

AASHTO Guide for Enterprise Risk Management

FIRST EDITION

2016



Documents

Document Sharing Hub

© 2016 by the American Association of State Highway and Transportation Officials. All rights reserved.
Duplication is a violation of applicable law.

AASHTO Executive Committee

OFFICERS:

President: **Paul Trombino**, Iowa
Vice President: **David Bernhardt**, Maine
Secretary-Treasurer: **Carlos Braceras**, Utah
Executive Director: **Bud Wright**, Washington, DC

REGIONAL REPRESENTATIVES:

REGION I: **Leslie Richards**, Pennsylvania, One-Year Term
Pete Rahn, Maryland, Two-Year Term
REGION II: **Paul Mattox**, West Virginia, One-Year Term
Charles Kilpatrick, Virginia, Two-Year Term
REGION III: **Charles A. Zelle**, Minnesota, One-Year Term
Randall S. Blankenhorn, Illinois, Two-Year Term
REGION IV: **Brian Ness**, Idaho, One-Year Term
Carlos Braceras, Utah, Two-Year Term

AASHTO Subcommittee on Asset Management

The Subcommittee on Asset Management includes members from the **Standing Committee on Planning (SCOP)**, **Standing Committee on Highways (SCOH)**, **Standing Committee on Rail Transportation (SCORT)**, **Standing Committee on Public Transportation (SCOPT)**, and the **SCOH Maintenance Subcommittee**.

Chairman: **Tim Henkel**, Minnesota

Secretary: **Stephen Gaj**, FHWA

AASHTO Liaison: **Matthew Hardy**, Ph.D.

Acknowledgements

The following people contributed to the preparation or review of this guide.

CONTRACTOR TEAM

Principal Investigator: **Gordon Proctor**, Gordon Proctor & Associates

Shobna Varma, The Starisis Corporation

Jeff Roorda, Jeff Roorda and Associates, Inc.

NCHRP PROJECT PANEL

Chair: **Timothy A. Henkel**, Assistant Commissioner, Minnesota DOT

Majed N. Al-Ghandour, P.E., Manager—Program Management—Planning and Programming Division, North Carolina DOT

Anthony E. Carson, Risk Management Specialist, District of Columbia DOT

Heather Catron, Vice-President, HDR Engineering, Inc.

Kimberly Joy Doran, Acting Director—Enterprise Risk Management Bureau, New York State DOT

Evangelos I. Kaisar, Associate Professor—Director, Florida Atlantic University

Margaret Ann "Annie" Searle, Principal, ASA Risk Consultants

Michelle A. Tucker, Chief Risk & Ethics Officer, California DOT

FHWA Liaison: **Michael J. Graf**

TSA Liaison: **Edward Detwiler**, Program Analyst

AASHTO Liaison: **Matthew Hardy**, Program Director for Planning and Policy

NCHRP STAFF

Lori Sundstrom, Senior Program Officer

DISCLAIMER

The opinions and conclusions expressed or implied herein are not necessarily those of the Transportation Research Board, the National Academies, or program sponsors.

Table of Contents

■ Foreword	1	Step 2: Provide the Tools for Managing Risks	34
■ Introduction—About This Guide	3	Step 3: Integrate Risks into Key Agency Processes	36
How to Use This Guide	4	Summarizing the Tasks and Responsibilities	39
■ Chapter 1: Defining Risk Management	5	■ Chapter 3: Establishing the Risk Context	43
Summary	5	Summary	43
Clarifying Risk and Risk Management	7	Identifying Risk Focus Areas and Risk Owners	43
Managing Risks Complements Performance	7	Assigning Risks and Forming Teams to Assess Them	43
Enhancing Decision Making by Evaluating Risks	10	Clarifying the Objectives and Their Environment	44
Allocating Scarce Resources	11	Setting the Context around the Objective	44
Identifying and Mitigating Threats	12	Examples of Applying the Risk Management Process	46
The Levels of Risk Management	13	Tools for the Context-Setting Exercise	47
The Risk Management Process	15	Basis for Further Decision Making	48
The ISO Concepts	16	■ Chapter 4: Identifying Risks	53
Establishing the Context	16	Summary	53
Risk Identification	17	Risk Identification: First Step of Risk Assessment	53
Risk Analysis	18	Beginning the Risk Identification Process	53
Risk Evaluation	18	Techniques for the Risk Identification Workshop	54
Risk Management	18	■ Chapter 5: Analyzing Risks	61
Communication and Monitoring	19	Summary	61
Level of Effort for Enterprise Risk Management	20	Understanding the Causes and Effects of Risks	61
Relying on Risk Management to Improve Performance ...	21	Determining the Cause of the Risks	63
■ Chapter 2: Establishing the Risk Process	25	Cause-and-Effect Analysis	65
Summary	25	Risk Analysis Tools	66
Essentials for ERM: Policies, Tools, and Processes	25	Strengths, Weaknesses of Qualitative and Quantitative Scales	66
Step 1: Adopt a Risk Management Policy	26	Consequence Categories	70
A Sample Risk Management Policy	32	Likelihood Table or Scale	72

Rating Opportunities	76	Georgia Department of Transportation	113
■ Chapter 6: Evaluating Risks	79	Case Study of Asset Management Liability in Australia..	114
Summary	79	A Case Study of U.S. Transit Agency Risk Management .	115
The Risk Appetite	79	Managing Risks to Highway Safety	116
Dynamic and Continuous Evaluation of the Risk Appetite...	82	Australian, Canadian, and British Frameworks	117
Risk Prioritization	82	U.S. Risk-Based Highway Safety Examples	120
■ Chapter 7: Managing Risks	85	Managing Risk from External Threats	123
Summary	85	General Risk or Threat Assessments	123
The Five Ts	87	Climate Change Risks	124
■ Chapter 8: Communicate, Consult, Monitor...	95	Rock Fall Hazard Programs	127
Summary	95	Seismic Risk Assessment Approaches.....	129
Using the Agency's Risk Process	95	Bridge Scour Risks	130
Populating the Risk Register	96	A Case Study of Balancing Investments in Assets and Preparing for External Threats	130
The Risk Map	98	Managing Risks to Financial Resources	132
Key Risk Indicators as Leading Metrics.....	100	Managing Information and Decision Risks	135
Communicating with and Monitoring the External Environment	101	General Information System Risks	135
Consulting with Stakeholders	101	Managing Risks to Models	139
Measuring Risk Management Maturity	102	Managing Risks to Business Operations.....	140
■ Chapter 9: Managing Risks to Key Programs .	105	Traditional Risk Management.....	140
Summary	105	Risks from Theft, Fraud, and Malfeasance.....	140
Managing Risks to Transportation Assets	105	Controlling Risks to Inventory.....	143
Examples of Risk in Asset Management Manuals.....	106	Managing Employee Safety and Workers' Compensation	144
Asset Management Manuals	106	Managing Risks to Programs and Projects	146
U.S. Asset Management Plans.....	111	Guidebook on Risk Analysis and Management Practices to Control Project Costs.....	146
New York State Department of Transportation Risk Assessment	111	Caltrans Project Risk Management Handbook.....	146
Colorado Department of Transportation Asset Management Plan	112	Project Risk Management Guidance for WSDOT Projects.....	147
Minnesota Department of Transportation	113		

Guide for Managing Risk on Rapid Renewal Projects.....	147	Vermont Risk Register	174
Managing Risks on Complex Projects.....	148	NCDOT Risk Register	180
■ Chapter 10: Critical Review of the State of the Practice and Case Studies	149	Washington DOT Risk Register	182
Summary	149	Funding Risks.....	186
State of the Practice	149	Financial Risk Tools.....	189
Corporate Sector Summary.....	149	Basic Spreadsheet Tools	191
From Financial to Enterprise Risk Management	150	Incorporating Elements of the Delphi Technique	193
Risk Management Embedded in Corporate Practice	152	Deterministic Computations Incorporating Variability	194
Corporate Summary	158	Incorporating Randomness in Uncertain Variables	196
NCHRP Studies Summary	158	Stochastic Methods — Monte Carlo Simulations	199
Case Studies of U.S. Practice	159	Illustrative Example	199
Australian Risk Management Summary	167	Results from a Customized Simulator	200
■ Chapter 11: Advanced Risk Tools	173	Commercially Available Software	204
Summary	173	Other Tools to Facilitate Decision Making	209
Risk Registers	173	Conclusions.....	211
		Glossary	213

List of Figures

Figure 1-1. Figure Illustrates the Concept That Risk Management and Performance Management Operate as Parallel, Complementary Disciplines	8
Figure 1-2. Risk Management Can Be an Enabler That Supports Asset and Performance Management.....	11
Figure 1-3. Levels at Which Risk Management Is Practiced.....	13
Figure 1-4. The ISO Process	17
Figure 2-1. Example of a Risk Map.....	29
Figure 2-2. Risk Map Color Coded by Importance of Risks	35
Figure 2-3. Risk Management Flows through the Organization, Cascading from Strategic Risks to Programs, Projects, and Activities—The Risk Manager, Manual, Training, Tools, and Website are Key Enablers in the Process	39
Figure 3-1. Internal and External Factors Can Create Risks	46
Figure 3-2. Internal and External Factors Greatly Influence the Risks and Opportunities Public Agencies Face	48
Figure 4-1. The Three Elements of Risk Assessment.....	54
Figure 4-2. Categorized Risks to the Pavement Program.....	59
Figure 5-1. Bowtie Diagram	64
Figure 5-2. Cause-and-Effect Diagram	65
Figure 5-3. Consequence and Likelihood Scale	67
Figure 5-4. Types of Pavement Risks and Their Consequences	72
Figure 5-5. Pavement Program Risk Map.....	76
Figure 6-1. Risk Treatment Threshold Graphic	81
Figure 8-1. Risk Reduction Map.....	99
Figure 8-2. National Highway Construction Price Trends	100
Figure 11-1. Variability of Projected State Funds During Plan Period.....	192
Figure 11-2. Variability in Projected Bridge Costs Due to Inflation during Plan Period	192
Figure 11-3. Projected Uses at Different Inflation Rates	194
Figure 11-4. Variability in Projected Sources at Different Rates	195
Figure 11-5. Chart Showing the Results of One Iteration of Projected Sources and Uses Using Randomly Generated Values of the Uncertain Variables within the Ranges Recommended by the Expert Panel during the TAMP Period	197

Figure 11-6 Comparison of the Results of One Iteration of Projected Sources Using Random Annual Variability with the Projections Using Base Case Variation as Recommended by the Expert Panel.....	198
Figure 11-7 Comparison of the Results of One Iteration of Projected Uses Using Random Annual Changes in Inflation with the Projections Using Base Case Inflation as Recommended by the Expert Panel	198
Figure 11-8 Histogram of Projected Funding Gaps Using Monte Carlo Simulation	204
Figure 11-9 Sample Output Chart Format with Summary Statistics for NPV of Future Pavement Costs	208
Figure 11-10 Tornado Chart Showing the Relative Impact of Various Uncertain Inputs on the Simulation Results.....	208
Figure 11-11 Decision Tree Showing Options and Potential Outcomes with Associated Probabilities and Costs of a Decision Involving the Completion of a Geotechnical Study	211

List of Tables

Table 2-1. Risk Types and Their Owners.....	33
Table 2-2. Sample Risk Update Report	38
Table 2-3. Matrix of Responsibility, Accountability, Consultation, and Who Is Informed of the Steps Needed to Implement an Enterprise Risk Management Program.....	40
Table 3-1. Issues Surrounding the Context of Asset Management Risks	49
Table 3-2. Sample Highway Safety Objective and Risk Context	50
Table 3-3. Sample Project Oversight Objective and Risk Context.....	51
Table 3-4. Sample ITS Objective and Risk Context.....	51
Table 4-1. Risks to a Theoretical Pavement Program	58
Table 5-1. Consequence Table	67
Table 5-2. Consequence Descriptions for the Enterprise Level.....	68
Table 5-3. Consequence Levels for Program Risks	69
Table 5-4. Consequence Levels for Project or Activity Risks.....	69
Table 5-5. Application of Consequence Levels to the Pavement Program Risks.....	70
Table 5-6. Consequence Table for Program Risks	71
Table 5-7. Likelihood Scale.....	73
Table 5-8. Risk Matrix Values Table.....	74

