

# RISK MANAGEMENT TOOLKIT FOR PUBLIC POWER UTILITIES



## VOLUME II: RISK ASSESSMENT



NOVEMBER 2024

## Table of Contents

Introduction.....	3
Background .....	3
Volume II – Risk Assessment.....	3
Objectives.....	3
Prepare and Develop the Risk Assessment Criteria.....	3
Developing Likelihood and Impact Scales.....	3
The Risk Scoring Process.....	6
Initial Risk Scoring.....	7
Documenting Controls and Mitigation Strategies .....	8
Evaluating Risk with or without Residual Risk Scoring .....	8
Approaching Risks Without Residual Risk Scores.....	8
Calculating and Using Residual Risk Scores.....	9
Setting Up Risk Tolerance and Limits .....	10
Heat Mapping for Visualizing Prioritized Risks .....	12
Appendix A.1: Simple Risk Scoring Criteria.....	14
Appendix A.2: Expanded Risk Scoring Criteria .....	15
Appendix A.3: Expanded Risk Scoring Criteria .....	16
Appendix B: Simple Risk Register with Risk Scoring .....	17
Appendix C: Setting Up Risk Tolerance and Risk Limit Checklist.....	18
Appendix D: Simple Risk Register with Applied Risk Tolerance and Limit .....	19
Appendix E: Plotting Residual Risk Scores on a Heat Map .....	20
<i>Attachment II-1: Risk Assessment Workshop Guide</i>	
<i>Attachment II-2: Risk Assessment Workshop PowerPoint Template</i>	
<i>Attachment II-3: Risk Tolerance and Risk Limit PowerPoint Presentation Template</i>	
<i>Attachment 4: Risk Register Template</i>	

# Introduction

## Background

Risk assessment follows risk identification and constitutes the second major step in advancing a public power utility's enterprise risk management, or ERM, program. During risk assessment, utilities evaluate the likelihood and impact of identified risks based on data informed by various sources. By quantifying the impact levels associated with these risks, utilities can prioritize investments.

## Volume II – Risk Assessment

Volume II of the Public Power Risk Management Toolkit provides guidance for utilities as they progress in establishing their ERM program. This volume addresses the steps involved in assessing and prioritizing risks, building upon the foundational knowledge presented in Volume I, which focused on ERM program establishment and risk identification.

## Objectives

- Understand the process and steps required to create a risk prioritization scoring system.
- Discover the steps and strategies to secure senior leadership approval for risk mitigation.
- Master how to strategically plan and conduct risk assessments to advance an ERM program.
- Explore strategies for documenting risk scoring, controls, mitigation plans, and calculating residual risks.
- Understand how to establish risk tolerance levels that align with strategic objectives.
- Examine the relationship between risk assessment and prioritization, ensuring risks are addressed within defined tolerance and limits.

## Prepare and Develop the Risk Assessment Criteria

Risk scoring involves evaluating and assigning a numerical value to the likelihood and potential impact of each identified risk. Preparing for risk scoring includes defining clear criteria and ensuring uniform evaluation processes. Engaging senior leadership in establishing these criteria is crucial for maintaining accuracy and consistency.

### Developing Likelihood and Impact Scales

*Likelihood* refers to the probability of a risk event occurring, while *impact* represents the extent to which that event can affect the utility's objectives. When assessing impact, it is critical to evaluate how different vulnerabilities could exacerbate potential risks and the severity of the consequences. The keys to defining risk scoring criteria are to maintain simplicity and achieve consensus with senior leadership on the scoring method.

To develop meaningful scoring criteria, the risk management committee should include a comprehensive range of impact components, such as:

- **Financial impact** – the direct cost associated with the risk event, such as repair costs, fines, or lost revenue.
- **Operational impact** – the effect on service delivery, including potential for outages, delays, or disruptions.

- **Reputational impact** – the damage to the utility’s public image and trust, which could affect customer satisfaction and community support.
- **Compliance impact** – the regulatory penalties or non-compliance with laws and standards
- **Health and safety impact** – the risk to employee or public health and safety, including potential injuries or fatalities

An essential part of this process is recognizing how vulnerabilities — weaknesses in systems, processes, or safeguards — can influence both the likelihood and impact of a risk event. For example, outdated cybersecurity defenses or inadequate infrastructure maintenance increase both the probability and severity of certain risks.

The risk management committee should conduct further research, engage with stakeholders, and leverage existing utility data — particularly from the risk identification process — to develop a comprehensive framework for scoring likelihood and impact. This framework should integrate vulnerabilities to provide a more accurate risk assessment. Once developed, the scoring criteria should be validated by senior leadership and submitted for governing board approval to ensure alignment with the utility’s strategic goals.

The following two examples show how vulnerabilities influence the likelihood and impact of risks.

