Managing Risk Across the Enterprise:

Final Quick Guide for
State Departments of Transportation

Prepared for

The National Cooperative Highway Research Program

of

The National Academies

Gordon Proctor & Associates

Dublin, Ohio

The StarIsis Corporation

Lewis Center, Ohio

Jeff Roorda and Associates, Inc.

Springwood, Australia

June, 2016

ACKNOWLEDGEMENT OF AUTHORSHIP

DISCLAIMER

ABSTRACT

This quick guide summarizes how state transportation agencies can establish and benefit from an enterprise risk management program. It highlights the recommendations of a more extensive guide to be published under the same NCHRP project. Both guides define risk management and illustrate how it complements strategic planning and performance management. The guide defines enterprise risk management as the formal and systematic effort to control uncertainty and variability on an organization's strategic objectives by managing risks at all organizational levels. The guide recommends managing risk at four levels: enterprise, program, project, and activity. It also advises how to create an effective risk management program and what tools an agency will need.

NATIONAL COOPERATIVE HIGHWAY RESEARCH PROGRAM

Managing Risk Across the Enterprise:

Strategic Objectives

Risk Management

Asset Management

Performance Management

A Quick Guide for

State Departments

of Transportation

TRANSPORTATION RESEARCH BOARD

Contents

Managing Risk, Increasing Performance

State transportation agencies informally manage risk every day. However, few use enterprise risk management to document those risks or the decisions they make to measure, manage, and mitigate them. By establishing a formal risk management program, agency leaders can adopt a best practice from the corporate world and common among high-performing transportation agencies abroad.

This Quick Guide explains why and how to use enterprise risk management (ERM). It summarizes a more extensive guide that provides detailed steps for establishing risk management programs.

Creating a risk management program improves agency performance by

- increasing credibility by acknowledging the uncertainties that surround complex agency objectives such as achieving highway safety targets or sustaining long-term asset conditions;
- demonstrating due diligence by documenting the risks an agency faces and illustrating the steps taken to mitigate them;
- improving performance by preparing for the uncertainties that can impede agency objectives;
- reducing threats to the public; and
- encouraging innovation by stressing that managing risks is also about capitalizing on opportunity.

Risk management does not replace performance or asset management but rather it complements them, as seen in Figure 1. If performance and asset management are drivers of strategic objectives, then risk management is a navigation system. It helps leaders at all levels scan the horizon and identify risks that could impede their objectives.

Risk management complements the performance-based approach codified by recent transportation acts. As agencies adopt new, more sophisticated performance objectives, they face increasing risks. An example is the long-range asset management plans that agencies are adopting. As agencies set condition targets for thousands of bridges and hundreds of thousands of lane miles of pavements for a decade, they will face many uncertainties and risks. These include unpredictable state and federal funding, volatile material prices, the uncertainty of bridge and pavement models, and the ability of their own agencies to deliver the proper asset treatments. Agencies control some of these risks, but many they do not. Embracing risk management provides agency

Figure 1 Enterprise risk management complements performance and asset management.

leaders with another tool to achieve their performance management objectives and to communicate the risks they cannot control.

Even if not spurred by federal legislation, U.S. transportation agencies are well served by enterprise risk management. Applying risk management to transportation agencies transfers a sound management practice from the corporate world to the public sector. In the corporate world, risk management is a basic competency. In a complex environment, achievement of organizational goals depends on managing many internal and external risks. Failure to measure, manage, and mitigate these risks increases the likelihood of failure. If risks and uncertainties are inevitable, failing to prepare for them is irresponsible.

What Is Enterprise Risk Management?

Unlike in common usage, "risk" involves more than just threats or hazards. This guide defines risk as *the positive or negative effects of uncertainty or variability on agency objectives.*

This definition holds several implications. First, risks are not always negative. In modern management frameworks, managing risk is about managing uncertainty, variability, threats, hazards, and even opportunities. All of these can affect organizational objectives. Second, managing risk is about managing performance. All performance objectives face risk, particularly in the complex environments in which transportation agencies operate. Achieving objectives relies on both internal and external factors that are subject to uncertainty and variability. Ignoring those risks is to ignore impacts on performance. If performance management exists to achieve objectives, then risk management exists to identify and mitigate the risks to those objectives. Risk management can not only mitigate threats to safety but also mitigate and manage risk to performance. In much of the corporate world, risk management underpins performance. It is not only about safety.

Third, managing risks is about managing opportunities. This may seem counterintuitive, but taking few risks equals earning few rewards. A low-risk investment portfolio produces low returns. Every organization needs to take risks to achieve its objectives, particularly as public expectations of organizational performance grow. Careful evaluation can lead to well-reasoned risks that produce substantial rewards and accomplishment. Often the magnitude of achievement correlates to the degree of risk. This realization led the World Road Federation to say that risk management could be redefined as "opportunity management." [1] This concept is particularly refined in the world of finance where risk is not bad but is merely a measure of potential loss or reward.

"Risk management" is the architecture an agency establishes to manage its risks, more precisely defined as *the cultures, processes, and structures that are directed toward the effective management of potential opportunities and threats.* This guide assimilates recommendations from international risk guides, several of which emphasize that to be successful, risk management has to be actively used. It helps to think of "managing risks" as

an active verb phrase instead of "risk management" as a static noun phrase. This leads to the definition of the risk management process as *the systematic application of policies, procedures, and practices to the identification and management of uncertainty or variability on achievement of agency objectives.*

When this guide speaks of "enterprise risk management," it refers to the managing of risks at all levels of an organization. Traditionally, in most state transportation agencies, risk management is most common at the project level. It is used to manage threats to a project's cost, scope, schedule, quality, or impacts. If one understands project risk management, one can understand enterprise risk management. It is defined as *the formal and systematic effort to control uncertainty and variability on an organization's strategic objectives by managing risks at all levels of the organization*. Enterprise risk management scales up to the organization-wide level the management of risks just as project risk management does at the project level.

The expansion of enterprise risk management reflects the growing expectation that executives need to manage risks to accomplish the organization's objectives. The concept is that risk management is the mirror image of performance management, as Figure 2 shows. Without controlling risks, performance is difficult to guarantee. The two disciplines operate in parallel, with performance management setting objectives and risk management identifying their potential obstacles. The disciplines do not compete. They complement each other to support performance.

Figure 2. Risk and performance management operate as complementary mirror images.

The concept that it is incumbent upon leaders to manage risks acquired legislative foundation with the passage of the Sarbanes-Oxley Act in 2002. Among other things, it requires corporate executives to adopt sound risk management and disclosure practices to protect investors. Corporations are to manage the risks they take and to disclose those risks to shareholders. The intent is to enable investors to be better informed and to reduce their exposure to corporate bankruptcies, such as occurred with Enron Corp. and WorldCom Inc. The Risk Management Society reports that after these failures, there was an increasing tendency for risk management practices to expand from specialized application at the project or activity level to application across the organization as enterprise risk management.[2] One prominent risk author contends that modern civilization is in significant part defined by its efforts to understand and control risk.[3] Efforts by modern societies to understand and reduce the causes of dis-

ease, crime, and warfare are viewed within the broad context of identifying, analyzing, treating, and monitoring risks to their citizens. In Great Britain, Australia, and New Zealand, risk management is an expected, basic competency of transportation agency executives. They are expected to manage risk as a core competency just as they would ensure the financial integrity of their agency or be expected to manage threats to public safety. In the corporate world and in much of the international public sector, risk management is not exotic. It's a core competency.

