Project Management Institute

GLOBAL**STANDARD**

THE STANDARD FOR RISK MANAGEMENT IN PORTFOLIOS, PROGRAMS, AND PROJECTS

THE STANDARD FOR RISK MANAGEMENT IN PORTFOLIOS, PROGRAMS, AND PROJECTS

Library of Congress Cataloging-in-Publication Data

Names: Project Management Institute.
Title: The standard for risk management in portfolios, programs, and projects.
Description: Newtown Square : Project Management Institute, 2019. | Includes bibliographical references and index.
Identifiers: LCCN 2019009876| ISBN 9781628255652 (paperback) | ISBN 9781628255669 (ePub) | ISBN 9781628255676 (kindle) | ISBN 9781628255683 (web pdf)
Subjects: LCSH: Project management. | Risk management--Standards. | BISAC: BUSINESS & ECONOMICS / Project Management.
Classification: LCC HD69.P75 S7374 2019 | DDC 658.4/04--dc23
LC record available at https://lccn.loc.gov/2019009876

ISBN: 978-1-62825-565-2

Published by:
Project Management Institute, Inc.
14 Campus Boulevard
Newtown Square, Pennsylvania 19073-3299 USA
Phone: +610-356-4600
Fax: +610-356-4647
Email: customercare@pmi.org
Internet: www.PMI.org

To place a Trade Order or for pricing information, please contact Independent Publishers Group:
Independent Publishers Group
Order Department
814 North Franklin Street
Chicago, IL 60610 USA
Phone: +1 800-888-4741
Fax: +1 312-337-5985
Email: orders@ipgbook.com (For orders only)

For all other inquiries, please contact the PMI Book Service Center.
PMI Book Service Center
P.O. Box 932683, Atlanta, GA 31193-2683 USA
Phone: 1-866-276-4764 (within the U.S. or Canada) or +1-770-280-4129 (globally)
Fax: +1-770-280-4113
Email: info@bookorders.pmi.org

10 9 8 7 6 5 4 3 2 1

NOTICE

The Project Management Institute, Inc. (PMI) standards and guideline publications, of which the document contained herein is one, are developed through a voluntary consensus standards development process. This process brings together volunteers and/or seeks out the views of persons who have an interest in the topic covered by this publication. While PMI administers the process and establishes rules to promote fairness in the development of consensus, it does not write the document and it does not independently test, evaluate, or verify the accuracy or completeness of any information or the soundness of any judgments contained in its standards and guideline publications.

PMI disclaims liability for any personal injury, property or other damages of any nature whatsoever, whether special, indirect, consequential or compensatory, directly or indirectly resulting from the publication, use of application, or reliance on this document. PMI disclaims and makes no guaranty or warranty, expressed or implied, as to the accuracy or completeness of any information published herein, and disclaims and makes no warranty that the information in this document will fulfill any of your particular purposes or needs. PMI does not undertake to guarantee the performance of any individual manufacturer or seller's products or services by virtue of this standard or guide.

In publishing and making this document available, PMI is not undertaking to render professional or other services for or on behalf of any person or entity, nor is PMI undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances. Information and other standards on the topic covered by this publication may be available from other sources, which the user may wish to consult for additional views or information not covered by this publication.

PMI has no power, nor does it undertake to police or enforce compliance with the contents of this document. PMI does not certify, test, or inspect products, designs, or installations for safety or health purposes. Any certification or other statement of compliance with any health or safety-related information in this document shall not be attributable to PMI and is solely the responsibility of the certifier or maker of the statement.

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES

1

INTRODUCTION

Risk is an uncertain event or condition that, if it occurs, has a positive or negative effect on one or more objectives. Positive risks are opportunities, while negative risks are threats.

The practice of risk management includes planning the approach, identifying and analyzing risks, response planning and implementation, and ongoing monitoring of risks. Risk management is an essential aspect of all organizational activities. This standard describes the application of risk management within an enterprise risk management (ERM) context that includes the portfolio, program, and project domains. Risk management shapes the decision-making processes across the organization and within each of the domains.

The degree to which risk management is pursued can be the difference between success and failure. PMI's 2015 *Pulse of the Profession®* report found that for organizations that apply a formal risk management approach, 73% of projects meet their objectives, 61% finish on time, and 64% are completed within the approved budget [1].[1]

Risk management allows an organization to:

- Anticipate and manage change,
- Improve decision making,
- Proactively implement typically lower-cost preventive actions instead of higher-cost reaction to issues,
- Increase the chances to realize opportunities for the benefit of the business,
- Generate broad awareness of uncertainty of outcomes,
- Act upon the transformations taking place in its business environment, and
- Support organizational agility and resilience.

Risk management also establishes iterative connections among portfolios, programs, and projects and links these connections with ERM and organizational strategy.

[1] The numbers in brackets refer to the list of references at the end of this standard.

1.1 PURPOSE OF THIS STANDARD

This standard describes the concepts and definitions associated with risk management and highlights the essential components of risk management for integration into the various governance layers of portfolios, programs, and projects with the following major objectives:

- Describe the fundamentals of risk management,
- Support the objectives of and demonstrate the link to ERM, and
- Apply risk management principles, as appropriate, to portfolio, program, and project domains as described in the PMI foundational standards.

This standard fulfills a business need to provide a standard for risk management in portfolio, program, and project management that defines the essential considerations for risk management practitioners. It expands on the knowledge contained on risk management in the relevant sections of the PMI foundational standards.

This standard can be used to harmonize practices between ERM and portfolio, program, and project management, regardless of the life cycle approach used.

PMI is committed to providing global standards that are widely recognized and consistently applied by organizations as well as practitioners. Increasingly, organizations are requiring practitioners to use risk management practices in portfolio, program, and project management as an integral part of their ERM framework.

1.2 APPROACH OF THIS STANDARD

This standard presents the *what* and *why* of risk management. The following concepts are elaborated in this standard:

- Purpose and benefits of risk management;
- Principles and concepts of risk management in portfolios, programs, and projects;
- Risk management life cycle in portfolios, programs, and projects; and
- Integration of risk management within portfolios, programs, and projects.

This standard provides guidance on integrating risk management practices into all key areas of enterprise, portfolio, program, and project management. The aim is to ensure that the management of risk is an inherent, natural part of all management domains. The scope of this standard is to provide guidance and not to impose uniformity of processes across portfolios, programs, and projects. When planning and implementing risk management, it is essential that each team consider the characteristics of the organization, portfolio, program, or project. The approach presented in this standard is based on risk management principles that can be used as guidance when designing specific management or business processes adapted to the organizational environment and nature of the work.

1.3 PRINCIPLES OF RISK MANAGEMENT

There are specific core principles that underlie the process of risk management. The seven principles provided in Sections 1.3.1 through 1.3.7 guide the risk management processes and are integral to effective risk management.

1.3.1 STRIVE TO ACHIEVE EXCELLENCE IN THE PRACTICE OF RISK MANAGEMENT

Risk management allows organizations and teams to increase the predictability of outcomes, both qualitatively and quantitatively. This principle is about reaching the appropriate level of organizational process maturity (the ability of an organization to apply a certain set of processes in a consistent manner) and the optimal level of performance. Excellence in risk management is not achieved by the strict and exhaustive application of related processes. Rather, excellence can be achieved by (a) balancing the benefits to be obtained with the associated cost and (b) tailoring the risk management processes to the characteristics of the organization and its portfolios, programs, and projects. Process excellence in risk management is itself a risk management strategy.

1.3.2 ALIGN RISK MANAGEMENT WITH ORGANIZATIONAL STRATEGY AND GOVERNANCE PRACTICES

The practice of risk management in organizations is developed and evolved in coexistence with other organizational processes, such as strategy and governance. The nature of portfolios, programs, and projects is such that circumstances may change frequently. Adjustments become necessary as the organization evolves, for example, when changes to decision-making processes, timing, scope, and speed are made.

1.3.3 FOCUS ON THE MOST IMPACTFUL RISKS

Successful organizations are able to effectively and efficiently identify the risks that directly influence goals and objectives. The challenge for most organizations is making the best use of resources by focusing on the right risks. This depends on the characteristics of the organization, its environment, internal maturity, culture, and strategy. Determining the most impactful risks can be difficult. Organizations develop and improve by refining the processes for risk prioritization.

1.3.4 BALANCE REALIZATION OF VALUE AGAINST OVERALL RISKS

Risk management seeks to find the proper balance between the exposure to risk and the expected business value creation or realization. Initiatives presenting a low level of risk may not create a sufficient level of value and performance. On the other hand, initiatives presenting a high, expected performance may expose the organization to an unacceptable level of threat.