<b>Risk Example: Ransomware Attack</b>	
Threat	A ransomware attack targeting the utility’s IT systems
Vulnerability	Outdated firewall and antivirus software
Likelihood	Moderate to High: Given the outdated security, the utility is more susceptible to attack
Impact	<ul style="list-style-type: none"> <li>• Financial: Potential ransom payment, system restoration cost</li> <li>• Operational: Disruption of billing systems or grid management</li> <li>• Reputational: Loss of customer trust and negative media coverage</li> <li>• Compliance: Failure to meet cybersecurity regulations, leading to fines</li> <li>• Health and safety: Minimal direct safety impact, but emergency systems could be affected during system downtime</li> </ul>
<b>Risk Example: Aging Infrastructure</b>	
Threat	Failure of critical equipment, such as a transformer explosion
Vulnerability	Aging transformers beyond their expected lifespan, with delayed maintenance
Likelihood	High: Given the condition of the infrastructure, failure is likely
Impact	<ul style="list-style-type: none"> <li>• Financial: High costs for emergency repairs and equipment replacement</li> <li>• Operational: Potential widespread outages, disrupting customer service</li> <li>• Reputational: Decline in customer satisfaction and damage to the utility’s reputation</li> <li>• Compliance: Failure to meet infrastructure maintenance standards could result in penalties</li> <li>• Health and safety: Risk of injury to workers or the public during equipment failure</li> </ul>

Utilities can begin by adopting the likelihood and impact scales used by other public power utilities. The utility risk management committee should customize these scales as it gains more experience with the ERM process. The example criteria Grant County Public Utility District in Washington state uses, shown in Table 1, can serve as a useful reference for developing a utility’s likelihood and impact levels.<sup>1</sup>

To make informed decisions, utilities should use historical data, industry benchmarks, and insights from similar utilities. Open source resources include the Department of Energy’s [State and Regional Energy Risk Profiles](#), the Midwest Reliability Organization’s [annual risk assessments](#), the Western Electricity Coordinating Council’s [risk management analyses](#), Aon’s [Global Risk Management Survey](#), NC State University Enterprise Risk Management Initiative’s annual [Executive Perspectives on Top Risks Survey](#), [Deloitte’s Power and Utilities Industry Outlook](#), and [EY’s annual utility sector outlook](#). Utilities can build relationships with other utilities or engage with APPA’s Risk Management Working Group to gather insights on the ERM criteria other public power utilities use. This data can help tailor the scales to better reflect the specific risk environment and operational context.

**Table 1. Grant County Public Utility District Likelihood Scale**

Likelihood	Likelihood Criteria
Very Unlikely	Virtually no chance it will happen in the next 5 years
Unlikely	Not likely to happen in the next 5 years
Possible	Somewhat likely to happen in the next 5 years
Likely	Will probably happen in the next 5 years
Highly Likely	Almost certain to occur in the next 5 years

Grant County PUD uses a detailed impact scale to measure the significance<sup>2</sup> of its identified risks. Table 2 details the significance scale for Grant County PUD’s ERM program.

**Table 2. Grant County Public Utility District Significance Scale**

Significant Scale	Revenue Impact	Health and Safety	Reputation	Legal
Not Significant	<\$500K	No medical treatment required	Minor, adverse local public attention or complaints	Minor legal issues, non-compliance and breaches or regulation
Slightly Significant	\$500K - \$2.5M	Requires hospitalization but no irreversible disability	Attention from media and/or heightened concern by local community	
Moderately Significant	\$2.5M - \$30M	Requires hospitalization but no irreversible disability	Significant adverse national media/public/ NGO attention	Serious breach of regulation with investigation or report to authority and/or moderate fine possible
Highly Significant	\$30M - \$100M	Single fatality and/or severe irreversible disability to one or more persons	Serious public or media outcry, loss of customer/ investor confidence	Major breach of regulation or major litigation

<sup>1</sup> *Enterprise Risk Management Update*. Grant PUD, October 12, 2021. [www.grantpud.org/block/documents/615f74a19d370-2021-10-12-commission-presentation-packet.pdf](http://www.grantpud.org/block/documents/615f74a19d370-2021-10-12-commission-presentation-packet.pdf). Accessed November 2024.

<sup>2</sup> Grant PUD defines “significance” as “the impact to the organization of a risk event occurring. Significance scales should include multiple types of measurement. For example, financial impact, environmental impact, reputational impact, and legal impact to name a few.”

Significant Scale	Revenue Impact	Health and Safety	Reputation	Legal
Extremely Significant	Greater than \$100M	Multiple fatalities or significant irreversible effects to >5 persons.	Complete loss of public, customer, and/or investor confidence	Significant prosecution and fines. Very serious litigation including class action.

For utilities just starting their ERM program or smaller utilities without the means to measure impacts across various categories, a simpler approach using subjective scales for both likelihood and impact may be more practical. This method allows the risk management committee to assess risks effectively without the need for extensive data.

**Table 3. Example Simple Likelihood Criteria**

Level	Likelihood Criteria
1	Rare: Unlikely to occur, <5% chance
2	Unlikely: Could occur occasionally, 5% - 20% chance
3	Possible: Might occur, 21% - 50% chance
4	Likely: Will probably occur, 51% - 80% chance
5	Almost Certain: Expected to occur, > 80% chance

**Table 4. Example Simple Impact Criteria**

Level	Impact Criteria
1	Insignificant: No significant impact
2	Minor: Limited impact, easily manageable
3	Moderate: Noticeable impact, manageable
4	Major: Significant impact, requires attention
5	Catastrophic: Severe impact, critical

When assigning numerical values to the likelihood and impact criteria, utilities can create a more precise and quantifiable risk scoring system. For example, likelihood levels can be rated on a scale from 1 to 5, where 1 represents a very low probability and 5 represents a very high probability. Similarly, impact levels can be rated on a scale from 1 to 5, where 1 indicates minimal impact and 5 indicates severe impact. This more detailed risk scoring can incorporate factors such as existing insurance policies, deductibles, cash reserves, and daily profit margins. By doing so, utilities can achieve a comprehensive understanding of their risk landscape and make more informed decisions.