Don't Overcomplicate It

To understand effective enterprise risk management, one needs to understand a paradox. At its highest enterprise levels, risk management is not that complicated. Practitioners say it is not expensive, complex, or difficult to understand. At its most basic, enterprise risk management requires agencies to ask themselves these questions:

- What objectives really matter?
- What uncertainties surround those objectives?
- What can we do about those uncertainties?
- Are we managing them?
- Are we communicating them to decision makers and stakeholders?
- Do any of these uncertainties create an opportunity?

Transportation agency risk managers from British Columbia, to Washington, to England, and to New Zealand all advise to "keep it simple," at least at the enterprise level. Although complex and sophisticated probabilistic tools exist for detailed *measurement* of risks, the *management* of enterprise risks is straightforward. The management of risks involves executives creating a risk management program in which staff at the program, project, and activity levels formally identify and document the risks to their objectives. Then, they report those risks to the executives and state how they intend to manage them. Regularly, the executives confer with the risk owners on the effectiveness of the risk-mitigation efforts.

The risk management efforts are incorporated into key agency processes such as developing agency budgets, state transportation improvement programs (STIPs), and long-range plans. Incorporating risk into these documents and processes increases their credibility and realism. If an agency adopts a 10-year asset management plan, it will be assuming funding levels for assets to be set during the next two federal transportation reauthorizations, at least 10 annual federal appropriation cycles, and five biennial state budgets. No one knows what those appropriation levels will be for 10 years. That uncertainty is a major risk, which if not acknowledged, undermines the credibility of the asset management plan. As planning horizons extend and objectives become more complex, the rationale for risk management grows.

The effective risk management program also looks for opportunities. If a new technology, process, or strategy holds opportunity but also risks, the risks can be evaluated. If they

seem to be less than the possible reward, the agency documents the calculated risk and takes it to achieve a greater reward for the public. Risk management is not about battening down the hatches and trying to protect against all threats. It is about taking measured risks after calculating the potential reward. Risk is like prescription medication. Dosed properly, it cures ailments. Abused, it can be disastrous.

The risk taking and risk mitigation occurs in a formal, documented, widely communicated process that extends throughout the organization. This reflects the enterprise-wide nature of enterprise risk management. Although the effort is enterprise-wide and comprehensive, it does not require substantial new staff, nor does it replace existing performance-management systems. Instead, it is ingrained as a practice within the existing performance management system. At the same time that agency officials are managing performance, they also identify, report on, and manage the risks to that performance.

The Benefits of Enterprise Risk Management

Agency leaders in Australia, England, Canada, New Zealand, and the United States say they receive many benefits from implementing enterprise risk management. The executives reported that risk management improved their agencies' performance by supporting strategic planning and performance management. "It basically aligns the corporation and all the subsidiaries with the strategies of the company and

The corollary to risk supporting performance is that if an agency lacks performance objectives, risk management may be less useful. When goals, objectives, and targets are precise and ambitious, the risks to them are more numerous. An agency with few targets will face few risks to them.

the board," said an official of TransLink, the regional transportation agency serving greater Vancouver, British Columbia. "When you don't have a strategic plan everyone goes off in different directions. This way it zeros in on the top risks of the organization." TransLink officials emphasized that risk management is not a separate function but rather a way of doing business that permeates from the board to garage floor. "It is not something that is a task to do but is embedded in your organization as part of your culture." They described risks as the "things that keep you up at night" and the management of them as the natural responsibility of every manager.

The agency began in 2006 to implement risk management, but renewed emphasis came in 2008 with a government-directed reorganization of the agency's board that brought in private-sector board members. The corporate executives immediately asked to see the agency's risk registers because the managing of risks is such a basic expectation in the corporate world. Now, the chief executive provides the board performance and risk updates at every board meeting.

Federal Highway Administration (FHWA) representatives reported that risk management is an effective communication tool for improving the management of objectives. It provides a means to communicate consistently across the organization about what threats and opportunities face the agency. The FHWA staff described enterprise risk management as a key component of strategic planning and management. Although costs and benefits are difficult to measure, the FHWA staff compared the question of "what is the benefit of risk management" to "what is the benefit of having a vision and goals for your organization? If you have goals, you have risks to those goals and to be able to describe those risks is important."

The England Highway's Agency staff describes a similar set of benefits from its risk management program. It supports performance and helps to head off performance obstacles. When some new issue arises, they ask "why didn't we see this coming?" "What precautions did we put in place and why didn't they work?" Like any program, the risk management effort can grow stale when it is not regularly updated. When used effectively, it keeps the organization focused on the issues that could derail its success.

Creating Risk Management Policy, Tools, and Processes

Three major components are essential for risk management success: (1) base risk management in policy, (2) create tools for employees to understand risks and succeed in managing them, and (3) integrate risk management into key processes that ingrain the managing of risks in both strategic objectives and everyday tasks.

Creating a risk-and-performance-based organization involves significant change management. The policy, tools, and process trio (Figure 3) creates an official, self-reinforcing series of influences that establishes the legitimacy of risk management, removes knowledge or participation barriers, and requires employees to participate in the risk management process on a continuing basis. The trio of policy, tools, and process can reduce the chance that managing risks remains an isolated checklist function performed only occasionally when required by a management deadline.

A key first step is for the agency director, commissioner, or commission to issue a clear policy stating that the agency will adopt and ingrain risk management into its strategic planning and performance management processes. The policy can cite the many benefits of risk management and build on them to explain the imperative to adopt a risk management framework. A sample poli-

Figure 3. Policies, tools and processes can ingrain risk management into an agency.

cy is provided.

A Sample Risk Management Policy

It is the policy of this department to manage the risks to our strategic objectives, programs, projects, activities, and, most importantly, the public. We will identify and manage our risks to

- reduce the chance of harm to the public and the public's interests;
- improve decision making by weighing risks with potential rewards;
- encourage rational risk taking when it can result in public benefits;
- increase value by reducing spending on low-risk activities and increasing investments to reduce major risks;
- provide clarity and transparency in our decision making so the public better understands the risks we face; and
- support achievement of our objectives and performance targets.

All employees are expected to understand what risks are and how we manage them. All employees shall understand their role in managing risks at every level. We will assign and manage risks at the following levels.

Strategic risks are those that could affect the entire department and help or hinder the achievement of its major priorities. These risks will be managed by the director, senior staff, and commission.

Program risks are those that could affect performance of our major programs, including safety, pavements, bridges, maintenance, information technology, local programs, project delivery, finance, and human resources. These risks are the responsibility of the program managers.

