

## **Risk Governance for Water Utilities:**

*How and why to implement risk-related decision-making for your organization.*

370 Harvey Rd  
Manchester, NH 03103  
P: 603.606-5937  
F: 603-606-5936  
[www.bridge-soft.com](http://www.bridge-soft.com)





## **ABSTRACT**

Following the completion of their vulnerability assessments, U.S. water utilities have been faced with the challenge of prioritizing expenditures to address those vulnerabilities against existing capital and operational expenses. Regardless of the funding source (rates, SRF, grants), the challenge remains the same – how to determine, justify, and then communicate these priorities. Implementing comprehensive and consistent risk governance can address this challenge and also provide a framework for improving a utility’s ability to continuously meet its mission objectives to reliably deliver safe drinking water.

## **INTRODUCTION**

For water utilities, threats are faced on many levels (safety, security, asset failure, financial, etc...) and they have needs for ranking, treating, and reporting on those threats. The reality is that there is often risk governance being performed by multiple departments and/or groups for different categories of risk using inconsistent methodologies and/or tools within the same organization.

### ***Why is risk governance important?***

Implementing a properly constructed risk governance plan for the entire organization can greatly enhance decision making and stakeholder communication. For example, asset management programs and security vulnerability assessments are typical programs for critical infrastructure organizations. The former is valuable for determining the best use of capital expenditures, reducing maintenance costs, etc., while the latter is valuable (if not mandatory) for quantifying and ranking security threats. However, how does one determine the relative importance of replacing an aging process pump versus installing perimeter security cameras? A comprehensive, standardized approach to risk management can provide the following benefits:

- **Improved decision making** is made possible due to several factors. First, a *consistent* methodology is used across different departments and/or disciplines. This allows for a comparison of risks across the entire organization (e.g. new pump vs. security cameras), allowing for priorities to be established with the best possible information. These improved decisions can manifest themselves in cost savings and improved operational readiness.
- **Returns on investment are maximized** based on improved decision making. Using a consistent process for ranking potential projects increases the likelihood that limited funds will be invested wisely. Additionally, a well executed risk assessment will clarify the total cost of implementing a project across its entire life cycle – not just the initial capital outlay.
- **Better communication** with stakeholders is made possible by providing a defensible, logical basis for decision-making. This can improve the likelihood of obtaining funding from management boards and/or government grants by building credibility.

In order to relate these benefits to a real world example, consider these recent headlines:

“San Francisco audit says water not secure”<sup>1</sup>

“Audit: Agency slow to upgrade security”<sup>2</sup>

These newspaper articles refer to a city audit which found that “...the Public Utilities Commission has failed to implement security enhancement projects at its facilities in a timely manner”<sup>3</sup>. The city’s budget report contains sixty references to “risk”, including risks of failure, errors, claims exposure, theft, break-ins, vandalism, illegal acts, seismic events, contractor programs, layoffs, accident, injury, etc... Clearly, a sound risk management program would have, at a minimum, provided auditors with a clear explanation of the plan and timetable for implementing the security enhancements.

Arguably, one of the most important benefits of risk governance is cost avoidance. Though difficult to predict and quantify, the failures of systems or practices can have dire consequences. Consider the following well known outbreaks:

<i>Year</i>	<i>Location</i>	<i>Incident</i>	<i>Sick (Dead)</i>	<i>Est. Cost</i>
1987	Carrollton, Georgia	Cryptosporidium	13,000 (0)	?
1989/90	Cabool, Missouri	E. Coli O157:H7	243 (4)	?
1993	Milwaukee, Wisconsin	Cryptosporidium	403,000 (40)	\$28M - \$96M
1996	Sydney, Australia	Cryptosporidium	0 (0) ?	\$15M - \$70M
2001	Walkerton, Canada	E. Coli O157:H7	2,300 (7)	\$64.5 - \$155M

These incidents exemplify the extreme consequences of the failure of a water supplier to meet its mission objective of supplying safe drinking water to its customers. When tabulating the final cost of such failures, there are direct and indirect costs to be considered. The direct costs are operational in nature and the most easily quantifiable. They include loss of revenue, cleanup costs, damage to assets, mitigation costs, legal expenses and costs for ongoing testing and/or monitoring. The indirect costs are less obvious and are related to the costs born by the community in the incident’s aftermath. These include lost productivity and/or revenue, medical and pharmacological costs, impact on tourism, increases to insurance premiums, and industrial treatment costs. While there is no guarantee that a comprehensive risk governance program would have prevented any of these, it is a logical assumption that it would have lowered the likelihood of their occurrence and, one would hope, mitigate their impact.

