# Risk Management in Critical Infrastructure Protection:

## An Introduction for State Utility Regulators

Miles Keogh
Sharon Thomas
NARUC Research Lab

September 2016

NARUC

The National Association of Regulatory Utility Commissioners

With support from the U.S. Department of Energy

**Acknowledgements and Disclaimers**

The report you are reading was created under the National Council on Electricity Policy & Energy Assurance program, a project of the National Association of Regulatory Utility Commissioners (NARUC) Research Lab. This material is based upon work supported by the U.S. Department of Energy under Award Number DE-OE0000578.

This report was authored by the NARUC Research Lab. Throughout the preparation process, the members of NARUC provided the authors with editorial comments and suggestions. However, the views and opinions expressed herein are strictly those of the author(s) and may not necessarily agree with positions of NARUC or those of the U.S. Department of Energy.

Special thanks to The U.S. Department of Energy.

Please direct questions regarding this report to Miles Keogh, NARUC's Director of NARUC Research Lab, mkeogh@naruc.org; (202) 898-2200 and Sharon Thomas, Senior Program Officer, NARUC Research Lab, sthomas@naruc.org; (202) 384-1572.

## Introduction

This is a paper about risk management: what it is, how regulators can use it, and how they can ask questions to explore its use by the regulated utilities and other stakeholders they interact with. Regulators are increasingly advised to rely on decisions based on risk management - that's often good advice, but to take advantage of it, state commission officials may want to become more familiar with what risk management is and how it is employed. Many regulators are familiar and comfortable with risk-based processes and the qualitative and quantitative methods for understanding risk, but many are not. If you don't know a stochastic method from a kick in the knee, this primer is meant for you. It's not our goal to be comprehensive here, just to get you on-boarded to the conversation. Risk management is a complex discipline that leverages statistics and other quantitative methods, as well as psychology and other qualitative methods, and you can spend your entire life earning degrees in its theory and application. Instead, this paper lays out an introduction to what risk management is, and gives a few starting points for regulators interested in augmenting their processes with it. In particular, it focuses on the basic concepts of risk management and on ways that regulators can employ risk-informed thinking to make choices around the areas of critical infrastructure protection and energy assurance.

## Reading the future with risk management

Decisions about how to invest in, and secure, our country's power sector infrastructure are complex: markets, technology and policy interact in complex ways over time that make the future diabolically hard to predict. Should I build a 40 year power plant when all I have is a five year fuel price forecast? What hazards may emerge in ten years threatening hardware that will be in the field for twenty? What if growth turns out to be twice as much as expected, or half? Regulators answer these types of unanswerable questions each day, by balancing options informed by their intuition with information generated through their formal or informal use of risk management. That's right: you are probably using risk management without even realizing it. At its heart, risk management is a process that helps deal with the fact that the future is unknowable.

> *Every successful technology of thought, be it science or philosophy, is a time machine — it peers into the past in order to disassemble the building blocks of how we got to the present, then reassembles them into a sensemaking mechanism for where the future might take us. (Maria Popova, 2015)*

It's a powerful resource to regulators because they are futurists: they have to peer into the unknowable mists of what may happen in the coming years and try to see a prudent path enabling utilities to seize opportunities and avoid the worst pitfalls. What tools can they use to help separate the impossible from the probable? What means can they use to make good choices when preparing for tomorrow means more than using your best guess? There's no fortune telling or crystal ball

needed. Regulators can make better choices about the future using a process called Risk Management.

## The magic risk management equation

The power grid faces a number of potential events that are hard to predict, some of them good and some of them very bad. Evaluating risk and managing it in a critical infrastructure context generally focuses on unwanted events, and to do this means examining three factors:

Risk = probability | vulnerability | consequence

In practice, understanding risk this way means understanding:

1. **Probability**: (how likely is it? Is there any kind of statistical recurrence for how often it happens, like flooding or storms?
2. **Vulnerability**: how exposed to this event are we? Coastal states will be more vulnerable to tsunami than inland states, companies with extensive and aging data networks may have more cyber vulnerabilities to manage, etc., and
3. **Consequence**: how bad would the event be? In the power grid, this is traditionally measured by duration and extent of outages, but long duration outages, outages affecting critical facilities, and other complexities complicate the questions one could ask.

In fact, regulators consider these kinds of questions implicitly in many of their investigations of the prudence of company spending and activity. Although they have to make decisions under conditions of uncertainty, they may or may not be familiar enough with risk management as a discipline to leverage it in informing their choices. This primer explores risk management from the particular lens of its use in making decisions that protect critical utility infrastructure. It does not serve as a substitute for more complete works on the topic, but it should be enough to give a basic vernacular so that you understand what people are talking about when risk management comes up in regulatory proceedings, and to point you in the direction of resources that can provide deeper context.

## The case for using risk management

Why is risk management such an important area for regulators to understand? What's wrong with just using our best judgement? When we understand problems better we make better choices about solutions, and risk management clarifies problems to help us see the range of ways to manage them more clearly. In their indispensable guide to risk management for regulators, Jan Beecher & Steve Kihm (2016) argue that our intuition is shaped by experiential and cognitive biases. If regulators rely on their intuition or best judgement, recent experience

can lead to an overly narrow conception of what the possible outcomes are. Essentially, human beings are biased to think the way things will go in the future is a lot like how they've been going lately. Unsurprisingly, the future does not work that way. Risk management provides information that helps us understand ways that the future may be different than the recent past. This isn't to say that regulators should depend wholly on number crunching and abandon their experience and judgement: good decisions aren't just a function of data but also of wisdom. The human element in deciding the best course of action is the most important element. Risk management simply gives us clearer information about the possibilities.

## Understanding risk management

Risk is a very trendy word in the power sector, which means it's badly mis-used. For example, we often use the word "risk" when we mean "threat", and threats are just one component of risk. A threat is a potential event that is unwanted, and that we cannot be certain will happen.