1.3.5 FOSTER A CULTURE THAT EMBRACES RISK MANAGEMENT

Risk management is an inherent and essential part of the portfolio, program, and project management framework. The practice of risk management is propagated, recognized, and encouraged throughout the organization. A culture of risk management encourages (a) the identification of threats rather than ignoring them and (b) the identification of opportunities by cultivating a positive mindset within the organization—one that is more open to accept and harness the positive changes impacting the various initiatives.

1.3.6 NAVIGATE COMPLEXITY USING RISK MANAGEMENT TO ENABLE SUCCESSFUL OUTCOMES

Managing risks is an essential part of reducing and handling the complexity within organizational initiatives. The ability to identify and manage risks is directly dependent on the level of complexity of the initiatives. Concentrating efforts on clarifying the objectives, requirements, and scope of initiatives facilitates the identification of risks and enhances the ability to manage them, thus lowering the exposure of these initiatives to unforeseen situations. The more organizations navigate complexity using risk management, the more they will be able to optimize the use of resources, increase the return on investments, and improve overall performance and business results.

1.3.7 CONTINUOUSLY IMPROVE RISK MANAGEMENT COMPETENCIES

The nature of risks to which an organization is exposed and the available technology to manage those risks are changing. Technology allows organizations to manage risks more effectively and to better focus on the risks' impacts. Through continuous improvement of risk management competencies, organizations and individuals can develop sustainable competitive advantages that contribute to overall organizational performance.

1.4 STRUCTURE OF THIS STANDARD

This standard can be used to review portfolio, program, and project management processes from a risk management perspective. It is organized as follows:

Section 1—Introduction

Section 2—Context and Key Concepts of Risk Management

Section 3—Framework for Risk Management in Portfolio, Program, and Project Management

Section 4—Risk Management Life Cycle in Portfolio, Program, and Project Management

Section 5—Risk Management in the Context of Portfolio Management

Section 6—Risk Management in the Context of Program Management

Section 7—Risk Management in the Context of Project Management

Appendix X1—Development of *The Standard for Risk Management in Portfolios, Programs, and Projects*

Appendix X2—Contributors and Reviewers of *The Standard for Risk Management in Portfolios, Programs, and Projects*

Appendix X3—Portfolio Risk Management Controls

Appendix X4—Program Risk Management Controls

Appendix X5—Project Risk Management Controls

Appendix X6—Techniques for the Risk Management Framework

Appendix X7—Enterprise Risk Management Considerations for Portfolio, Program, and Project Risk Management

Appendix X8—Risk Classification

2

CONTEXT AND KEY CONCEPTS OF RISK MANAGEMENT

Risk is inherently present in all organizations. Risks present organizations with challenges but may also offer a competitive advantage when both threats and opportunities are managed proactively. Risk management provides a comprehensive and integrated framework for addressing and managing risk at all levels of the organization, from portfolios through programs, projects, and operations.

2.1 KEY CONCEPTS AND DEFINITIONS

All organizations face the uncertainty of both internal and external events. Uncertain present and future challenges can be dealt with by formulating and applying a sound business strategy toward realizing a set of objectives and managing risks. Risk management provides insight into risks that need to be addressed in support of reaching those objectives and takes advantage of opportunities. When opportunities occur, they are called benefits.

2.1.1 RISK

An individual risk is an uncertain event or condition that, if it occurs, has a positive or negative effect on one or more objectives. Overall risk is the effect of uncertainty that affects organizational objectives at different levels or aspects. Risk arises from all sources of uncertainty, including individual risks in the portfolio, program, and project domains. These risks represent the exposure of the organization and its stakeholders to the consequences of uncertainty on the realization of the organization's strategy and business objectives. Once the risk occurs, it is then managed within the various governance layers (enterprise, portfolio, program, and project) by driving the resulting outcomes.

Uncertainty is inherent in the nature of portfolios, programs, and projects. Risk arises out of uncertainty and generates uncertainty. The more risks one can identify, the more uncertainty is indicated. One of the key factors that determines the ability to identify risks is ambiguity. When ambiguity is low, the level of information available is high, which allows the identification of risks. Uncertainty and ambiguity are factors where assessment and open

evaluation drive risk management efforts. Assessments and open evaluations allow for the determination of the proper risk management strategy and define how risks will be managed throughout the portfolio, program, and project management life cycles, the iterations of these life cycles, and their interactions.

2.1.2 OPPORTUNITIES

Opportunities are risks that have a positive effect on one or more objectives. Opportunity management helps to identify and understand possible ways in which objectives can be achieved more successfully.

Moving beyond the traditional view of risk as a value destroyer to seeing risk as a potential value enhancer requires creativity and vision, and a system that allows these opportunities to flourish and lead to organizational success.

A consistent portfolio, program, and project management system helps to:

- Identify and assess opportunities that are often linked, and
- Improve the organization's ability to accept and pursue opportunities.

2.1.3 THREATS

Threats are risks that would have a negative effect on one or more objectives. Threat management involves the use of risk management resources to:

- Describe risks,
- Analyze risk attributes,
- Evaluate the probability of risk occurrence and impact as well as other characteristics, and
- Implement a planned response, when appropriate.

Similar to managing opportunities, managing threats is a staged process. Both use a structured life cycle framework to ensure that the process is robust and complete as described in Section 4. Should threats occur, they are called issues and are listed in the issue log.

2.1.4 RISK ATTITUDE

Risk attitude is a disposition toward uncertainty, adopted explicitly or implicitly by individuals and groups, driven by perception, and evidenced by observable behavior. Risk attitude represents an organization's approach to assess and eventually pursue, retain, take, or turn away from risk. Risk attitudes can range from risk averse to risk seeking.

Organizations seek to establish a consistent method for evaluating and responding to risk across the enterprise. One obstacle to developing that consistency is an individual's different or inconsistent attitudes toward risks—and those attitudes may vary according to the circumstance.

In summary, risk attitude is an individual's or group's preference to evaluate a risk situation in a favorable or unfavorable way and to act accordingly. However, risk attitudes are not necessarily stable nor homogeneous.

2.1.5 RISK APPETITE

Risk appetite is the degree of uncertainty an organization or individual is willing to accept in anticipation of a reward. Risk appetite guides the management of risk and the parameters the organization uses in deciding whether or not to take on risk. In addition, risk appetite defines what types of risks an organization pursues.

A risk appetite determination represents the start of embracing risk. Figure 2-1 shows the interrelationship of risk appetite and its direct influence on business strategy, the risk management framework, and the underlying policy and processes. The resulting risk appetite determination defines the amount and type of risk that the organization is willing to take in order to meet its strategic objectives.

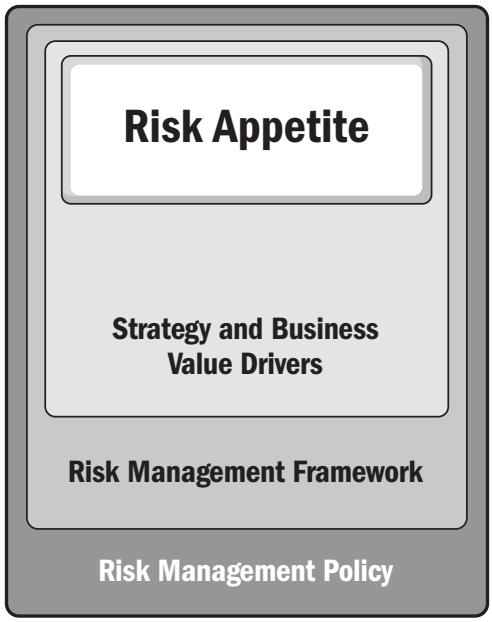


Figure 2-1. Risk Appetite and Its Relationship with Organizational Strategy

Risk appetite expresses the level of risk the organization is willing to take in pursuit of its portfolio, program, and project objectives. Portfolio, program, and project risk is not a singular, but rather a multifaceted concept.

As organizations grow, expand, and evolve, so do the risks they face. The type, prominence, and appetite for risks change at different points in the life cycle of an organization and during the life cycle of its programs and projects.

2.1.6 RISK THRESHOLD

Risk threshold is the measure of acceptable variation around an objective that reflects the risk appetite of the organization and its stakeholders. A key element of risk strategy is the establishment and monitoring of enterprise, portfolio, program, and project risk thresholds. Examples of risk thresholds include:

- Minimum level of risk exposure for a risk to be included in the risk register,
- Qualitative or quantitative definitions of risk rating, and
- Maximum level of risk exposure that can be managed before an escalation is triggered.

Establishing risk thresholds is an integral step in linking portfolio, program, and project risk management to strategy alignment and is performed as part of early planning. Based on the risk appetite of the organization, governance may also be responsible for ensuring that risk thresholds are established and observed, and when the risk should be escalated to a higher governance level.

2.2 RISK MANAGEMENT IN ORGANIZATIONS

The organization's governance body is ultimately responsible for setting, confirming, and enforcing risk appetite and risk management principles as part of its governance oversight. An organization's governance also determines which risk management processes are appropriate in terms of organizational strategy, scope, context, and content.