- Action Item:** Collaborate with stakeholders to define and develop the risk scoring criteria for the utility.
- Action Item:** Collaborate with senior leadership to validate the risk scoring criteria and secure approval from the governing board.
- Action Item:** Finalize the utility's risk scoring criteria and document using [Appendix A.1](#).
- Action Item:** Review and utilize [Appendix A.2](#) and [Appendix A.3](#) if considering a more robust risk scoring criteria.

## The Risk Scoring Process

To initiate the risk scoring process, the risk management team should conduct risk assessment workshops or interviews after developing the risk scoring criteria. The risk assessment workshops or interviews are important for evaluating and prioritizing risks based on detailed

insights from stakeholders who encounter these risks daily, such as operations managers, safety officers, IT specialists, maintenance supervisors, customer service managers, and emergency response coordinators.

## Initial Risk Scoring

Risk scoring guides the initial assessment of risks based on their likelihood and impact. The risk assessment workshop focuses on applying the utility’s scoring criteria to evaluate identified risks. Stakeholders who are typically involved in day-to-day operations provide valuable insights into the probability and potential consequences of each risk. Table 5 details the steps to follow when assigning and calculating the initial risk scores.

**Table 5. Steps for Assigning and Calculating Initial Risk Scores**

Step	Task
Determine Likelihood Level <sup>3</sup>	<ul style="list-style-type: none"> <li>Evaluate the probability of each risk occurring using the established likelihood scale, such as analyzing historical data to identify trends in risk events</li> </ul>
Determine Impact Level	<ul style="list-style-type: none"> <li>Assess potential consequences of each risk using the established impact scale, incorporating input from subject matter experts to gauge severity and potential operational disruptions</li> </ul>
Assign Initial Likelihood and Impact Scores	<ul style="list-style-type: none"> <li>Assign numerical scores (1 to 5) to each risk based on likelihood and impact assessments, using team discussions or workshops to reach consensus on scoring</li> </ul>
Calculate Initial Risk Scores	<ul style="list-style-type: none"> <li>Multiply the likelihood score by the impact score to determine the risk score (i.e., risk score = probability x impact), ensuring clear documentation of each calculation for transparency</li> </ul>
Document Initial Risk Scores	<ul style="list-style-type: none"> <li>Record initial risk scores and assigned likelihood and impact scores in the risk register, utilizing a centralized digital tool (e.g., Excel or a risk management software) for accessibility and updates</li> </ul>
Review Initial Risk Scores	<ul style="list-style-type: none"> <li>Validate initial risk scores with stakeholders through collaborative meetings to discuss scores and make necessary adjustments based on group insights</li> </ul>

Consider the following factors when engaging in risk scoring with stakeholders:

- The risk management team should calculate the initial risk score and share it with stakeholders for revision during the workshop.
- Ensure participants have the list of risks and scoring criteria beforehand (i.e., provide a simple version of the risk register).
- Use the approved scoring criteria to assess each risk’s likelihood and impact.
- Allow participants to express their perspectives and then work toward consensus regarding the likelihood and impact of each risk.

In situations where utilities are resource constrained, conducting a comprehensive workshop may not be practical. In such instances, an alternative, streamlined method for risk scoring can be adopted:

- Conduct individual or small-group sessions with key personnel who have detailed knowledge of specific risks.

<sup>3</sup> Public power utilities should follow DOE guidance for assessing risks in state energy security plans (SESP). They should gather both internal and external documents, such as incident reports, historical data, maintenance logs, performance reports, financial statements, and budget records.

*Risk Assessment Essentials Guide for State Energy Security Plans*. U.S. Department of Energy, April 2024. [www.energy.gov/sites/default/files/2024-05/DOE%20CESER-Risk%20Assessment%20Essentials%20Guide%20for%20State%20Energy%20Security%20Plans.pdf](http://www.energy.gov/sites/default/files/2024-05/DOE%20CESER-Risk%20Assessment%20Essentials%20Guide%20for%20State%20Energy%20Security%20Plans.pdf)



- Start with individual assessments using the established criteria, followed by a brief group review to consolidate and gain consensus on the scores.

### Documenting Controls and Mitigation Strategies

Controls are proactive measures put in place to prevent or detect risks, such as implementing firewalls to protect against cyberattacks and conducting preventive maintenance programs to ensure the reliability of utility operations. Mitigation strategies, on the other hand, are actions taken to reduce the severity or impact of risks when they occur, such as training employees to recognize cyber threats and building redundant infrastructure to maintain service continuity during equipment failures.

Stakeholders, drawing from their firsthand understanding of risks and existing measures, play an important role in documenting controls and mitigation strategies. They provide insights into the effectiveness of current controls and strategies, identify gaps, and ensure the documented measures are practical and aligned with real-world conditions. Table 6 outlines the steps to follow in documenting existing controls and mitigation strategies.

