CYBER RISK ASSESSMENT

RISK ASSESSMENT TIPS

- Refer to CESER's *Risk Assessment Essentials* for consistent methodologies.
- Follow the **CIA Triad**: Confidentiality, Integrity, Availability—evaluate the importance of each aspect to your methodology.
- Choose balanced scoring scales (e.g., 1–5); ensure meaningful differences between numbers.

QUALITATIVE VS. QUANTITATIVE CHALLENGES

- **Qualitative:** Uses a corresponding number that represents descriptive words (e.g., *low = 1, medium = 2, high = 3*) to assess risk impact. This is useful for capturing judgment-based insights when detailed data isn't available.
- **Quantitative:** Uses real numbers informed by measurable data (e.g., monetary values or historic probabilities) to assess risk. This is more costly, time consuming, and difficult than a qualitative assessment.

TOP THREE SOURCES

THREAT SOURCES:

VULNERABILITY SOURCES:

CONSEQUENCE SOURCES:

Category		Annual Threat Probability (% per year)		
Score	Tier	Uniform Scale	Adjusted Uniform Scale	Rough Order of Magnitude Scale
1	Low	0%-20%	0%-10%	<1%
2	Med-Low	20%-40%	10%-20%	1%-5%
3	Medium	40%-60%	20%-30%	5%-15%
4	Med-High	60%-80%	30%-40%	15%-35%
5	High	80%-100%	>40%	>35%

CYBER RISK ASSESSMENT STEPS

IMPACT AREAS TO CONSIDER

- Security
- Evacuation
- Environment
- Tactical
- Strategic
- Economic
- Fatalities

KEY CONSIDERATIONS

- **Stakeholders May Assess Risk Differently:** Focus on broad concurrence from stakeholders or adjust assumptions as needed. Bring subject matter experts together to discuss consequences and impacts.
- **Credible Sources:** Collect information from reliable datasets, industry briefs, and SMEs. Surveys are helpful for gathering quantitative insights.
- **Defensible and Replicable Assessments:** Prioritize methodologies that can be justified and replicated across time and cases.

U.S. DEPARTMENT of ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

Pacific Northwest NATIONAL LABORATORY

NASEO National Association of State Energy Officials

PNNL-SA-218830