RISK MANAGEMENT TOOLKIT FOR PUBLIC POWER UTILITIES

AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

VOLUME III: RISK MITIGATION AND COMMUNICATION

DECEMBER 2024

Table of Contents

Introduction

Background

As utilities face various operational, financial, and regulatory challenges, it is important to clearly convey risk-related information to senior leadership and stakeholders. Risk communication involves sharing details about the nature and impacts of risks, as well as the strategies employed to manage them. This ensures decision-makers are well-informed and able to make sound adjustments.

Continuous monitoring focuses on regularly assessing risk management strategies and the performance of communication efforts. This includes setting up key risk indicators (KRIs), gathering feedback, and adjusting communication plans as necessary. By incorporating these practices into the ERM framework, public power utilities can enhance transparency, foster informed decision-making, and improve organizational resilience.

Volume III – Risk Mitigation and Communication

Building on the foundation in previous volumes of the Risk Management Toolkit, Volume III focuses on actionable steps to address the risks that have been identified, assessed, and prioritized. This volume provides strategies for treating and mitigating these risks and guidance on communicating risk management efforts effectively to leadership and stakeholders.

Volume III Objectives

- Provide clear and actionable guidance for developing and implementing risk mitigation strategies.
- Equip public power utilities with practical steps to treat and mitigate prioritized risks.
- Offer tools and templates to facilitate communication of risk management strategies to leadership and stakeholders.
- Foster continuous monitoring and improvement of risk management practices.

Understanding Risk Treatment

Risk treatment is the process of selecting and implementing measures to manage risk that has been identified and prioritized. The goal is to reduce the likelihood and/or impact of potential risks to a level that aligns with the utility's strategic objectives.

Review of Risk Prioritization

Before exploring specific risk treatment strategies, the ERM team should revisit the prioritized risks identified during the utility's risk assessment process. The ERM team needs to ensure that risk scores and assessments are updated quarterly or in alignment with the utility's reporting schedule to keep leadership informed and current. Below are steps to consider when reviewing risk prioritization.

Table 1. Steps for Reviewing Prioritization

Step	Tasks
Gather the risk register	• Collect the latest risk register that includes risk scores, assessments, and prioritization
Verify risk data	• Ensure all risk data are up to date, including any latest information or changes in the operating environment that could affect risk scores
Consult key stakeholders	• Engage with department heads or risk owners to confirm the relevance of the risks and whether any need to be re-prioritized
Update the prioritization list	• Adjust the prioritization of risks based on new data or insights gathered • Focus on top-tier risks that pose the greatest threat to the utility's operations and strategic goals

☐ **Action Item:** Review and validate the utility's risk register, ensuring all information is current and updated.

Defining Risk Treatment

Once the risks are reviewed and prioritized, the ERM committee needs to determine the appropriate treatment for each risk. Risk treatment involves taking actions to manage or mitigate risks based on their priority. The goal is to reduce the likelihood or impact of risks to an acceptable level, aligning with the utility's strategic objectives. The risk treatment options fall into four categories:

- **Avoidance** is discontinuing activities that generate high risks.
- **Mitigation** is implementing measures to reduce the risk's likelihood or impact.
- **Transfer** is sharing the risk through insurance, contracts, or partnerships.
- **Acceptance** is choosing to retain the risk and prepare for its consequences.

Selecting the right treatment option involves balancing the cost of treatment with the potential impact of the risk. It is important to align these decisions with the utility's strategic goals and available resources. Below are steps to consider when selecting risk treatment options.

Table 2. Steps for Selecting Risk Treatment Options

Step	Tasks
Evaluate each risk	• For each prioritized risk, evaluate the potential treatment options
Analyze cost and benefits	• Compare the costs of each treatment option against the benefits, considering both financial and operational impacts
Consider strategic alignment	• Ensure the chosen treatment option supports the utility's long-term strategic objectives and resource availability
Involve leadership	• Develop a stakeholder communications plan and obtain approval from senior leadership • Present the recommended treatment options to senior leadership for approval, especially for high-priority or high-impact risks
Document the decision	• Record the chosen treatment option for each risk in the risk register, including rationale for the decision and any required actions