**Table 6. Steps for Documenting Controls and Mitigation Strategies**

Step	Task
Document Existing Controls and Mitigation Strategies	<ul style="list-style-type: none"> <li>• Record existing procedures, policies, and tools for identified risks by conducting stakeholder interviews, using checklists for thorough documentation, reviewing policies, and centralizing information in a document management system (e.g., Excel, internal SharePoint)</li> </ul>
Assign Risk Owners	<ul style="list-style-type: none"> <li>• Designate individuals or teams to manage each identified risk by identifying relevant stakeholders, defining responsibilities, communicating expectations in a kickoff meeting, and implementing a tracking system for accountability</li> </ul>
Review and Update	<ul style="list-style-type: none"> <li>• Update the risk register with details on controls, mitigation strategies, and risk owners by scheduling regular reviews, utilizing collaborative tools for real-time updates, analyzing trends from historical data, and presenting updates to senior leadership for approval</li> </ul>

### Evaluating Risk with or without Residual Risk Scoring

Utilities can take two approaches to evaluating risks: mitigation without calculating residual risk scores and quantifying residual risks to prioritize mitigation strategies.

#### Approaching Risks Without Residual Risk Scores

Smaller utilities do not need to calculate residual risk scores to start addressing identified risks. After completing the risk assessment, utilities can immediately focus on the most critical risks. This straightforward approach allows for timely action without the complexity of formal scoring. Below are steps to follow when evaluating identified risks without calculating residual risk scores.

Smaller utilities might prefer to start addressing risks without calculating residual scores, while larger or more mature utilities can benefit from the structured prioritization that scoring offers. Regardless of the approach taken, both should focus on aligning risk assessment with strategic goals.



**Table 7. Approaching Risks Without Residual Risk Scores**

Step	Task
Identify High-Priority Risks	<ul style="list-style-type: none"> <li>Review risk assessment results and highlight risks with the highest potential impact</li> </ul>
Apply Existing Controls	<ul style="list-style-type: none"> <li>Use established policies and procedures to manage identified risks effectively</li> </ul>
Allocate Resources	<ul style="list-style-type: none"> <li>Distribute staff and budget to focus on the identified high-priority risks</li> </ul>
Monitor and Adjust	<ul style="list-style-type: none"> <li>Regularly review risk outcomes and adjust strategies based on effectiveness</li> </ul>

## Calculating and Using Residual Risk Scores

Residual risk is the level of risk that remains after the application of controls and mitigation strategies. For utilities with more advanced risk management processes, calculating residual risk scores can help prioritize risks and allocate resources more effectively.

Most utilities with ERM programs use residual risk scores to prioritize mitigation actions and guide decisions on resource allocation, investment, and insurance planning. This step clarifies control effectiveness and areas needing improvement. While it adds an extra step for the risk management committee, it simplifies future risk mitigation. Utilities can choose the robustness of their residual risk scores, from simple surveys to in-depth interviews. Below are steps to follow in calculating residual risk scores.




**Table 8. Calculating Residual Risk Scores**

Step	Task
Evaluate Effectiveness of Existing Controls and Mitigation Strategies	<ul style="list-style-type: none"> <li>Review control effectiveness using metrics and stakeholder feedback, such as staff surveys on safety and incident report analysis</li> </ul>
Adjust Likelihood and Impact Scores	<ul style="list-style-type: none"> <li>Update likelihood and impact scores based on control effectiveness, lowering the likelihood if training reduces equipment failures</li> </ul>
Calculate Residual Risk Scores	<ul style="list-style-type: none"> <li>Use the same scoring criteria used for initial risk scoring (see earlier section)</li> <li>Calculate the residual risk score using the formula: residual risk score = adjusted likelihood x adjusted impact</li> </ul>
Document Residual Risk Scores	<ul style="list-style-type: none"> <li>Record residual risk scores and updated likelihood/impact in the risk register via a shared platform for team access</li> </ul>
Review and Validate Residual Risk Scores	<ul style="list-style-type: none"> <li>Validate scores with stakeholders through meetings with risk owners and department heads to confirm updates</li> </ul>
Update Risk Register	<ul style="list-style-type: none"> <li>Refresh the risk register with new residual scores and control changes, sharing updates with senior leadership</li> </ul>

Table 9 outlines an example of how the Sacramento Municipal Utility District (SMUD) evaluated its risks by comparing them against residual risk exposure and industry benchmarks.<sup>4</sup>

<sup>4</sup> Board Policy Committee Meeting and Special Board of Directors Meeting – Item 2: Enterprise Risk Management, Sacramento Municipal Utility District, November 16, 2022. <https://www.smud.org/-/media/Documents/Corporate/About-Us/Board-Meetings-and-Agendas/2022/Nov/Information-Packet--Policy-Committee--November-16-2022.ashx>. Accessed November 2024.

**Table 9. SMUD’s Comparative Risk Exposure**

North Carolina State ERM Initiative and Protiviti Top 10 Enterprise Risks Specific to Energy and Utilities Industry		SMUD’s Corresponding Risks	SMUD’s Current Residual Risk Exposure
1	Succession challenges, ability to attract and retain top talent	<b>Operational risk:</b> Strategic workforce agility Competitive workforce total rewards Diversity, Equity, Inclusion and Belonging Change Management	
2	Uncertainties in supply chain including the viability of key suppliers, scarcity of supplies, volatile shipping and delivery options, or stable prices in the supply chain ecosystem may make it difficult to deliver services	<b>Operational risk:</b> Supply Chain	
3	Regulatory changes and scrutiny heightened, impacting how processes are designed and how products or services are produced and delivered	<b>Operational risk:</b> Regulatory compliance <b>Strategic risk:</b> 2030 Zero Carbon Plan Carbon emissions Renewable Portfolio Standards; CEC: Integrated Resource Planning <b>External risk:</b> Legislative & regulatory Natural hazards	The current residual risk exposure ranges from medium to high  ↔ 

- Action Item:** Refer to the following supplementary materials to assist with workshop planning, development, and execution.
  - o [Attachment II.1: Risk Assessment Workshop Guide – Workshop Planning Guide](#)
  - o [Attachment II.2: Risk Assessment Workshop PowerPoint Template – Workshop PowerPoint Template](#)
- Action Item:** Review an example of a simple risk register with risk scoring and controls/mitigation strategies documented in [Appendix B](#).