Risk is also often conflated with uncertainty, and while they are related – they both are ways of looking at the unknown - they are different. Uncertainty describes the range of immeasurable possibilities, assessed subjectively. Risk refers to measurable probabilities, assessed quantitatively. In other words, risk is a perspective on the unknown that uses probabilities and other objective measurements to winnow out things that are impossible, and narrow down how much is simply unknown (Bernstein, 1998). Risk management is usually applied to the future, to unforeseeable events, and to describing reasonable responses to them.

It's easy to dismissively argue that you can't predict the future, but in fact you can narrow down a lot about what may or may not happen in the future. "Unknowable" things are more understandable than you may think. Let's say I ask you to guess how big my house is. Don't answer "I have no idea" – you have some idea! Is it smaller than a cardboard box? Larger than the Empire State Building? You've already narrowed down the range of the unknown with probabilistic conceptual tools akin to those we use to predict events in risk management.

Risk may seem scary, but it's not. Risk management in most critical infrastructure contexts is understood negatively: risk is something to avoid in these conversations. Outside a context of dealing with threats though, risk can be positive, and when described in a financial context is often something sought out by investors. More fundamentally, risk is simply a fact of life – it's unavoidable when making decisions under conditions of uncertainty, and cannot be eliminated (Beecher & Kihm, 2016). Regulators who use risk management effectively are aware that you can reduce *exposure* to risk, *mitigate* its effects, or *shift* it to others, but you cannot eliminate it as long as the future is unpredictable.

Other industries that employ risk management (particularly finance) also understand that risk is symmetrical: it has both negative and positive characteristics. In the financial world, a company can earn more money by taking on more risk and managing it effectively. When making choices to improve shareholder value, companies are often motivated to take on risk to earn greater

returns (Beecher & Kihm, 2016). Whether an investor is willing to take on more risk in the hopes of higher returns is a question of **risk tolerance**. If the value of returns appears to exceed the chances of loss, and the investor has a high risk tolerance, chances are he or she will go for it. Risk tolerance is a value judgement made by the person choosing to take the risk. It is an important concept for regulators as well, because it informs how much they are willing to expose utilities, ratepayers, and other stakeholders to risk. We'll offer more information on how you can establish your risk tolerance later in the paper.

## Using risk management for critical infrastructure protection

Why is critical infrastructure protection a good arena for the application of risk based concepts by state commissions? It is because even though we have seen catastrophic disasters and severe weather events like Katrina, Sandy and so forth, a range of **"black sky" hazards**[1] that are difficult to anticipate and predict and are not part of our recent frame of reference. Again, we are biased to think the future will look like the recent past, and so we are poorly prepared when it does not.

Starting in 2013, NARUC (and others in the power sector) began exploring a new class of threats to reliable service, threats that expand in scope or duration beyond the range of that the United States has experienced in the past decade. These threats – sometimes termed "high impact, low frequency" events have been explored as a category unto themselves, yielding consequences that are larger and more devastating than "grey-sky" events like hurricanes Sandy, Katrina, and Irene (among others), cyber intrusions in the power sector, or the criminal attack on the Metcalf substation in California. The entry-level of the range of a "Black Sky" event would be the Tohoku / East Japan earthquake and tsunami of 2011. NARUC's 2014 primers on Resilience in Regulated Utilities (Keogh, 2013) and on Resilience for Black Sky Days (Stockton, 2014) outlined some of the challenges for regulators posed by these events.

Building from this background, NARUC ran a number of workshops on how to deal with unpredictable infrastructure protection challenges in 2014-2016 in five regions, including several exercises on cost recovery decision-making. These were played out for regulators in five regions of the country in 2014-2015, and in 2016 for a national audience and for a group of state legislators. Various questions that state regultors and legislators are faced with when making decisions abour resilience of critical infrastructure were explored using a fictional utility company. NARUC did this by taking participants through a number of "calamity" scenarios – both natural and man-made events – to see how risk-informed choices can be made with imperfect information. The information given to participants was overarchingly qualitative in nature, with only minimal quantitative data, to allow participants to understand how value

[1] a term used by electric infrastructure security experts when discussing a multi-regional collapse of the North American power grid, resulting in a devastating societal impact presenting extraordinary problems for public safety and power restoration (Stockton, 2014).

judgements come into play when decision-makers are choosing between resilience options. First the fictional power company presented a list of potential or anticipated events that could take place and have adverse consequences. Then the utility proposed a list of investments it felt prudent to undertake in order to mitigate the risks of the anticipated events. Thereafter, participants assessed the threat/likelihood, vulnerability, consequence, and risk of all the anticipated events tha the utility explained (this was based on whether or not this event actually occurs in the participants' home states at each table). Next, participants were presented with mitigation strategies to combat the various threats and they had to assess how much to approve based on the amount requested by the utility company, as well as the rationale for the amount chosen. Lastly, the participants evaluated how their investment decisions faired, in terms of whether their investment paid off, broke even, or if the benefits were mostly unrealized.

To solve these problems, we asked regulators to explore using checklists that articulate specific actions that can help companies be prepared. We also asked them to look at evaluating the probability that something could happen, the vulnerability they had to that event, and the seriousness of the consequences if it happened, and informed by these three factors, to prioritize preparedness. Here is an outcomes chart that was made by one team in our resilience exercise from May 2016 in Denver – note that this was one team's judgement, uninformed by data, but that helped them prioritize their preferences for preparedness.

*One team's ranking of risk for catastrophic events, Denver, 2016*

| **EVENT** | **PROBABILITY** | **VULNERABILITY** | **CONSEQUENCE** | **RISK** |
|---|---|---|---|---|
| *Storms* | High | Medium | Medium | *High-medium* |
| *Cyber attack* | Low | High | High | *High* |
| *Electromagnetic pulse* | Low | Medium | High | *Medium* |
| *Downed trees* | High | High | Low | *Medium* |
| *Flooding* | Medium | Medium | Medium | *Medium* |
| *Pandemic* | Low | Medium | High | *Low* |

Some of the groups used tools provided by the NARUC workshop organizers that specifically highlighted the risk factors associated with different kinds of events, and asked participants to prioritize spending based on consequence, likelihood, and threat. One of the key lessons learned by participants is that those who explored the potential hazards using that risk-informed perspective performed better than those who used intuition and judgement without prioritizing events using risk management. Without exploring the likelihood, vulnerability, and consequences, participants made decisions based strictly on their intuition and recent experience. Asking fundamental risk-oriented questions helped the best teams clarify their challenges and identify better management strategies.