## **Terminology**

At this time, it is necessary to provide some definitions. Any discussion of “risk” is complicated by the fact that there are so many different areas of specialization/concentration, standards, methodologies, and applications that it often leads to confusion. Indeed, many risk standards and methodologies employ terminology that is inconsistent and confusing. Consider these varied definitions for “risk analysis” among the following risk standards:

<i>Organization/Publication</i>	<i>Definition</i>
AS/ANZ:4360	Determination of likelihoods and consequences
Codex Alimentarius	Risk Assessment + Risk Management + Risk Communication
EMPRES	Hazard Identification + Risk Assessment + Risk Management + Risk Communication
FERMA	Risk Identification + Risk Description + Risk Estimation
International Programme on Chemical Safety	Risk Assessment + Risk Management + Risk Communication

Most risk standards and/or methodologies contain very similar if not identical steps when examined at a high level. However, their definitions tend vary greatly. Many of the definitions and discussions in this paper will defer to the Australia/New Zealand Risk Management Standard (AS/ANZ 4360), which is quite generic in nature and similar to most other standards.

For the purposes of this discussion, the phrase “risk governance” will refer to a mindset more than a methodology. It is a management directive to institute a culture of risk-based decision making in which priorities are set and decisions are made according to a consistent approach to the consideration of risk factors. “Risk Management” will refer to the process of identifying and quantifying risks, assessing those risks through analysis and evaluation, and implementing treatments to reduce the likelihood and/or consequences of their occurrence.

## **Trends**

There are domestic and global trends that will test an organization's ability to manage risk. In the U.S., the Environmental Protection Agency estimates that as much as \$1.2 trillion will be required<sup>4</sup> through 2019 to meet water and wastewater infrastructure needs. The aging infrastructure will require significant investment by utilities that must at the same time be cognizant of reducing security vulnerabilities. It is likely that access to state and federal funds and/or grants will be prioritized by, if not contingent upon, sound risk management planning (see Government Accounting Office report GAO-04-461, "Water Utility Asset Management"). The Department of Homeland Security has developed a risk management methodology (RAMCAP) for determining critical infrastructure priorities and funding will be disbursed accordingly.

On a global level, Australia has been pushing the standards for water suppliers from a regulatory perspective. In 2003, the State of Victoria passed the "Safe Drinking Water Act" which, among other things, required that "Water suppliers must prepare, implement and review risk management plans." It formed the cornerstone of their new approach to regulation, which now emphasizes risk management over prescriptive approaches. On a national level, the National Health and Medical Research Council (NHMRC) in collaboration with the Natural Resource Management Ministerial Council (NRMCC) developed the "2004 Australian Drinking Water Guidelines" (ADWG), which incorporates a preventative risk management approach and elements of ISO 9001 (Quality Management), ISO 14001 (Environmental Management), AS/NZS 4360 (Risk Management) and the Hazard Analysis and Critical Control Point (HACCP) system.

The World Health Organization (WHO) has also drafted "Guidelines for Drinking-water Quality" that are being considered and/or adopted in many regions of the world including the European Union and emerging third world countries in Africa and Asia. "The Guidelines are intended to support the development and implementation of risk management strategies that will ensure the safety of drinking-water supplies through the control of hazardous constituents of water. These strategies may include national or regional standards developed from the scientific basis provided in the Guidelines."<sup>5</sup>

Given the globalization of the world economy and the "flattening of the earth" (ref. Thomas Friedman's book, "The Earth is Flat: A Brief History of the 21<sup>st</sup> Century"), it is inevitable that these trends will begin to affect the U.S. water and wastewater industries. As more public water suppliers' assets are purchased by European-owned operations companies, risk governance is slowly but surely becoming more prevalent.