- ☐ **Action Item:** Refer to Appendix A for examples of mitigation strategies categorized by their respective risk treatment options.
- ☐ **Action Item:** Refer to Appendix B for examples of cost-benefit analysis related to various risk treatments aimed at mitigating identified and prioritized risks.
- ☐ **Action Item:** Refer to the following supplementary materials to assist with presenting risks and mitigation recommendations to senior leadership.
  - Attachment III.1: Prioritized Risks & Action Plans PowerPoint Template – Presentation of prioritized risks and recommended mitigations to senior leadership
  - Attachment III.2: Risk Communication Plan Template – Recommended steps and template messaging for communicating with relevant stakeholders

Implementing Risk Mitigation Strategies

Risk mitigation involves taking specific actions to reduce the likelihood or impact of a risk. This can include implementing new policies, investing in technology, training staff, or redesigning processes. Effective mitigation strategies not only protect the utility from potential risks but also enhance operational efficiency and resilience.

Developing a Mitigation Plan and Establishing Key Risk Indicators

A mitigation plan outlines specific actions to address prioritized risks. To ensure these actions are effective, utilities should establish key risk indicators (KRIs) within the plan. KRIs provide early warnings of potential risks, allowing utilities to identify and address vulnerabilities before they escalate.

For example, an increase in phishing attempts (a KRI for cyber risk) can prompt enhanced cybersecurity measures, such as employee training and system upgrades. Similarly, low frequency of vegetation management near power lines (a KRI for wildfire risk) can lead to increased activities to reduce wildfire risks. By continuously monitoring KRIs, utilities can develop targeted mitigation plans that address specific risks, ensuring a more resilient and secure operation.

Essentially, KRIs act like an early warning system, helping utilities stay ahead of problems and strengthen their risk management plans.

Table 3. Steps for Developing Mitigation Plans

Step	Tasks
Identify mitigation measures	• Brainstorm potential actions that could reduce the likelihood and impact of each risk • Consider technical, organizational, and procedural measures
Assign responsibilities	• Clearly define who will be responsible for implementing each mitigation measure • This should include specific departments or individuals
Establish KRIs	• For each mitigation action, define relevant KRIs to predict and monitor potential risks • These KRIs should align with the utility's strategic goals
Develop a timeline	• Create a timeline for implementing each mitigation action • Ensure milestones are set and deadlines are realistic
Allocate resources	• Identify the resources (financial, human, or technological) needed to implement the mitigation actions and ensure they are available
Document the plan	• Consolidate all information into a detailed mitigation plan document for stakeholder sharing and future reference

☐ **Action Item:** Refer to Appendix C for examples of KRIs relevant to the risks faced by public power utilities.

☐ **Action Item:** Revise the utility's risk register to incorporate details on mitigation strategies for prioritized risks, ensure alignment with strategic goals, and specify timelines or deadlines for implementing these actions.

Monitoring and Reviewing Mitigation Efforts

Monitoring and reviewing mitigation efforts ensures actions are successfully reducing risk and being executed as planned. A key part of this process is using KRIs established during the development of the utility's risk mitigation plan. Table 4 lists steps to consider when monitoring and reviewing the utility's mitigation efforts.

Table 4. Steps for Monitoring and Reviewing Mitigation Efforts

Step	Task
Track KRIs	• Regularly monitor the KRIs established in the risk register to identify emerging risks and take timely action
Conduct regular reviews	• Schedule periodic reviews of the mitigation efforts to evaluate their effectiveness and make necessary adjustments if necessary
Engage with stakeholders	• Involve key stakeholders in the review process to ensure transparency and gather input on potential improvements
Document findings	• Record the results of each review, include any changes made to the mitigation plan and reason for those changes

Communicating Risk to Leadership and Stakeholders

Communicating risks and mitigation strategies keeps leadership and stakeholders informed about the utility's challenges and management steps. This clear, concise communication builds trust and supports informed decision-making.