Project risks are those that could affect the cost, scope, schedule, quality, and impact of construction projects. These risks are assigned to project managers in the programs of new construction, pavements, bridges, safety, roadway, local projects, and maintenance.

Activity risks are those that could affect major ongoing activities, such as snow and ice control, incident response, maintenance of traffic control devices, communication network operations, equipment maintenance, and data collection.

Each risk owner shall develop a risk register in accordance with our Risk Manual. It shall be reviewed at least quarterly and needed changes noted. It is the responsibility of risk owners to report upward to senior management and laterally to peers if risks to his or her area could affect other objectives, programs, projects, or activities. Communication shall be continuous and effective.

All risk owners are expected to update their risk registers and provide them to the department's risk center, according to the Risk Manual. The risks shall be shared with staff, and

each risk manager is expected to keep his or her staff informed of their role in managing the risks in their area.

Figure 4. Risks are managed at one of four levels, with dynamic movement between levels based on the importance of a risk.

The policy references the four levels of risk management recommended in this guide. As seen in Figure 4, the guide recommends managing risks at the enterprise, program, project, and activity levels. This allows nearly all of the major functional areas of a transportation department to engage in risk management. Risk owners focus on the risks of most importance at their level, but if those risks increase they could escalate to a higher level of focus. For instance, if a key project escalates in cost enough, it could threaten the entire program of projects. Or a breakdown in a key agencywide activity could become so severe that it becomes a risk to major objectives of the organization and is elevated to an enterprise risk. Although risks initially are assigned to one of the four levels, the practice of risk management should be dynamic. As the degree of threat or opportunity rises and falls, a risk could rise to the enterprise level or fall down to the project or activity manager to address.

The Risk Management Process

This guide uses as a risk process the one published by the International Organization of Standardization (ISO) in 2009. ISO is a Switzerland-based federation of national standards bodies that organizes subject matter experts from the public and private sectors to develop, critique, and adopt internationally recognized standards.

The ISO process has been adopted by Australian and Canadian associations and is widely recognized in the United States. Its conceptualized process, shown in Figure 5, illustrates its similarity to other "plan, do, act, check" processes developed since the days of William Shewhart in the 1930s. It bears similarities to total quality management, Six Sigma, Lean, and other process-improvement processes. Like those processes, ISO risk management

starts with a recognition of the organization's strategic objectives and focuses an organization's attention on achieving them through a continuous review and improvement process.

The ISO process in Figure 5 represents the concepts and considerations that make up the risk management process, not necessarily discrete steps that are used in all instances. In some cases, such as a transportation agency commission adopting its first risk management program, users may methodically step through every stage of the ISO process. In other cases, such as an activity manager updating his or her risk management program, users may not proceed in lockstep with the Figure 5 components. Although each concept is important, the guide does not suggest that the rote following of each step is required in all instances. Practical judgment is recommended based on the complexity of the risk application.

Develop Tools and Resources

The following tools and resources lead staff through each phase of the risk process. The tools also help agencies establish risk registers and other reporting mechanisms that track, monitor, and communicate risks to key stakeholders.

Figure 5. The ISO process used in many risk guides.

Appoint a Risk Manager

The page 12 checklist summarizes the steps an executive can take to establish a risk management program. Among the first is to appoint an enterprise risk manager or risk management subject matter expert. This person can lead development of the needed tools, including the risk workshop tools and scales that will be described here. The risk manager also can directly support the senior leadership in managing the agency-wide efforts. Executives from England, Canada, Australia, and elsewhere noted that a relatively small staff of one or two people were usually adequate to manage an agency's risk process. However, more staff may be required depending on the agency's level of effort. Staff generally serve as facilitators and subject matter experts. Most risk management tasks become inherent in the performance management duties of the owners of the programs, projects, and activities.
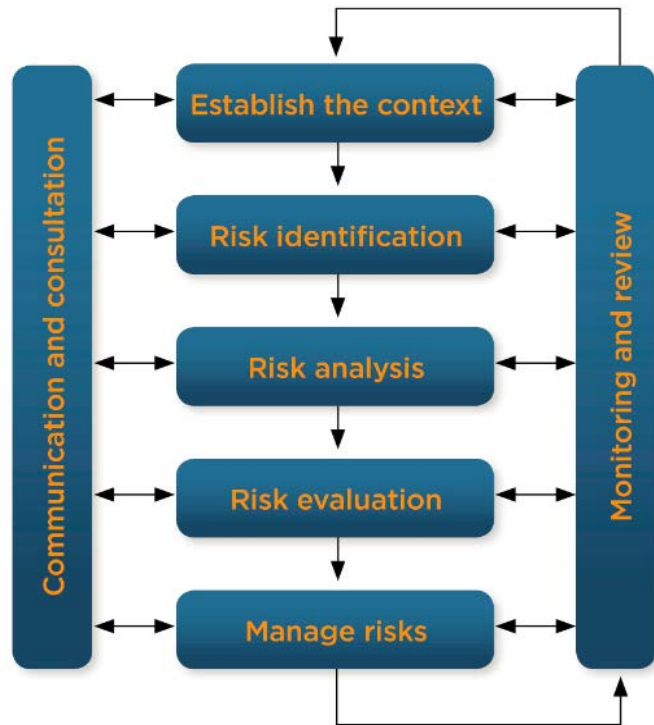
Provide Staff Training

Because risk management is new, it is likely that the risk manager will institute training for staff to understand and learn how to manage their risks. Implementing a risk management culture requires a substantial change-management effort. Training plays a key role. Risk management training is available through the National Highway Institute (NHI) and other public- and private-sector providers.

Develop a Risk Manual or Guide

The risk manager should consider developing an agency risk management guide or handbook. This could detail how the organization chooses to apply the general risk management process to its unique environment. The guide can address elements specific to the agency, including

- how it wants the risk management process to interface with other key cycles, such as development of the STIP and long-range plan;
- reporting formats and cycles;
- who the risk owners are;
- how each owner should develop a risk appetite or tolerance;
- how units should communicate with each other and with other levels about changes in their risk profile that could affect other areas; and
- the expected training and performance levels.

Create Risk Tables and Registers

Among the most important tools the risk manager can provide are risk registers and risk maps or scales such as the one in Figure 6. These generally are simple tools, but they are used almost universally to document the consequences and likelihood of risks and to note what treatment options are to be taken.