## **Industry Overview**

Risk management has taken many forms in the water and wastewater industries around the globe. In the U.S., water utilities were required by H.R. 3448 (Public Health Security and Bioterrorism Preparedness and Response Act of 2002) to conduct vulnerability assessments for terrorist attack and/or other intentional acts. These assessments were conducted with varying methodologies but generally consisted of a comprehensive assessment of several threats (e.g. terrorist attack, vandalism) against all of the utility's critical assets. In addition to these vulnerability assessments, many water utilities also employ asset management techniques in order to support best practices, improve infrastructure reliability, and reduce costs. Asset management involves managing the risk of asset failure. In some cases, publicly held utilities or operations companies must comply with section 404 of the Sarbanes-Oxley Act of 2002 by performing annual assessments of internal controls over financial reporting. Once again, a compartmentalized approach to risk management is applied to the organization's financial risks.

These are only three very common examples of risk assessment and/or management that are being employed by many organizations right now. The following table lists departments, or “organizational contexts”, that could benefit from risk management:

<i>Context</i>	<i>Description</i>	<i>Examples</i>
Asset Management	Risks associated with the failure of assets	Replace/refurbish pump
Contracts	Risks relating to vendors, contractors, etc.	Cost/reliability comparison of suppliers
Emergency Management	Preparedness for emergency response	Disaster recovery plans, equipment, and contracts
Finance	Risks associated with financial and economic conditions	Raw material price fluctuations
Information Systems	Risks of computer and/or SCADA system failures	Software change management policies
Occupational Safety	Risks of personal injury and/or workers' compensation	Vehicle accidents
Operations and Maintenance	Risks for day to day plant operations	Raw water temperature fluctuations

## Water Safety Plans

“The most effective means of consistently ensuring the safety of a drinking-water supply is through the use of a comprehensive risk assessment and risk management approach that encompasses all steps in water supply from source to consumer.”<sup>6</sup> The WHO guidelines refer to such plans as “Water Safety Plans” (WSP). A WSP utilizes the results of a risk assessment to characterize hazards to the water supply and identifies control measures that are designed to control the risks and their acceptable limits. A monitoring plan then establishes the frequency with which the control measures are monitored. Finally, verification procedures ensure that the plan is working effectively.

## WHAT IS RISK MANAGEMENT?

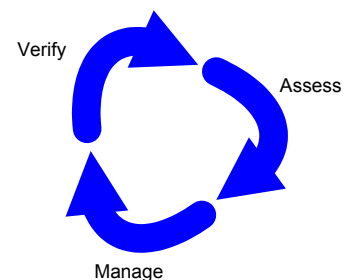
*Risk management is an iterative process consisting of well-defined steps which, taken in sequence, support better decision-making by contributing a greater insight into risks and their impacts. The risk management process can be applied to any situation where an undesired or unexpected outcome could be significant or where opportunities are identified. Decision makers need to know about possible outcomes and take steps to control their impact.*<sup>7</sup>

This definition is provided by the Australian risk management standard AS/ANZ 4360:1999. It describes risk management as an “iterative process” that supports “better decision-making”. While it may be applied with a limited scope (e.g. single department, specific assets and/or threats), its benefits are most greatly realized when the entire organization adopts a consistent approach for all risks.

While there are many methodologies and techniques for implementing a risk management plan, the three basic steps are consistent; assess, manage, and verify. While it is beyond the scope of this paper to provide instruction and/or guidelines for such plans, it will introduce and attempt to explain many of the concepts.

## The Process

“Risk Assessment” is arguably the most inconsistent and confusing phrase related to the subject. It is one reason why communication is such an important component of risk governance. Any discussion must be clear in its definitions of these terms, especially when they take place outside of the organization where other parties may have completely different interpretations of terminology. Having said this, the risk assessment phase, as covered in this discussion, refers to the identification, analysis (quantification), and evaluation of risks.



## From Threats/Hazards/Vulnerabilities to Risks

Many organizations are aware of and/or have conducted vulnerability assessments, whereby a list of vulnerabilities is compiled for a given threat or threats against a list of assets. What is the difference between a vulnerability and a risk? The difference is that vulnerability simply *identifies* a threat, whereas risk *quantifies* the threat. This is accomplished by establishing a likelihood and consequence for the particular risk. We all live with the risk that our homes could be struck by a large meteorite at any given moment. While we know that the consequences of such a threat would be devastating and potentially deadly, we also understand that the likelihood of this occurring is extremely low. Therefore, we take no steps whatsoever to reduce this risk, which constitutes an *acceptable risk*. Comparatively, many homes located on shorelines of hurricane-prone geographies are built on stilts. This reduces the risk that their homes will be washed into the ocean when a storm surge hits. The likelihood of a hurricane striking their region in combination with the consequence of a three meter storm surge warrants the cost of construction.