Table 5-9. Likelihood and Consequences of Risks to the Pavement Program	75
Table 5-10. Threat and Opportunity Table	77
Table 7-1. Residual Risk after Treatment	91
Table 7-2. Team's Recommendations for Managing Pavement Program Risks.....	92
Table 8-1. Complete Risk Register	97
Table 8-2. Simplified Risk Register	98
Table 8-3. Scorecard of Risk Management Activity	99
Table 8-4. Risk Maturity Matrix	103
Table 9-1. Example Risk Register from the CDOT Asset Management Plan	112
Table 9-2. Caltrans Retrofit Criteria	129
Table 11-1. Vermont DOT Risk Matrix	174
Table 11-2. Critical Enterprise Risks from Pavements	174
Table 11-3. Critical Enterprise Risks from Bridges	175
Table 11-4. Critical Enterprise Risks from Budget, Planning and Programming	176
Table 11-5. Critical Enterprise Risks from Data Management and Systems	177
Table 11-6. Number of Risks Associated with VTrans' Strategic Goals and Objective.....	179
Table 11-7. NCDOT Risk Matrix	180
Table 11-8. Snapshot from NCDOT's Risk Register for Pavements.....	181
Table 11-9. Snapshot from NCDOT's Risk Register for Pavements.....	182
Table 11-10.WSDOT Risk Likelihood and Severity Rating.....	184
Table 11-11.Risk Identification and Risk Evaluation Component of WSDOT Risk Register.....	184
Table 11-12.Risk Statements with Level of Risk by Category	185
Table 11-13.Example of Scores for Information Technology Risks in WSDOT	185
Table 11-14.Projected Sources of Funds for a Sample DOT During its 10-year TAMP Period	188
Table 11-15.Projected Uses of Funds for a Sample DOT During its 10-year TAMP Period	188
Table 11-16. Historical Sources and Uses for a Sample DOT.....	190
Table 11-17.Summary of Recommendations from Expert Panel for Variability in Uncertain Parameters during TAMP Period	193
Table 11-18.Projected Sources, Uses and Gaps (including Present Value Computations) during TAMP Period Using Base Case Recommendations from Expert Panel for Variability in Uncertain Parameters	195

Table 11-19. Sensitivity of the New Present Value of Projected Gaps during TAMP Period to Changes in Various Uncertain Parameters (Highlighted Portions Represent Base Case Values for Those Parameters)	196
Table 11-20. Rate of change in Various Categories of Uses and Sources Based on 30 Years of Historic Data	200
Table 11-21. Estimated Values of the Various Sources and Uses over the 10-Year TAMP Period Using Deterministic and Stochastic (One Iteration) Methods	201
Table 11-22. Summary Results Showing the Computation of the NPV of the Projected Gaps along with the Probability of Occurrence of the Computed Stochastic Values	203
Table 11-23. Historical Rates of Change for Various Uses for a Sample DOT	205
Table 11-24. Statistical Parameters with and without Outliers	205
Table 11-25. Selection of Distributions for Uncertain Input Variables	206
Table 11-26. Snapshot of Results from One Iteration for Various Categories of Projected Uses	206
Table 11-27. Comparison of Deterministic Versus Stochastic Projections	206

Foreword

The *AASHTO Guide for Enterprise Risk Management* explains how state transportation agencies can establish and benefit from an enterprise risk management program. It defines risk management and illustrates how it complements strategic planning and performance management. The guide explains how the managing of risk provides agencies with a new set of skills to increase the likelihood that they will achieve their strategic objectives. The guide focuses upon enterprise risk management which is defined as the formal and systematic effort to control uncertainty and variability to an organization's strategic objectives by managing risks at all levels of the organization. The guide also explains how to manage risks at four levels, the enterprise, program, project, and activity levels. The guide includes extensive summaries of how risk management is being applied nationally and internationally to typical transportation program areas.

This work was sponsored by the American Association of State Highway and Transportation Officials in cooperation with the Federal Highway Administration, and was conducted by the National Cooperative Highway Research Program (NCHRP). This guide is based on research conducted under NCHRP Project 08-93, *Managing Risk Across the Enterprise: A Guidebook for State Departments of Transportation*.

Introduction—About This Guide

This guide for state departments of transportation (DOTs) provides a comprehensive framework to identify and manage risk. It will help state DOTs plan, staff, implement, and evaluate consistent and effective enterprise risk management efforts. It demonstrates the benefit and strategic value of enterprise risk management to executive and senior staff while building on the findings of previous research and international scan findings. The guide defines risk management, explains its components, and illustrates how it can improve performance, credibility, and transparency.

For U.S. transportation agencies, risk management generally has been confined to managing risks to construction project cost, scope, and schedule. The expansion of interest in enterprise risk management reflects a growing recognition that risk management can play an important, broader role. It can help organizations manage risks to all objectives, not just those related to project schedules and scopes.

Risk management is the natural complement to performance and asset management. Performance management leads agencies to set goals and direct resources to achieve them. However, all goals include uncertainties and risks. Risk management helps identify, measure, manage, and mitigate those risks. It provides a realistic assessment of the uncertainties or impediments surrounding an organization's objectives and a systems approach to addressing them. As agencies move into the performance era inaugurated by the Moving Ahead for Progress in the 21st Century Act (MAP-21), they will find enterprise risk management to be a complementary framework to help them achieve their performance objectives.

Risk management also helps make difficult investment tradeoffs. By casting decisions in terms of risk, agencies can clarify and explain investment priorities.

Even if not spurred by MAP-21, 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 viewed as a basic competency. It recognizes that 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 consider them is irresponsible.

This guide helps an agency create an enterprise risk management program. It defines enterprise risk management as a comprehensive approach to addressing risks at all levels of the organization. Because an agency's strategic objectives depend on achieving goals and targets at every level, enterprise risk management drills down to the program, project, and activity levels. It illustrates the integration of risk management into an agency's key programs by explaining how it can be applied not only to strategic objectives, but also to the following:

- Transportation asset management
- Highway safety
- External threats, such as climate change
- Financial forecasting
- Information or decision risks
- Program and project risks related to costs, scopes, and schedule
- Traditional business operation risks, such as theft and workforce injuries.

This guide expands on earlier research. The report on National Cooperative Highway Research Program (NCHRP) Project 20-24 (74), *Executive Strategies for Risk Management by State Departments of Transportation*, analyzed information from 43 state DOTs and identified executive-level strategies for implementing enterprise-wide risk management. A 2011 international scan of transportation agency risk management practices found that leading transportation agencies in Australia, England, Germany, the Netherlands, and Scotland have mature risk management policies and procedures. It is entitled *Transportation Risk Management: International Practices for Program Development and Project Delivery*. The 2012 NCHRP Web-Only Document 183, *Guide for Managing NEPA-Related and Other Risks in Project Delivery*, addressed risks related to National Environmental Policy Act (NEPA) decision making.

How to Use This Guide

A well-known adage says some people just want to tell time and others want to know how to build a clock. This guide is designed for both.

Chapter 1 is an executive summary that distills every other section of the guide. A reader who only wants the “what” and “why” of risk management could read just this chapter to get an overview of the entire guide.

Chapter 2 is a “getting started” section that explains how to create a risk management program. It presents the policies, tools, and processes needed to create an ongoing risk management program. It describes what is needed to implement and sustain an enterprise risk management program.

Chapters 3 through 8 are quite detailed and describe the steps agency staff can take to manage risks at all levels of the organization. They include tools to be used in workshops to identify and assess risks. They also describe agency-wide practices to compile identified risks and sort them for executive decision making. They conclude with a section on measuring an agency’s risk management maturity.

Chapter 9 provides more detail on how risk is being applied nationally and internationally to typical transportation program areas. It summarizes how U.S. and international transportation agencies apply risk management to key programs such as highway safety and asset management, and to traditional business operations such as purchasing and inventory control.

Chapter 10 is a critical review of the state of practice, both in public and private sectors.

Chapter 11 is an advanced section that demonstrates risk management tools, such as Monte Carlo simulation that quantifies risk probabilities.

Chapter 1: Defining Risk Management

Summary

This chapter defines risk, risk management, and the risk management process. It also explains how risk management complements performance management. The guide recommends applying risk management at four levels of the organization: enterprise, program, project, and activity. Finally, it summarizes the risk management process.

Understanding modern risk management requires understanding new vocabulary. Unlike in common usage, “risk” involves more than just threats or hazards. In this guide, risk is defined as follows:

Risk is the positive or negative effects of uncertainty or variability on agency objectives.

This definition holds several implications for understanding risk management. 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. A negative risk could be a flood. A positive one a new technology.

Second, managing risk is about managing performance. All performance objectives include 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.

Third, managing risks is about managing opportunities. This may seem counterintuitive, but few risks equal few rewards. 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 merely a measure of potential loss or reward.

Definition of Risk Management

Building on that discussion, this guide uses the following definition of risk management:

Risk management is the cultures, processes, and structures that are directed toward the effective management of potential opportunities and threats.

Similar to the definition of risk, this definition of risk management reflects several aspects of modern enterprise risk management.

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

First, the reference to cultures recognizes that optimally, risk management should be ingrained in the daily processes of an organization from high-level strategic functions to frontline daily operations. The Australian state of Victoria has a well-defined and formal risk management policy that emphasizes its use should not be limited to specialists but rather practiced by staff every day. It defines its culture as “the way we work around here.”² It recommends that risk management create a culture in which all employees understand risks and are willing to take well-considered ones.

Second, the references to processes and structures recognize that risk management is a process-driven framework that includes well-defined steps. Performance management requires structured processes to set goals and direct complex resources to achieve those goals. If risk management parallels and supports performance management, it also requires processes, structures, and formality based on organizational policy.

This guide also emphasizes that risk management should be an active discipline. Therefore, the guide adopts this definition for the risk management process:

The risk management process is the systematic application of policies, procedures, and practices to the identification and management of uncertainty or variability on achievement of agency objectives.

This definition accentuates the active, continuous nature of risk management. This guide recommends that it be an ongoing process. For instance, updates on risks and how they are being managed could be incorporated into daily briefings, monthly management reports, budget documents, and updates to an agency’s

commission. Many risk authors say risk management success is unlikely to be achieved by one-off activities or delegation to technical staff. One private-sector author wrote that executives either continuously engage in risk management or they are condemned to routinely practice crisis management.³ If risk to objectives is constant in a complex environment, then the managing of risk should be continuous.

An extensive literature review was completed before this guide was developed. It summarized more than 120 sources, many of them from the private sector, where risk management is more mature and defined. A common theme of the risk management sources was that risk management should be thought of as a hands-on,

participatory practice. Some authors suggested a shift in definition from emphasizing “risk management” to emphasizing “managing risks.” Their suggestion was to turn the concept from a noun into a verb. Emphasizing the managing of risks highlights the active, participatory nature of successful risk management. When discussion focuses on risk management, it implies that setting up the architecture—or process and structures—is paramount. What many authors emphasize is that the active use of the architecture is most important.

To summarize, this guide differentiates three concepts necessary to understand the application of risk management.

“Risk is the positive or negative effects of uncertainty or variability on agency objectives.”

“Risk management is the cultures, processes, and structures that are directed toward the effective management of potential opportunities and threats.”

“The risk management process is the systematic application of policies, procedures, and practices to the identification and management of uncertainty or variability on achievement of agency objectives.”

2 Department of Treasury and Finance. *Victorian Government Risk Management Framework*. Victorian Government, Melbourne, Australia, March 2011, p. 17.

3 Lam, J. *Enterprise Risk Management from Incentives to Control*. John Wiley & Sons, Hoboken, NJ, 2003, pp. 4, 83–89.

- Risks are positive or negative things, events, actions, variability, or threats that create uncertainty for objectives.
- Risk management is the architecture for managing risks.
- The risk management process is the active use of that architecture for managing risks.

