

Activity: Developing Vulnerability Statements and Assigning Vulnerability Severity Scores

Goal of this Activity

In this activity, you will identify potential vulnerabilities that your power sector may face from possible threats, form vulnerability statements, and assign a severity score to each.

Introduction

The output of this activity will provide a foundation for understanding the vulnerabilities that your power sector may face at different planning scales of concern, such as city, national, or regional/multinational.

Exercise 1: Developing Vulnerability Statements

Use the table below to identify the vulnerabilities associated with the top five threats identified in prior activities. The vulnerability statement answers the “why” question or “why might this threat impact the power sector?” For each of the threats and associated impacts in the table below, begin by asking the question, “why does this threat impact the power sector?” Reaching the final vulnerability of the power sector may require asking this question multiple times. The vulnerability statement should not propose a solution—instead, it offers an objective statement of what makes the power system vulnerable. Developing these statements likely requires discussions with colleagues because there is no simple formula.

Key Terms

Before identifying vulnerabilities, it is helpful to clarify a few key terms in relation to power sector resilience.

Vulnerabilities—weaknesses within infrastructure, processes, and systems, or the degree of susceptibility to various threats. Different measures can be taken to reduce vulnerability or improve adaptive capacity to threats to the power sector. Vulnerabilities are typically identified through stakeholder interviews, technical analyses, and/or literature reviews¹.

Threats—anything that can expose a vulnerability and damage, destroy, or disrupt the power system. Threats can be natural, human caused, or technological. Threats are not typically within the power system operator’s control. They can include wildfires, hurricanes, storm surges, and cyberattacks. For additional information on threats, refer to the *Threats* section of this guidebook¹.

Impacts—the extent to which a threat affects power sector infrastructure and processes (e.g., a typhoon causes wind damage to transmission lines which disrupts power to customers for a specific duration).

Exercise 2. Vulnerability Severity Scores

After drafting all five vulnerability statements in the table below, we can assess the severity of each vulnerability on the power sector and assign a severity score. As described in the *Guide to Vulnerabilities* section, assign each vulnerability statement a severity score based on how problematic the exposure of this vulnerability could be. Assign one of the following scores to each of the five vulnerabilities listed below:

High | **Medium-High** | **Medium** | **Low-Medium** | **Low**

Refer to the *Guide to Vulnerabilities* section for a description of the thresholds for this scoring system.

Threats	Impacts	Why?	Vulnerability Statements	Severity Scores
Example <i>Lightning strike</i>	<i>Damaged poles, power outage</i>	Why? ↑	<i>Lack of lightning protection on transmission and distribution equipment increases the likelihood of a lightning strike damaging transmission poles, leading to a power outage.</i>	<i>Medium</i>
Threat 1		Why? ↑		
Threat 2		Why? ↑		
Threat 3		Why? ↑		
Threat 4		Why? ↑		
Threat 5		Why? ↑		