## Risk Assessment

The first step in risk assessment is identification. Using a systematic approach, a list of all hazards to be considered is compiled, regardless of whether or not they are in the control of the organization. What can happen? How can it happen?

Once risk identification is complete, it is necessary to establish the evaluation criteria. These criteria typically involve categories such as operational, social, environmental, technical, financial, occupational health & safety, etc...

The final step in risk assessment is modeling. Risk is the relative level of potential harm that is posed by a particular hazard as determined by its *likelihood* and *consequence*. While this definition constitutes the vast majority of applications for risk assessment, it is important to note that risk assessments are frequently utilized in the evaluation of opportunities as well. Techniques and methodologies for risk modeling is a complex subject. A brief description of the three types of risk modeling follows.

## Qualitative Modeling

Qualitative risk analysis is most intuitive and frequently practiced technique. It involves the development of likelihood and consequence rating systems and then assigning one of each to all of the hazards. A risk table determines the final-level risk based on the combination of each factor.

		Likelihood				
		Almost Certain	Likely	Moderately Likely	Unlikely	Rare
Consequence	Catastrophic	E	E	E	H	H
	Major	E	E	H	H	M
	Moderate	E	H	H	M	L
	Minor	H	H	M	L	L
	Insignificant	H	M	L	L	L

### Semi-Qualitative Modeling

Semi-qualitative modeling uses calculated values for risk, likelihood, and/or consequence. It is considered to be “qualitative” because the factors that are plugged into the calculations are qualitative assessment of various factors. Consider the following example<sup>8</sup>:

$$\text{Risk} = \text{Attractiveness} \times \text{Consequence}$$

$$\text{where Attractiveness} = \sqrt{[(0.5 \times \text{Disruption to Operations} + 0.5 \times \text{Public Perception}) \times \text{Inherent Robustness}]}$$

$$\text{where Consequence} = [(0.4 \times \text{Economic impact}) + (0.2 \times \text{Facility downtime}) \times (0.4 \times \text{Social/Environmental Impact})]$$

“Disruption to Operations” table of values:

Score	Description
5	Extreme level of perceived disruption by the threat source of the importance of the asset &/or process to operation of the system or network
4	High level of perceived disruption by the threat source of the importance of the asset &/or process to operation of the system or network
3	Medium level of perceived disruption by the threat source of the importance of the asset &/or process to operation of the system or network
2	Low level of perceived disruption by the threat source of the importance of the asset &/or process to operation of the system or network
1	No perceived disruption by the threat source of the importance of the asset &/or process to operation of the system or network
0	No possible disruption by the threat source of the importance of the asset &/or process to operation of the system or network

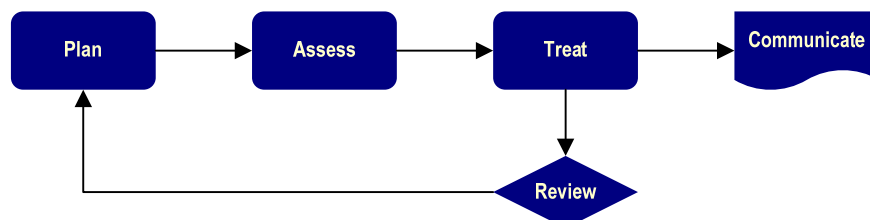
### Quantitative Modeling

Quantitative techniques for risk modeling utilize statistical methods for calculating likely outcomes and their magnitudes. Some of the more commonly employed techniques are:

- Monte Carlo Analysis – Used to simulate complex processes and generate probable results. Determines probability that a certain event will occur and understanding of the magnitude of the event.
- Neural Nets – Computer systems that mimic the structure of the human brain – neurons, synapses, dendrites, and axons. They are highlighted by their ability to “learn” and are adept at pattern recognition, signal processing, and target classification.
- Bayesian Analysis – Facilitates the use of new information to update initial probability estimates.