Tailoring the Risk Communication

When communicating risk, tailor the message to the audience, as stakeholders have varying levels of understanding and concern. The ERM committee should customize communication for each group and conduct regular reports on risk mitigation progress to keep senior leadership and stakeholders informed about actions taken and any new risks. [1]

Table 5. Steps for Tailoring Risk Communication

Step	Tasks
Identify the audience(s)	• Identify who needs to be informed about the risk and assess their level of expertise
Define the key message	• Clarify the main point that needs to be communicated, focusing on what the audience needs to know
Use appropriate language	• Avoid jargon and technical terms when communicating with non-experts • Use clear, simple language
Provide context	• Explain the significance of the risk within the broader context of the utility's operations and objectives
Gather data	• Collect relevant data, particularly on KPIs to monitor effectiveness of risk mitigation strategies
Prepare reports	• Reports should include updates on KPIs, progress on mitigation efforts, and any necessary adjustments to the risk treatment plan
Update stakeholders	• Provide regular updates to stakeholders, keeping them informed about the progress of mitigation actions and any changes in the risk landscape • The frequency of these updates should align with the criticality of the risks involved
Review and revise	• Continuously review and refine communication efforts to ensure they remain effective and aligned with the utility's evolving needs • This iterative process helps maintain clarity and relevance in risk communication

☐ **Action Item:** Refer to the following supplementary materials to assist with communicating risks to senior leadership and stakeholders.

- ○ Attachment III-3: Senior Leadership Reporting PowerPoint Template – Presentation of ERM program updates to senior leadership
- ○ Attachment III-4: Stakeholder Risk Briefing PowerPoint Template – Presentation of ERM program updates to stakeholders

Continuous Monitoring and Adjustment

Risk communication is an ongoing process that requires continuous monitoring and adjustment. As risks and mitigation efforts evolve, communication strategies must be updated to reflect these changes accurately. Below are best practices for continuous monitoring and adjustment for the utility's ERM program.

- Solicit feedback from stakeholders to understand the clarity and usefulness of communication. This feedback provides insights into how well the information is being received and whether it meets stakeholder needs.
- Use existing forums such as all-hands meetings or departmental briefings to communicate risk updates. This integrates risk communication into regular operations and ensures broad reach.

[1] *Publicly available reporting samples from other public power utilities include the ERM Quarterly Reports from Grant County Public Utility District, Omaha Public Power District, and Lincoln Electric System.*

- Provide frequent updates to stakeholders, adjusting the frequency based on the criticality of the risk. For example, critical risks may require immediate updates, while less urgent risks can be addressed in regular reports.
- Based on feedback and monitoring results, communication plans should be revised, as necessary. This could involve updating reports, modifying presentation formats, or changing communication frequency to better address evolving needs.

Appendix A: Risk Treatment Examples

For many risks, there are often several treatment options available. Here is an example of common risks and the typical treatments used to mitigate them.

Risk Example	Risk Treatment	Example of Risk Treatments
Cybersecurity breach	Mitigation, Acceptance	• Implement multi-factor authentication (MFA) for all systems • Regularly update and patch software • Conduct employee cybersecurity training • Develop and evaluate a cyber incident response plan
Natural disasters (e.g., wildfires, hurricanes)	Transfer, Acceptance, Mitigation	• Purchase comprehensive insurance coverage • Contracts and indemnity provisions • Establish mutual aid agreements with other utilities • Partner with local governments for coordinated disaster response
Aging infrastructure	Avoidance, Mitigation	• Prioritize capital investment in infrastructure modernization • Decommission obsolete equipment • Implement predictive maintenance programs to avoid failures
Demand forecasting errors	Mitigation	• Utilize advance data analytics for more accurate forecasting • Diversify energy sources to manage unexpected demand fluctuations • Implement demand response programs to balance load during peak periods
Supply chain disruptions	Transfer, Mitigation	• Develop and maintain unconditional delivery obligation contracts with suppliers • Invest in inventory management systems to track critical supplies • Contract with third-party organization provides to ensure supply continuity
Workforce shortage or aging workforce	Mitigation	• Implement workforce development programs • Partner with local colleges for training and recruitment • Offer attractive retirement benefits to retain senior employees while mentoring younger staff
Reputation damage due to service outage	Mitigation	• Improve communication channels with customers, including social media • Invest in grid resiliency projects • Develop a public relations strategy to manage customer expectations and provide transparency during outages

Appendix B: Cost Benefit Analysis Examples for Risk Treatment Options

Cost-benefit analysis (CBA) supports public power utilities in evaluating and selecting risk treatment options. By comparing costs against benefits, utilities can allocate resources effectively to mitigate risks while aligning with operational, financial, and compliance priorities. The table below outlines CBA examples for various risk categories, demonstrating a structured approach to risk management.