The enterprise risk function often resides in the executive management organization due to the direct relationship between the success of achieving organizational strategic goals and employing an effective risk management process.

When assessing the seriousness of a risk or combination of risks, uncertainty and the effect on endeavors or objectives are considered. The uncertainty dimension is commonly described as *probability*, and the effect is often referred to as *impact*.

The definition of risk includes both (a) distinct events that are uncertain but can be clearly described and (b) more general conditions that are less specific but may also give rise to uncertainty.

The definition of risk also encompasses uncertain events that could have a negative or positive effect on objectives. Both of these uncertain situations are considered to be risks when they could have an adverse or positive effect on the achievement of objectives. It is essential to address both situations within an enterprise, portfolio, program, and project risk management process. Addressing threats and opportunities together (i.e., addressing both in the same analysis and coordinating the responses to both when they overlap) allows for synergies and efficiencies.

It is important to distinguish risks from risk-related features. Causes are events or circumstances that currently exist or are certain to exist in the future, which might give rise to risks. Effects are conditional future events or conditions that directly affect one or more objectives if the associated risk occurs.

A risk may have one or more causes and, if it occurs, may have one or more effects. When a risk event occurs, the risk ceases to be uncertain. Threats that occur are termed issues, and opportunities that occur are benefits to the enterprise. Portfolio, program, and project managers are responsible to resolve these issues and manage them efficiently and effectively. Issues may entail actions that are outside the scope of the portfolio, program, and project risk management process; therefore, these issues are escalated to a higher management level according to the organization's governance policy.

2.3 DOMAINS OF RISK MANAGEMENT

Risk management is an integrated framework that spans organizational levels. Aside from simply predicting what could happen, the aim of risk management is to develop the means to support the achievement of organizational objectives, realization of the strategic vision, and creation of value.

Risk management strongly influences decision making at the enterprise, portfolio, program, and project levels. At the enterprise level, the entire organizational strategy is the set of strategic and business management actions for countering business threats and exploiting business opportunities. These decisions and actions are often executed within the portfolio as part of its individual components: programs, projects, and operations.

The various perceptions and perspectives regarding risk management in each portfolio, program, and project management domain feed into one another in an iterative, interactive, and dynamic manner. Risks may be interconnected, have dependencies, and interact via feedback loops (see Figure 2-2). Details of this interaction are provided in Sections 5, 6, and 7.

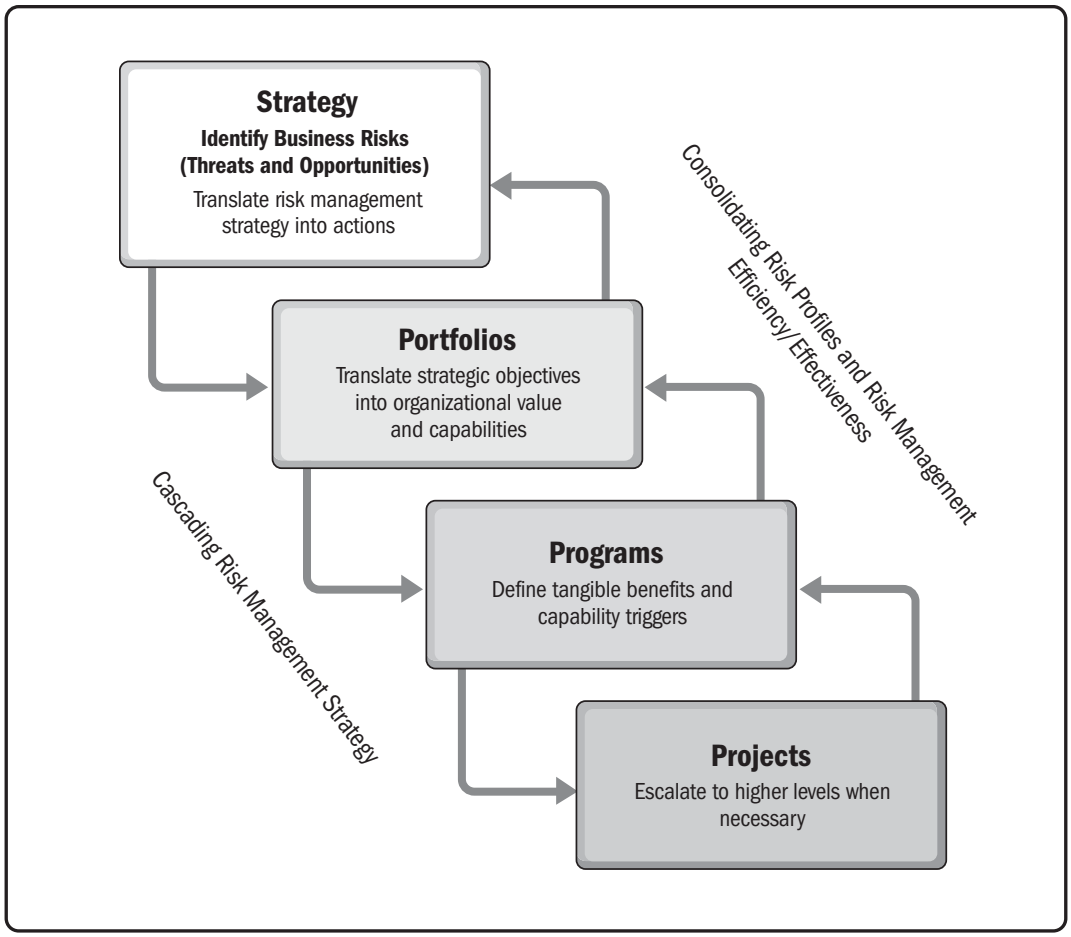


Figure 2-2. Cascading of Risk Management Strategy into Portfolios, Programs, and Projects

2.3.1 ENTERPRISE

The primary purpose of risk management is the creation and protection of value. ERM is an approach for identifying major risks that confront an organization and forecasting the significance of those risks to business processes. The way in which risks are managed reflects the organization's culture, capability, and strategy to create and sustain value. ERM addresses risks at the organizational level including the aggregation of all risks associated with the enterprise's portfolio of programs and projects.

When exploring alternative strategies, ERM enables the alignment of each portfolio, program, and project component with the organizational strategy. ERM establishes the connections between the various governance levels through the bottom-up escalation of identified risks and the top-down definition of risk management strategies. The top-down process triggers the creation of programs, projects, and other activities aimed at exploiting specific opportunities and addressing business threats.

ERM provides a systematic, organized, and structured method for:

- Identifying and assessing all risks an organization faces,
- Developing suitable responses,
- Communicating status with stakeholders, and
- Assigning responsibility to monitor and manage risks in alignment with the strategic objectives of the organization.

ERM is an ongoing process that supports the plan-do-check-act sequence for continuous improvement. ERM is not limited to compliance and disclosure requirements nor is ERM a replacement for internal controls and audit. The application of ERM varies depending on the organization and could vary from year to year based on overall risk appetite, stakeholder expectations and requirements, and the internal and external environment.

There is no one-size-fits-all approach to performing ERM. The ERM function, structure, and activities vary with each organization. ERM is responsible for ensuring that all organizational risks are addressed and properly managed and monitored.

Risk management in the enterprise management context of integrated portfolio, program, and project management consists of:

- Elaborating the risk governance framework;
- Identifying operational and contextual risks at each level of the integrated governance framework, including both negative risks (threats) and positive risks (opportunities);
- Analyzing the identified risks from both the qualitative and quantitative perspectives and identifying the governance layer best suited to manage them according to the escalation rules in place within the portfolio, program, and project management framework;
- Defining an appropriate risk management strategy based on increasing the probability and/or impact of positive risks (opportunities) and decreasing the probability and/or impact of negative risks (threats);
- Identifying the risk owner and assigning the risk;
- Implementing the corresponding strategies and activities related to anticipative and/or responsive actions;

- Monitoring the effectiveness and efficiency of the risk management strategies deployed within the enterprise, portfolio, program, and project management framework;
- Ensuring alignment between portfolio, program, and project management risk governance models and the ERM strategy; and
- Promoting effective risk management within the entire enterprise through a risk management culture.

2.3.2 PORTFOLIO

Portfolio risk management categorizes risks as structural, component, and overall risk. Structural risks are risks associated with the composition of a group of projects and the potential interdependencies among components. Component risks at the portfolio level are risks that the component manager escalates to the portfolio level for information or action. Overall, portfolio risk considers the interdependencies between components and is, therefore, more than just the sum of individual component risks. Risk efficiency is a key element of managing risk at the portfolio level. Efficiency is achieved through adjusting the mix of portfolio components to balance risk and reward such that overall portfolio risk exposure is managed.