The color coding seen in Figure 6 allows for heat-map–like summaries of which risks are critical, which are moderate, and which can be tolerated. These maps are used as icons to communicate the staff's assess-
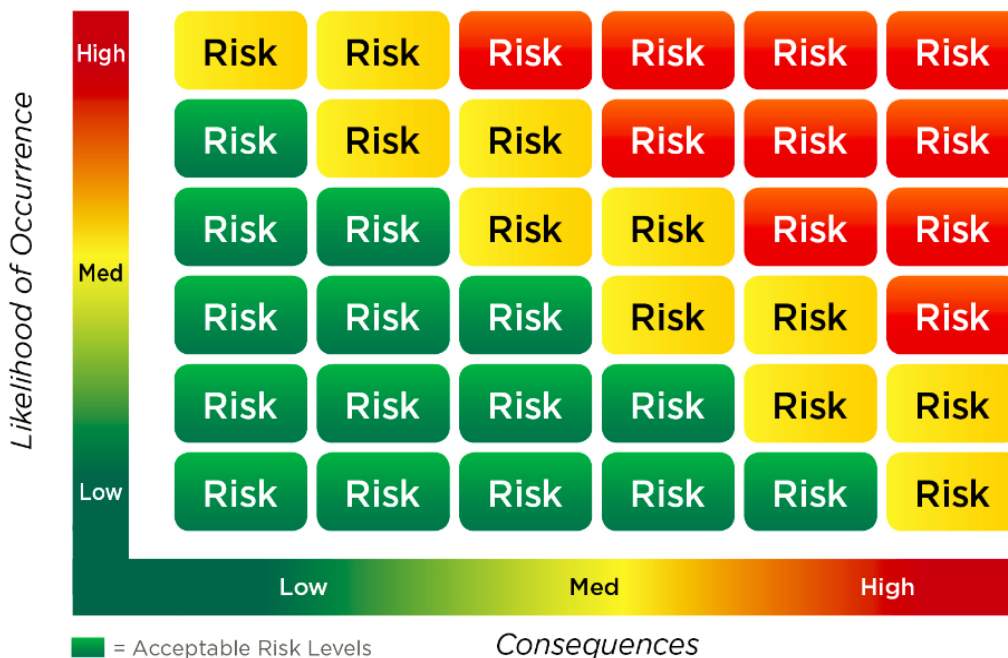

Figure 6. An illustration of a risk map.

ment of the relative importance of various risks and which should rise to the top of the agency's concerns. These frequently are used in status reports and other updates.

Create a Risk Website or Other Reporting Mechanism

The active use of the risk management process—or the active managing of risks—is critical. The agency leader will probably want to instruct the risk manager to create a risk management website or other repository for risk registers, risk plans, and related materials. The rapidly changing nature of risks reduces the effectiveness of static paper reports and increases the effectiveness of real-time websites and updates. A website can house the risk registers, manuals, and supporting materials. It also can serve a news and information function by sharing updates to risk profiles, advice on training opportunities, and other items of interest on managing risks.

Keeping Tools Simple, Keeping Risk Management Practical

Risk measurement and management can be complex and sophisticated but generally only when the risks lend themselves to statistical analysis. On Wall Street, assessing the risks of a given stock or investment involves complex equations and assessment of how one possible investment compares to thousands of others. However, on Wall Street the thousands of stocks all can be categorized based upon decades of experience of how comparable investments fared. Similarly, in the insurance field, risk measurement involves sophisticated actuarial analysis of the likelihood of paying out a benefit.

In enterprise risk management, however, the risks executives face are so diverse they do not lend themselves to statistical analysis. Statistical analysis is less appropriate for assessing the risk that Congress won't fund the next appropriation, or that an earthquake will strike in the next decade. Staff can use probabilities for measuring some risks, but generally, enterprise or strategic risks are best assessed by sound staff judgment and experience.

Reliance on staff experience is one example of a larger pattern of advice taken from the risk management literature: keep it simple. One risk management author advocates for a "modesty of tools and a boldness of goals."[4] By this, he means that it is more important for executives to actively manage their known risks than to acquire complex risk analysis tools. Enterprise risk managers are more likely to rely on the judgment of veteran staff to qualitatively weigh common enterprise risks than they are to invest in complex software systems in an attempt to quantify hard-to-measure risk factors.

> ## A checklist to establish an enterprise risk management program
>
> 1. **Establish in policy that the agency will adopt enterprise risk management.**
>   a. Assign strategic or agency risks to the director.
>   b. Incorporate strategic risks in key policy documents.
>   c. Assign program risks to program owners.
>   d. Assign project risks to project managers.
>   e. Assign activity risks to activity owners.
>   f. Articulate the agency's risk appetite or threshold.
> 2. **Create tools enabling employees to manage risks.**
>   a. Create a risk unit and/or appoint a chief risk officer.
>   b. Provide training.
>   c. Develop an agency risk manual or guide.
>   d. Create risk measurement tables and risk registers, which are simple tools for evaluating risks.
>   e. Create a risk website or other repository for the risk effort and products.
> 3. **Integrate risk management into agency processes.**
>   a. Set the priorities and context for managing agency risks.
>   b. Develop an annual cycle for the risk process and the update of risk registers.
>   c. Create an ongoing communication and monitoring process and cycle.
>   d. Integrate risk management into critical agency processes, such as developing the budget, long-range plan, state transportation improvement program (STIP), and annual work programs.

An FHWA international scan team that examined risk management practices abroad in 2010 came back with the advice to "keep it simple."[5] The experience of staff was the most important component of the risk identification and assessment process they saw abroad. When an Australian transportation agency risk manager visited the United States in 2012, his advice was to focus on capturing risks identified by staff and apply common sense assessment to them. He discounted the use of complex software tools and mathematical computations. He said his agency would rather manage its risks than spend time managing software.

Integrating Risk into Agency Processes

To be meaningful, risk management should be integrated into key agency processes such as budgeting, developing a STIP, and adopting a long-range plan. One particularly useful step is to review risks when reviewing performance. Agencies such as TransLink and the English Highway Agency review risk management efforts during board meetings when executives are reviewing monthly or quarterly performance reports. The point is to not divorce the risk effort from other normal business cycles. The intent is to integrate them.

In agencies with mature risk management processes, it is obvious that risk is integrated into key business processes. The Bay Area Rapid Transit Authority (BART) in greater San

Francisco adopted a 2015–2024 capital plan and strategy that emphasizes how risk is considered in many business functions.[6] BART developed asset management plans for six broad categories of assets such as guide ways, facilities, and fleet vehicles. In each asset management plan, it considers the risks to sustaining those assets in sound condition. Management efforts throughout the year are focused on reducing the impacts of risks that include a majority of infrastructure that is more than 40 years old, increasing demand for service, and the inability to replace needed rolling stock until late in the 10-year plan. BART identified the risk of not meeting service expectations until the new rolling stock is acquired as a significant risk for its staff and executives to manage.

The Queensland (Australia) Department of Transport and Main Roads incorporates risk as a major departmental consideration in many program areas such as bridge inspection, highway safety, and pavement management. Its annual report describes its operating environment as containing several strategic risks, including meeting growing transportation demand to support economic growth; making optimum tradeoffs between system operation and maintenance; engaging with government, industry, and community partners; planning for disasters; addressing changing demographics and transportation patterns; and maintaining internal business operation systems to meet changing conditions.[7] It reports to its minister and the public in its annual report that it will counter those risks by adopting innovative funding strategies, relying more on technology to lower costs, increasing public-private partnerships to fund transportation, and using strategic planning tools to prepare for disasters. Its annual report includes numerous references to how risk is considered in basic functions, such as trying to reduce distracted driving, selecting school zones for flashing lights, prioritizing rail safety programs, selecting vehicles to be stopped for safety inspections, developing highway safety advertising campaigns to target high-risk behaviors, focusing on employee safety and workplace accident reduction, and reducing red tape for low-risk activities. An audit and risk committee is one of six department-wide governance committees. It includes both internal and external representatives, including a representative of a private accounting firm and a representative from a Canadian transportation agency. Its function is to ensure the integrity of the agency's financial statements and oversee the risk management functions.