### Setting Up Risk Tolerance and Limits

For public power utilities, establishing risk tolerance and limits requires considering broader responsibilities like public health, safety, and operational reliability. Risk tolerance refers to the level of uncertainty or risk a utility is willing to accept, while risk limits set the maximum acceptable risk in specific operations to ensure safety and reliability.

This step follows the calculation of residual risk scores, ensuring limits are based on the remaining risk after existing controls. Setting these thresholds earlier could lead to misalignment, as utilities need a clear picture of post-mitigation risks to prioritize effectively.

At this point, the risk assessment is considered complete, providing a clear understanding of risks and required actions. The next step is for senior leadership and the risk management team to set risk tolerance and limits that align with the utility’s strategic goals. Once risk tolerance and limits are established, utilities can prioritize risks exceeding these thresholds and focus on mitigation strategies. This allows the utility to focus on mitigating risks that exceed these thresholds and take appropriate action.

**Table 10. Example Risk Tolerance Levels and Risk Limits**

Risk Category	Risk Details	Tolerance Level	Residual Risk Score Scale	Risk Limit
Operational Downtime	Minimal operational downtime ensures service reliability and prevents customer dissatisfaction. For public power utilities, keeping downtime below X hours helps maintain consistent service.	Low (X-X hours)	1-4: Low risk 5-8: Moderate risk 9-10: High risk	Immediate action required if downtime exceeds X hours; investigate causes of downtime immediately, implement corrective actions, and communicate with stakeholders regarding service status
Financial Loss	Limits financial exposure to manageable levels, ensuring the utility can absorb potential losses without significant impact on its operations or financial stability.	Moderate (\$X - \$XXX)	1-4: Low risk 5-7: Moderate risk 8-10: High risk	Review and mitigate if financial loss exceeds \$XXX; conduct a financial review, identify contributing factors, and adjust financial strategies or budget allocations as necessary
Safety Incidents	Maintaining a low threshold for safety incidents helps ensure a safe working environment and compliance with safety regulations. This limit helps to minimize risks to personnel and prevent potential hazards.	Low (X - X incidents per year)	1-4: Low risk 5-7: Moderate risk 8-10: High risk	Immediate review and action required if incidents exceed X per year; perform an incident investigation, update safety protocols, and provide additional training or resources to staff
Customer Outages	Restricting customer outages to X incidents per year helps maintain high service levels and customer satisfaction. This level is low enough to prevent widespread dissatisfaction while allowing for minor issues.	Low (X - X incidents per year)	1-4: Low risk 5-7: Moderate risk 8-10: High risk	Immediate corrective action required if outages exceed X per year; assess the cause of outages, enhance response strategies, and inform customers about ongoing efforts to improve service reliability
Cybersecurity Breaches	Ensures measures are in place to reduce the likelihood of a breach.	Moderate (X - X incidents)	1-4: Low risk 5-7: Moderate risk 8-10: High risk	Immediate review and improvement if breaches exceed X incidents; conduct a thorough security audit, enhance cybersecurity measures, and implement staff training on security protocols.

Table 10 serves as a framework for public power utilities to explore various topics related to setting up their risk tolerance and limits. It provides examples that utilities can consider based on their unique goals and priorities. Risk tolerance levels and risk limits will vary based on the utility’s strategic goals and other factors, such as the utility’s size and budget. However, utilities can consult with each other to gain insights into how their peers are establishing risk tolerance and limits, which can help inform their own approach.

The development of risk tolerance and limits is a critical responsibility of the risk management team. In some cases, utilities may opt to focus initially on high-impact risks, allowing for a more strategic approach to risk management. This process should be conducted in collaboration with risk owners and subject matter experts to ensure that the established limits align with the utility’s operational and strategic goals.

- **Action Item:** Refer to the following supplementary materials to assist with defining the utility’s risk tolerance and risk limits.
  - [Appendix C](#) – Checklist of tasks and activities to consider when working with senior leadership to establish risk tolerance and risk limits.
  - [Attachment II.3: Risk Tolerance and Risk Limit PowerPoint Template](#) – Presentation template for risk tolerance and risk limit engagement with senior leadership.

## Prioritizing Mitigations According to Assessment Results, Risk Tolerance, and Limits

By focusing on high residual risk areas, utilities can optimize resource allocation and develop targeted mitigation strategies to address the likely risks with the highest impact. This approach supports informed decision-making, allowing senior leadership to direct resources and investments where they are most needed, enhance resilience, and ensure operational stability. It also facilitates clear communication of risk management efforts to stakeholders. Below are steps to consider when prioritizing risks based on risk assessment results and considering the utility’s risk tolerance levels and limits.