Risk Category	Identified Risk	Risk Treatment Option	Costs	Benefits	Net Benefit	CBA Outcome
Operational Risk	Critical equipment malfunction leading to operational disruptions	Equipment Maintenance Program	$2 million annually	Reduced equipment failures, improved reliability	Avoidance of $10 million annually in potential downtime losses	Maintenance programs provide consistent reliability and reduce long-term disruptions
		Equipment Modernization Project	$20 million initial investment	Enhanced reliability, reduced maintenance costs	Avoidance of $50 million over ten years in downtime and repair costs	Modernization requires higher upfront investment but delivers substantial long-term benefits
Cybersecurity Risk	Data breach compromising sensitive data (PII)	Cybersecurity Awareness Training	$500,000 annually	Reduced risk of employee-related data breaches	Avoidance of $2 million annually in potential regulatory fines and reputational damage	Training is a cost-effective measure to mitigate human-related cybersecurity risks
		Advanced Threat Detection Tools	$5 million initial investment	Enhanced detection of threats, quicker response times	Avoidance of $15 million over five years in breach-related costs	Advanced tools offer significant benefits but require higher upfront costs
Safety/ Compliance Risk	Employee safety incidents (minor)	Safety Training and PPE Upgrades	$1 million annually	Improved employee safety, reduced incident rates	Avoidance of $3 million annually in medical and compensation costs	Training and PPE upgrades are cost-effective in maintaining compliance and reducing incidents
		Automation of Hazardous Tasks	$10 million initial investment	Significantly reduced risk of safety incidents	Avoidance of $20 million over ten years in incident-related costs	Automation provides long-term safety improvements and operational efficiency

Appendix C: Key Risk Indicators Examples

KRIs can be developed during the mitigation planning phase, the initial risk assessment, or when updating the risk register. Identifying KRIs early ensures proactive monitoring, while refining them during mitigation planning links metrics directly to controls. Utilities can also update KRIs as risks or priorities evolve, ensuring adaptability and effective risk management.

Risk Identification				Risk Assessment							
					Post-Mitigation						
Risk ID	Risk Description	Category	KRI	Controls/ Mitigation Strategies	Proposed Risk Owner	Likelihood Level	Impact Level	Residual Risk Score	Risk Tolerance	Risk Limit/ Threshold	Status
R001	Critical equipment malfunction leading to operational disruptions	Operational	# of equipment failures	Regular maintenance schedule Spare parts inventory Equipment monitoring system	Operations Manager	2 (Unlikely)	4 Major	8	High (8-10)	Immediate action if score exceeds 8; >2 failures per quarter	Within limit but requires immediate attention
R002	Cyber-attack compromising sensitive data	Cybersecurity	# of phishing attempts detected	Network security protocols Regular security audits Employee cybersecurity training	IT Specialist	2 (Unlikely)	3 Moderate	6	Moderate (4-7)	Review and strengthen controls if score exceeds 7; >10 attempts per month	Within limit; monitor regularly
R003	Employee safety incidents (minor)	Safety/ Compliance	# of minor safety incidents reported	Safety training programs Personal protective equipment Incident reporting	Safety Officer	3 (Possible)	2 Minor	6	Moderate (4-7)	Review safety protocols if score exceeds 7; >5 incidents per month	Within limit; review safety protocols
R004	Increased energy procurement costs	Financial	Monthly average energy cost deviation (%)	Long-term power purchase agreements Diversified energy sources Regular market analysis	Procurement Manager	3 (Possible)	3 Moderate	9	High (8-10)	Immediate action if score exceeds 8; >5% above the budgeted threshold	Exceeds limit and requires immediate attention