Planning, designing, and implementing an effective portfolio risk management system depends on organizational culture, top management commitment, stakeholder engagement, and open and fair communication processes. Portfolio risk management is important for the success of managing portfolios where the value lost due to component failure is significant, or when the risks of one component impact the risks in another component.

As defined in *The Standard for Portfolio Management* [2], portfolio risk management ensures that components achieve the best possible success based on the organizational strategy and business model. Portfolio risk management can be viewed as the management activities related to adapting the mix of portfolio components to the evolution of the organization's business environment. Similar to enterprise strategy, the result of portfolio risk management strategy is defining and launching new components or closing other ones. Portfolio components can be responses to identified threats or opportunities in alignment with the organization's overall business strategy.

2.3.3 PROGRAM

Program risk management strategy ensures effective management of any risk that can cause misalignment between the program roadmap and its supported objectives to organizational strategy. It includes defining program risk thresholds, performing the initial program risk assessment, and developing a program risk response strategy.

Program risk management determines how risks are to be communicated to governance layers and strategic levels of the organization. This level of strategic alignment requires that program risk thresholds take into account the organizational strategy and risk attitude. Program risks go beyond the sum of the risks from each project within the program. Program risk management applies the concepts of portfolio risk management to the set of program components.

The Standard for Program Management [3] describes program risk management strategy as:

- Identifying program risk thresholds,
- Performing an initial program risk assessment,
- Developing a high-level program risk response strategy, and
- Determining how risks are to be communicated and managed as part of governance.

Program risk management aggregates operational risks for component projects and activities and handles the specific risks at the program level, which is dependent on the layers of accountability defined in the portfolio, program, and project governance models. Also, the perspective on risk at the program level is more focused on the immediate impact of risks than on the expected benefit.

2.3.4 PROJECT

Project Risk Management is a Knowledge Area of project management that identifies and manages project risks that could impact cost, schedule, or scope baselines.

A Guide to the Project Management Body of Knowledge (PMBOK® Guide) [4] describes Project Risk Management as the processes of conducting risk management planning, identification, analysis, response planning, response implementation, and monitoring risk on a project. The objectives of Project Risk Management are to increase the probability and/or impact of opportunities and to decrease the probability and/or impact of threats in order to optimize the chances of project success. The *PMBOK® Guide* states that when unmanaged, these risks have the potential to cause the project to deviate from the plan and fail to achieve the defined project objectives. Consequently, project success is directly related to the effectiveness of Project Risk Management.

Project Risk Management supports project objectives by adapting or implementing the courses of action and project activities to take advantage of emerging changes in the project environment. Thus, the project baselines (i.e., scope, schedule, and cost) are risk informed. All risks undergo qualitative analysis, and some risks undergo quantitative analysis when the risk impacts the baseline and/or when analysis of the combined effect of multiple risks is required.

2.4 KEY SUCCESS FACTORS

Enterprise (which includes organizational project management [OPM]), portfolio, program, and project risk management is conducted in a manner consistent with practices and policies. In addition, portfolio, program, and project risk management is conducted in a way that is appropriate to the characteristics of the endeavor. Specific criteria for the success of each risk management process are listed in the sections dealing with those processes. These key success factors for risk management enable the realization of the principles discussed in Section 1.3 and are illustrated in Figure 2-3.

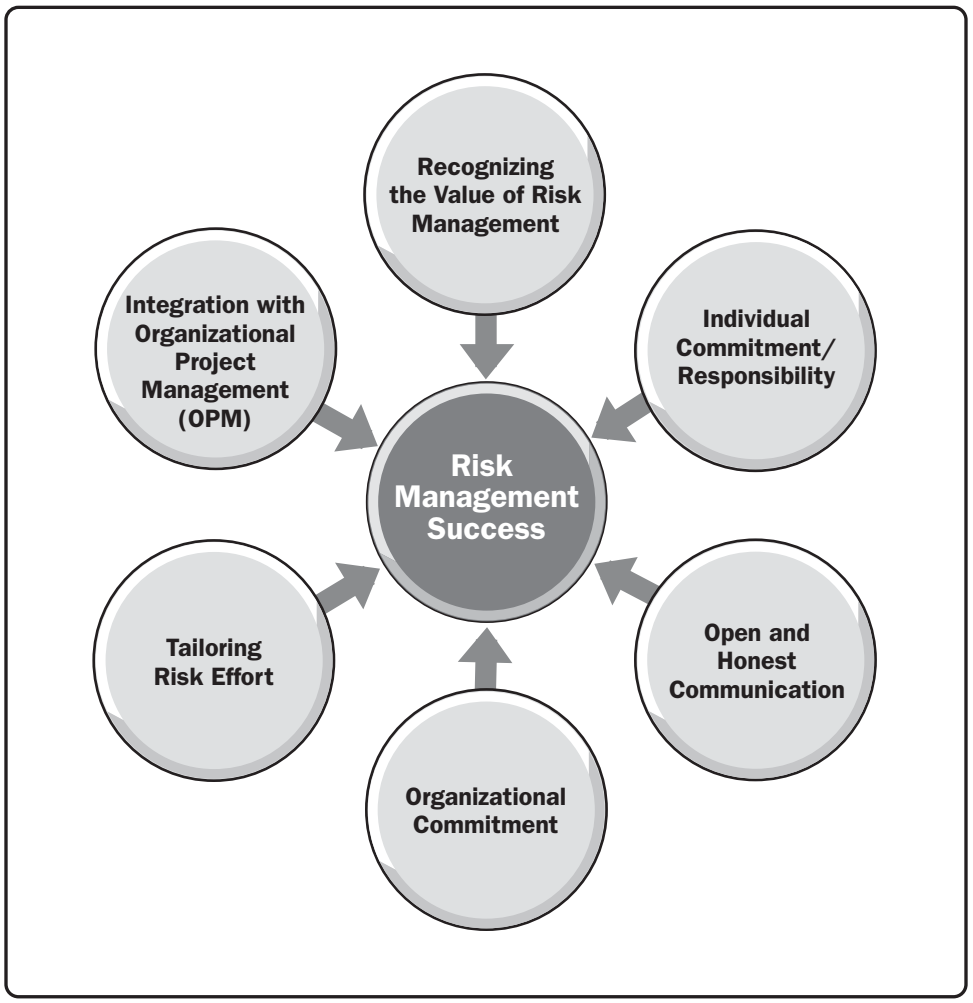


Figure 2-3. Key Success Factors for Risk Management

The key success factors include:

- **Recognizing the value of risk management.** Portfolio, program, and project risk management is recognized by organizational management, stakeholders, and team members as a valuable discipline that provides a positive return on investment.
- **Individual commitment/responsibility.** Portfolio, program, and project participants and stakeholders accept responsibility for undertaking risk-related activities as required. Risk management is everyone's responsibility.
- **Open and honest communication.** Everyone is involved in the risk management process. Any actions or attitudes that hinder communication about risk reduce the effectiveness of risk management regarding proactive approaches and effective decision making.
- **Organizational commitment.** Organizational commitment is established only when risk management is aligned with the organization's goals, values, and ERM policies. Risk management actions may require the approval of or response from others at levels above the portfolio, program, or project manager.
- **Tailoring risk effort.** Risk management activities are consistent with the value of the endeavor to the organization and with its level of risk, scale, and other organizational constraints.
- **Integration with organizational project management.** Risk management does not exist in a vacuum isolated from other organizational project management processes. Successful risk management requires the appropriate execution of organizational project management and ERM processes, including the allocation of resources necessary for the effective application of risk management.

3

FRAMEWORK FOR RISK MANAGEMENT IN PORTFOLIO, PROGRAM, AND PROJECT MANAGEMENT

Risks are present in every organizational activity, especially across endeavors such as portfolios, programs, and projects. Organizational inertia is inherently risky because products and services become stale over time and organizations may lose their competitiveness due to societal and technological changes. Risks can be difficult to manage because a single risk can have a different impact on various components of portfolios and programs, and across the various levels of an organization. Organizations and professionals need to balance threats and opportunities and the dilemmas of inaction versus action. This section addresses this dilemma by providing the framework for risk management across the enterprise and its portfolio, program, and project management activities.

3.1 BUSINESS CONTEXT OF RISK MANAGEMENT IN PORTFOLIO, PROGRAM, AND PROJECT MANAGEMENT

All organizations encounter internal and external factors that influence their ability to achieve desired objectives. Achieving those objectives is rarely ensured. All organizational activities involve risk—even inaction.

An organization manages risk through people, processes, technology, and information. Portfolio, program, and project managers are responsible for risks associated with their endeavors. These managers are responsible for working with stakeholders at various levels of the organization and applying a systematic, integrated approach to risk management.