**Table 11. Steps for Prioritizing Mitigations Based on Utility’s Criteria**

Step	Tasks
Sort Risks by Residual Risk Scores	<ul style="list-style-type: none"> <li>• Arrange risks in descending order based on their residual risk scores, using a risk management tool to automate sorting for efficiency and accuracy</li> </ul>
Evaluate Residual Risk Scores to Risk Tolerance	<ul style="list-style-type: none"> <li>• Assess whether residual risk scores exceed established risk tolerance levels by comparing scores with documented tolerance thresholds</li> <li>• Identify risks requiring additional mitigation, involving cross-functional teams to discuss potential solutions</li> </ul>
Assess Against Risk Limits	<ul style="list-style-type: none"> <li>• Check if any residual risk scores surpass predefined risk limits by referencing the utility’s risk framework</li> <li>• Prioritize these high-risk items for immediate attention, setting up action plans for enhanced controls or mitigation strategies through dedicated team meetings</li> </ul>

- **Action Item:** Update the risk register to further prioritize risks according to the utility’s assessment results, risk tolerance, and risk limits.
- **Action Item:** Review [Appendix D](#) for an example of how the risk register appears once residual risk scores have been compared against the utility’s criteria.
- **Action Item:** Review [Attachment 4: Risk Register Template](#) for additional examples and to update the utility’s risk register.

## Heat Mapping for Visualizing Prioritized Risks

Heat maps are valuable tools for visualizing risk prioritization. They offer a clear and intuitive method to present the comprehensive results of the risk assessment process. Additionally, heat maps serve as a valuable instrument for the ERM team to verify the accuracy and thoroughness of the risk assessment.

Public power utilities can develop heat maps to effectively demonstrate the results of their risk assessment process and risk prioritization. Table 12 outlines the steps to follow when developing heat maps.

**Table 12. Steps for Developing Heat Maps**

Step	Tasks
Create Risk Matrix	<ul style="list-style-type: none"> <li>Draw a 5x5 grid with likelihood on the x-axis and impact on the y-axis, using tools like Excel or risk management software to easily create the grid</li> </ul>
Plot Risks	<ul style="list-style-type: none"> <li>Place each risk's residual score in the corresponding cell based on its likelihood and impact scores</li> <li>Use collaborative workshops to agree on the placement of critical risks</li> </ul>
Assign Colors to Risk Levels	<ul style="list-style-type: none"> <li>Apply a color-coding system to represent risk levels, e.g., green for low risk, yellow for moderate risk, and red for high risk</li> <li>Use Excel's conditional formatting to automate the color-coding process</li> </ul>
Generate the Heat Map	<ul style="list-style-type: none"> <li>Use Excel, Google Sheets, or specialized software to generate the heat map and automatically apply color codes for visual clarity</li> </ul>
Analyze the Heat Map	<ul style="list-style-type: none"> <li>Review the heat map in team meetings to identify high-risk areas that require attention, using it to prioritize mitigation actions and allocate resources effectively</li> </ul>

The basic heat map depicted in Figure 1 is an example of how to assign the appropriate colors for different sections. This heat map reflects the provided example of likelihood and impact criteria from the previous section.

		Likelihood				
		1 (Very Unlikely)	2 (Unlikely)	3 (Possible)	4 (Likely)	5 (Almost Certain)
Impact	5 (Catastrophic)	Green	Yellow	Yellow	Red	Red
	4 (Major)	Green	Yellow	Yellow	Red	Red
	3 (Moderate)	Green	Green	Yellow	Yellow	Red
	2 (Minor)	Green	Green	Green	Yellow	Yellow
	1 (Negligible)	Green	Green	Green	Green	Yellow

Figure 1. Sample of a basic heat map reflecting likelihood and impact criteria

- Action Item:** Refer to [Appendix E](#) to review a sample of a basic heat map and plotting residual risk scores.
- Action Item:** Utilize [Attachment 4: Risk Register Template](#) to develop the utility's heat map.
  - Update the utility's heat map template according to the risk assessment criteria (Likelihood and Impact Levels).
  - Plot the utility's identified risks based on their residual scores.

## Appendix A.1: Simple Risk Scoring Criteria

Use the tables below to document and tailor the utility's risk scoring criteria.

### Likelihood Criteria

Level	Impact Criteria	Description
1	Rare: Unlikely to occur, <5% chance	
2	Unlikely: Could occur occasionally, 5% - 20% chance	
3	Possible: Might occur, 21% - 50% chance	
4	Likely: Will probably occur, 51% - 80% chance	
5	Almost Certain: Expected to occur, > 80% chance	

### Impact Criteria

Level	Impact Criteria	Description
1	Insignificant: No significant impact	
2	Minor: Limited impact, easily manageable	
3	Moderate: Noticeable impact, manageable	
4	Major: Significant impact, requires attention	
5	Catastrophic: Severe impact, critical	