Lessons learned in a tabletop context may not always guarantee results in the real world. When it's not an exercise, how do we decide whether to invest in storm preparedness, cybersecurity, EMP protection, flood response, or vegetation management? Will we make better choices if we outline a list of standard steps to take, or will more prudent action be driven by an expectation that those protecting those assets will prioritize actions based on probability, vulnerability, and consequence?

## Making decisions using risk management

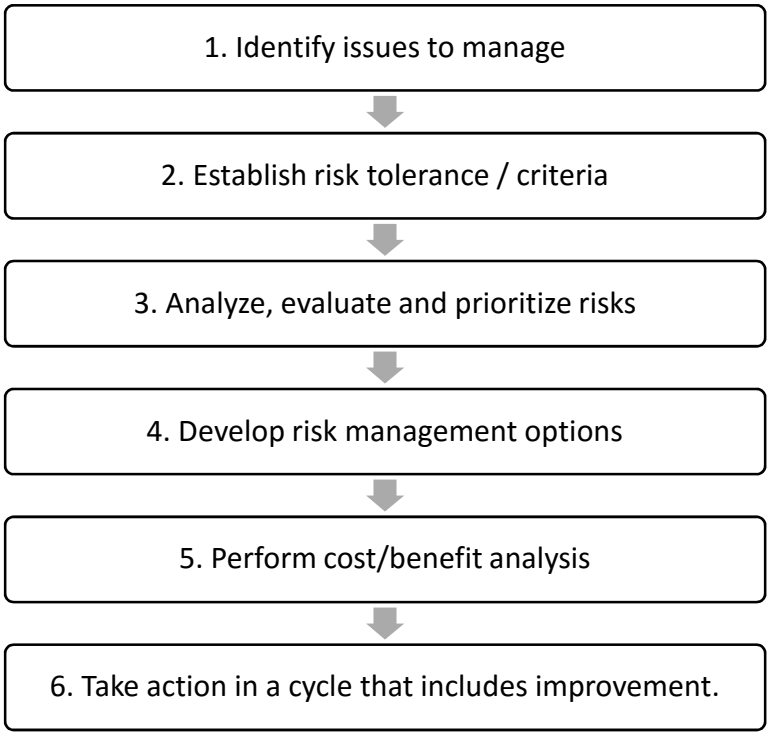
In our workshops, we asked regulators to use qualitative assessments to describe risk and prioritize actions, but in the real world, more quantitative assessments and methods give better information about the possibilities and are very useful. Even for economic regulators steeped in rate calculations and load forecasting, these quantitative methods may seem complicated and intimidating. If you've had only brief exposure to risk management, you probably have a lot of questions. What are company experts talking about when they say they use Bayesian or stochastic methods? Is a "Monte Carlo run" some kind of casino scandal? When are subjective or qualitative tools sufficient, and when do you need to crunch numbers help narrow down the unknown?

For regulators overseeing expenditures by companies using limited resources, maybe the most important question is where to best put those resources to most effectively manage risk. This section explores two issues: what risk-based processes regulators can use at their commissions to inform their own decisions, and what risk management tools are being used by companies to manage their infrastructure investments.

A good time to try implementing a risk management process in your own decision-making is when confronting a question that has a lot of unknowns in your commission. Critical infrastructure protection is a good issue area to explore with this mechanism: there are a range of trade-offs, many unknowns, interdependencies galore, and potential events that are low probability but high consequence. A lot of attention has been paid recently to the notion that utility cybersecurity is a risk management problem, so risk-informed decision-making may be particularly appropriate as a mechanism for regulators to explore this set of issues.

When companies explain that they are using risk-based approaches to manage their choices, it may be helpful to have an understanding of what a risk-based approach looks like. These will vary based on the company's (or commission's, if you're using it yourself) approach, but one example that illustrates the steps in a risk-based decision-making framework is illustrated below:

*Structure of a risk-informed decision set*




## Executing risk management

The next section of this paper walks through what each step entails.