Clarifying Risk and Risk Management

A precise vocabulary is required for transportation agencies to discuss risk management with policy makers, such as legislators. This is because the terms “risk” and “risk management” traditionally have meant different things to different industries.

Twenty years ago in most corporations, risk management focused on managing insurance costs and claims. The risk manager analyzed workplace injuries and took steps to reduce them. The risk manager also focused on ensuring that smoke detectors were used and that employees wore seat belts while driving company vehicles. Then, managing risks was narrowly focused on managing insurance claims, and most definitions of risk and risk management were tailored to an industry’s unique niche.

In the finance world, risk management means calculating the potential variability from different investments. Managing risks involves complex mathematical calculations of probability to determine how much an investment house should pay for complex hedges, puts, and calls to protect itself from unexpected market downturns. Puts and calls allow investors to sell at a price floor or buy at a pricing ceiling, which hedges against excessive losses.

In the insurance industry, risk is the value of an insurance policy and the likelihood that a claim may have to be paid. Managing risks relates to calculating the price of underwriting policies. In the aviation field, risk management focuses on reducing plane crashes, hijackings, and terrorist threats.

These narrow definitions led to the development of another term to describe the broader management of risks to an organization’s strategic objectives, or enterprise risk management (ERM). Similar to other publications, this guide adopts this definition:

Enterprise risk management is 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.

Managing Risks Complements Performance

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 1-1 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. Performance management can be thought of as the drivetrain of an organization, and risk management can be considered a navigational aid. When working in concert, they help an organization achieve its strategic objectives. The disciplines do not compete, but instead complement each other to support strategic objectives.

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 is an international, non-profit association of risk professionals and it 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.⁴



Figure 1-1. Figure Illustrates the Concept that Risk Management and Performance Management Operate as Parallel, Complementary Disciplines

Various risk management standards and guidelines cite similar rationales or benefits for adopting enterprise risk management.^{5 6 7} Because risk is common, people and organizations have always managed risks informally even if they did not adopt a formal or rigorous risk process. The modern rationale for formal risk management is to acknowledge the universality of risks and systematically adopt processes to identify and manage them. The alternative to risk management is accepting informal, anecdotal decisions and occasional threats, disruption, and setbacks caused by threats or risks in the natural, economic, social, or political environments. The many frameworks for risk generally cite similar benefits, such as risk management results in fewer surprises for an organization, it exploits opportunities, it improves planning and decision making, it protects value, and it increases the well-being of stakeholders. Increasingly, risk management is considered a basic component of sound governance. Much like acceptable accounting and fiscal controls, risk management is expected as a basic corporate competency.

4 Risk Management Institute. Risk Maturity Model FAQ. 2006 [cited June 30, 2014]. Available from <http://www.rims.org/resources/ERM/Pages/RiskMaturityModelFAQ.aspx>.

5 International Organization for Standardization (ISO). ISO 31000:2009 Risk Management—Principles and Guidelines. ISO, Geneva, Switzerland, 2009.

6 Standards Australia. AS/NZS ISO 31000:2009 Risk Management—Principles and Guidelines. Australian Government, Sydney, Australia, August 2010.

7 Treasury Board of Canada Secretariat. Guide to Integrated Risk Management [cited June 11, 2014]. Available from <http://www.tbs-sct.gc.ca/tbs-sct/rm-gr/guides/girm-ggirtb-eng.asp>.

Another rationale for risk management is that the lines between good risk management and overall good management are blurring in today's environment of high-performance expectations.⁸ Risk management used to be more of a specialty discipline in industry, much like human resources. Today, financial and environmental regulations create pressures on executives to ensure that their organizations are anticipating and responding to risks. Now, risk management is a core discipline, one that executives need to embrace as a personal and corporate responsibility. In the world of corporate governance, many concerns of running a large organization are being reframed in terms of risk, which means that the role of risk managers and their tools will be increasingly important.

The extensive literature on modern management and performance shows a clear link between controlling risks and increasing an organization's performance. As the consequences of failure increased, so did the importance of managing risks. As the transportation system evolved from stage coaches to canal boats to railroads to commercial aviation, the consequences of risks increased. Executives who failed to identify and reduce those risks increased the chance of their organization's failure to achieve expected performance. The literature reveals a clear evolution from the early writers on quality such as Walter Shewhart⁹ and Edwards Deming, who focused on organizational performance, to modern authors such as James Lam,¹⁰ who argues that managing risks equates to improving organizational performance and reliability.

As evident in MAP-21, the private sector's emphasis on managing risks is now migrating into the public sector. Although MAP-21 does not present a fully articulated vision of risk management, it incorporates risk principles into provisions for highway safety and transportation asset management (TAM). Section 119 requires states to develop risk-based TAM plans to achieve specific condition targets on the National Highway System (NHS). These provisions require state transportation departments to achieve performance targets and, presumably, to manage the risks to achieving those targets.

Manage Risks to Manage Objectives

Bernstein contends that modern civilization is in significant part defined by its efforts to understand and control risk. Efforts by modern societies to understand and reduce the causes of disease, crime, and warfare are viewed within the broad context of identifying, analyzing, treating, and monitoring risks to their citizens. Bernstein was a successful investment fund manager and the first editor of the *Journal of Portfolio Management*. Among his six books is *Against the Gods: The Remarkable Story of Risk*, which traces risk management from a practice in which similar merchants or tradesmen protected each other against catastrophic loss to the evolution of sophisticated mathematically-based, risk management strategies. The development of mathematical models of probability and statistical analysis by such well-known figures as Bayes, Pascal, and Fermat provided the mathematical foundations for quantified risk management.

Today, risk management is a broadly applied field that is specialized by profession. Risk managers are common in fields as diverse as retailing, in which they focus on reducing inventory theft; aviation, in which they focus on safety; and investing, in which they focus on providing guaranteed returns and hedging against significant losses. A central premise of many authors is that sophisticated management and responsible social leadership are impossible without managing risks.

⁸ Kaplan, R., et al. *Managing Risk in the New World*. Harvard Business Review, October 2009, pp. 69–75.

⁹ Shewhart, W. *Economic Control of the Quality of Manufactured Product*. Reprinted by ASQ Quality Press, Milwaukee, WI, 1931.

¹⁰ Lam, J. *Enterprise Risk Management from Incentives to Control*. John Wiley & Sons, Hoboken, NJ, 2003, p. 4.

Enhancing Decision Making by Evaluating Risks

Another rationale for risk management is to enhance decision making by realistically stating the internal and external risks that face a performance objective. The magnitude of risks increases as agencies develop more ambitious objectives that involve more complexity and longer horizons. A simple example relates to the risks state agencies face when they develop MAP-21 highway safety plans. As the agency expands its ambitions to achieve and sustain crash-reduction targets for several years, the external and internal uncertainties grow significantly. As performance objectives increase in complexity, managing risks to those objectives grows in importance and the tradeoffs become more complex.

Public Expectations for Managing Risks

The New South Wales Treasury (2012) says in the *Risk Management Toolkit* for New South Wales (Australia) Public Sector agencies:

"In a globally connected world, both the types and magnitude of risk we face are increasing, while our tolerance for ineffective risk management is diminishing. Simply put, many more things can go wrong and with more far-reaching consequences. At the same time, the community increasingly expects public-sector agencies to manage these risks to minimize any negative consequences.

But increased uncertainty in the world today can also offer possibilities. Recognizing and responding to opportunities, as well as effectively managing for things that could go wrong, will not only support the success of your agency in meeting its objectives, but also ensure that your agency remains relevant and resilient into the future."

Risk management, asset management, and performance management become linked when decision makers weigh short-term investment requests with long-term, risk-reducing investment options. In the short term, a worst-first investment may seem to reduce the most immediate performance risk. However, over the long term an investment in preservation today may reduce much larger performance risk in the future. The linkage of risk, asset, and performance management becomes more apparent when long-term performance horizons are used. When agencies adopt a 10-year asset management horizon and try to sustain asset conditions for the lowest cost over the long term, the risks of not investing in preservation and maintenance become clear. The lack of investment in maintenance creates a much greater investment and performance risk in the later years of the long-term asset management plan.

The credibility of such ambitious plans lies, in part, on the degree to which they acknowledge the risks they face. The plan's success requires cooperation among many transportation, law enforcement, education, and emergency-response agencies. Years of consistent fund-

ing and coordinated efforts by the various parties will be required. No one agency can guarantee the success of the safety plan. As a result, when the agency acknowledges the risks and uncertainty facing the plan, the credibility and reality of the plan increases.

MAP-21 reflects the influence of Australian and British risk management practices on U.S. transportation laws. Statutes in the Australian states of New South Wales, Victoria, and Queensland all rely on risk management to enhance long-term decision making. Their statutes require transportation departments to adopt strategic planning, performance management, accrual accounting, and risk-based asset management as a suite of good-management practices. This quartet collectively results in agencies needing to do the following:

- Identify strategic objectives.
- Use performance measures and performance management to achieve those objectives.
- Rely on accrual accounting and long-term financial plans to get ahead of the curve on any looming, unfunded financial needs related to achieving those targets.
- Use risk-based asset management for the long-term, sustainable performance of infrastructure.

These practices were examined by scanning teams from the Federal Highway Administration (FHWA) International Technology Scanning Program in 2005, 2010, and 2012.^{11 12 13}

All three scan teams acknowledged the benefits of risk-based performance management and reported on its contribution to agency performance and decision making. One team developed the graphic in Figure 1-2 to illustrate the integral role that risk management can play in supporting asset and performance management. The graphic illustrates risk management as an enabler for performance management and asset management to achieve the agency's strategic goals. Both performance management and asset management objectives can be stifled by risks and uncertainties.

Failing to acknowledge, measure, and manage these uncertainties is to overlook obvious risks that affect the credibility and success of the agency's decisions. The scanning reports explained how the Australian and British transportation agencies had embraced risk management as an enabler of their performance and asset management decision making.

Allocating Scarce Resources

Another function of risk management is to help allocate scarce resources. Nearly all transportation agencies are unable to afford all the legitimate needs they face. By restating decisions in terms of risk, agencies are able to clearly communicate why they have invested scarce resources in some projects and activities but not others. By clearly stating their performance objectives and risks, they can better define an acceptable risk and they can better plan for future budgets.



Figure 1-2. Risk Management Can Be an Enabler That Supports Asset and Performance Management

- 11 Braceras, C., et al. *Linking Transportation Performance and Accountability*. Federal Highway Administration, Washington, DC, 2010, pp. 2, 37–38, 44.
- 12 Curtis, J., et al. *Transportation Risk Management: International Practices for Program Development and Project Delivery*. Federal Highway Administration, Washington, DC, 2012.
- 13 Geiger, D., et al. *Transportation Asset Management in Australia, Canada, England, and New Zealand*. Federal Highway Administration, Washington, DC, 2005, pp. xii, xiii, 5, 11, 13, 20, 27, 37–39, 42, 46, 52–53, 56, 59, 63, 83, 88.

Agencies have used risk-based decisions for decades to allocate resources, but those decisions are often not discussed in terms of risk or the risk tradeoffs are not formally documented. Nearly all transportation agencies seek higher condition levels for high-volume assets because poor conditions on those facilities increase the likelihood of crashes, congestion delays for more users, or greater impedance to the movement of goods and people. As agencies develop risk-based asset management plans, they can use risk to explain why investments need to be greatest on higher functional classes to respond to the greater risks those facilities face. Before MAP-21's expansion of the NHS, it included 162,944 miles of the nation's key corridors. In 2008, the NHS included only 4 percent of the nation's total route mileage and 6.7 percent of total lane miles, but it carried 44.3 percent of vehicle miles traveled (VMT).¹⁴ The NHS also carried 75 percent of heavy truck traffic and 90 percent of tourist traffic.¹⁵ Only 19.5 percent of the nation's bridges are on the NHS, but they comprise 49.2 percent of the nation's total bridge deck area. From a risk-based standpoint, poor conditions on the NHS create significant risks to the safe movement of goods and people. If agencies need to reduce service levels on other routes to preserve the NHS, risk management provides a decision framework.