Figure 3-1 represents the context of organizational activities, from the abstract (or the top of an organization) to the specific (or the bottom) where discrete tasks are completed. Risk permeates throughout the pyramid. The organizational strategy sets the direction through the vision and mission, and strategy defines specific goals and objectives for the organization. This is all-encompassing and includes operational and change activities.

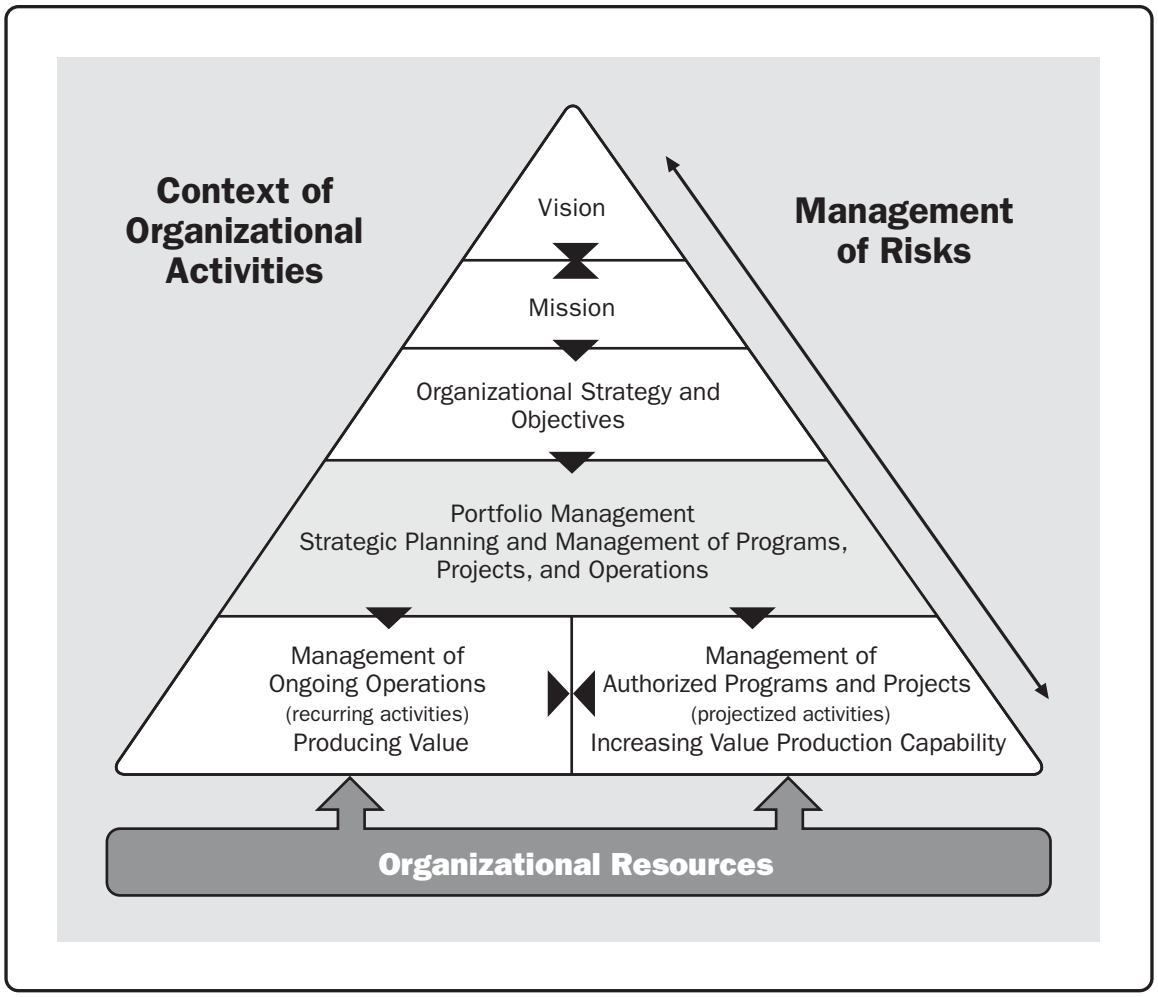


Figure 3-1. Risk across the Various Levels of the Organization

Goals and objectives are aligned with strategies. The attainment of business benefits and value requires the execution of operational and change plans. Organizations realize the benefits of change by executing plans and their associated activities, which result in the successful attainment of portfolio, program, and project objectives. Change by its very nature can be uncertain. For most organizations, change is inevitable and is necessary to maintain and sustain competitiveness. To manage change successfully, organizations require a robust, well-thought-out strategic execution plan to implement portfolios, programs, and projects in a consistent manner over time. This requires the

adoption of an effective organizational project management (OPM) implementation. OPM is a framework in which portfolio, program, and project management are aligned with strategy and integrated with organizational enablers in order to achieve strategic objectives. Portfolio, program, and project management targets business objectives that support the organizational strategy. Some threats arise when strategy or business objectives are not aligned with the organization's mission, vision, and core values. Additional threats arise when business objectives do not support strategy or when endeavors, such as portfolios, programs, and projects, are not aligned with business objectives. Opportunities could be enhanced when strategy and business objectives are well aligned.

3.1.1 ORGANIZATIONAL FRAMEWORK

As shown in Figure 3-2, risk management includes all domains of the organization: enterprise, portfolio, program, and project. ERM is an approach to managing risk that reflects the organization's culture, capability, and strategy to create and sustain value. It covers the policies, processes, and methods by which organizations manage risks (both threats and opportunities) to advance the mission and vision of the organization. Portfolio risk management derives its policies, processes, methods, and tolerance from the ERM framework and tailors it for the management of portfolios. Similarly, programs and projects adopt their respective risk management practices from the portfolio framework.

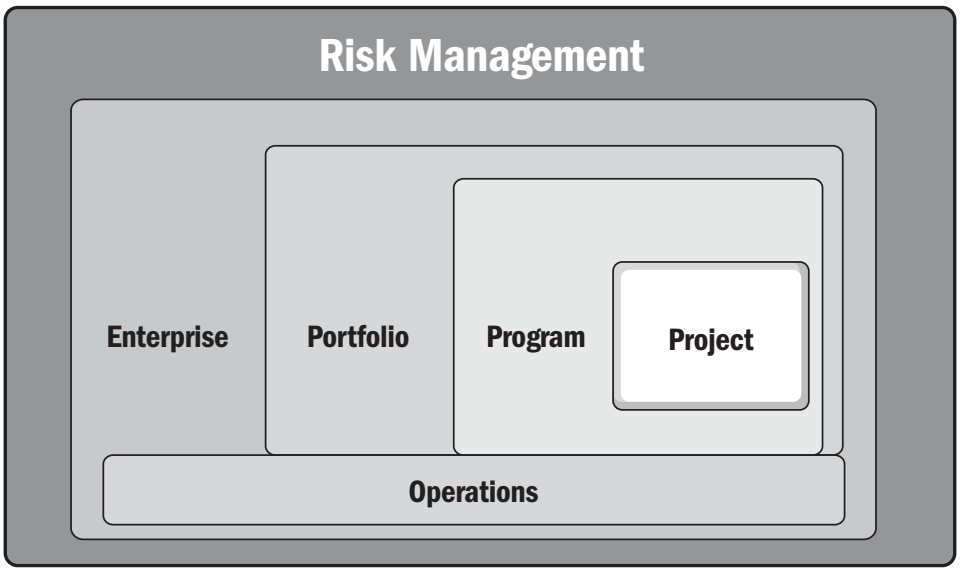


Figure 3-2. Risk Management across Domains of Organizational Activities

The governance board typically oversees ERM in that it steers the process with significant and proactive management engagement. The portfolio, program, and project managers manage and monitor communications with internal and external stakeholders, which is required to instill the importance and values of risk management, expected culture and behavior, and risk attitude.

3.1.2 ORGANIZATIONAL CONTEXT

The application of ERM is influenced by industry, regulations, and organizational context. By understanding the context in which the organization exists, portfolio, program, and project managers can tailor the optimal approach to risk management for their endeavors and simultaneously assist the organization in assessing and responding to risks. Many factors can also impact the extent of risk management practices. Some of these factors include capital availability, competitive landscape, and risk attitude.

3.1.3 STRATEGIC AND ORGANIZATIONAL PLANNING

Risk management in portfolios, programs, and projects aligns with the setting of strategic vision, mission, goals, values, and business objectives. It provides the inputs for pursuing different alternatives. Strategic goals and business objectives are developed to realize the organization's vision and mission in line with core values. Once these goals and objectives are set, they become inputs for risk management. If there are potential conflicts between strategic goals and the portfolio of work, then the risk is escalated to the proper level of management. See Figure 3.1.