1. Identify your issues to manage

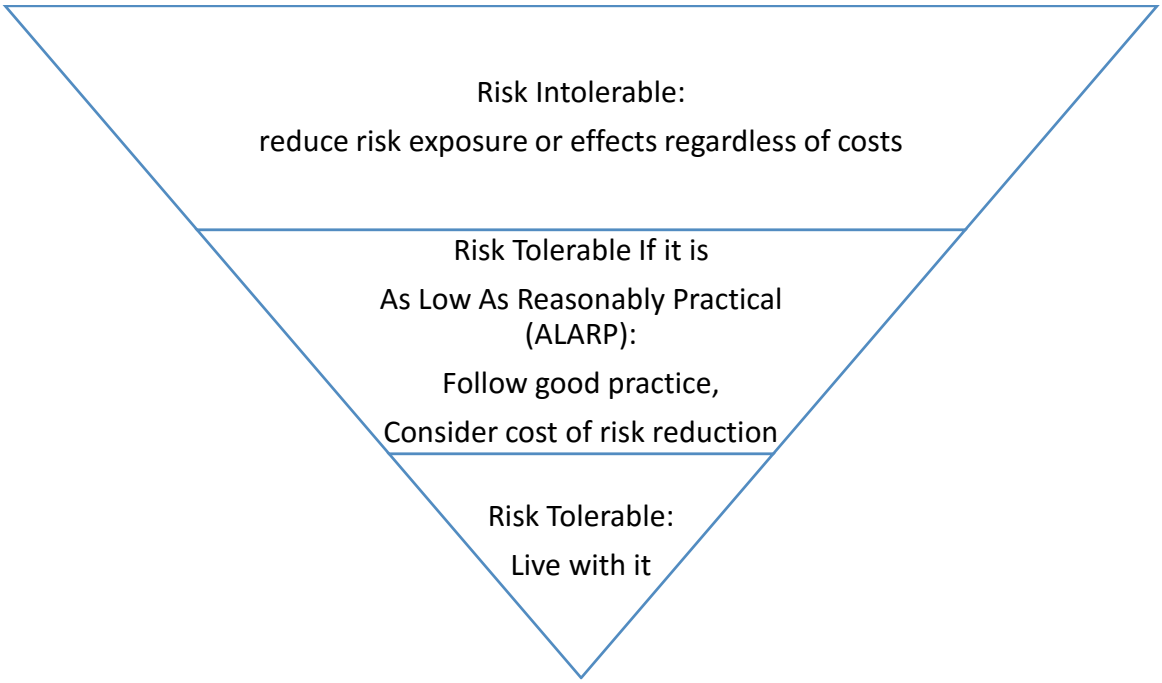
The range of potential issues to examine is infinite so a first step is articulating what issues you're going to include. A risk manager would start by identifying potential areas to consider, then establish a baseline for where they are today. For example, they might say the issue of concern is water, note that the system is impervious to rain but may have critical systems in a flood-prone area. The decision-maker would establish an objective, the position they would like to get to, in this case, mitigating flood risks.

2. Establish your risk tolerance

Identifying your values helps determine how much risk you're willing to live with, how much you're willing to deal with, and how much you're driven by existential threat to mitigate completely. For example, we probably have a high tolerance for rain, and a low tolerance for exposure to heavy flooding, and would act differently in response to those threats. A triangle graphic may help differentiate between what you can live with and what you cannot - this range of tolerances is illustrated by the ALARP triangle below, and it may be helpful in deciding

which risks are must-mitigate completely, must address to keep risks as low as reasonably possible (ALARP), and which risks are nuisances to live with.

## The ALARP Triangle: How Much Risk Can I Handle?




(UK HSE, 2016)

The risk manager would identify the threshold that they are willing to live with – they may say a thousand year flood is beyond the management scope, but a 5 year flood would be within the range of threats to manage. That process establishes the values that inform their risk tolerance.

3. Analyze risks and prioritize them

Once risks are scoped and tolerance is established, it is time to ask about what is known and unknown, and to distinguish perceived risk from calculated risk. To do this, a risk-management decision starts by describing threat, probability, and consequence. Understanding these three variables helps you understand whether something feels like a big risk, or whether it actually is a big risk. This is helpful when managing a mix of knowns and unknowns, for example how to protect against an event that has never happened before, or whose consequences are unpredictable.

This is where an important obstacle comes in relating to uncertainty. For many of the threats being managed, it may be difficult to get or make data about how likely, how vulnerable, or how consequential the event is. Subjective and qualitative methods can be very helpful, but qualitative tools can create data that can inform decision-maker judgements with some objectivity. (That said, the best quantitative approaches are only as solid as the assumptions and inputs you use to calculate the outcomes. Start with biased assumptions and you're going to get biased results.)

The degree to which risk managers have information determines whether their choices are being made under certainty, under risk, or under uncertainty, and each of these three states comes with their own ways of moving forward (Hoppock &Echeverri, 2014).

For *decisions under certainty* – where data exists or strong inferences can be made about risk factors - the decision-maker can use projections or deterministic methods to select a direction. A deterministic approach tries to yield a single answer that always describes the outcomes of an experiment. It assumes your outcome is certain if the input to the model is fixed; no matter how many times you recalculate it, you get the same result. Examples include the way we traditionally evaluate reliability such as with SAIDI, SAIFI, CAIDI, and MAIFI. These analytic frameworks have strong data underpinnings and use rigorous projections that may not be available in all decision-making contexts, and illustrate areas where strong deterministic approaches can be successful. Transmission planning that evaluates failure contingencies is another example of a deterministic approach that uses, and generates, a large amount of data that's repeatable. Some characteristics of deterministic methods are that they are much less data intensive (compared to a probabilistic approach, described later), planners are well-versed with deterministic criteria used in planning, and the planning criteria is well-established and well-understood. (EPRI, 2014)

What if there's less data than you need to make a completely informed choice? For *decisions under uncertainty* - where there are a range of potential outcomes in a single calculation – probabilistic methods are better suited. A probabilistic approach is intended to give you a distribution of possible outcomes, and describes all outcomes and the likelihood of each outcome occurring. Stochastic models are a common method for generating probabilistic data.. These methods use statistics to infer outcomes based on randomly selected alternatives. This is helpful when you have a huge amount of scenarios that far exceed the ability of decision-makers to model. Scenarios are randomly determined from the range of possibilities; having a random probability distribution or pattern that may be analyzed statistically but may not be predicted precisely. A number of stochastic methods exist but each of these, in some way, use inputs and assumptions to model a range of possible results to determine the range of likely, unlikely, and barely probable events.

Characteristics of a probabilistic approach are that it is very data intensive; little industry-wide planning criteria is currently established. Considerably more research may be needed and

there is a lack of skill-set and subject expertise for this approach to be used in utility planning for critical infrastructure protection (EPRI 2014).

A third approach is "what if" modeling that is more deterministic and precise – you can understand what would happen at a deep level of detail for a small number of variables – but isn't as useful for more complex problems that have multiple inputs, criteria, variables, and potential outcomes.