### “Management” Defined

The word management means to exert control over a situation or situations. It follows, therefore, that simply cataloguing a list of risks (risk register) is merely an assessment and falls short of exerting control over them. Thus, management requires actions that will reduce and/or eliminate risks. These are referred to as “treatments” or “control measures”. It follows, therefore, that applying control measures will change the likelihood and/or consequence of a particular threat, thus resulting in a different risk altogether – known as “residual risk”. Finally, it is not sufficient to perform this process once; it should be an iterative process that continually monitors the effectiveness of the control measures, identifies new risks, and adjusts the control measures to steadily improve awareness and reduce overall risk.



## CHALLENGES

### ***Risk Perception***

In the course of executing a risk assessment, it is important to understand that there are potential biases of the team, including one's own. Since risk assessments are predominantly built upon a foundation of qualitative analyses and rankings, those decisions are based on human thought patterns which are usually governed more by perceptions than facts. Indeed, research indicates that human decision making is highly irrational and based upon evolutionary coping mechanisms; fight, flight, and play dead. In the context of risk management, these mechanisms tend to manifest themselves in terms of semantic risk patterns<sup>9</sup>, whereby risks are typically assigned to one of the following categories:

- Risks posing an **immediate threat**, such as chemical storage facilities
- Risks dealt with as a **blow of fate**, such as natural disasters
- Risks posing a threat to **one's own strength or ability**, such as car accidents
- Risk as a **gamble**, such as lotteries or insurance
- Risk as an **early indicator of insidious danger**, such as global warming or viruses

Another factor that can compromise the objectivity of a risk analysis is the low probability of occurrence. As previously stated, human decision making is based more on perceptions than facts and this is especially true when attempting to evaluate probability. Here again, psychological research has identified patterns of choices utilized in place of more fact-based analysis<sup>10,11,12</sup>:

- **Availability bias** refers to the tendency for easily recognized risks to be overestimated (e.g. person who has lost a loved one in a car accident). The more personally one has experienced a particular hazard, the greater their tendency to overestimate its likelihood.
- **Anchoring effect** is the tendency for risks that are associated with recent or known events to be overestimated (e.g. chemical plant explosion).
- **Distribution of risks over time** is more acceptable than single, large disasters. When risks are similar in nature and occurrences are more or less evenly spread over time (such as automobile fatalities), they tend to be tolerated much more so than less frequent, more concentrated losses (such as fatal airline crashes).
- **Assessment bias** tends to move consequence ratings to the median for risks with high degrees of uncertainty. This can result in low risks being overestimated and high risks being underestimated in such situations.

### ***Group Dynamics***

Most properly executed risk assessments occur in a team or group environment. As such, there will always be group dynamics affecting the thought processes, actions, and decisions of various members of the group. It is the responsibility of management and the facilitator to mitigate (as much as possible) the factors that contribute to some of the potentially detrimental elements of group dynamics.

The eventual results of a risk assessment will lead to decisions that may directly affect the jobs and/or careers of the participants. For this reason, the risk models must be scrutinized in order to minimize **desired outcomes**. People will tend to present risks more favorably to advance their personal or professional objectives, which may influence them to overestimate risk for the purpose of obtaining additional budgetary funding, or to underestimate risk in order to emphasize some level of achievement.

It follows, therefore, that assuming the final risk models are built as objectively as possible, decisions based on the risk assessment will likely result in **winners and losers**. This is one more instance where

communication is paramount – particularly with the “losers”. It is important to dispassionately present and thoroughly explain the reasons behind a decision and the overall benefits to the organization.

## **Consistency**

Consistency is particularly important (and challenging) for water utilities. In fact, it may be more important to be “consistent” than to be “correct”. This is because the objective of most risk assessments is to *rank* rather than *calculate* risks for the purpose of prioritizing mitigation or treatment efforts. As an example, consider the process of arranging persons according to their height. It is not critical that the exact height of each individual be known – only that *relative* height of one to another is accurate. A consistent approach to modeling and decision making during the risk assessment is one way to improve the efficacy of the effort.