3.1.4 LINKING PLANNING WITH EXECUTION THROUGH PORTFOLIO, PROGRAM, AND PROJECT MANAGEMENT

Portfolio, program, and project management refers to domains in the organizational project management (OPM) framework for managing capabilities and enhancing existing value or creating new value. Portfolio management serves as the bridge that connects strategic planning with business execution. By focusing on selecting the right portfolio components (e.g., programs, projects, and operational initiatives), portfolio management enables organizations to achieve alignment with strategy and to invest their resources wisely and effectively. Program and project management are then responsible for the implementation.

These activities are performed within an environment that is full of risks. While OPM enables an organization to leverage its results and implementation success and supports a healthy organization within a competitive and rapidly changing environment, it is not risk free. Therefore, it is essential for organizational leaders and managers

to recognize the importance of managing risks to tackle threats and enable opportunities. Portfolio, program, and project managers work inclusively to (a) identify, analyze, evaluate, prioritize, recommend, plan, and implement risk responses; (b) monitor progress; and (c) adjust risk responses as appropriate.

3.2 SCOPE OF ACCOUNTABILITY, RESPONSIBILITY, AND AUTHORITY

The accountability, responsibility, and authority of risk management are shared by stakeholders involved in portfolio, program, and project management.

- *Accountability* is individual by nature and derived from a position held in the organization. Accountability is related to authority in that one is usually held accountable within one's limits of authority. However, one still may be held accountable beyond one's authority to act.
- *Responsibility* resides in an individual by the assignment of a function or task. By accepting the assignment, an individual takes on the associated responsibility. The fact that others higher in the organization may also be held responsible or accountable does not diminish the responsibility held by the individual. The assigning individual still is held accountable for the delegated task, but responsibility is passed to the assigned individual.
- *Authority*, like responsibility, may be delegated and gives an individual the ability to make decisions within defined bounds.

3.2.1 ACCOUNTABILITY AT THE ENTERPRISE LEVEL

The objective of risk management is to apply knowledge, skills, and good practices to manage the area of focus within the risk threshold that is acceptable to the organization, whether at the enterprise, portfolio, program, or project level. The purpose is to minimize the impact of threats to protect the organization from loss and to embrace opportunities that translate to value. The management of risk across the continuum of portfolios, programs, and projects requires collaboration throughout the enterprise, and the recognition that failure to allocate the appropriate amount of resources could jeopardize the organization's strategic objectives.

Portfolio, program, and project management are responsible for supporting management policies, defining roles and responsibilities, setting targets, and overseeing implementation. The managers of the work are responsible for keeping senior management apprised of ongoing risk exposure and corresponding actions.

3.2.2 ACCOUNTABILITY AT THE PORTFOLIO LEVEL

In some cases, portfolios may exist for brief periods; however, portfolios often exist for as long as the organization itself exists. As a result, portfolio managers may oversee activities or authorize components that may take several years for the organization to realize the value of the investment. Any change in this landscape has direct implications on the organization's strategic objectives. Specific external factors can include regulatory requirements or mandates, market conditions, and organizational restructuring.

Portfolio risk management tackles strategic, execution, and structural risks. Whereas program risk management evaluates risk across a related set of components, portfolio risk management is broad and considers risks that could impact unrelated components and operational activities within the portfolio. As a result, portfolio managers address several challenges when managing risk because portfolio-level risks encompass both external and internal factors by bridging organizational strategy to implementation.

3.2.3 ACCOUNTABILITY AT THE PROGRAM LEVEL

At the program level, the risks that are evaluated span the related components and, if triggered, could have a positive or negative impact on one or more other components. Working with the component managers, it is the responsibility of the program manager to identify and manage these risks. Rather than manage these risks individually within the component, program managers ensure that program risks are managed through coordination.

When managing strategic risk, program managers may identify new risks that exceed the organization's risk appetite and could directly impact the program. Strategic risks present both a threat and an opportunity. The program manager evaluates and reviews a set of response options for consideration with the governance body.

Within the program, risks can affect the delivery of specific components. The program managers advise their component managers of any shared risks and response plans that relate to individual components. There may be economies of scale and scope in that the shared risks may be managed by initiating one risk response at the program level.

3.2.4 ACCOUNTABILITY AT THE PROJECT LEVEL

At the project level, the objective of risk management is to (a) decrease the probability and impact of negative risks and (b) increase the probability and impact of positive risks specific to project deliverables or objectives.

Project managers are accountable for evaluating, reporting, and managing both individual and overall project risks within the constraints of the project. They may escalate certain risks to, or receive guidance from, sources such as the program manager, portfolio manager, project management office, governance board, and other leadership entities, depending on the complexity of the initiative and organizational inputs.

All project team members have the responsibility for managing risk, for example, the identification of risk during initiation, clarification of the trigger events, or awareness of potential new risks that could affect the endeavor.

3.3 GENERAL APPROACHES TO RISK MANAGEMENT

As risks are pervasive throughout portfolio, program, and project management activities, a systematic approach for managing risks is essential for the organization to achieve its strategic objectives. In this context of risk management, considerations include, but are not limited to, the following:

- Events or circumstances that may occur in the future (their variability and ambiguity);
- Events that could have a positive or negative impact on one or more objectives of the enterprise, portfolio, program, or project;
- Probability of the event occurring;
- Impact of the event should it occur; and
- Ability of the organization to influence favorable outcomes or minimize negative consequences.

3.3.1 FACTORS FOR EVALUATING RISK

Across the continuum of enterprise, portfolio, program, and project risk management, risks exist at all levels of the organization. Figure 3-3 provides a framework for classifying risks in one of four quadrants based on available information and the degree of ambiguity and variability. See Appendix X8 on Risk Classification for additional information.

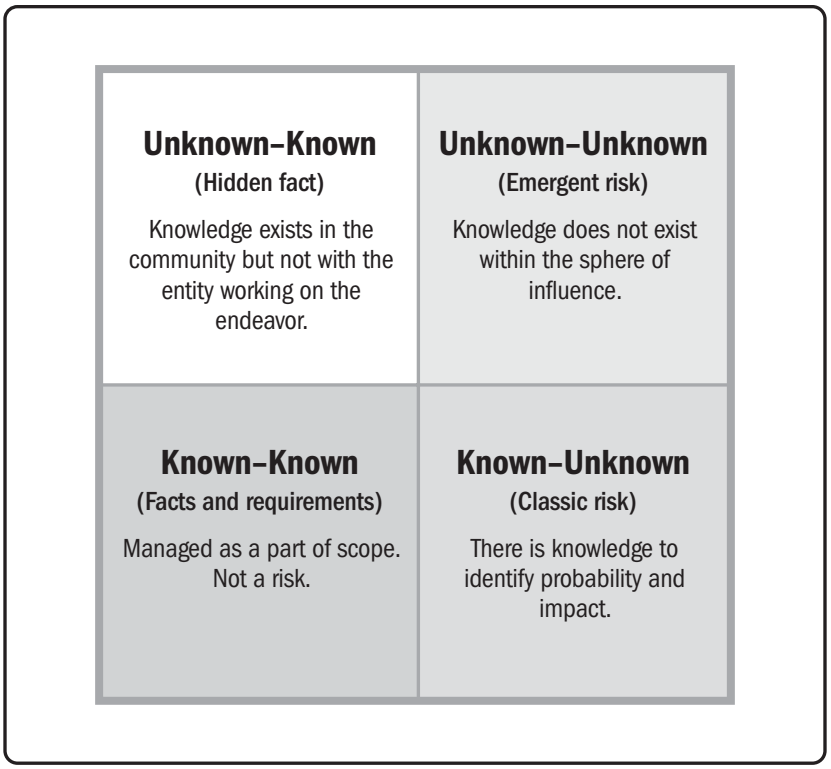


Figure 3-3. Risk Classification

In order for risk management to take place, portfolio, program, and project managers need to identify the risk probability and impact.

- **Probability.** The chance of a risk occurring can range from slightly above 0% to just below 100%.
- **Impact.** Risks, should they occur, can have either a positive or negative consequence for the organization. The magnitude or significance of the impact may have varying implications and influences.

There are additional factors to consider when evaluating risks. Some are included in Appendix X6 on Techniques for the Risk Management Framework.

4

RISK MANAGEMENT LIFE CYCLE IN PORTFOLIO, PROGRAM, AND PROJECT MANAGEMENT

Organizations build adaptive frameworks to ensure alignment with environmental competitiveness and confront increasing complexity associated with goal attainment and decision making. Complexity is an inherent characteristic of portfolios, programs, and projects and their environment, which is difficult to manage due to various aspects involved in the workflow: human behavior, system behavior, uncertainty, and ambiguity. Complexity impacts stability, predictability, and capacity of both the organization and its activities to sustain its business. For additional information, refer to *Navigating Complexity: A Practice Guide* [5].

An integrated view of risk management is required to define the right construct in the organization's governance and operations. By establishing the appropriate framework, an organization is able to:

- Articulate objectives,
- Define external and internal parameters for processing an effective risk management life cycle, and
- Establish risk criteria within the scope for the remaining processes through iterative activities.