TransLink integrates risk management into annual priority-setting efforts throughout its 7,000 employee operation. The three-person risk management team works with the agency staff at key points in the annual performance cycle of reviewing past performance, developing updated annual work plans, and incorporating risk management into the work plans. The central staff assist the agency units with coordinating workshops, facilitating meetings, and helping work units complete performance and risk plans. Those plans progress up through the agency to unit heads, division heads, and ultimately to the chief executive and board. The role of risk management staff is to facilitate training and risk analysis, develop risk registers, and provide overall program assistance. The bulk of the risk efforts are deeply ingrained into the management planning and performance review of the individual work-unit managers. TransLink officials said the risk management level of effort is not viewed as extensive or onerous because it is such an integral part of the

agency performance management process.

This guide recommends an ongoing performance-review process that incorporates risk management into key steps, as shown in Figure 7. It recommends that the director, secretary, or commission annually reaffirm the risk policy and identify the agency's strategic risks that the executive staff will manage. The process then cascades through the organization with the updating of the risk registers at the program, project, and activity levels. The staff updates their risk registers and populates them with the central risk website. During the department's normal performance management review processes, the executives and staff also review whether the risk management efforts are effective or if there
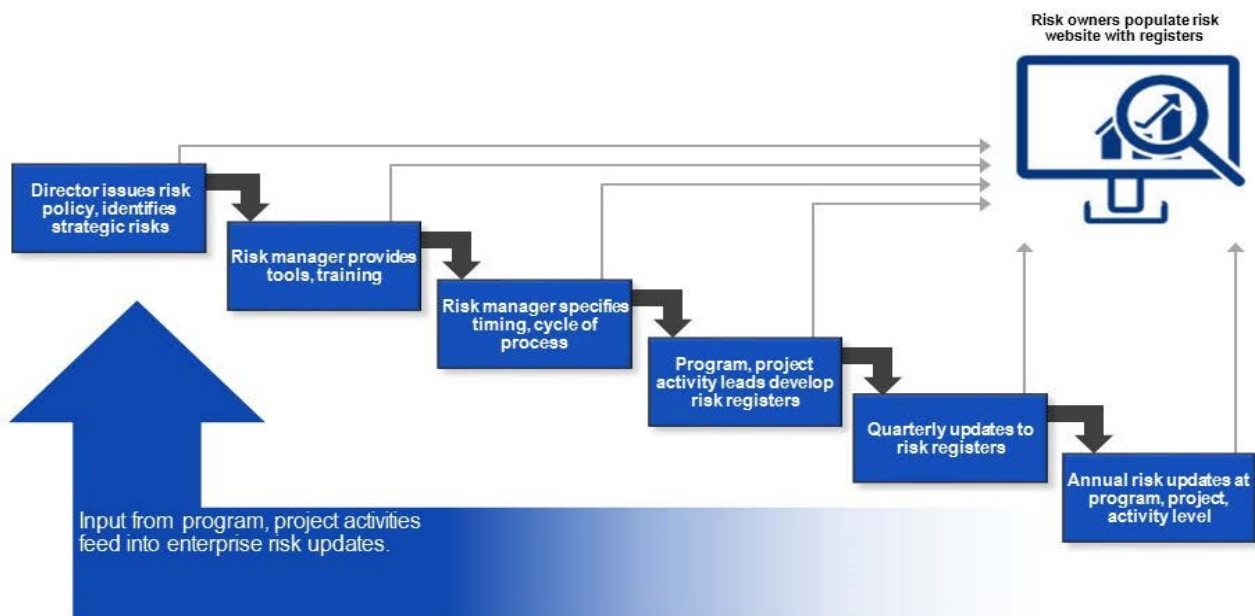
Figure 7 The risk management and update cycle.

are changes in the agency's risks. Throughout the year, the agency reports to the governor, commission, legislature, and other stakeholders if new risks arise that could affect performance or if existing risks have been managed. The process should be dynamic and responsive to changes affecting the agency's performance objectives.

Identifying, Assessing, and Managing Risks

Whether at the enterprise level or at the activity level, the steps of risk management are similar. The ISO approach incorporated in the guide calls for a systematic analytical process. As part of the adoption of the risk management policy or development of the agency's risk management manual, the risks are assigned to specific risk owners. While the senior team assumes ownership of the enterprise-wide risks, program owners take on

risks for their programs, project managers assume their projects' risks, and activity leaders assume those risks. The risk owners form teams who often participate in formal workshops to conduct their risk assessments. As noted earlier, the ISO approach parallels a performance management framework, so throughout its steps the focus is on identifying and managing risks to agency performance.

The risk assessment process should be an open, participatory one that encourages solicitation of a wide range of perspectives. Some authors note that broadening the circle of participants will bring out observations that may not be apparent to the process owners who work with an issue every day. Some authors also suggest that an opportunity for anonymous input be provided. Sometimes risks are created by internal performance or processes that staff may be uncomfortable raising in open sessions. The overall approach to the risk assessment process should be participatory, far-reaching, and candid.

Setting the Context

The risk workshop or risk effort begins by setting the context. Workshop participants examine the objective, program, project, or activity to be achieved. It is critical to keep the risk effort grounded on the performance objective. Workshop participants review the objectives to be achieved and the internal organizational issues and external environmental ones that could create risks or opportunities affecting the objectives. An important aspect of the context-setting stage is to identify the external environment surrounding the objective, as shown in Figure 8. Are there social, cultural, or political sensitivities surrounding the objective? Do external agencies or stakeholders express strong interest in this objective or do they influence or regulate it? What statutory or regulatory considerations are attached? The point is to develop a realistic understanding of what the agency is trying to achieve and what the internal, external, legal, financial, and cultural issues surrounding it are that could create a risk or opportunity or affect how the agency decides to manage it.

A key consideration at this early stage is for the workshop participants to consider the agency's risk appetite. That is, the quantitative or qualitative statement by the agency as to the degree of risk it will accept surrounding this objective. If the objec-

Figure 8 Internal and external factors create uncertainties and opportunities.

tive is of high priority, such as ensuring workplace safety, there is low tolerance for accepting risk. For other issues, the agency may be willing to take more risks. The English Highways Agency says it is willing to take calculated risks with public-private partnerships to leverage external financing. However, for risks to public integrity, it has a very low tolerance. The workshop participants should understand the degree of risk the agency is willing to take surrounding a given objective. The group also should establish in the context phase if their objective links to others. If it does, they should consider how the risks they identify will affect other department objectives.