Conversely, among the routes with the highest crash risks are rural, relatively low-volume two-lane roads, particularly at night. Because many crashes on two-lane routes are widely dispersed, investing scarce safety funds into spot locations may not provide significant benefits. This led FHWA and many state transportation departments to encourage risk-based systemic safety investments to reduce the risk of lane-departure crashes.¹⁶ Strategies include systemic treatments to shoulders, lane delineation, advanced warning signs at curves and intersections, improved lighting, and other broadly applied treatments. The logic of these approaches can be used to explain the risk-based investments agencies are making to improve system-wide safety, as opposed to investing only in locations where crashes already have occurred.

Identifying and Mitigating Threats

The emphasis on risk management as a complement to performance management and decision making is not intended to diminish the traditional role risk management can play in reducing threats and hazards. With society's concerns about highway safety, terrorism, climate change, and other threats, risk management can provide an additional framework for prioritizing hazards. More detail on managing risks from external threats and building agency resiliency are in Chapter 9.

An example of how risk management can assist in the assessment of vulnerabilities from climate change is FHWA's *Climate Change and Extreme Weather Vulnerability Assessment Framework*.¹⁷ It incorporates a risk-based approach to assessing an agency's vulnerability to flooding, storm surge, severe weather, and other impacts from climate change. The Washington State Department of Transportation (WSDOT) piloted the framework and developed a risk-based analysis of how climate change could affect its geographically diverse state. It examined issues such as sea level changes and storm surges along the coast, mountain stream flooding and slides caused by increased rainfall, and increased fires caused by drought.¹⁸ WSDOT illustrated the utility of risk management as a framework for climate-impact assessment.

14 US Department of Transportation. System Characteristics: Highways and Bridges. *2008 State of the Nation's Bridges, Highways and Transit: Conditions and Performance* [cited March 3, 2013]. Available from <http://www.fhwa.dot.gov/policy/2008cpr/es.cfm#c2a>.

15 Slater, R. The National Highway System: A Commitment to America's Future. *Public Roads*, Vol. 59, No. 4, March 2013.

16 Federal Highway Administration Office of Safety. *A Systemic Approach to Safety—Using Risk to Drive Action* [cited Dec. 15, 2014]. Available from <http://safety.fhwa.dot.gov/systemic/>.

17 FHWA. *Climate Change & Extreme Weather Vulnerability Assessment Framework*. Federal Highway Administration, Washington, DC, December 2012.

18 Maurer, M. and C. Roalkvam. *Climate Impacts Vulnerability Assessment*. Washington State Department of Transportation, Olympia, WA, November 2011.

Austroroads, the transportation association of Australia and New Zealand, provides a highway safety manual that uses the International Organization for Standardization (ISO) and Australian international risk guidelines. It illustrates how standard risk frameworks lend themselves to identifying, mitigating, and monitoring threats and hazards to motorists, pedestrians, bicyclists, and other groups.

Risk-based processes for assessing the scour potential of bridges are well defined.¹⁹ An international scanning report²⁰ documented how more sophisticated risk-based inspections and design can reduce risks of bridge failure, over-design, and over-inspection. It explained how some European agencies use risk to allocate scarce bridge-inspection resources. Newer, low-risk bridges may be inspected fully every several years to allow inspection resources to be reallocated to more frequent, in-depth inspections of high-risk, high-volume structures. Inspecting every bridge on the same cycle may expend resources where they are not needed and consume resources needed for monitoring higher-risk structures.

The Levels of Risk Management

Most risk frameworks recommend that risk be managed at multiple levels. This guide includes four levels of risk management, although the levels can vary by the framework adopted. The four, illustrated in Figure 1-3, are enterprise, program, project, and activity.

Managing risks at multiple levels is emphasized for several reasons. First, strategic objectives usually cannot be achieved without coordinating many functions throughout the organization. Strategic objectives generally are complex, multifaceted undertakings that require executing steps at many levels. Hence, it often is not possible for executives to ignore frontline functions and expect strategic objectives to be achieved.



Figure 1-3. Levels at Which Risk Management Is Practiced

19 Stein, S. and K. Sedmera. *NCHRP Web-Only Document 107, Risk-Based Management Guidelines for Scour at Bridges with Unknown Foundations* [cited Dec. 15, 2014]. Available from <http://www.trb.org/Main/Blurbs/157792.aspx>.

20 Hida, S., et al. *Assuring Bridge Safety and Serviceability in Europe*. Federal Highway Administration, Washington, DC, 2010.

Also, severe problems at the activity or project level can escalate to become a strategic risk. If a critical project—such as deployment of a new software program—fails, it can create cost and controversy that rise to a strategic risk. A cost increase on a project can be so severe that it affects the entire program of projects, creating a strategic risk. An episode of malfeasance in an organization can create substantial reputational risks that executives need to address to ensure the organization retains its credibility. In keeping with the advice that managing risks should be an active undertaking by all executives, it is advisable to address risks throughout the organization.

Enterprise risk management already has been 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.” As Figure 1-3 shows, enterprise risks generally are the responsibility of senior executives and policy makers. Several risk management authors advise senior executives to make risk management part of their routine management processes. Once a risk process is in place and ongoing reporting of risks is established, the executives monitor their risk register and risk-mitigation processes much like the captain of a ship monitors activities on the bridge. The executive and his or her team scan the horizon for new risks, ensure that identified risks are being managed, and monitor that risk strategies are working. Exceptions at the program, project, or activity level are reported to the executives if they become significant enough to be potential enterprise risks.

This guide uses the Project Management Institute’s definition of a program:²¹

A program is a group of related projects managed in a coordinated way to obtain benefits and control not available from managing them individually.

Portfolio Risks

The Project Management Institute recognizes another level of risk management between the strategic and the program: portfolio management. It defines a portfolio as a collection of projects or programs and other work that are grouped together to facilitate effective management of that work to meet strategic business objectives. Examples are bridge and pavement programs included in an asset management portfolio or all the information technology equipment, resources, and personnel in an information portfolio. Although agencies could manage at the portfolio level, the concepts are so similar to program management that this guide does not address portfolio management.

An example is a transportation agency’s bridge or pavement program. It may consist of a random collection of bridge and pavement projects, but in a performance-based organization it more likely represents a strategic collection of preservation, maintenance, rehabilitation, and replacement projects intended to achieve and sustain condition targets for a reasonable life-cycle cost. The program includes ancillary support functions, such as operation of a pavement management system or data-collection activities, critical to success of the program objectives.

A program manager is the primary person responsible for identifying, measuring, and managing the program risks. The same steps for managing risks shown in Figure 1-4 occur at every level. The difference is the extent and scope of risks to be managed. A typical transportation agency would manage multiple programs, such as an information program, various infrastructure-class programs for pavements and bridges, project delivery programs, environmental compliance programs, and

21 Project Management Institute. *The Standard for Program Management*. 2nd ed. Project Management Institute, Newtown Square, PA, 2008, p. 5.

safety programs. Each would have its own risk manager who monitors the program risks and reports to the enterprise level if serious risks arise that could affect the program objectives.

Programs generally exist to achieve organizational goals and objectives. Failure in a program is likely to ripple through an organization's strategic goals and objectives.

A project is defined as follows:

*A temporary endeavor undertaken to create a unique product, service, or result.*²²

Managing risks to projects is the most widely practiced form of risk management in most transportation departments. It generally involves identifying and managing risks to project cost, scope, and schedule. Increasingly, however, agencies are also concerned about managing compliance risks. These could be risks to environmental compliance commitments or commitments to adjacent property owners to reduce noise and other construction impacts. The Minnesota Department of Transportation (MnDOT) also includes quality as a basic project risk it seeks to control.

The final level of risk is at the activity level. An activity is defined as follows:

A coordinated set of ongoing actions taken to support projects or programs.

The activity level is not included in most risk management frameworks. However, it is included in this guide because of the large number of important activities that transportation agencies perform. Functions such as counting traffic, updating asset inventories, conducting winter operations, maintaining drainage structures, and maintaining traffic signals are critically important. All face numerous risks and uncertainties that, if they become serious, can affect projects, programs, and conceivably strategic objectives. In one 2014 case, a state transportation agency is under a U.S. Department of Justice agreement to clean and repair catch basins to comply with storm water runoff regulations. The lack of routine catch basin maintenance has risen to be a costly, strategic risk that diverts resources from other programs and other strategic objectives. In this case, the risks in a day-to-day activity have become so severe they endanger other strategic goals of the agency. Breakdowns in many activities hold the potential to affect strategic objectives. Breakdowns in right-of-way acquisition processes can delay project and program delivery. Environmental permitting can impede both project delivery and maintenance activities. Activities as routine as stocking parts can become strategic impediments if they reduce the number of operable snowplows during the winter. At many levels, the impact of breakdowns in activities can create project, program, and even strategic risks.

Also, managing risks to activities is relevant to transportation agency personnel. Many are employed at the activity level. By presenting strategies for managing risks to activities, the guide illustrates how risk management can be relevant and useful to personnel at every level of an organization.

The Risk Management Process

This guide uses as a basic risk management process the one published by 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 professional standards.

²² Project Management Institute. *A Guide to the Project Management Body of Knowledge*, 3rd ed. Project Management Institute, Newtown Square, PA, 2004, p. 5.

The ISO process has been adopted by Australian and Canadian associations and is widely recognized in the United States. Its conceptualized approach, shown in Figure 1-4, illustrates its similarity to other “plan, do, act, check” frameworks developed since the days of Shewhart in the 1930s. It bears similarities to total quality management, Six Sigma, Lean, and other process-improvement frameworks. Like those frameworks, the ISO risk management process 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 Concepts

The ISO process in Figure 1-4 represents the concepts and considerations that comprise 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 framework. In other cases, such as an activity manager updating his or her risk management program, users may not proceed in lockstep with the Figure 1-4 components. Although each concept is important, this guide does not suggest that the rote following of each step is required in all instances. Practical judgment is recommended.

Establishing the Context

The first step in the ISO process is to acknowledge and identify the context of the organization.

- What is the organization’s or work unit’s mission?
- What are its challenges?
- What is changing in its environment?
- What authority and resources does it have?
- What objectives has it identified or have been assigned to it?
- What are its legal, political, and social environments?

Risk management must be practical to be effective. It must address the pressing challenges and opportunities of the organization or it will not be relevant. Throughout, this guide emphasizes that risk management exists to help organizations achieve their mission and objectives, so the first step is to document those objectives and the context in which the agency is trying to achieve them.

Another early step is to identify the organization’s risk appetite. This can be either a qualitative or quantitative expression of the degree of risk an agency is willing to accept. The appetite varies by type of risk.

An example of a qualitative risk appetite is expressed by England’s highway agency, Highways England, which has very low tolerance or risk appetite for fraud, theft, or malfeasance. Employees are instructed to take few risks that expose the agency to them. However, it has a much higher risk appetite for pursuing opportunities through public-private partnerships (PPP) and innovative contracting. Although PPPs and innovative contracting bring risk of potential costs or losses to the agency, they also bring substantial possibility of gain in leveraging new resources or providing new projects to the public. Although both PPPs and theft provide a chance for loss of public resources, PPPs offer a possibility of significant gain and lack the potential reputational risks that come with incidents of theft or malfeasance. The Highways Agency risk policy encourages employees to take risks, but not to take significant risks in areas where the risk appetite is low.