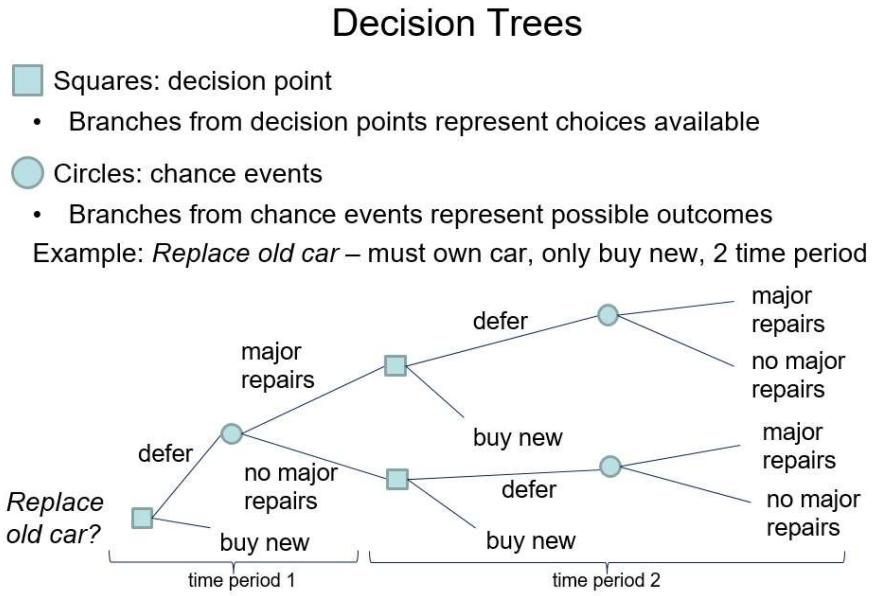
Even in areas where quantitative analysis will prove challenging, eliminating unknowns will clarify alternatives and postulating possible futures will illustrate the values and risk tolerance of stakeholders. A quantitative approach shouldn't overwhelm the reasoned judgements of decision-makers, and number-crunching may partner well as a supplement to approaches that determine human elements like intentions and values. Among qualitative approaches, having a few methods to complement each other helps give you information from different angles, so a probabilistic approach may be used to supplement a deterministic approach. Using sensitivities – changing your inputs to see what happens to the outcomes of models – can also help validate the quality of the information produced. Decision-makers may want to use more than one tool, leveraging qualitative and quantitative methods - to reduce unknowns.

**What is Monte Carlo simulation?** It's a commonly-used stochastic modeling method that runs all the knowable possibilities and gives a range of possible outcomes and the probabilities they will occur for any choice of action. It shows the extreme possibilities along with possible consequences for middle-of-the-road decisions.

Ultimately, there are some decisions with far more unknowns than predictable knowns. For problems like these, there are still ways you can get a clearer picture of what is possible. One potent tool is the development of scenarios to limit an infinite problem set to a limited number of situations which we can imagine as being possible (Morgan, 1992). From there we can determine whether there are choices that maximize benefits, limit regrets, and effectively mitigate risks. For decisions under uncertainty, scenarios can be articulated using this process:

1. Enumerate driving trends and extrapolate your scenarios
2. Characterize uncertainty
3. Set decision criteria

Decision-making under uncertainty can leverage tools that help clarify your choices, like influence diagrams and decision trees. Influence diagrams and decision trees are useful to identify key variables that affect your decision and to represent path dependencies (how one choice leads to others, creating or eliminating others.) Here is an example of a decision-tree around whether to replace a car:




*Source: Duke University NARUC risk training, (Hoppock & Echeverri, 2014)*.

You already have many tools available to formulate probabilities at your commission. You can draw from:

- Your professional intuition
- Other sources – consultants, etc.
- Expert elicitation

Once the assumptions and models are met, you can change the assumptions and re-consider the problem to see if different inputs and assumptions yield outcomes that make any sense. This is called "sensitivity analysis."

Again, the most important tool here is the judgement of the person making the decision, and where there is limited data, this tool can still play a critical role by informing Bayesian probabilities. *Bayesian* probability is one interpretation of the concept of probability. In contrast to interpreting probability as frequency or propensity of some phenomenon, *Bayesian* probability is a quantity that is assigned to represent a state of knowledge, or a state of belief (CPUC 2016). Bayesian methods ask, "How confident are you that something will happen?" or "How likely do you feel this is?"

Tabletop discussion and scenario-based exercises are another important tool for understanding unknowns. These convene experts and stakeholders to explore specific scenarios, and they are the basis for the interactive exercises that NARUC has used in developing this paper as well as exploring countless other policy challenges. In our 2010 guide to building tabletops, we noted that they are intended to generate discussion of various issues regarding a hypothetical

simulated emergency. Tabletop exercises are another way to explore potential scenarios in a way where some events are deterministically determined but the responses to those events are unknown, and the links between responses are unclear. They're also a great tool for preparedness because they create relationships between those who may be responsible for responding to future threats.

4. Develop risk management options

Once you've identified and explored what your risks are (qualitatively or quantitatively), what should you do about them? Remember, risk isn't something you can eliminate: your choices are to reduce your exposure to it, manage the potential effects, or shift it (Beecher & Kihm, 2016).

Reducing exposure to risk generally means tightening up your vulnerabilities. One example of reducing exposure to risk in critical infrastructure protection using the flood example highlighted above would be to move critical equipment away from areas that regularly experience flooding. For unpredictable or historically unprecedented events, such as an EMP strike or act of terrorism, decision-makers can focus on contingency analysis and component failure.

Diversification is another risk exposure reduction tool. In finance this means that you can combine volatile stocks into a portfolio that has less risk than a single non-volatile stock because the portfolio's parts aren't correlated – when one goes down, others could go up. Diversification works on the power sector too: diversification (not simply redundancy) yields flexibility and fewer single points of failure. Two redundant gas power plants will both lose service in a gas interruption; diversifying to have gas and hydro eliminates both operational and supply chain vulnerabilities.

Mitigating effects generally means spending on institutions and systems for protection or recovery. Resilience investments also reduce failure probability and help minimize consequence. Our 2014 paper, Resilience in Regulated Utilities, explores this term in a regulatory context at length, but for the purposes of this paper, let's suppose resilience means that service can be degraded to a high degree without failure, and that restoration is quick. Resilience offers choices that take vulnerabilities off the table.