The purpose of establishing a framework is to align resources and processes to the organization's strategies and objectives. The risk management life cycle works within the risk management framework to ensure risks are managed in a structured manner regardless of the portfolio, program, or project life cycle approach.

4.1 INTRODUCTION TO THE RISK MANAGEMENT LIFE CYCLE

The risk management life cycle described in this section illustrates a structured approach for undertaking a comprehensive view of risk throughout the enterprise, portfolio, program, and project domains. Even though the way of managing risks differs between these domains and from one organization to another, an overall life cycle approach outlines a sequence of logical phases that can be iterated and includes the following processes:

- Plan Risk Management,
- Identify Risks,
- Perform Qualitative Risk Analysis,
- Perform Quantitative Risk Analysis,
- Plan Risk Responses,
- Implement Risk Responses, and
- Monitor Risks.

The risk management life cycle is shown in Figure 4-1. It has a dedicated, procedural, and iterative workflow of activities and processes, supported and performed across the enterprise and within the portfolio, program, and project domains. Because of the evolutionary nature of risk, the risk management life cycle ensures a repeatable workflow of processes that supports strategic decision making. All these activities are performed in an integrated way within and across the portfolio, program, and project domains.

The iterative workflow of the risk management life cycle is embedded within a strategic execution framework where portfolio, program, and project management are linked to organizational cultural foundations, capabilities, and the use of organizational functions or performance domains. It is understood that once a portfolio, program, or project is closed, the risk management process terminates and the appropriate lessons learned are documented. The framework enables the overall risk processes to be implemented through a risk management plan within each domain as described in Sections 5, 6, and 7.

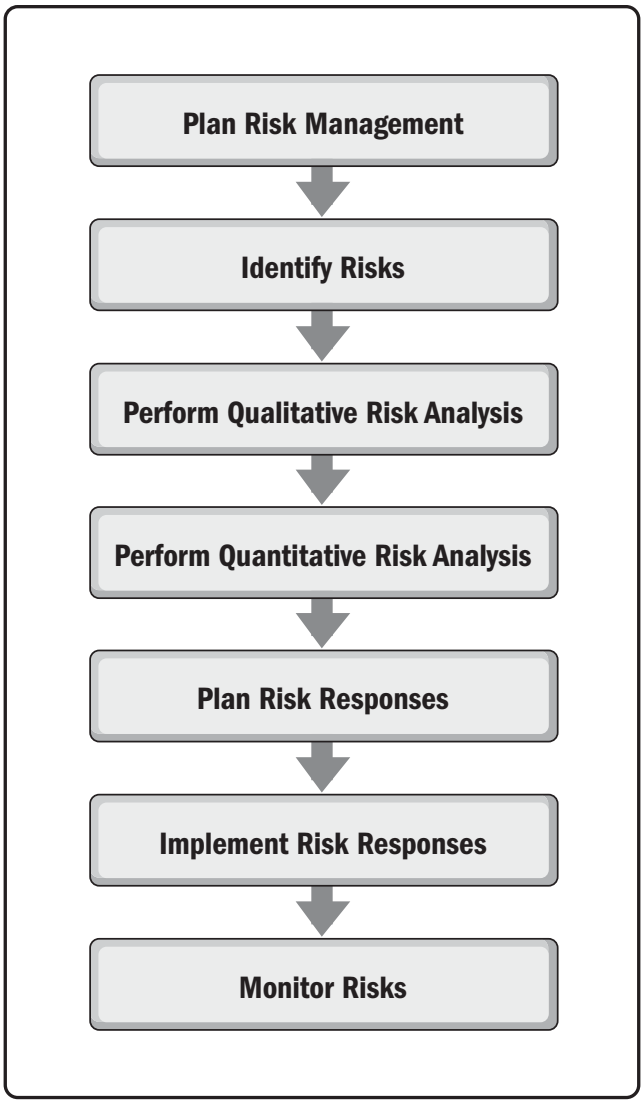


Figure 4-1. The Risk Management Life Cycle Framework

4.2 PLAN RISK MANAGEMENT

Effective risk management requires the creation of a risk management plan. This plan describes how the risk management processes are to be carried out and how they fit in with other processes. On a broader level, the risk management plan describes the relationships among the risk management processes; general portfolio, program, or project management; and the management processes in the rest of the organization. Initial risk management planning is carried out early in the overall planning of the work, and the corresponding activities are integrated into the overall management plan. The risk management plan may need to be adapted as the needs of the work and stakeholders become clearer or change.

The feasibility of risk management planning is dependent upon the features of the organization in which it is carried out. The rules and guidelines defined in the risk management plan reflect (a) the culture of the organization, (b) its capabilities regarding people and facilities, and (c) its values, goals, and objectives. The risk management plan identifies and describes relevant organizational procedures and any other enterprise environmental factors that apply, such as strategic risk management, enterprise risk management (ERM), and corporate governance processes.

4.2.1 PURPOSE OF PLAN RISK MANAGEMENT

The objectives of the Plan Risk Management process are to: develop the overall risk management strategy, decide how the risk management processes will be executed, and integrate risk management with all other activities. The risk management plan defines both the normal frequency for repeating the processes in addition to specific or exceptional conditions under which the corresponding actions are initiated. The corresponding risk management activities are integrated into the portfolio, program, or project management plan.

4.2.1.1 RISK APPETITE IN PLAN RISK MANAGEMENT

The level of risk that is considered acceptable depends on the risk appetite of the relevant stakeholders. The risk appetite of the stakeholders may be influenced by a number of factors. These factors include the stakeholders' ability to tolerate uncertainty and the relative importance of achieving specific objectives. The output of this analysis is then considered when applying the risk management processes.

Guidelines and rules for escalating risk-related information to management and other stakeholders reflect the stakeholder's risk appetite and expectations. As the work evolves, maintaining effective communications with the stakeholders enables portfolio, program, and project managers to become aware of any changes in the stakeholders' attitudes and adapt the risk management approach to take into account any new factors.

The risk management plan provides terminology used to describe risks, which allows participants to share a common understanding of the terms. The risk management plan also defines the critical values of risk management and the thresholds that serve as parameters in a manner consistent with the scope of the work and the attitudes of the stakeholders. Similarly, the risk management plan specifies the key numerical values required in quantitative analysis or for decision making in risk response planning or risk monitoring.

4.2.1.2 TAILORING AND SCALING THE RISK MANAGEMENT PLAN

Portfolios, programs, and projects are exposed to different types of risk, so each step in the risk management life cycle is tailored and scaled to meet the various risk characteristics. The management processes are also tightly integrated between the portfolio, program, and project domains.

The results from this initial step are documented and communicated, and subsequently reviewed by the stakeholders to ensure a common understanding of the scope and objectives for the risk management process.

The risk management plan includes the tailored risk management processes, which are based on the process maturity of the organization. Scalable elements of the process that are a part of risk management planning include, but are not limited to:

- Available resources,
- Escalation paths,
- Methodology and processes used,
- Tools and techniques used,
- Supporting infrastructure,
- Review and update frequency, and
- Reporting requirements.

4.2.2 SUCCESS FACTORS FOR PLAN RISK MANAGEMENT

The criteria for a valid risk management plan include:

- Acceptance by the stakeholders,
- Identification of bias and correcting for it,

- Alignment with the internal and external constraints and priorities,
- Balance between cost or effort and benefit, and
- Completeness with respect to the needs of the risk management process.

4.3 IDENTIFY RISKS

Once the risk management scope and objectives are agreed, the process of identifying risks begins, with care taken to distinguish genuine risks from nonrisks, such as concerns and issues. It is unlikely that all risks are, or even can be, identified at the outset. Over time, the level of risk exposure may change as a result of the decisions and actions taken previously and of externally imposed changes.

4.3.1 PURPOSE OF IDENTIFY RISKS

The purpose of risk identification is to identify risks to the extent practicable. The emergent nature of risk requires the risk management process to be iterative, repeating the risk identification activities in order to find risks that were not previously evident.

A variety of risk identification techniques is available, each with its own strengths and weaknesses (see Appendix X6 on Techniques for the Risk Management Framework). One or more techniques are selected, as appropriate, for meeting the needs of a specific portfolio, program, or project. The aim is to expose and document all knowable risks, recognizing that some risks are inherently unknowable and others emerge later in the work. Input is sought from a wide range of stakeholders when identifying risks, since each stakeholder may have a different perspective on the risks facing the portfolio, program, or project. Historical records and documents may also be reviewed to help identify risks.

When a risk is first identified, preliminary responses may be identified at the same time. These are recorded during the Identify Risks process and are considered for immediate action when such action is appropriate. When such responses are not implemented immediately, they should be considered during the Plan Risk Responses process.