Risk Identification

After documenting the objective and its context, the risk team moves on to identifying the threats, opportunities, and uncertainties that surround its objective. It is important to cast a wide net at this stage because if risks are not identified they cannot be managed. This step in the risk workshop is often facilitated with exercises such as brainstorming, review of scenarios, or developing checklists. They may be preceded by interviews with subject matter experts. The point is to use individual and group techniques to stimulate thinking and spur the group to identify the internal and external issues that could affect performance, both positively and negatively. While it is important to identify threats, it also is important to identify opportunities, partners, and new strategies that could assist with reducing threats and increasing the likelihood of success.

A helpful tactic when identifying risk is to methodically lead a group through categories of potential risks, which include

- **Health and safety risks** both to the public and to agency staff and stakeholders, such as contractors' personnel;
- **Operational risks,** including variability or uncertainty in agency processes;
- **Economic risks**, such as those caused by cost increases or other changes in the underlying economics of a proposed objective or project;
- **Political risks** that arise from uncertainties or changes in the political climate, such as shifting public sentiment or a change in political leadership;
- **Regulatory risk**, such as that created by new regulatory requirements;
- **Information risk** caused by uncertainty or variability in sound information for decision making;
- **Natural environment risks**, such as those caused by storms, seismic events, and other natural disasters;
- **Fraud or malfeasance risk** that relates to the agency's exposure to criminal behavior, such as theft, collusion, or receipt of benefits for which a party is not eligible; and
- **Litigation risks** caused by the agency's failure to abide by standards, policies, or statutes.

Discussing each type can prompt the recognition of risks or opportunities that may not

come to mind initially.

Risk Analysis

In the risk analysis phase, risk teams refine the organization's understanding of the risks. They use four steps.

- First, they identify the causes and effects of risks, usually based on their expert judgment.
- Second, they estimate the likelihood of the risk occurring. Likelihood can range from being certain to occur every year to being likely only once a century.
- Third, they estimate the consequences, from negligible to catastrophic.
- Fourth, they multiply likelihood by the consequence to achieve a rating: R = L X C.

This simple equation is the basis for nearly all the international frameworks reviewed for the risk guide.

The bow-tie analysis illustrated in Figure 9 captures the concept of this stage. The participants identify the causes of a risk, shown on the left side of the diagram, and the potential outcomes, shown on the right. Shown as small vertical bars are the known control measures. Analysis such as with bow-tie diagrams, fishbone diagrams, or other illustrations help the group identify the causes and effects of a threat or opportunity.

Figure 9 The bowtie diagram shows risk causes, control measures, and consequences.

As with several elements of risk analysis, the result can be qualitative or quantitative, depending on the data available. The result of the qualitative risk analysis phase could be as simple as a team of experts saying that something is likely to occur and that it would be bad if it did. Or the risk team participants could produce a probability-based scenario of likelihood and impact that provides a quantified analysis, including upper and lower likelihood levels and impacts. The concepts for the qualitative and quantitative analyses are the same, but they vary on the data points available to analysts.

An important consideration at this stage is to bear in mind that risks can be positive or negative. A later phase may capitalize on the risk by managing its downsides and exploit-

ing its potential. That nuance may affect this phase, in which the root cause of the risk is clarified and its effects estimated. What causes the risks and its effects can be an important consideration later in how to treat, transfer, terminate, tolerate, or take advantage of the risk as an opportunity.

After the causes and effects of risk have been documented, the risk team moves on to estimating the consequence and likelihood of the risks. Consistent with the "keep it simple" advice, this stage normally relies on the expert opinion of participants as opposed to a complex quantitative analysis. The participants use scales provided by the department's risk team to ensure consistency. It may be necessary to provide different scales for different programs. A scale used to rate project risks may not be appropriate for rating political risks. Although the scales may vary *between* programs, it is important to keep them consistent *within* programs so that risks can be compared with common denominators.

Table 1 illustrates a simple consequence table. It provides participants with significant granularity to assign a consequence value to a given risk. As seen, the scale increases from a value of 1 for a negligible risk consequence to 70 for a severe one. As noted, it is up to the group to agree upon a consequence value to assign to each risk they consider.

Table 1 A risk consequence table.

Consequences			
1	10	40	70
Low	Moderate	High	Severe

Table 2 provides an example of another tool for the participants, a common description of how the agency defines the consequence levels. This example is for risks at the enterprise level. These simple consequence tools serve several functions. They help different groups

Table 2 A consequence table that defines consequence levels.

Enterprise Risk Consequence Levels	
Levels of Consequence	Affects the health and well-being of the citizenry, the agency's ability to comply with statutes, the ability to achieve strategic objectives, or the cost of programs by more than 20 percent
Severe	Affects the safety of individuals or the ability to achieve program goals or causes a more than 10 percent change in program budgets
High	Affects program objectives or budgets by between 5 and 9 percent
Moderate	Affects program objectives or budgets by less than 5 percent
Low	Affects the health and well-being of the citizenry, the agen-

	cy's ability to comply with statutes, the ability to achieve strategic objectives, or the cost of programs by more than 20 percent

use similar scales so that executives later can compare disparate risks. They also help clarify for workshop participants what the agency means when it asks them to identify a risk as negligible or substantial. Finally, they also document due diligence. The use of such common formats and the recording of the workshop participants' scores provides a record of decision as to how the agency decided to take some risks and to avoid others.

At this point, it also is important for the participants to understand that they are now identifying the consequence levels for untreated risks. Later, the consequence or likelihood may be reduced by the groups if they identify risk management options that could treat the risks, leaving what is known as the residual risk.

The next step is for the group to estimate the likelihood of the risk. Although a risk such as a major earthquake could have substantial consequence, if it is highly unlikely to occur in a given time frame, it will be rated as a low short-term risk but higher long-term one. The time frame should be clarified. There probably will be a longer time frame for major enterprise risks such as the risk of a hurricane or seismic event. Although the risks may be low in any given year, over a 5- or 10-year period they are frequent enough to warrant risk management strategies. Therefore, for enterprise risks such as seismic events or delivery of strategic objectives, the time frame may be 10 years or longer. For an activity or a project, the time frame may be as short as 2 years. As noted in the discussion of consequence levels, an agency may have different consequence tables for different levels of risk. The same is true for likelihood tables. To the extent possible, however, they should be consistent across the program, projects, and activities, and each level should have the same likelihood table.

The likelihood scale in Table 3 provides similar, standardized values for the risk team to assess the likelihood of a risk. Note that the word "likelihood" as opposed to "probability" is used. This is because the likelihood is based on staff judgment and no statistical validity is inferred.

Table 3. A likelihood table that defines frequency and likelihood values.

Likelihood Table			
Level	Frequency	Likelihood	Value
Almost certain	Occurs almost annually	95 percent	5
Probable	Occurs approximately once every two years	50 percent	4
Possible	Occurs approximately once every five years	20 percent	3
Rare	Less than once every 10 years	Less than 10 percent	2
Exceptionally rare	Occurs once every 100 years	1 percent or less	1

The risk matrix (Table 4) illustrates how the consequence and likelihood tables are used to produce an initial risk rating. The likelihood value is multiplied by the consequence value to produce a risk value. Using these scales, the highest value is 350, and the lowest is 1.