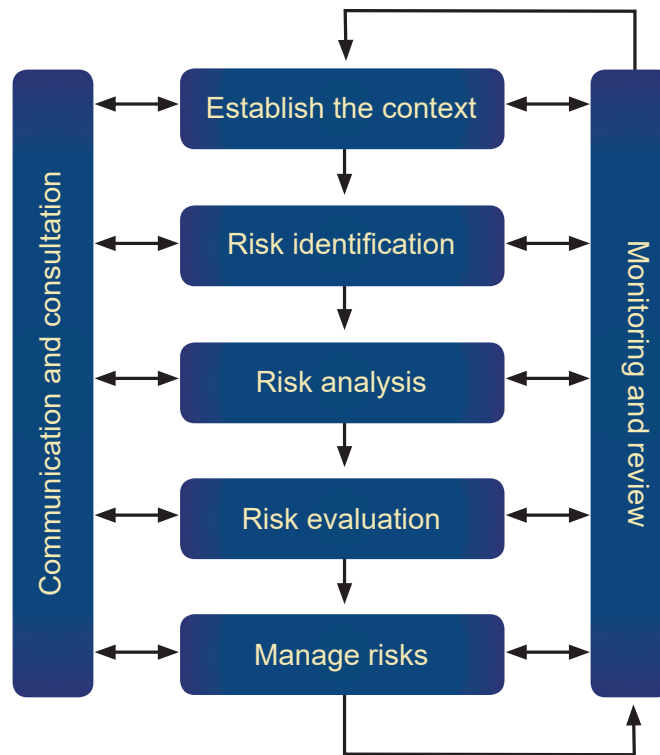


Figure 1-4. The ISO Process

An example of a quantitative risk appetite is the New Zealand Transit Authority's policy of keeping the miles traveled on low-friction routes to no more than two percent of its highway network. Low skid numbers increase the potential risks for motorists who face increased stopping distances and less pavement friction in curves. The agency is willing to tolerate the risks posed by two percent of its system having poor skid conditions, but not more than two percent.

The expression of the risk appetite reflects the policies, philosophies, objectives, and legal requirements the agency faces. The appetite is used later in the guide as a threshold to measure which risks to tolerate and which to treat.

Risk Identification

Risk identification and the next two steps, risk analysis and risk evaluation, are grouped under the general title of risk assessment. Each is discussed individually here with more detail in Chapters 4 and 5.

In the risk identification phase, the organization casts a wide net to compile all the credible risks it can identify. Depending on the level of the analysis, these could be risks to the enterprise, programs, projects, or activities. Ideally, risk managers at all levels of the organization identify their risks, and decision makers classify them and assign them to the appropriate risk managers.

This guide's chapters on risk identification, risk analysis, and risk evaluation discuss tools and techniques to draw out a comprehensive list of risks from staff. Typical strategies to identify risks include conducting workshops and surveys, organizing groups of subject matter experts, reviewing performance reports, and reviewing direction given to the organization by policy or executive groups. The intent at this phase is to

identify a comprehensive set of risks inside and outside the organization. As the ISO standard notes, if risks are not identified, they cannot be managed.

Risk Analysis

Risk analysis involves several steps. First is identifying the root cause of risks. The root cause plays a significant role in later stages when an organization evaluates risks and decides if and how to treat them.

A second step in this phase is to identify the possible negative and positive outcomes. The type of consequence and its magnitude will have a major bearing on whether mitigation steps will be taken and to what degree.

A third step is to estimate the likelihood of the risk occurring. This likelihood can be developed by extrapolating from past occurrences, expert judgment, or estimates of likelihood.

The consideration of all three factors provides the input for the next phase, risk evaluation.

Risk Evaluation

Based on the root cause of the event, its possible impact, and its likelihood, the organization can develop a rank-order list of risks. The risks can be prioritized based on the combination of impact and likelihood.

In this phase, risk managers evaluate and rank the risks based on the criteria of the agency. Evaluation and ranking can be conducted several ways. Risks can be categorized by how they affect enterprise, program, project, or activity objectives. They can be ranked according to the risk they pose to compliance with statutes or other nonnegotiable requirements. They can be listed in rank order and prioritized by their impact and likelihood.

Risk Management

In this phase, the guide differs from the ISO framework, which addresses “treating” risks after they have been identified and evaluated. The guide expands this step to “managing” risks because the response could involve actions other than treatment. Some risk guides and frameworks also refer to this stage as “risk response.”

In this phase, the agency decides if and how to react to the risk. It may decide that the negative consequences are low or unlikely, so the agency will tolerate or accept the risk. The agency may also see the risk as an opportunity and try to capitalize on it.

In this phase, five typical options exist:

Tolerate: The agency could decide that the risk is low, the chance of occurrence is unlikely, or the risk is outside of agency control. In these cases, normal monitoring or treatment is the only option. Examples include the risk of Congressional failure to fund transportation programs. The agency may monitor the risk and communicate its potential consequences, but it is forced to tolerate the risk. Another example is the risk posed by a potential rock fall location that presents a moderate risk, but would be costly to mitigate. The agency may decide to tolerate this risk while continuing to monitor the site.

Treat: If treatment is possible and its benefits outweigh its costs, the agency could decide to act on and mitigate the risk. This could be done many ways, depending on the type of the risk. A high-risk rock fall location may be treated. A high-risk bridge may be instrumented to improve monitoring or it may be repaired or replaced. A new organizational policy and procedure may be adopted to reduce a perceived risk of theft or malfeasance. Depending on the degree of risk, treatment cost, and perceived success of treatment, the agency may decide to take action to treat the risk.

Transfer: Transferring risk is common in the private sector, but less so in the public sector. The most common way to transfer risk is to buy insurance. Individuals and businesses transfer risk continuously by purchasing insurance on their homes, vehicles, and even their lives. Insurance for transportation agencies is less common but is used occasionally. Some more common risk-transfer tactics include requiring contractors and consultants to provide performance bonds, owners protective liability insurance, and professional liability insurance. In a design – build project, some design risks are transferred to the contractor. In a mature risk management program, an agency looks for cost-effective ways to transfer risks.

Terminate: Another risk-response option is to terminate the risk by stopping a practice or eliminating the source of the risk. Systematically replacing timber bridges with concrete or steel structures represents an effort to terminate the risk posed by timber structures. Replacing buried guardrail ends with crash attenuators terminates the rollover risk posed by buried rail. Although some risks can be terminated, many cannot. A private contractor may decide not to provide snow and ice services because of the risk that the investment in equipment and personnel will not be returned in years with little snowfall. A transportation agency cannot eliminate such risks. In fact, society created the organization to take such risks. In the public sector, risks inherent in mandated activities many times cannot be terminated.

Take advantage: A fifth option is to take advantage of the risk. This can occur after an agency has carefully evaluated a risk and decided that its potential upside exceeds the likelihood of its negative consequences. An example is an agency deciding to embrace design – build contracts or PPPs or adopt a new construction material. Every new process brings some risk, but it may be offset by greater rewards. Although it sounds counterintuitive to think of opportunity as a risk, the two are closely related. The result of a risk analysis is often to seize on an opportunity or take advantage of the risk.

Differing Terminology

This guide uses 5Ts as an alliterative, easy-to-remember set of risk responses. Other frameworks use different risk-response terminology. ISO includes seven risk-response options, while the Project Management Institute (PMI) includes three negative risk or threat responses and three positive response options. A National Highway Institute (NHI) course includes four threat responses and four opportunity responses. Chapter 7 includes some typical alternative risk-response terminology in addition to the 5Ts. It is less important which terminology an agency adopts and more important that the agency uses terminology consistently.

Communication and Monitoring

The ISO standard and many authors emphasize the continuous nature of effective risk management. This continuous involvement takes two general forms: communication and monitoring.

The continuous nature of communication and monitoring reflects two key facts. First, a large number of internal and external stakeholders affect agency risks and communicating with them is necessary. Second, risks are generally fluid and changeable. Continuous monitoring occurs to determine if risk factors remain as expected or if circumstances increase or decrease the risk likelihood.

These elements—communication and monitoring—reflect the emphasis on thinking of risk management as a verb, not a noun. The steps reflect the agency’s active monitoring and managing of its risks and the effectiveness of its risk responses. A heavy rain may turn a moderate rock fall risk site into a high-risk one. A sudden spike in bid prices should prompt a review of whether inflation risks are rising and will hurt the larger construction program. As discussed in this guide, the risk management framework assumes that the agency will identify policies, personnel, structures, and processes to continuously monitor and effectively communicate about the risk environment.

Level of Effort for Enterprise Risk Management

Leaders of fiscally strapped agencies may be reluctant to assume additional costs for enterprise risk management. The discussion in this guide of continuous monitoring and comprehensive risk identification may lead to the assumption that large staffs are needed for enterprise risk management.

Practitioners in U.S., Canadian, British, Dutch, and Australian agencies say, however, that only a few key staff are needed to support an enterprise risk management effort as long as the leadership embraces it and staff throughout the organization incorporate it into normal management activities. Risk managers at FHWA; Highways England; TransLink in Vancouver, British Columbia; and Australian agencies compare the level of effort to that of any good management practice, such as managing to performance. Although performance management may include central staff to measure agency-wide performance, the large majority of effort is incorporated into the everyday jobs of managers. Just as managers routinely set priorities, measure performance, and manage staff, they would add risk reporting as a regular management duty.

As of January 2016, the coordinator of Highways England reported that his nationwide organization has an active risk management program, but it does not have a full-time risk manager, although it plans to recruit one. Central staff who coordinate performance management also support and coordinate the agency’s risk management effort.²³ The effort produces monthly reports to the Highways Agency’s board that are part of larger corporate updates. An initial flurry of activity was needed several years ago when the agency wrote its policy and established its risk management processes. Now, coordinating the risk management program is a part-time effort of the central performance-management staff. They coordinate the identification and management of risks among the many divisions. However, even at the divisional level, risk management is a common management task ingrained among others, so it is difficult for the agency to identify the total cost of its risk management effort. The agency does not perceive it as a burdensome effort, but as one managers are expected to absorb as part of their normal due diligence.

The Dutch national transportation agency, Rijkswaterstaat, or the Ministry of Infrastructure and the Environment, said it could not easily estimate the cost of its enterprise risk management program because it is so integrated into the daily activity of staff and is not a stand-alone task.²⁴ Rijkswaterstaat staff report that they use risk considerations in many areas of management, as well as with infrastructure management. Considerations of risk are so ingrained that they have difficulty extracting the costs of risk management from other routine management activities.

The FHWA enterprise risk management staff also report that the costs of its enterprise risk management efforts are such a small fraction of the agency budget and are so ingrained in normal management activities

²³ Personal correspondence with Peter Bohen, Highways England. December 2014.

²⁴ Personal correspondence with Jenne van der Velde, Rijkswaterstaat. December 2014.

that it is difficult to estimate the costs.²⁵ The risk efforts require less than one full-time staff equivalent for the entire agency of about 2,600 people. A Washington-based staff member coordinates the risk effort along with performing other duties. Sixty-seven units in the FHWA headquarters and state divisions produce risk registers. While many staff are involved, the annual effort for each staff person probably is less than a day or two. They meet annually to produce their risk register and periodically throughout the year to update it.

TransLink is Metro Vancouver's regional transportation authority. It operates regional transit, highway, cycling, and commuting options as well as Intelligent Transportation System programs. It has about 7,000 employees, of which about 5,800 are bus or rail operators. It has a mature, comprehensive enterprise risk management program that requires the part-time efforts of three staff.²⁶ Those three employees also contribute to strategic planning and performance management functions. The TransLink leadership views risk management as an essential function, but not one that consumes substantial resources. They describe a system in which three central staff work 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 matriculate up through the agency to unit heads, division heads, and ultimately to the chief executive and board. The role of risk management staff are to facilitate training, provide risk analysis, and develop risk registers and 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.

A former Minnesota Department of Transportation executive who initiated that agency's risk program also said the effort did not require extensive staff resources. No more than three staff members were focused on supporting the effort while the largest effort occurred when staff and managers identified and addressed risks as part of their normal managerial duties.

A paradox arises when describing enterprise risk management. It sounds complex because it reaches throughout the agency. However, the executives say in concept and practice it does not have to be. One said that to be successful with risk management, executives should not make it more complicated than it really is. At its core, it involves asking knowledgeable stakeholders what risks surround the agency's objectives and what steps they should take to manage them.