## Appendix A.2: Expanded Risk Scoring Criteria

Impact Level	Financial (Liquidity Ratios)	Reputational	Regulatory/ Compliance	Operational	Health, Safety, Environmental
1 (Minimal)	Current Ratio > 2.0	Isolated incidents with no media coverage, quickly resolved	Full compliance with regulations, no fines or warnings	No significant operational disruptions, routine maintenance	No significant injuries or environmental impact
2 (Low)	Current Ratio 1.5-2.0	Localized customer complaints with limited media attention	Minor regulatory issues with corrective actions and low-level fines	Minor system disruptions with quick restoration	Minor injuries requiring medical treatment, small-scale environmental incidents
3 (Moderate)	Current Ratio 1.2-1.5	Regional service complaints with moderate media attention	Moderate regulatory infractions with potential for fines and increased scrutiny	System malfunctions with service interruptions up to a day	Hospitalizations due to safety incidents, moderate environmental spills
4 (High)	Current Ratio 1.0-1.2	Major negative media coverage with significant customer dissatisfaction	Serious non-compliance with substantial fines and regulatory intervention	Major system failure with service outages lasting several days	Serious injuries or fatalities, significant environmental incidents
5 (Severe)	Current Ratio < 1.0	National scandal with long-term customer trust erosion	Major violations with risk of revocation of operating license	Catastrophic infrastructure failure with extended service outages	Multiple fatalities or severe environmental disaster

This table categorizes risk impact levels for public power utilities across five areas – financial health (measured by liquidity ratios, which reflect the utility’s ability to meet short-term obligations); reputation (based on customer trust and media coverage); regulatory compliance (adherence to industry standards); operations (measuring the severity of service disruptions or infrastructure failures); and health, safety, and environmental concerns (safety incidents and environmental harm). A higher current ratio signals stronger financial stability, essential for utilities to manage unexpected costs.

This scoring criteria helps utilities assess risks with varying levels of severity, guiding them in addressing more frequent, day-to-day challenges and ensuring stability across core operational areas to maintain operational reliability and public trust.



## Appendix A.3: Expanded Risk Scoring Criteria

Impact Level	Financial (Liquidity Ratios)	Reputational	Regulatory/ Compliance	Operational	Health, Safety, Environmental
1 (Minimal)	Loss < 2% of annual revenue or negligible impact on financial stability	Isolated incidents with no media coverage, quickly resolved customer issues	Full compliance with regulations, no fines or warnings	No significant operational disruptions, normal maintenance activities	No significant injuries or environmental impact, incidents contained within utility property
2 (Low)	Loss 2-5% of annual revenue or minor impact on financial ratios	Localized customer complaints with limited media attention, manageable social media concerns	Minor regulatory issues with corrective actions required low-level fines	Minor system disruptions with quick restoration, minimal service impact	Minor injuries requiring medical treatment, small-scale environmental incidents with quick remediation
3 (Moderate)	Loss 5-10% of annual revenue or impact on ability to fund capital projects	Regional service quality issues leading to customer complaints and local media attention	Moderate regulatory infractions with potential for fines, increased scrutiny	Disruption due to system malfunctions or maintenance, service interruption for hours to a day	Hospitalizations due to safety incidents, moderate environmental spills with containment
4 (High)	Loss 10-20% of annual revenue or significant rate of return reduction	Major service outage with widespread customer dissatisfaction, high-profile media coverage	Serious non-compliance with environmental or safety regulations, substantial fines, or penalties	Major equipment or system failure, service outage lasting days	Serious injuries or fatalities, significant environmental incidents with regulatory intervention
5 (Severe)	Loss > 20% of annual revenue or breach of debt covenants	National scandal involving service failures, sustained negative media, and political intervention	Violation of critical regulatory requirements, leading to potential shutdown or loss of franchise	Complete failure of critical infrastructure, long-term service outage	Multiple fatalities or potentially dangerous situations due to utility failure, catastrophic environmental damage

This table outlines impact levels for utilities based on financial loss as a percentage of annual revenue, reputational damage, regulatory breaches, operational disruptions, and health, safety, and environmental risks. It quantifies financial impact directly through revenue loss, while emphasizing severe regulatory and operational consequences, including shutdowns or long-term outages.

Public power utilities may use this risk scoring criteria to prioritize risks with the greatest potential for operational and financial damage, helping guide decisions on mitigation strategies and resource allocation. It is particularly useful for evaluating high-impact, low-frequency events that could significantly disrupt service and long-term viability.

## Appendix B: Simple Risk Register with Risk Scoring

Risk Identification			Pre-Assessment			Risk Assessment				
Risk ID	Risk Description	Category	Pre-Mitigation			Controls/Mitigation Strategies	Post-Mitigation			
			Likelihood Level	Impact Level	Risk Score		Proposed Risk Owner	Likelihood Level	Impact Level	Residual Risk Score
R001	Critical equipment malfunction leading to operational disruptions	Operational	3 (Possible)	4 (Major)	12	Regular maintenance schedule Spare parts inventory Equipment monitoring system	Operations Manager	2 (Unlikely)	4 (Major)	8
R002	Data Breach compromising sensitive data (PII)	Cybersecurity	3 (Possible)	4 (Major)	12	Network security protocols Regular security audits Employee cybersecurity training	IT Specialist	2 (Unlikely)	3 (Moderate)	6
R003	Employee safety incidents (minor)	Safety/ Compliance	4 (Likely)	2 (Minor)	8	Safety training programs Personal protective equipment Incident reporting	Safety Officer	3 (Possible)	2 (Minor)	6
R004	Increased energy procurement costs	Financial	4 (Likely)	3 (Moderate)	12	Long-term power purchase agreements Diversified energy sources Regular market analysis	Procurement Manager	3 (Possible)	3 (Moderate)	9

### Analysis of the risk register above:

The residual risk scores indicate that while mitigation efforts have reduced the likelihood of risks, the high impact of critical equipment malfunctions and increased energy procurement costs continue to warrant ongoing attention and preparedness.