An example of how these tables are used to produce a risk rating is shown using an example from a theoretical pavement program (Table 5). This example assumes that in the risk identification phase, the pavement team identified the risks to the objective of achieving and sustaining pavement-condition targets for 10 years. The risks are categorized by type.

Table 4. A risk matrix that provides the expected value of likelihood and impact.

		Values	Risk Scores			
Likelihood	**Almost certain**	5	5	50	200	350
	Probable	4	4	40	160	280
	Possible	3	3	30	120	210
	Rare	2	2	20	80	140
	Exceptionally Rare	1	1	10	40	70
			Values			
			1	10	40	70
			Low	**Moderate**	**High**	**Severe**
			Consequences			

Likelihood and Consequence Matrix, or the Risk Matrix

Risk Evaluation

In the preceding step, the risk teams analyzed risks and estimated their likelihood and consequences. In this step, the teams compare the threats, opportunities, variation, and uncertainty with the agency's tolerance for risk. This tolerance is often called the risk appetite. The agency director, commission, or risk manager is responsible for articulating the risk appetite, which will vary by program area.

The risk appetite is the threshold or tolerance for risk. The ISO framework indicates that the risk appetite is a defined boundary. Decision makers can compare the quantified risk to that boundary and decide whether to treat the risk or capitalize on its potential. In some public sector cases, such as at the project level, the risk appetite can be clearly defined. The risk appetite may be that the agency is willing to take few risks that could delay a project by more than a given time, say two months. In many other areas of transportation agency decision making, however, the risk appetite cannot be so clearly defined. Defining the risk appetite can be quite subjective for a task such as estimating how much Federal-Aid funding will be available for the agency's bridge program in the 10th year of its asset management plan or how much risk the agency will accept for 500-year floods or

major earthquakes. Those risk appetites are much harder to quantify.

Risk appetites can be qualitative, such as the agency has a low tolerance for risks to environmental justice communities, or to populations with disabilities, or for environmental compliance. Conversely, the risk appetite could be high for trying new technologies, materials or processes if they hold promise for higher performance or cost savings.

Table 5. Risks to the pavement program.

Risks Identified for the Pavement Program	
Economic Risks	The decline in recent years in state revenue will continue and will erode the resources available to our pavement program, particularly for activities that are not eligible for federal funding, such as preservation treatments.
	The size of the Federal-Aid Highway Program is in question and creates uncertainty for long-term resources for pavement rehabilitation and replacement programs.
	Aggregate prices have continued to increase because of a shortage of sources and will erode the purchasing power of the pavement program.
	Volatile oil prices create uncertainty about the long-term cost of our pavement program because they affect binder and hauling prices. These could be opportunities.
	Consolidation in the pavement industry has reduced competition and appears to lead to higher prices.
Safety Risks	Decline in pavement friction increases the risk of crashes to the public.
	Increasing reliance on nighttime paving to reduce traffic impacts increases risk to staff and contractor employees.
Operational Risks	Decision makers still rely heavily on standard worst-first treatments that increase long-term pavement costs.
	Not all staff have been trained in pavement management strategies.
External Risks	Heavier trucks in the agricultural, timbering, and fracking industries are distressing many pavement sections.
	Increased storm events have washed out culverts and damaged pavements to a greater extent than in past decades.
	The department wants to increase the use of low-cost chip seal treatments but faces opposition from local governments that consider it an inferior pavement product. However, overcoming this opposition would create an opportunity for increased use of chip seals and higher pavement conditions at lower cost.
Information Risks	The department lacks complete asset inventories for items such as guardrails and signs, which complicates efforts to estimate project costs when these items are added to pavement projects.
	The department lacks complete histories of performance by pavement section, which reduces our understanding of how pavements have performed.

Risks Identified for the Pavement Program
The in-house pavement management system is outdated and is unable to perform important forecasting functions.

Managing Risk with the Five Ts

The risk teams use the scales to assign an initial, or untreated, risk value to each risk. Then, they evaluate if and how the risk can be managed. This guide uses the word "manage" instead of the word "treat" that is common in some risk management frameworks. This is because some risks may be opportunities that can be capitalized on or managed. Saying risk is "treated" implies it always is negative. Other guides use "risk response" for this activity. Risk managers have five options to manage risk, which are to tolerate, treat, transfer, terminate, or take advantage of the risk. Other guides use other terms such as avoid or accept.

Tolerating the Risk

Tolerating the risk is deciding to take no additional steps other than the normal controls inherent in the current business process. A decision to tolerate a risk could come as the result of several factors.

- The risk likelihood, consequence, or both are so low that the risk treatment is not cost-effective.
- The potential benefits of trying to capitalize on the risk are uncertain or do not appear to be worth the cost of pursuing an opportunity related to the risk.
- No effective control or treatment exists because of the following.

  o The agency lacks the authority.
  o It is outside the agency's capabilities.
  o It is caused by external forces that the agency cannot control, such as national sentiment.
  o The controls are unacceptable for social or cultural reasons.
  o The risk is legally required, such as risks related to environmental permitting or open records laws.

Treating the Risk

Treating risks is the most common response to risk assessment. Virtually every program, project, or activity in a department can be construed as an effort to treat one risk or another. Roads are paved to reduce risks to safe travel. Bridges are inspected to reduce the risk of collapse. Drivers are licensed to reduce the risk of unsafe driving. A wide range of options exists to treat risks.

Most guides offer this general advice for treating risks.

- Do not be overly conservative and try to treat all risks.

- Consider costs and benefits, and do not spend excessively to treat a risk unless it is of such social or cultural importance that nonmonetary considerations prevail.
- Ingrain the treatment into the work unit's functions to ensure that it
  - o has a clearly assigned owner;
  - o has sufficient resources and authority to be accomplished;
  - o can be measured and managed; and
  - o does not violate other legal, social, cultural, or operational constraints.

Transferring the Risk

Transferring risk shifts it to another party. The most common risk-transfer mechanism is purchasing insurance. While not as common in the public sector as in the private, some U.S. agencies do purchase insurance for specific assets or functions. More typical risk-transfer techniques include requiring contractors to have a performance bond that shifts some of the performance risk from the agency to the bonding company. Another is requiring contractors to have insurance for vehicles, workers' compensation, and professional liability.

Performance contracts can be another form of risk transfer. Performance risk is transferred if an agency contracts with a company to provide performance-based IT support services or if a contractor is required to build a facility and maintain it for a certain period. In both cases, performance risks are transferred, although at a cost.

Risk transfer is possible through agreement. Agencies may strike agreements with local agencies to share unexpected project cost increases if a project is primarily for local benefit. Agencies can require local parties to acquire or donate right-of-way for joint state-local projects if the agency believes the cost of right-of-way is unknown or could be a risk.

Risk transfer does not equate to risk avoidance. The agency still retains some risk that the insurance, bond, or agreement will not provide complete coverage if a default occurs. Also, risk transfer costs money, and the agency may not see a return on that expenditure if the insurance or bond is not needed.