Relying on Risk Management to Improve Performance

The executives contacted consistently 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 board," a Translink official summarized. "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 a not 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 task of every manager.

25 Interview with Michael Graff and Daniel Fodera, Federal Highway Administration Risk and Performance Management Unit. December 2014.

26 Interview with Paul Barley and Jacqueline Toering of TransLink. Telephone interview Dec. 11, 2014.

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 a performance and risk update at every board meeting. The managing of performance and risks to that performance are considered a basic management practice at TransLink.

Long Horizons, Complex Goals Involve Risks

The MAP-21 requirement for states to develop asset management plans illustrates an example of how increasingly longer planning horizons and more specific targets raise more performance risks. The asset management plan regulations are likely to require states to set performance targets for at least bridges and pavements on the NHS for the next 10 years. For an average state, achieving these targets will involve the following:

- Forecasting performance of thousands of bridges and lane miles of pavement 10 years into the future
- Estimating how much revenue will be allocated in the next two Federal transportation acts and the next five state biennial transportation budgets
- Estimating the performance of existing assets and the effectiveness of planned treatments
- Assuming the cooperation of hundreds of local governments that share responsibility for many assets

As the plan's horizons extend, its complexity increases, and as the participants multiply, the risks to achieving the targets in the asset management plan significantly expand. Nearly every aspect of a complex asset management plan involves risks related to planning, information, performance, evaluation, and budgeting.

The FHWA representatives reported that risk management serves as an effective communication tool for improving the management of objectives. It provides a means to communicate consistently across the organization about what are the threats and opportunities facing 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 precisely, 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 Highways England's staff describe a similar set of benefits for 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. However, when used effectively, it keeps the organization focused upon the issues that could derail its success.

A former MnDOT executive²⁷ reported he initiated risk management there to manage risks; facilitate communication across a large, diverse department; and to increase collaboration. The goal from the beginning was to integrate management of risks into the agency's extensive strategic planning and performance efforts, not to have risk management as a separate function.

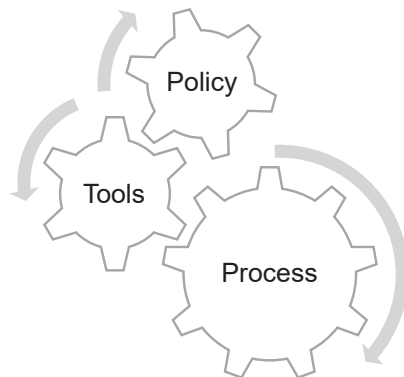
He described risk as a lens through which decision making could be improved. The agency faced an expensive, controversial rebuild of a complex interchange that raised community concern, a high price tag, and a lack of approval by FHWA. The agency reconsidered the project in terms of which movements in the interchange created the highest risks to mobility, safety, costs, and neighborhood impacts and scaled back the project to only those elements. By recasting the analysis of the interchange to focus only on its highest risks, the cost fell significantly, and community and FHWA approval was secured. He sees one of the un-

27 Interview with Tom Sorel, former MnDOT secretary.

recognized benefits of risk management as lowering agencies' backlog of unmet investment "needs." Just because an existing facility may not meet some current design or operational standard, it can be categorized as a need that leads to huge backlogs of investment that are so large as to discourage legislators from trying to address them. When the agency re-evaluates these backlogs in terms of which create the greatest risk, a smaller, more manageable list of critical needs emerges and is far easier to address.

Adding a risk management focus helped improve decision making in many aspects of MnDOT. It contributed to identification of risks that could impede delivery of the overall program, it encouraged management of risks to projects, and from a programmatic level it helped to reduce the perceived backlog of "need" to a more realistic, risk-based assessment of critical capital priorities.

Chapter 2: Establishing the Risk Process



Summary

Chapter 1 describes the “what and why” of risk management. This chapter provides the how. It proposes three essential elements: 1) An emphatic policy stating the agency will adopt risk management; 2) A set of tools enabling staff to practice risk management, and: 3) Integration of risk management into key agency processes. The premise is that agencies will not be successful without all three. The chapter also includes a checklist of items needed to establish an enterprise risk management program.

Essentials for ERM: Policies, Tools, and Processes

Many professional associations, governments, and business-consulting firms provide risk management frameworks or guides. More than a dozen government frameworks were reviewed as background for this guide.^{28 29 30 31 32 33 34 35 36 37 38 39 40} Of particular relevance are ones for managing risks in transportation agencies. Such guides exist in England, several Australian states, New Zealand, and MnDOT. The guides and frameworks demonstrate considerable consistency in describing how to create a robust risk management program.

All the guides say senior leaders and frontline managers should ingrain managing risks into the business processes and decisions of an organization. The international guides and frameworks stress that risk management should not be reduced to a list of steps that are routinely checked off. Instead, consideration of

- 28 International Organization for Standardization (ISO). *ISO 31000:2009 Risk Management—Principles and Guidelines*. ISO, Geneva, Switzerland, 2009.
- 29 New South Wales Treasury. *Risk Management Toolkit for NSW Public Sector Agencies Volume 1: Guidance for Agencies*. New South Wales Government, Sydney, Australia, 2012.
- 30 Victoria Department of Treasury and Finance. *Victorian Government Risk Management Framework*. Victorian Government, Melbourne, Australia, March 2011.
- 31 HM Treasury. *The Orange Book Management of Risk—Principles and Concepts*. HM Treasury, London, United Kingdom, October 2004.
- 32 Risk Management Branch and Government Security Office. *Risk Management Guideline for the BC Public Sector*. Province of British Columbia, Vancouver, British Columbia, March 2012.
- 33 HM Treasury. *Risk Management Assessment Framework: A Tool for Departments*. HM Treasury, London, United Kingdom, July 2009.
- 34 Queensland Government. *A Guide to Risk Management, Financial Management Framework*. Queensland Government, Brisbane, Australia, July 2011.
- 35 Standards Australia. *Risk Management Guidelines: Companion to AS/NZS 4360:2004*. Standards Australia International Ltd., Sydney, Australia, and Standards New Zealand, Wellington, New Zealand, December 2005.
- 36 Minnesota Department of Transportation. *Enterprise Risk Management Framework and Guidance*. Minnesota Department of Transportation, St. Paul, MN, 2013.
- 37 Braig, S., et al. *Strengthening Risk Management in the U.S. Public Sector*. McKinsey Working Papers on Risk, Number 28. McKinsey & Company, Washington, DC, May 2011.
- 38 New South Wales Roads and Traffic Authority. *Guideline for Risk Management*. New South Wales Government, Sydney, Australia, June 2009.
- 39 Transit New Zealand. *Risk Management Process Manual*. Transit New Zealand, Wellington, New Zealand, September 2004.
- 40 Committee of Sponsoring Organizations of the Treadway Commission. *Enterprise Risk Management—Integrated Framework Executive Summary*. September 2004 [cited Dec. 15, 2014]. Available from http://www.coso.org/documents/coso_erm_executivesummary.pdf.

risks should be a driver for executive and staff decision making. Risk assessment should be a part of business processes, including planning, programming, design, construction, information analysis, maintenance, highway operations, and other functions. As each function pursues its objectives, it should identify and manage the risks to those objectives.

Most risk management guides and frameworks implicitly or explicitly recommend three major components for risk management success:

- Base risk management in policy
- Create tools for employees to understand risks and succeed in managing them
- Integrate risk management into key processes that ingrain the managing of risks in both strategic objectives and everyday tasks

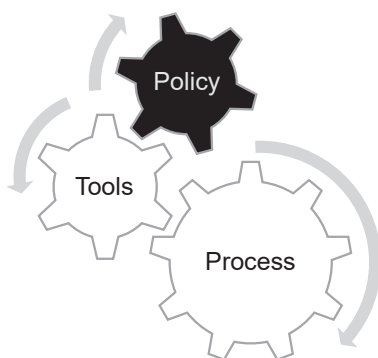
Creating a risk-and-performance-based organization involves significant change management. The policy, tools, and process trio can create an official, self-reinforcing series of influences that establish the legitimacy of risk management, remove knowledge or participation barriers by providing tools and training, and require 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.

Some change-management authors⁴¹ note that the degree to which an organization adopts a new innovation such as risk management relies on three factors:

1. The degree to which leadership emphasizes the change
2. The centralization, complexity, and cohesiveness of the internal management structures for accepting direction
3. The degree of outside influence and the organization's openness to that influence

The adoption of policies, tools, and processes attempts to address all three factors. The policy and leadership engagement emphasizes the importance of risk management. The tools give employees the means to identify and manage their risks, and the process engages the internal management structures. External reporting of risks to legislators and FHWA increases the outside influence that encourages the agency to continue managing its risks.

This chapter examines the adoption of the policy, the development of the tools, and the integration of risk management into agency processes.



Step 1: Adopt a Risk Management Policy

A key first step is for the agency director, commissioner, or commission to issue a clear policy stating 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. The following are among the benefits frequently noted in risk management policies:

41 Rogers, E. *Diffusion of Innovation*, 5th ed. Free Press, London, United Kingdom, 2003, pp. 411–420.

Enhancing performance: By clearly identifying the risks and uncertainty facing an agency's objectives, the agency can better understand the steps needed to ensure success.

Increasing credibility: Every public organization relies on outside stakeholders for its success. Legislators must appropriate resources, suppliers must produce the inputs, the public must support the agency's objectives, and regulatory agencies must approve its actions. Risk management acknowledges the role of these stakeholders and demonstrates how the agency cannot single-handedly achieve its objectives.

Increasing transparency: A risk analysis can explain an agency's rationale for why it takes some risks and avoids others. A documented risk analysis illustrates that the agency has considered the risks and rewards of an action and proceeded based on the best available information.

A checklist to establish an enterprise risk management program

1. Establish a 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.
-

Performing due diligence: An agency that does not actively identify the risks to its stakeholders or objectives is more subject to criticism that it is negligent. Risk management can provide some legal defense as well as provide defense against criticism that the agency was negligent in considering risks that should have been self-evident.

Providing value: Most guides emphasize that risk management increases value by allowing an agency to neither over-protect nor under-protect against risks. Accepting reasonable risks can provide increased rewards to the public, such as may come from a successful new product or process. Similarly, adopting well-reasoned risk treatments can reduce future costs to the public.

Protecting safety and public well-being: The best-understood risk management rationale is to protect against and prepare for threats. A well-planned emergency response plan can be an effective risk management strategy for mitigating the risks of hurricanes, floods, blizzards, and other natural disasters. Similarly, a risk-based rock fall program or roadway-flooding program can increase public safety and the resiliency of the transportation network.

Sharing responsibility: Transportation agency officials in Australia added another reason for adopting risk management, which is the sharing of responsibility for accepting unavoidable risks. They said when risks are formally documented in budgets or other required plans, the agency is informing the executive and legislative branches of the risks inherent in the undertaking. Acceptance of the budget or plan confers shared acceptance of the risk by the agency and the executive branch and the legislature. By noting its risks and incorporating acknowledgement of them into formal budgets and other legislated actions, the agency is sharing the acceptance of those risks with the larger body politic. An example is noting the risks caused by minimal funding for bridge and pavement maintenance. The low funding levels create risks of declining asset conditions. If the agency acknowledges those risks in its budget, adoption of the budget by the legislature and governor spreads the risks among the entire government.

1A: Assign Strategic Risks to the Director or Commission

The policy should note that strategic risks are ones that can affect the goals and objectives of the organization. If these risks are not managed, they can thwart the agency's overarching objectives and ripple through other programs, projects, and activities. An example of a strategic risk is the underfunding of maintenance or the agency's failure to deliver a program of new-capacity projects.

The director or commission can build understanding for risk management by citing in the policy its strategic benefits. Most obviously, mitigating strategic risks helps the agency achieve its broad goals and supports achievement of program, project, and activity objectives. By accepting responsibility for the strategic risks, the leadership demonstrates its commitment to risk management. The active engagement of leadership in identifying and managing strategic risks sends a strong signal of support throughout the organization. Leadership's buy-in and practice of risk management also provides examples to external stakeholders that the agency is actively managing its major strategic risks.