Shifting risk in critical infrastructure protection may sound like an idea to be avoided, but it's a common and trusted risk management strategy. Insurance policies manage risk at a lower cost than building perfect protection, shifting risk from companies to insurers. Mutual assistance agreements spread response risks from one company to a number, diluting their required investments and building strength in numbers. Building less redundant distribution shifts risk from companies to customers, who may go and invest in backup generators. Cybersecurity is one area where some have called for increased federal activity in network defense, shifting responsibilities – and risks – from the private sector to the public sector. Risk-shifting is well

understood in commissions as it is the subject of inquiry in many rate cases that involve multiple rate classes.

Although risk seems like something to try to escape, there are positive tradeoffs in accepting risk: more risk should mean lower cost, because investments in protection measures aren't included in the total cost. Generally, in the arena of critical infrastructure protection, less risk is likely to mean improved reliability in the face of unforeseeable events.

5. Perform cost-benefit analysis

State regulators have extraordinarily deep experience using economic analysis to perform cost benefit analysis, and doing these analyses in a probabilistic environment draws on those same methods.

In this approach, alternatives can be ranked using benefit/cost ratios. Capital investment is the cost whereas the reduction in operation and unreliability costs is a benefit. Larger benefit to cost ratio indicates a better alternative. A greater ratio indicates a better planning alternative and vice-versa. Utilities usually set a threshold value on the benefit/cost ratio for justification of an alternative. A benefit to cost ratio of less than 1 cannot be financially justified. A benefit to cost ratio greater than 1.5 or 2 is frequently used. Again, probabilistic reliability approaches are used to quantify benefits. (EPRI, 2014)

A number of economic analysis types align with a risk-based process for prioritizing. These include a total cost method, a benefit/cost method, and methods informed by customer perspectives on outages and the value of lost load.

Total Cost Method evaluates capital cost for protection investments, plus operating costs of including these protections, minus the unreliability cost created by outages. (There is a lot of variation depending on how you define "costs" and who they are allocated to.) Generally, if this math problem yields a positive number and the capital and operating costs are outweighed by the benefit or removing unreliability, the investment gets a green light. This method is especially effective for investments preventing threats at the top of the ALARP pyramid – those which are "Risk Intolerable" (UK HSE 2016).

A second approach, the Benefit/Cost method, divides the capital cost into a ratio that divides reductions in operating costs and unreliability costs by the capital cost of the control strategy being pursued. A ratio better than one is a green light to make the investment. This works to determine whether one is faced with situations with risks that are not as low as possible, or that are tolerable risks if the costs outweigh the benefits (EPRI 2014).

NARUC has also worked with states to explore what costs are useful as inputs to these methods. A study of Maryland customers performed in 2010 found that the reliability benefits and value of lost load varies widely based on customer class, activity, and time of year (Burlingame & Walton, 2010). Understanding the value of an investment to protect critical infrastructure may be more informative if regulators ask, *value to who*? Understanding

customer perspectives on cost-benefit analysis may yeield improved decision-making at this step of the process.

6. Implement Your Options With Continuous Improvement

You've identified your problems and evaluated the potential directions. Now a risk manager must enact the appropriate courses of action to accept, avoid, mitigate, share, or transfer risk. Responding to risk means establishing the security program and architecture and using the prioritized list of cost-effective strategies that best meet the gaps between where the organization is, and needs to be, to manage risk.

Beyond implementing protective measures, risk management means determining the ongoing effectiveness of risk response measures, monitoring changes and communicating those to create a cycle of continuous improvement. Implementation is incomplete without structured reporting and feedback. In its excellent 2012 risk management protocol[2] for cybersecurity risk management, the US Department of Energy identifies these steps to activate that cycle, working with different levels of an organization so that implementation agents and decision-making authorities mutually update, inform, and reinforce each others' responsibilities in risk management.

**Figure 4: RMP Information Flowchart**


[2] http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf

This type of communication is at the core of continuous improvement. Because the process includes the highest management levels, it supports a top-down approach that incorporates the organization's goals and objectives. It also facilitates a bottom-up communication of resource needs and implementation challenges (DOE 2012).

## State experience using risk management as a regulatory tool

Risk assessment and management approaches can exist on a spectrum of complexity, ranging from general qualitative descriptions of baseline infrastructure and profiles of preparedness, to more quantitative methods based on scoring and specific methods that analyze risks to energy assets and systems.

In 2013, Kentucky's Public Service Commission convened electric cooperatives and together they began participating in a cyber security review to help identify vulnerable parts of the electric system and provide information for mitigation plans (Guernsey, 2013). This effort entailed a the review of the cybersecurity programs at 6 Kentucky electric distribution cooperatives, which are not subject to NERC CIP standards, but are still using cybersecurity risk profiles that are appropriate for their risk profiles. Each cooperative discussed their cybersecurity programs in 21 areas of focus that were based on categories from ISO Standard 27002. For each area, the analysis provides a numerical indication, 1 – 5, of the progress the cooperatives have made in developing controls based on a risk profile indicative of the participating cooperatives, assumed to be representative of the class as a whole. Their analysis gives a comparative view of the condition of the cybersecurity plans of these cooperatives. It identifies control areas that have been effectively implemented in addition to areas that need improvement. The report also makes comparisons between cooperatives, to identify areas of competency by some participants that might be leveraged at other cooperatives planning to implement similar controls.

In 2010, the Maryland Public Service Commission took up consideration of costs from a customer perspective, acknowledging risk shifting between customers and utilities when evaluation of cost and benefit was limited to utility costs. By understanding costs from a customer perspective, and the factors that create variability in the value of lost load for customers, Maryland was able to improve its understanding of ways to optimize its reliability investments (Burlingame & Walton, 2013).