### Additional Recommendations:

- Smaller utilities should focus on cataloging a manageable number of high-priority risks, typically between 10 to 20. Prioritize risks with significant impact or likelihood to avoid resource strain and diminishing returns. Regular updates ensure alignment with the utility's evolving operational and strategic goals.
- Establish a clear process for identifying and escalating risks with near-term consequences. Use residual risk scores and triggers such as high impact, likelihood, or timing to flag risks for senior leadership review. Ensure these risks are promptly addressed to mitigate potential disruptions.

## Appendix C: Setting Up Risk Tolerance and Risk Limit Checklist

Utilities can use the following checklist to stay organized while collaborating with senior leadership to establish risk tolerance levels and risk limits tailored to the utility's needs and strategic goals. For utilities in the early stages of ERM, this checklist is invaluable for maintaining organization, ensuring no steps are overlooked, and preparing the ERM committee to effectively execute this aspect of the risk management process.

Step	Status
<b>Preparation</b>	
Summarize the key risks and impacts from the risk register	
Research industry examples for risk tolerance and limits	
Draft initial ideas for risk tolerance levels and limits	
<b>Setting Limits</b>	
Make sure risk levels match the utility's strategic goals	
Agree on how much risk is acceptable	
Decide on clear limits for each risk (e.g., financial loss caps)	
<b>Engage Senior Leadership</b>	
Set up a meeting with senior leadership to discuss risk tolerance and risk limits	
Present the risk register and initial proposals	
Get input from senior leadership on risk levels	
<b>Documentation and Approval</b>	
Document the agreed upon risk tolerance levels and limits	
Have senior leadership formally approve the guidelines	
<b>Implementation</b>	
Make sure risk levels and limits are part of daily operations	
Set up simple process to regularly check if risk tolerance levels stay within the risk limits	
<b>Review</b>	
Make changes with leadership input when necessary	

## Appendix D: Simple Risk Register with Applied Risk Tolerance and Limit

Risk Identification			Risk Assessment							
Risk ID	Risk Description	Category	Controls/ Mitigation Strategies	Post-Mitigation						
				Proposed Risk Owner	Likelihood Level	Impact Level	Residual Risk Score	Risk Tolerance	Risk Limit	Status
R001	Critical equipment malfunction leading to operational disruptions	Operational	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	Within limit but requires immediate attention
R002	Cyber-attack compromising sensitive data	Cybersecurity	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	Within limit; monitor regularly
R003	Employee safety incidents (minor)	Safety/ Compliance	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	Within limit; review safety protocols
R004	Increased energy procurement costs	Financial	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	Within limit but requires immediate attention

**Analysis of the risk register above:**

All residual risks are within acceptable tolerance levels and well below the critical risk limits, indicating effective control measures. However, the risk of critical equipment malfunction (R001) and risk of increased energy procurement costs (R004) are close to the tolerance threshold, suggesting the need for ongoing attention to prevent escalation. Cybersecurity (R002) and Employee Safety (R003) are well managed, providing senior leadership with confidence in the utility's current risk posture, though continuous monitoring and periodic review are recommended.

# Appendix E: Plotting Residual Risk Scores on a Heat Map

Using the example from [Appendix D](#), the residual risk scores (likelihood and impact scores after mitigation) are plotted on the following heat map. Based on these residual scores, the ERM committee can confirm that the risk assessment process aligns with their initial perception of the severity of these risks, considering the utility’s risk tolerance and limits.

- Plotting Appendix D examples on a heat map
  - R001: Critical equipment malfunction leading to operational disruptions (2,4)
  - R002: Cyber-attack compromising sensitive data (1,5)
  - R003: Employee safety incidents (minor) (3,2)
- Heat Map Interpretation
  - Top-Right Corner (High Impact, High Likelihood): These are critical risks requiring immediate action
  - Center Grid (Moderate Impact, Moderate Likelihood): Risks to monitor regularly
  - Bottom-Left Corner (Low Impact, Low Likelihood): These are lower-priority risks but should still be acknowledged

		Likelihood				
		1 (Very Unlikely)	2 (Unlikely)	3 (Possible)	4 (Likely)	5 (Almost Certain)
Impact	5 (Catastrophic)					
	4 (Major)		R001			
	3 (Moderate)		R002	R004		
	2 (Minor)	R003				
	1 (Negligible)					

The ERM committee should interpret the heat map as:

- Immediate action is required to address R001 and R004 due to its major impact. To address R001, the utility should implement regular maintenance schedules, manage spare parts inventory, and utilize equipment monitoring systems to prevent significant disruptions. To address R004, the utility should negotiate long-term contracts and consider hedging options, diversify energy sources, and establish a contingency fund.
- Although R002 has a catastrophic impact, its likelihood is very low, placing it in the moderate green zone. While R002 is within the limit, the utility should continue monitoring and maintain robust cybersecurity measures to address potential issues.
- Regular review and enhancement of safety protocols are necessary to address R003. The utility should improve safety training, ensure adequate personal protective equipment, and maintain an effective incident reporting system to manage minor safety incidents.