1B: Incorporate Strategic Risks into Key Policy Documents

The leadership also can demonstrate its commitment to risk management in several practical ways. The senior leadership or commission can include a discussion of risks in the agency budget. The budget is more than a list of funding categories. It can be an important policy document that actively engages the executive and legislative branches. Because of the complex environment and multiple stakeholders affecting transportation agencies, the program objectives set in the budget face a host of already-discussed risks. Agency leaders can use the budget document and testimony to illustrate the risks facing the agency's strategic objectives and how it intends to manage them.

Many agencies also have business plans, work plans, or other short-term operational plans^{42 43 44} that are more detailed than budgets and spell out the specific initiatives they intend to pursue in the year or biennium. Such plans generally list the agency's annual priorities, and they often list program priorities and identify specific projects to be delivered. A common strategy for integrating risk management into agency practice is to include a discussion of risks in these key agency documents. The documents both address critical strategic priorities and present high-profile opportunities for the practice of strategic risk management.

Perhaps the most effective application of strategic risk management by agency executives is their embrace of it in regular management meetings with staff and the assignment of risks to specific executives. Most agencies have periodic performance-reporting and policy-review meetings. These may occur with the agency's commission or internally with senior staff. Generally in such meetings, performance reports are reviewed and progress and problems are discussed. Incorporating the discussion of strategic risks in these sessions can create high-level focus on managing risks and send a strong signal to staff that risk management is an essential practice.

Senior leaders can use a risk map similar to the one shown in Figure 2-1 as an icon to illustrate the highest risks they will focus on. The risk map can be used in reports to the commission and staff, budget, STIP, and other agency reports to stress that leadership will emphasize control of these risks.

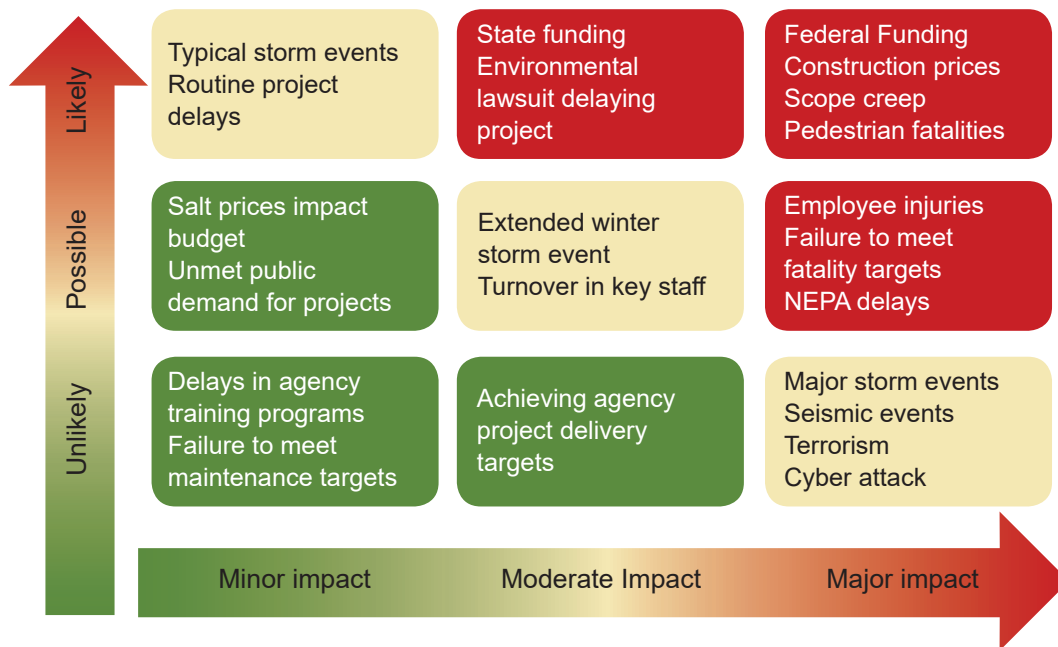


Figure 2-1. Example of a Risk Map

Risk maps such as Figure 2-1 allow at-a-glance identification of which risks the risk owner is managing most closely. In this case, monitoring the uncertain Federal funding process, tracking construction prices, and addressing an increase in pedestrian fatalities are the strategic risks the director or commission owns.

42 Maine Department of Transportation. Maine Department of Transportation Work Plan 2014-2015-2016. Augusta, Maine, January 2014 [cited Dec. 15, 2014]. Available from <http://maine.gov/mdot/projects/workplan/docs/WorkPlan2014-2015-2016Final.pdf>.

43 Ohio Department of Transportation. Ohio Department of Transportation 2010-2011 Business Plan. Columbus, Ohio, December 2009 [cited Dec. 15, 2014]. Available from <http://www.dot.state.oh.us/policy/2010-2011BusinessPlan/Pages/default.aspx>.

44 Virginia Department of Transportation. Virginia Department of Transportation Business Plan for FY 14-15. May 2013 [cited Dec. 15, 2014]. Available from <http://spotidoc.com/doc/168072/business-plan---virginia-department-of-transportation>.

These risks are estimated to have significant impact on agency objectives and to be likely to occur. Although potentially serious, risk episodes such as a major storm event, seismic event, terrorism, or bridge collapse are unlikely to occur in the near term. The agency develops contingency plans for these risks, but does not expect to do more than monitor them and keep contingency plans in place. The chapter on treating risks provides detail on how risk treatments are addressed.

For the senior leaders who own these strategic risks, the coloring represents the degree to which they will focus on these risks.

1C: Assign Program Risks to Program Owners

The next level of risks are program risks. As Chapter 1 states, programs are a group of related projects managed in a coordinated way to obtain benefits and control not available from managing them individually. The agency's risk policy should define programs and cite which programs it recognizes in the organization. It also should identify the program risk owners by position.

The duties and responsibilities of program owners to manage risks can be enumerated. These duties would likely include the following:

- Apply the ISO framework to their major program objectives and activities:
 - Identify risks to their program.
 - Analyze those risks.
 - Evaluate the risks.
 - Manage the risks.
 - Monitor and communicate effectively about the risks to other stakeholders.
- Ensure staff is adequately trained in risk management.
- Maintain effective controls over risks and document risk activities.
- Communicate effectively to senior managers and peers if risks exceed the risk appetite and threaten to impact program objectives.

1D: Assign Project Risks to Project Managers

In the risk policy, a relatively large number of project managers should be identified by position and the expectations for them enumerated. In many agencies, a project risk management process already exists. The agency enterprise risk policy can indicate how the application of risk management is scaled to the size, cost, or complexity of the projects being managed. Routine culvert replacements or resurfacings may have few risks and require simplified risk management efforts. Complex or expensive projects may have formal risk management plans that involve comprehensive consultation with all stakeholders to identify, measure, mitigate, and monitor risks to cost, scope, schedule, quality, and project impacts on neighborhoods, the environment, and traffic.

The section on developing a risk register provides detail on managing project risks. The policy could merely note that each project above a certain level of cost or complexity requires a risk management plan and risk register.

1E: Assign Activity Risks to Activity Leaders

Many activities occur in a transportation department. When they are successful they provide essential information or services that support projects, programs, and strategic objectives. When they break down, their effects can ripple through the organization and spill over into reduced service to the public. The following are the types of activities that are assumed to be addressed:

- Snow and ice control
- Traffic control device maintenance
- Incident response
- Drainage maintenance
- Counting traffic
- Providing network and telephone services
- Conducting modeling for pavements, bridges, and maintenance elements
- Vehicle maintenance

All of these types of activities are routine, but a breakdown in them can lead to significant problems for the public and the organization. Even a localized breakdown in a function such as vehicle repair can have a major impact on snow and ice control in the winter. The policy could note that all activity managers should develop a risk register and risk management plan for their activities and report to higher levels of management the risks that could impede the achievement of these activities to the identified standard of performance. Periodically, perhaps on a quarterly basis, the risk register is reviewed and updated if circumstances warrant.

For example, snow and ice control managers often acquire equipment and purchase salt during the summer. Delays in equipment repairs or purchase or spikes in salt prices or availability in the summer hold obvious potential risks for winter operations. Similarly, if traffic crews experience retirements or illness in signal crews, the routine preventive maintenance and inspection of traffic control devices could lag below acceptable protocols. These risks could be reported and managed. An increase in breakdowns in roadway loops and traffic cameras can presage a reduction in the quality of incident response. Increasing downtime in the computing network can create inefficiencies across the department. Each of these performance issues creates risks that the activity owners can be expected to manage. Table 2-1 illustrates the levels and types of risk to be addressed in the policy. It provides a list of the risk owners and summarizes the types of risks they are expected to manage.

1F: Set the Risk Appetite

The agency director or commission articulates the risk appetite, or at least the reference to how the many levels of risk appetite will be set. The risk appetite is the tolerance for risk the agency is willing to accept. It will vary by activity and risk type. Some expressions of risk appetite can be qualitative, such as the agency has a very low tolerance or threshold of acceptance of risk to ethical behavior, theft, or obvious threats to public safety. Other risk appetites can be quantitative, such as an agency wants 90 percent of its pavement over a 10-year period to be in fair or better condition. Agencies with a good understanding of risk and their risk appetite use them to make cross-program tradeoffs and to balance short-term and long-term needs. The risk appetite serves several purposes:

Clarity: It provides guidance to employees on what risks they should be willing to take and those they should avoid.

Table 2-1. Risk Types and Their Owners

Risk Levels	Owners	Types of Risks
Strategic Risks	CEO Senior staff Board or commission	- Financial risks to agency income - Operational risks caused by lack of staffing, training, or poor performance - External risks caused by political or social issues - Overall preparedness for disaster response - Information risks that create department-wide impacts, such as outdated management systems - Major regulatory or legal compliance risks
Program Risks	Leaders of major programs, such as safety, pavement, bridge, maintenance, information technology, project delivery, human resources	- Performance risks caused by lack of training, execution, or resources to deliver the program - Information risks caused by poor data in the program or inadequate analysis - Financial risks caused by increasing prices - Stakeholder risks caused by contractors or vendors essential to the programs - Major project risks if they exceed the level at which they can affect an entire program
Project Risks	Project managers	- Risks to the cost, scope, schedule, or quality - Project impacts on neighborhoods and environmental compliance
Activity Risks	Activity managers	- Performance risks caused by lack of training, equipment, or execution - Cost increases impinging on activity performance - Risks to execution caused by outside events, such as extreme weather

Value: The risk appetite allows decision makers to better understand how to make investment tradeoffs related to risks. If the agency has little tolerance for noncompliance with environmental regulation, the decision maker may increase spending to avoid that risk. Conversely, if the agency has a high-risk appetite for uncut grass, the program owners will not take risks to get the grass mowed. The risk appetite provides general guidance on the worth of risk-avoidance strategies

Encouraging risk taking: The risk appetite seldom will be zero. If the appetite were zero, the decision maker would never take a risk and would spend inordinately to avoid any risk. With a stated risk appetite, experimentation can be encouraged.

Complementing performance management: Because risk management enables sound performance, the risk appetite provides direction to decision makers who are trying to achieve performance targets.

Based on the risk appetite for each target, they will know how much extra effort or expense is justified to achieve the target. Agencies with mature performance management have learned that when unexpected events occur, it may be too expensive to achieve a target in a given year. For example, in years when floods occur, road condition targets may not be met. The risk appetite indicates how much variance in performance is acceptable.

There probably will be too many levels of risk appetite for each to be addressed specifically in the policy. The policy can include general direction, but instruct each risk owner to suggest and have approved a risk appetite. The various risk appetites can be included in each risk register and risk management plan.

These components of a risk management policy are combined in the following sample policy. It is intentionally brief and is expected to be complemented by a more-detailed risk management handbook or guide for agency personnel.