Since 2011, the California Public Utilities Commission (CPUC) has been advancing a new "risk-informed" process to support decision-making in the context of energy utility General Rate Cases (GRCs). The major goal is to improve safety performance of utility operations by applying a transparent set of utility processes to identify and prioritize hazards to public safety, to determine appropriate mitigation programs and projects to reduce or avoid those risks, and to translate those priorities, programs, and projects into the GRC budget requests.

This process began in 2011 when the CPUC formed a Risk Assessment Unit (RAU) within the Consumer Safety and Protection Division with the intent to incorporate risk information into General Rate Case (GRC) making by improving the CPUC's ability to identify hazards to public safety; assess the risks associated with hazards by examining the frequency and consequence of the hazard; and using safety as a top priority, decide on the most cost-effective method to mitigate the hazards and prevent accidents. The RAU was to review all regulated utilities, but its first priority was to assess hazards to the gas system. The RAU's initial project was to develop a Natural Gas System Hazard Database, which involved surveying other states, researching the Pipeline and Hazardous Material Safety Administration safety advisories, interviewing subject matter experts, and reviewing emerging risks. Through this process, the RAU first identified over 550 potential hazards, and after further consolidation and refinement of the list was able to reduce this to 17 potential hazards that impact public safety and would continue to receive RAU attention.

The CPUC's policy statement of 2014 stated that strove to achieve a goal of zero accidents and injuries across all the utilities and businesses it regulates. To carry out this mission, the CPUC implemented a Safety Action Plan to improve the internal safety processes of the CPUC, embedded a risk assessment process into the GRC,[3] developed processes to share risk information with stakeholders; and developed models to evaluate the safety portfolio of a utility.

When asked about their experiences, state regulators involved in our 2014-2016 workshops agreed that the main ongoing challenges for incorporating risk information into regulatory activity are: (1) building confidence in risk-informed decision-making; (2) developing metrics that are commonly accepted and utilized but companies and other key stakeholders (like law enforcement and other agencies); (3) identifying leading indicators of unmanaged risks; (4) distinguishing long-term objectives from short-term objectives; and (5) establishing clear risk communication standards for utilities, regulators, and interveners.

## Conclusion

Risk management is an important tool to help regulators understand issues and clarify courses of action when dealing with the future. It is an important tool, but like any tool is only as

[3] In November 2013, the CPUC opened a new rulemaking to consider changes to the General Rate Case (GRC) Plan as well as how to consider incorporating risk-based decision-making into GRCs for electricity and gas utilities. In December 2013, the utilities responded to the CPUC's data request from its November rulemaking, and a month later, the CPUC adopted its final decision that replaced the CPUC's Rate Case Plan that was adopted in 2007. The new plan requires use of a risk-based decision-making framework that includes the following as part of the GRC process: (1) Safety Model Assessment Proceedings (S-MAP); (2) Risk Assessment and Mitigation Phase proceeding (RAMP); and (3) annual verification reports for years 1, 2, and 3, including a Risk Mitigation Accountability Report a Risk Spending Accountability Report. After the third report is complete, the next GRC cycle begins. The new plan for General Rate Case applications went into effect in February 2015. (Source: http://www.ora.ca.gov/general.aspx?id=2606)

proficient as the skill of the person using it. Taking on risk management as a staple of regulatory action may require other changes in the way you work.

Understanding threats and evaluating the prudence of a risk-based approach may require new ways to communicate with companies. They may not want to divulge security-oriented information. Asking about processes, decision-criteria, methods used, and other indicative questions may give you insight into the prudence of these activities without requiring the actual steps taken to be brought into the light of public view.

As we've learned from exploring cybersecurity, there is tension between transparency and information protection. Manage your questions carefully and don't seek things you don't need. You may also want to develop an information-management protocol early. This would identify ahead of time who has access to information, how is it stored, how is it transmitted and handled, and other details relating to its legal, physical, and cyber protection.

In conclusion, don't be intimidated by the complexity of risk management. Some of our most intractable policy decisions will be improved by its use. It is powerful but adaptable to a range of uses, and it can be capably applied without a deep background in statistical methods or other analytic disciplines. In the area of infrastructure protection, it may help you see into the future and choose the best path through uncertainty.

## Appendix A: an example of using a risk-informed process for cybersecurity

Regulators nationwide have been showing interest in exploring the use of a framework developed by a stakeholder group convened by the National Institutes of Standards & Technology (NIST) to improve cybersecurity preparedness for critical infrastructure like the systems used by the electric grid.

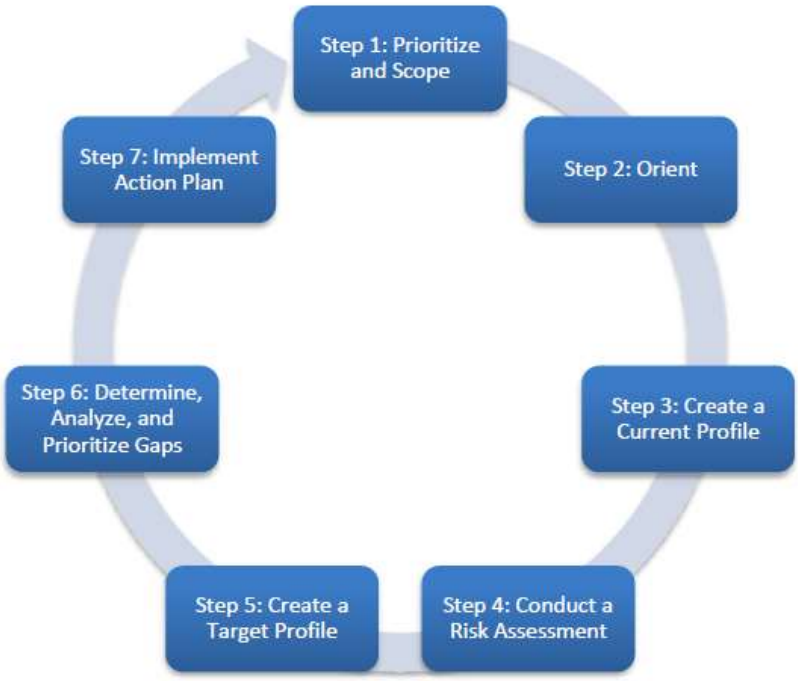
The NIST cybersecurity framework is intended to provide a structure for how companies can improve their cyber preparedness. Programs informed by the framework may look quite different even though they use the same structured approach. Regulators may wish to use the questions below to see whether, and how, organization implementing the framework can:

- Describe their current cybersecurity posture in terms of Functions, Category and Subcategory Outcomes, and Implementation Tiers for appropriate stakeholders.
- Describe the Current and Target Profiles for their cybersecurity programs.
- Assess progress toward the desired Target Profiles.
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process.
- Communicate the Current and Target Profiles and other risk management information to internal and external cybersecurity risk stakeholders.