## **CONCLUSIONS**

All U.S. water utilities (serving populations over 3300) have already undertaken a limited-scope risk assessment. The vulnerability assessment process required by the Bioterrorism Act required the systematic assessment of risks from terrorism and vandalism. Furthermore, many utilities also employ asset management (or capital improvement) plans, which assess the risk of asset failure. A **comprehensive, consistent** assessment of **all** risks faced by a water utility yields many benefits including improved decision-making, better returns on investment, and better communication. These benefits can lead to lower costs, improved stakeholder and consumer confidence, and – when incorporated within a water safety plan – a safer, more reliable water system.

## **RESOURCES AND LINKS**

### **Web Resources**

World Health Organization (Water Safety Plans):

[http://www.who.int/water\\_sanitation\\_health/dwq/wsp0506/en/](http://www.who.int/water_sanitation_health/dwq/wsp0506/en/)

International Risk Governance Council (Risk Governance – Towards an Integrative Approach):

[http://www.irgc.org/\\_cgidata/mhscms/\\_images/12326-3-2.pdf](http://www.irgc.org/_cgidata/mhscms/_images/12326-3-2.pdf)

Congressional Research Service (Risk Management and Critical Infrastructure Protection):

<http://www.fas.org/sgp/crs/RL32561.pdf>

The Institute of Risk Management:

<http://www.theirm.org/>

ASME (ASME Risk Analysis and Management for Critical Assets Protection (RAMCAP)):

[http://www.bfrl.nist.gov/PSSIWG/presentations/NSTCPresentation\\_0917041.pdf](http://www.bfrl.nist.gov/PSSIWG/presentations/NSTCPresentation_0917041.pdf)

NEWEA Asset Management Resource Center:

<http://www.newea.org>

### **Publications**

Glenn Koller, Risk Assessment and Decision Making in Business and Industry: A Practical Guide (CRC Press, LLC, 1999) ISBN 0-8493-0268-4

Standards Association of Australia, Risk Management: AS/ANZ:4360, 2004 (Standards Association of Australia, 2004).

## END NOTES

---

- <sup>1</sup> Gordon, R. “San Francisco audit says water not secure. Few safeguards along aqueduct.” San Francisco Chronicle, (August 11, 2005)
- <sup>2</sup> Jouvenal, J. “Audit: Agency slow to upgrade security.” San Francisco Examiner, (August 10, 2005)
- <sup>3</sup> San Francisco Board of Supervisors Budget Analyst, “Phase IV Management Audit of the Public Utilities Commission – Administrative Bureaus and Infrastructure Division”. Available online at “[http://www.ci.sf.ca.us/site/budanalyst\\_page.asp?id=33895](http://www.ci.sf.ca.us/site/budanalyst_page.asp?id=33895)”. [Accessed on September 2, 2005.]
- <sup>4</sup> Congressional Budget Office, Future Investment in Drinking Water and Wastewater Infrastructure, (Washington, D.C.: November 2002).
- <sup>5</sup> World Health Organization, Guidelines for Drinking-water Quality. Vol. 1 : 3<sup>rd</sup> ed. (Geneva, Switzerland: 2004).
- <sup>6</sup> World Health Organization, *Guidelines for Drinking-water Quality*
- <sup>7</sup> Standards Association of Australia. *Risk Management: AS/ANZ:4360*, 1999. Strathfield, NSW: Standards Association of Australia, 1999.
- <sup>8</sup> Courtesy of Victorian Water Utilities, *Security Vulnerability – Risk Assessment Guideline v2.5*
- <sup>9</sup> Renn, O.: “Perception of Risks,” The Geneva Papers on Risk and Insurance, 29, No. 1 (2004a), 102-114. As noted in International Risk Governance Council, *Risk Governance: Toward an Integrative Approach*, Sept, 2005.
- <sup>10</sup> Kahneman, D. and Tversky, A.: “Prospect Theory: An Analysis of Decision Under Risk,” *Econometrica*, 47, No. 2 (1979) 263-291. (From *Risk Governance*, 2005)
- <sup>11</sup> Tversky, A. and Kahneman, D.: “Judgement under Uncertainty. Heuristics and Biases,” *Science*, 85 (1974), 1124-1131. (From *Risk Governance*, 2005)
- <sup>12</sup> Ross, L.D.: “The Intuitive Psychologist and His Shortcomings: Distortions in the Attribution Process,” in: L. Berkowitz (eds.): *Advances in Experimental Social Psychology*, Vol.10 (Random House: New York 1977), 173-220.