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 important, 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 benefits to the public
- Increase value by reducing spending on low-risk activities and increasing investments to reduce major risks
- Provide clarity and transparency in decision making so the public better understands the risks
- Support achievement of objectives and performance targets

All employees are expected to understand what risks are and how to manage them. Every employee shall understand their role in managing risks at every level. Risks shall be assigned and managed 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, bridge, 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 the 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.

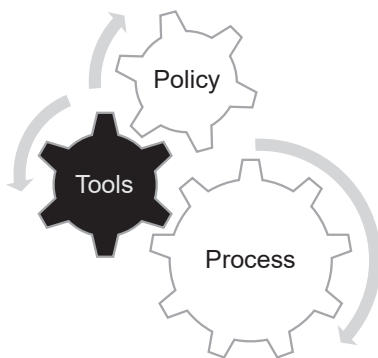
All risk owners are expected to update their risk registers and provide them to the department's risk center, according to the Risk Manual. The risks shall be shared with staff, and each risk manager is expected to keep his or her staff informed of their role in managing the risks in their area.

Step 2: Provide the Tools for Managing Risks

Most guides indicate that the following tools and functions are needed for an agency to manage risks successfully:

- Risk management unit or subject matter expert
- Training program
- Ongoing support and problem solving
- Guide or manual
- Website or other repository for posting risk registers and serving as an information clearinghouse
- A process to communicate vertically and horizontally throughout the agency.

2A: Appoint a Chief Risk Officer or Create a Risk Unit



The director or commission often appoints a chief risk officer or risk-management subject-matter expert or creates a risk unit. This person or unit is charged with tasks such as developing training, developing a manual, providing risk tools, and coordinating risk processes. This person or unit can play many roles, such as subject-matter expert, advocate, troubleshooter, and liaison.

Modern management structures often have this person report to the chief executive officer or a high-ranking executive. Some authors note that the risk manager's role has grown substantially in recent years. One analogy is that risk managers have moved from minor backseat passengers to those who help drive the car.⁴⁵ In past decades, the risk manager was a technician or mathematician who helped develop probabilities and control insurance costs. In the modern corporate environment, the risk manager is one of the chief enablers in an organization. She or he helps the organization identify, monitor, and mitigate its major risks. The chief risk officer also supports the cycle of risk management processes. These ongoing events are described in the risk management process.

2B: 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 in this change management. Training in risk management is available through the National Highway Institute (NHI) and other public- and private-sector providers.

2C: 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 framework to its unique environment. The guide can address elements specific to the agency, including the following:

- How it wants the risk management process to interface with other key cycles, such as development of the STIP and long-range plan

⁴⁵ Croughy, M., D. Galai, and R. Mark. *The Essentials of Risk Management*. McGraw-Hill, New York, NY, 2006, pp. 156–126, 397.

- Reporting formats and cycles
- Who are the risks' owners?
- 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
- What training and performance levels are expected?

2D: Create Risk Tables and Registers

Among the most important tools the risk manager can provide the staff are risk registers and risk consequence tables or scales as seen in Figure 2-2. 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.

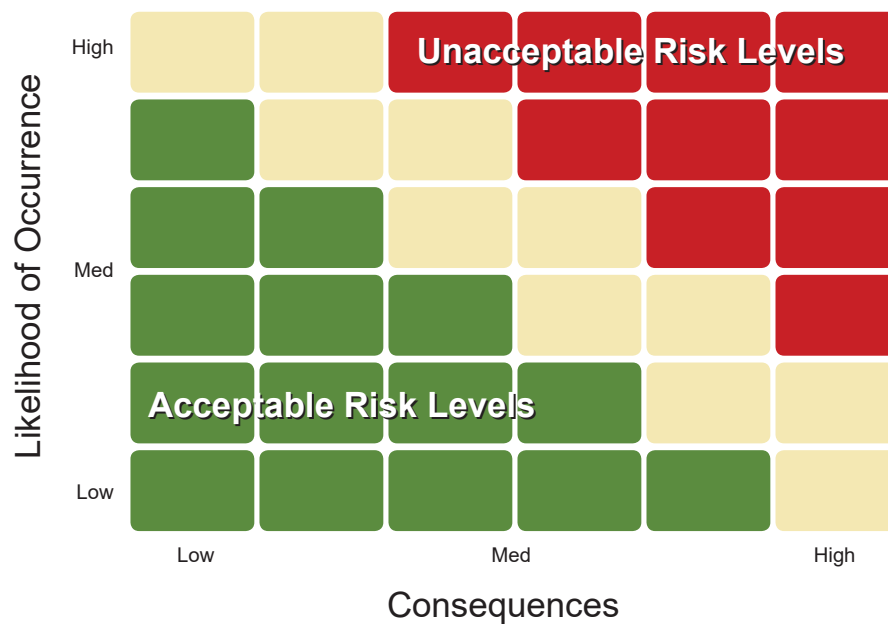


Figure 2-2. Risk Map Color Coded by Importance of Risks

Although these tools and how to use them are explained in greater detail in Chapters 5 through 8, they are discussed here to illustrate how they are necessary to establish a risk process. In the ISO and other risk frameworks, risks are considered from two complementary perspectives: What is their potential consequence and what is their likelihood? Risks with low consequence and low likelihood may warrant monitoring and routine risk treatments, but may not need extensive treatment. Conversely, risks with high consequence and high likelihood rise to the top of the risk-treatment priorities. Figure 2-2 includes a stylized representation of a risk map in which the consequences and likelihood of risks can be evaluated and plotted. These can be ordinal scales of high, medium, or low, or they can be interval scales such as a perceived likelihood of once a year, once a decade, or once a century.

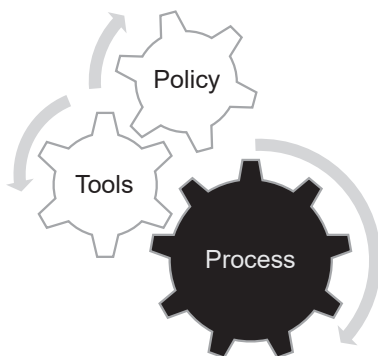
The risk register usually is a spreadsheet-like summary of the risks and their various attributes, including how the risk manager expects to treat them. They are discussed in more detail in Chapter 8. Risk registers occur at multiple levels. A risk register for strategic risks is fed by risk registers at the program, project, and activity levels. Risk registers often include color-coded scales to indicate the rank ordering of risks, similar

to heat maps. Risk registers serve several functions. They document what risks have been considered, the relative consequence and likelihood of the risks, and how the risks may spill over into other program areas. They also summarize the treatment. As part of the training and process, the risk manager should provide a standard risk register and risk-evaluation tables so that risks are measured consistently across the organization.

2E: 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 in a repository. 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.

Step 3: Integrate Risks into Key Agency Processes



While creating the risk management program, the director or commission should identify the processes the agency will use to actively manage risks. Preferably, these processes will be linked to every step of the agency's long-range planning, programming, budgeting, and performance management steps. Also, they should be continuous and work in parallel with the annual cycles to identify and execute performance objectives.

3A: Begin the Cycle: Set the Priorities and Agency Context

Risk management should focus on enabling agency objectives. It should not be a stand-alone requirement unrelated to the priorities of the organization. The first step in the process of integrating risk management into key agency functions is for the director or commission to re-emphasize agency priorities and the risks and opportunities surrounding them. It is helpful to precede this step with a strategic and environmental overview from the senior leadership. This could take the form of an analysis of strengths, weaknesses, opportunities, and threats or a simple report from the leadership. Either would result in an annual or periodic statement of the following:

- Any changes in the agency's strategic objectives since the last publication
- Updates on the legislative or budget environment that may influence agency priorities for the upcoming period
- Acknowledgement of changes in the external environment that may affect the agency's objectives or risks, such as changes in public sentiment, shifts in the economy, new legal requirements, and agency opportunities and obligations
- Changes in agency policy that need to be incorporated into the risk process

To integrate this step deeply into the agency process, it may be useful for the director or commission to link this cycle with the annual budgeting or STIP update process. The point is to not divorce the risk cycle from other normal business cycles. The intent is to integrate them.

It also could be helpful for the director or commission to accompany this overview with a summary of highlights of the past year's performance and management of risks. What risks were well managed? What risks created issues? Which risks have faded and which have risen in prominence since the last update? Because risk management enables performance management, a summary of how the agency performed in achieving its objectives provides a basis for updating risk registers at all levels of the organization.

This overview also could include any changes in agency targets or objectives. If units are managing risks to performance objectives, their starting point is to clearly understand the performance they are attempting to achieve. A key early step in the risk-management process is for agency leadership to clarify performance objectives.

3B: Populate the Risk Registers

The next step is for the risk owners to populate their risk registers using the five steps enumerated in the ISO process: establish the context, identify risks, analyze risks, evaluate risks, and manage risks. This step would logically be done in parallel with reviewing and updating the program, project, or activity performance management plan or program for the year. The risk manager would review his or her area's performance during the past year or business cycle, evaluate the strengths and weaknesses of the performance, and identify the performance objectives for the upcoming year or cycle. Once those are clarified, the five-step risk analysis determines if the risk register or risk management plan for the performance area should be updated. The agency's risk process can direct risk owners to extract from the risk registers simple risk management reports for each risk, such as Table 2-2. It is a sample update for managing risks to the objective of delivering projects on time. This update provides a summary of how the project-delivery team is proceeding with its efforts to manage the risks that prevented it from achieving its performance target.

To further integrate the risk management process into the organization, these types of risk reports can be incorporated in the annual performance plans for individual staff, included in department business plans, or stated as objectives at the divisional level. Clearly communicating and sharing these identified risks to the project-delivery process informs everyone in the department with a role in reducing the risks to project development.

Table 2-2. Sample Risk Update Report

Performance Objective: On-time project delivery to achieve the objectives of the Long-Range Plan, Transportation Improvement Plan, Asset Management Plan, and Highway Safety Plan			
Target	90% of project development milestones achieved within 30 days of schedule		
2014 Performance	↓ 79% achievement of project-development milestones		
Performance Issues	Inability to clear utilities from rights of way Slow reviews in specialty areas, such as drainage and lighting Inability to secure environmental permits on time		
2015 Risks	Utility Clearance	Specialty Reviews	Permitting
Risk Severity	High	Moderate	Moderate
Strategy to Manage the Risks	1. Earlier coordination with utility companies 2. Augmenting staff with consultant assistance 3. Partnering with utilities 4. Training of project-development staff	1. Improved coordination with specialty reviews to achieve on-time reviews 2. Increased use of consultant reviewers	1. Partnering with resource agencies 2. Training with design consultants to anticipate permit needs 3. Improved scheduling of permit requests

3C: Identify the Communication and Monitoring Function

The director or commission needs to instruct the risk manager to identify methods of two-way communication so the leadership can monitor the treatment of risks and the risk manager can alert leadership to changes in the risk environment. Most risk guides recommend formal and continuous communication channels to enable active, ongoing, hands-on management of risks as they arise.

On at least a quarterly basis, risk owners should review risk registers and convey changes in the risk profile through the following:

- Executive staff meetings in which progress toward the annual performance measures is reviewed and effectiveness of risk treatments is evaluated
- Ongoing reports to agency dashboards and the risk website on risk-mitigation efforts and results.

3D: Refresh with an Annual Update

The cycle is completed each year with evaluation of agency performance for the past year and identification of changes in agency objectives, targets, or risks for the upcoming year. These objectives, targets, and risks are cascaded into the agency's priorities and risk efforts at the strategic, program, project, and agency levels. The cascading or linkage occurs by incorporating the risks into key agency documents and processes, such as the budget, employee work plans and evaluations, unit work plans, and STIP.

At the annual update, the director and risk manager should consider whether any strategic-level risks have moderated so they can be downgraded to program, project, or agency risks. Conversely, have any risks from other levels become so severe that they are elevated to strategic risks to be managed by the executive staff? An example is a new statewide payment system that poses a risk in its first year if it has the potential to disrupt business operations while it is deployed and debugged. As the system becomes routine, the agency downgrades it to an activity risk and it is treated by the billing staff. If an environmental agency threatens