A series of trainings were run by NIST and NARUC in Washington DC in 2016, with the aim to help utility regulators understand how the NIST cybersecurity framework supports the regulatory ecosystem. Workshops were held in July and September 2016. Objectives of the workshop included providing an introduction to the cybersecurity framework; explaining the steps involved in implementing the cybersecurity framework; sharing of participant experiences in their home states on using the cybersecurity framework; and providing guidance to help regulators develop a foundation for having discussions with their utilities about their cybersecurity practices.

NARUC developed the following questions for regulators to ask companies implementing the cybersecurity framework. The hypothesis being tested is that if a company has credible responses that indicate that it is addressing these areas, it is likely that it is developing a credible cyber program. The questions below are intended to help state regulators understand the company's implementation approach.

Figure 1. Framework Implementation Approach




Source:
http://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf

## *1. Prioritize & Scope*

Has your organization determined where it wants to apply the Framework to evaluate and potentially guide the improvement of the organization's cybersecurity capabilities?

## *2. Orient*

Has your organization used a risk-based process to identify what people, information, technology, and facilities are within the scope of its cybersecurity program? Has your organization identified the appropriate regulatory and Informative References (e.g., cybersecurity and risk management standards, tools, methods, and guidelines?)

## *3. Develop a current profile*

Has your organization identified its current cybersecurity and risk management state? How?

## 4. Conduct a risk assessment

Has your organization performed (or had someone perform) a risk assessment for the in-scope portion of the organization? Did this leverage the organization's risk management strategy, organization-defined risk assessment approach, in-scope regulatory requirements, cybersecurity and risk management standards, and other relevant tools, methods, and guidelines?

## 5. Create a target profile

Has your organization identified goals that will mitigate risk commensurate with the risk to your organizational and critical infrastructure objectives?

## 6. Determine, Analyze, and Prioritize Gaps

Has your organization:

- Analyzed gaps between the current state and your Target Profile?
- Evaluated the potential consequences from these gaps?
- Determined which gaps need attention?
- Identified actions to address gaps?
- Performed a cost-benefit analysis on those actions?
- Prioritized actions (based on Cost Benefit Analyses and consequences)
- Created a plan to implement those prioritized actions?

## 7. Implement your action plan

What progress has your organization made in:

- Implementing the identified actions by priority?
- Tracking progress against your plan?
- Monitoring and evaluating progress against key risks, metrics, and performance indicators?
- Reporting its progress to key decision-makers and stakeholders?
- Re-assessing progress, and implementing a program that seeks out ongoing gaps, corrective steps, and implements these as part of a cycle of continuous improvement?

# References


Beecher, Jan & Steve Kihm, 2016 *Risk Principles for Public Utility Regulators,* Michigan State University Press http://msupress.org/books/book/?id=50-1D0-33F6#.V-6rySRtHwA

Bernstein, Peter L. 1998, *Against the Gods: The Remarkable Story of Risk,* Wiley Publishing

Keogh, Miles & Christina Cody, 2013 *Cybersecurity for State Regulators v2.0,* NARUC http://pubs.naruc.org/pub/5371F985-2354-D714-513A-AC5E3D644808

Popova, Maria "The best reads of 2015", https://www.brainpickings.org/2015/12/21/best-books-2015/

Weinberg, George & John Schumaker, 1974, *Statistics: An Intuitive Approach*, Brooks / Cole Publishing

Stockton, Paul, 2014 *Resilience for Black Sky Days,* NARUC http://www.sonecon.com/docs/studies/Resilience_for_Black_Sky_Days_Stockton_Sonecon_FINAL_ONLINE_Feb5.pdf

NIST, 2014, *Cybersecurity Framework,* https://www.nist.gov/cyberframework

UK Health & Safety Executive, 2016 *"ALARP 'at a glance'",* http://www.hse.gov.uk/risk/theory/alarpglance.htm

Hoppock, David & Dalia Patino Echeverri, 2014, *Decision Making Under Uncertainty and Risk Assessment Training*, Duke University, Durham NC, Sponsored by NARUC April 30th, 2014 & available by request, mkeogh@naruc.org

EPRI, 2014, *PRA White Paper – A White Paper on the Incorporation of Risk Analysis Into Planning Processes* prepared for NARUC and EISPC http://pubs.naruc.org/pub/536DCF19-2354-D714-5117-47F9BA06F062

DOE, 2014, *Energy Sector Cybersecurity Framework Implementation Guidance* http://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf

DOE, 2012, Electricity Subsector Cybersecurity Risk Management Process (RMP) Guideline. http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf

Guernsey, 2013, *Kentucky Public Service Commission Cybersecurity Risk Assessment & Risk Mitigation Plan Review,* prepared for NARUC & available by request, mkeogh@naruc.org.

CPUC 2016, “Risk Assessment and Safety Unit Webpage”, http://www.cpuc.ca.gov/riskassessment/ accessed September 2016.

Burlingame, Mark & Patty Walton, 2013, A *Cost-Benefit Analysis of Various Electric Reliability Improvement Projects. From the End Users' Perspective* prepared for NARUC & available by request, mkeogh@naruc.org.

Morgan, Granger 1992, *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis* Cambridge University Press