Terminating the Risk

Another risk-response option is to terminate the risk by stopping a practice or eliminating the source of the risk. This may be an option if an agency can replace a high-risk product with a lower-risk one such as replacing timber bridges with more durable concrete ones. For many functions, however, agencies cannot terminate the risks. It is inherent in their mission that agencies undertake high-risk functions, such as working around traffic or maintaining roads at night. To the extent that terminating a risk is an option, it should be considered as a risk management strategy.

Taking Advantage of the Opportunity Inherent in the Risk

The final T is taking advantage of the risk. This option has almost as many forms as treat-

ing the risk. Risk taking is essential and should be a regularly selected option. Without tak-ing well-reasoned risks, the agency cannot maximize the return to its stakeholders. The key is to take well-reasoned risks in which the rewards are likely to outweigh the negative consequences. Facing risks can compel the organization to consider new options, such as

- trying new materials and construction techniques to lower costs or improve quali-ty;
- streamlining outdated practices with new technology and procedures; and
- dropping low-return assets, processes, or functions to eliminate their inherent risk and consolidating investments into higher-return assets or processes.

A measure of success for a risk management program is the number of new innovations it encourages.

Capturing Risk Benefits and Estimating Residual Risk

For risks that are treated, the risk team reassesses the likelihood and consequence of the risk based on its assumption of how the treatment would affect it. If the treatment elimi-nates the possibility of the risk occurring, the team can re-score the likelihood value to "rare." Or if it believes the treatment lowers a risk from "severe" to "moderate," it can record that value. If a risk is not treatable or if it decides to tolerate the risk, the score is not changed. At this step, risk team members estimate the degree of effectiveness and recalculate the residual risk, as shown in Figure 10.

Figure 10 A risk map showing the reduction in risk, or the residual risk, after treatment.

As Figure 10 shows, the team identified six risks for treatment. The team lowered the like-lihood or consequence values and recorded its logic for future reference. Risks beyond

the agency's control, such as the amount of federal funding, are not treated but are only monitored. The heat map shown in Figure 10 illustrates the priorities for treatment. The management system, the shift from worst-first treatments, improvement to the asset inventories, and improvement in performance histories produce substantial risk reductions. Those activities would be singled out for effort by the department. The transfer of the promising risk-reduction efforts into the agency's performance plan represents another linkage between the risk management and performance management efforts. The risk management strategies that most reduce risks to program objectives become performance objectives and are assigned to the appropriate staff for implementation.

Further linkage to the agency's performance efforts is documented in the risk register, as shown as Figure 11. The risk register is a simple spreadsheet-like report that summarizes a risk and its treatment status. The risk registers for all risks should be compiled on the agency website and used during periodic updates to the board, commission, or the owners of the risks. Intentionally simple, the risk register is intended to provide at-a-glance

Risk ID	Description	Impact	Risk level					Comments	Status
P13	The in-house pavement management system is outdated and is unable to perform important forecasting functions…	and impedes decision making while an updated system could improve pavement programming, and program effectiveness.	Initial Risk Level					Development of new PMS under way and milestones to date achieved. Project nearing 50% complete.	Good
Type			Likelihood		Consequence				
Informational and operational risk				Value		Value			Action Required
			Almost Certain	5	Severe	40	200		
Owner			Residual Risk After Treatment						Continued diligence on managing contractor, project.
Meredith Smith, Pavement Manager			Possible	3	Moderate	10	30		
	Risk Reduction Value				170	High Priority			

summation of a risk and its treatment status. The risk register in Figure 11 is for one risk treatment effort, the development of a pavement management system.

Figure 11 A risk register for the pavement management system.

Ongoing Communication and Monitoring

Now that the agency's risks have been assessed and treatments recommended, the risk management processes are put to full use. The active, ongoing review of the risks and the effectiveness of their treatments are the most important aspects of the risk management process. Many of the risk identification and assessment processes are relatively simple. Each, however, serves as a trigger to engage agency personnel in thinking about the risks their agency faces and how they could address them. The real benefits of risk management come from acting on the information.

Risk management is most useful when agencies have robust performance management systems. During communication and monitoring, the risk management program operates in parallel with the performance management functions. As agencies measure progress

toward performance, they also measure progress toward managing the risks to the performance. Risk management updates are performed in parallel with performance updates.

Other than when the risk management process is initiated, communication and monitoring are not steps or milestones in the risk management process. They are continuous functions that are highlighted during

- monthly performance review meetings;
- presentations to the commission, if the agency has one;
- performance reviews of managers and other risk owners;
- updates of agency budgets, STIPS, TIPS, and long-range plans; and
- updates to the transportation asset management plan, highway safety plan, and highway safety improvement plan.

While these bullets refer to specific events or reports, updating the risk registers can occur any time events warrant. Midstream events, such as natural disasters, legislative action, economic crises, or performance breakdowns can trigger a risk rating update and prompt an agency to increase its focus on a risk or downgrade risks that are mitigated.

Capturing the Benefits of Risk Management

U.S. agencies may become more interested in risk management as a result of the risk-based requirements in the Moving Ahead for Progress Act in the 21st Century (MAP-21.) But even if not spurred by MAP-21, U.S. transportation agencies can benefit from enterprise risk management. In a complex environment, achievement of organizational goals depends on managing many internal and external risks. Failure to measure, manage, and mitigate these risks increases the likelihood of failure. As performance expectations increase, so does the expectation that agencies will anticipate and manage the many risks they face.

As one author has noted, leaders either practice risk management or they routinely practice crisis management.[8] Risk management will not prevent crises or disasters, but it does help executives anticipate them and consider scenarios for managing them. Risk management also can demonstrate due diligence and forethought. Risk management can help with making difficult financial tradeoffs. As agencies explain why they make some critical investments and defer others, the weighing of risk can document the soundness of those decisions. Risk management also allows an agency to communicate the many external factors that influence its success but that it cannot fully control. As U.S. agencies embrace performance management, they are likely to see risk management as its natural complement.

[1] World Road Association (PIARC) Technical Committee 3.2. 2010. *Towards Development of a Risk Management Approach.* PIARC, Paris, France, p. 33.

[2] Risk Management Institute. 2006. http://www.rims.org/resources/ERM/Pages/RiskMaturityModelFAQ.aspx. (As of June 30, 2014).

[3] Bernstein, P. 1996. Against the Gods: The Remarkable Story of Risk. John Wiley & Sons, New York.

[4] Coleman, T. 2011. A Practical Guide to Risk Management. The Research Foundation of the CFA Institute.

[5] Braceras. C. and R. Tally, et al. 2010. Linking Transportation Performance and Accountability, a Report of the FHWA International Technology Scanning Program. Accessed at http://www.international.fhwa.dot.gov/pubs/pl10011/ pp 2, 37-38, 44.

[6] Bay Area Rapid Transit Authority FY15–FY24 Short Range Transit Plan and Capital Improvement Plan.

[7] Department of Transport and Main Roads Annual Report 2013–2014.

[8] Lam, James. 2003. Enterprise Risk Management. John Wiley and Sons, Hoboken, N.J., p.4.