*

ERM Policy Statement

Purpose: Define the principles, responsibilities, and commitments that guide the ERM program. The ERM policy statement provides a framework for risk management practices and ensures alignment with the utility's strategic objectives.
Template: *The ERM policy of [utility name] commits to [outline the key principles or commitments, such as risk identification, assessment, and mitigation]. We will [describe the responsibilities of different stakeholders or departments] to ensure that risks are managed effectively and in alignment with our strategic goals. This policy will be reviewed and updated [state frequency, e.g., annually] to adapt to changing conditions and challenges.*
Your ERM Policy Statement: *The ERM policy of [insert your ERM policy statement here].*

Instructions

- ☐ **Complete the Mission Statement**
  - Reflect on the core purpose of your ERM program.
  - Consider how your ERM efforts align with your utility's broader goals.
- ☐ **Develop the Vision Statement**
  - Envision the future state you want to achieve with your ERM program.
  - Think about the long-term benefits and impact on your utility.
- ☐ **Develop ERM Policy Statement**
  - Identify key principles and roles and review frequency.
  - Complete the template to align with strategic objectives.
- ☐ **Review and Refine**
  - Get feedback from stakeholders and revise as needed.
- ☐ **Communicate and Integrate**
  - Share and use these statements to guide ERM development.

Appendix D: Sample Risks to Public Power Utilities

Below are samples of inherent risks that public power utilities face in their daily operations. Utilities may refer to this list to help them identify risks within their utilities.

Risk Category	Risk Titles
Financial	• Customer expectations and affordability • Increasing costs of insurance • Aging power infrastructure • Fluctuating energy prices
Operational	• Physical damage to infrastructure • Third-party vendor vulnerabilities • Supply chain disruptions affecting equipment • Interdependency with other power generation sources • Lack of job-specific personnel training • Insider threats • Lack of equipment maintenance • Human errors during operations
Safety	• Physical threats to the grid (vandalism, natural disasters) • Workplace safety for utility employees • Inadequate public safety power shutoffs • Lack of incident management planning • Lack of emergency response planning • Ineffective facility housekeeping
Strategic	• Talent gap due to retiring workers • Shift toward clean energy and renewable sources (such as decreased demand, or variability of power from distributed energy resources) • Growth in load demand for power generation due to increasing population, artificial intelligence utilization, etc. • Interdependency with other critical infrastructure • Increased misinformation online and on social media • Policy changes in energy regulation • Technological advancements by competitors
Compliance	• Non-compliance with safety standards • Environmental regulation violations • Failure to meet cybersecurity standards • Non-adherence to labor laws • Inadequate reporting and documentation practices
Reputational	• Negative media coverage • Public backlash from rate increases • Poor customer service experiences
Technology	• Cybersecurity threats • Data breaches • Failure of critical IT systems • Technology obsolescence • Integration issues with new technologies
Environmental	• Severe weather events (e.g., wildfire, droughts, etc.) • Long-term weather impacts • Regulatory changes requiring costly compliance

Appendix E: Sample Risk Identification Workshop Agenda

Below is a sample agenda that utilities can use to orchestrate in-house risk identification workshops.

Time	Activity	Details
9:00 - 9:15 AM	Welcome and Introduction	Overview of objectives, agenda, and ground rules.
9:15 - 9:30 AM	Introduction to ERM	Brief discussion on risk management principles.
9:30 - 10:30 AM	Brainstorming Session	Participants identify potential risks through guided brainstorming.
10:30 - 10:45 AM	Break	
10:45 - 11:15 AM	Categorize Identified Risks	Grouping risks into categories (operational, financial, safety, etc.).
11:15 - 12:00 PM	Document Risks	Documenting risks identified by participants through note including data points on their perspective of the risks' likelihood, impacts, suggested risk owners, and existing mitigation strategies.
12:00 - 1:00 PM	Lunch	
1:00 - 2:00 PM	Risk Prioritization	Assessing and prioritizing risks.
2:00 - 3:00 PM	Wrap-Up and Feedback	Summarizing the workshop, confirming action items, and gathering feedback.

Appendix F: Risk Identification Form Template

The risk team can utilize this sample form and share with participants to complete prior to the workshop. This will help participants gather and organize their feedback on the potential risks they identify during this process. Participants should document only one risk in the form and should utilize multiple forms to document multiple risks.

Risk Title						**Proposed Risk Owner**	
Risk Description							
Alignment to Utility's Strategic Goal (if applicable)							
Root Causes of this Risk Are there any specific causes/scenarios that you wish to highlight for this risk? If so, please provide your input below.						**Consequences** List consequences of this risk below.	**Stakeholders Impacted** List stakeholders within the utility impacted by this risk below.
Preliminary Risk Assessment							
Risk Rating	**1**	**2**	**3**	**4**	**5**	**Current Controls/Mitigations in Place**	
Likelihood 1 – rare 2 – unlikely 3 – possible 4 – likely 5 – almost certain							
Impact 1 – insignificant 2 – minor 3 – moderate 4 – major 5 – catastrophic							