All identified risks are recorded, and a risk owner may be identified at the same time. The risk owner is the individual responsible for monitoring the risk and for selecting and implementing an appropriate risk response strategy. It is the responsibility of the risk owner to manage the corresponding risk throughout the subsequent risk management processes.

4.3.2 KEY SUCCESS FACTORS FOR IDENTIFY RISKS

Success in achieving the objectives of Identify Risks includes, but is not limited to:

- Early identification,
- Iterative identification,
- Emergent identification,
- Comprehensive identification,
- Explicit identification of opportunities,
- Multiple perspectives,
- Risks linked to objectives,
- Complete risk statement,
- Ownership and level of detail,
- Frequent and effective communication, and
- Objectivity to minimize bias.

4.4 PERFORM QUALITATIVE RISK ANALYSIS

Qualitative risk analysis evaluates the importance of each risk in order to categorize and prioritize individual risks for further attention. It also provides a mechanism for evaluating the level of overall portfolio, program, or project risk.

4.4.1 PURPOSE OF PERFORM QUALITATIVE RISK ANALYSIS

Qualitative techniques are used to gain a better understanding of individual risks. Qualitative techniques consider a range of characteristics such as probability or likelihood of occurrence, degree of impact on the objectives, manageability, timing of possible impacts, relationships with other risks, and common causes or effects.

Assessing individual risks using qualitative risk analysis evaluates the probability that each risk, if it occurs, would have on the portfolio, program, or project objectives. As such, this assessment does not directly address the overall risk that results from the combined effect of all risks and their potential interactions with each other. This can, however, be achieved through the use of quantitative risk analysis techniques.

Qualitative risk analysis is applied to the list of risks created or updated by the Identify Risks process to provide management with the characteristics of the risks that have the most influence (positive or negative) on achieving the objectives. Risks that are assessed as high priority, which either threaten or enhance the achievement of objectives, are highlighted in the Plan Risk Responses process. These risks may be further analyzed using quantitative risk analysis.

4.4.2 KEY SUCCESS FACTORS FOR PERFORM QUALITATIVE RISK ANALYSIS

Success in achieving the objectives of the Perform Qualitative Risk Analysis process includes, but is not limited to:

- Use agreed approach,
- Use agreed definitions of risk terms,
- Collect credible information about risks, and
- Perform iterative qualitative risk analysis.

4.5 PERFORM QUANTITATIVE RISK ANALYSIS

The Perform Quantitative Risk Analysis process provides insight into the combined effect of identified risks on the desired outcome. This process takes into account probabilistic or component-wide effects, such as correlation between risks, interdependency, and feedback loops. It provides an indication of the degree of overall risk faced by the portfolio, program, or project.

4.5.1 PURPOSE OF QUANTITATIVE RISK ANALYSIS

The Perform Quantitative Risk Analysis process provides a numerical estimate of the overall effect of risk on the objectives. Results from this analysis are used to evaluate the likelihood of success in achieving objectives and to estimate any contingency reserves.

Analyzing uncertainty using quantitative techniques provides a more realistic estimate than a nonprobabilistic approach. However, quantitative risk analysis is not always required or possible. Therefore, during the Plan Risk Management process, the benefits of quantitative risk analysis should be weighed against the effort required to ensure that the additional insights and value justify the additional effort.

However, a partial risk analysis, such as qualitative risk analysis, prioritizes only individual risks and therefore does not produce measures of overall risk where all risks are considered simultaneously. Calculating estimates of overall risk is the focus of the Perform Quantitative Risk Analysis process. Specific risks are usually best understood and quantified at a detailed level. By contrast, objectives are specified at a higher level. An overall risk analysis, such as one that uses quantitative techniques, estimates the implication of all quantified risks. Thus, quantitative risk analysis and subsequent assessments of risks are enhanced by a comprehensive understanding of the individual risks and their relative importance with respect to objectives. The overall risk may determine the priority that should be placed on particular individual risks.

Estimating overall risk using quantitative methods helps to distinguish the quantified risks that threaten objectives beyond the tolerance of the stakeholders from those risks that are within acceptable tolerances even when the risk is considered. The risks that threaten objectives beyond the stakeholders' tolerance may be targeted for vigorous risk responses aimed at protecting the objectives that are most important to the stakeholders.

4.5.2 KEY SUCCESS FACTORS FOR PERFORM QUANTITATIVE RISK ANALYSIS

Success in achieving the objectives of quantitative risk analysis includes, but is not limited to:

- Prior risk identification and qualitative risk analysis,
- Appropriate model,
- Competence with the corresponding technical analysis tools,
- Commitment to collecting credible risk data,
- Unbiased data, and
- Interrelationships between risks in quantitative risk analysis.

4.6 PLAN RISK RESPONSES

The Plan Risk Responses process determines the effective response actions that are appropriate for the priority of the individual risks and for the overall risk. This process takes into account the stakeholders' risk attitudes and the conventions specified in the risk management plan, in addition to any constraints and assumptions that were determined when the risks were identified and analyzed. Once individual risks have been prioritized, appropriate risk responses are developed for both threats and opportunities. This process continues until an optimal set of responses has been developed. A range of possible responses exists for both threats and opportunities.

Five responses may be considered for dealing with threats:

- **Escalate.** Escalation is appropriate when a threat is outside of the portfolio, program, or project scope or when the proposed response exceeds a given manager's authority. Escalated risks are managed at the enterprise domain, portfolio domain, program domain, or other relevant part of the organization. Ownership of escalated threats is accepted by the relevant party in the organization. A threat is usually escalated to the appropriate level that matches the objective that would be affected if the threat occurred.
- **Avoid.** Risk avoidance is when the portfolio, program, or project team acts to eliminate a threat or protect activity from risk impact. It may be appropriate for a high-priority threat with a high probability of occurrence and a large negative impact. Avoidance may involve changing some aspect of the management plan or changing the objective that is in jeopardy in order to eliminate the threat impact entirely. Should the risk materialize, it would have no effect with respect to the objective. The risk owner may also take action to isolate the objective from the risk's impact if it were to occur.
- **Transfer.** Transfer involves shifting responsibility of a threat to a third party to manage the risk and to bear the impact if the threat occurs. Risk transfer often involves payment of a risk premium to the party taking on the threat.
- **Mitigate.** In risk mitigation, action is taken to reduce the probability of occurrence and/or impact of a threat. Early mitigation action is often more effective than trying to repair the damage after the threat has occurred. Where it is not possible to reduce probability, a mitigation response might reduce the impact by targeting factors that drive the severity.
- **Accept.** Risk acceptance acknowledges the existence of a threat, but no proactive action is taken. This strategy may be appropriate for low-priority threats, and it may also be used where it is not possible or cost effective to address a threat in any other way. Acceptance can be either active or passive. The most common active acceptance strategy is to establish a contingency reserve, including amounts of time, money, or other resources to handle the threat if it occurs. Passive acceptance involves no proactive action apart from periodic review of the threat to ensure that it does not change significantly.

Five responses may be considered for dealing with opportunities:

- **Escalate.** This risk response strategy is appropriate when an opportunity is outside the portfolio, program, or project scope or when the proposed response exceeds a given manager's authority. Escalated opportunities are managed at the program domain, portfolio domain, or other relevant part of the organization. It is important that ownership of an escalated opportunity is accepted by the relevant party in the organization. Opportunities are usually escalated to the right level that matches the objectives that would be affected if the opportunity occurred.
- **Exploit.** The exploit strategy may be selected for high-priority opportunities where the organization wants to ensure that the opportunity is realized. This strategy seeks to capture the benefit associated with a particular opportunity by ensuring that it definitely happens, increasing the probability of occurrence to 100%.

- **Share.** Sharing involves transferring ownership of an opportunity to a third party so that the third party shares some of the benefit if the opportunity occurs. It is important to carefully select the new owner of a shared opportunity to ensure capture of the opportunity for the benefit of the portfolio, program, or project. Risk sharing often involves payment of a risk premium to the party taking on the opportunity.
- **Enhance.** The enhance strategy is used to increase the probability and/or impact of an opportunity. Early enhancement action is often more effective than trying to improve the benefit after the opportunity has occurred. The probability of occurrence of an opportunity may be increased by focusing attention on its causes. Where it is not possible to increase probability, an enhancement response might increase the impact by targeting factors that drive the size of the potential benefit.
- **Accept.** Accepting an opportunity acknowledges its existence, but no proactive action is taken. This strategy may be appropriate for low-priority opportunities, and it may also be adopted where it is not possible or cost effective to address an opportunity in any other way. Acceptance can be either active or passive. The most common active acceptance strategy is to establish a contingency reserve, including amounts of time, money, or other resources to take advantage of the opportunity if it occurs. Passive acceptance involves no proactive action apart from a periodic review of the opportunity to ensure that it does not change significantly.

Responses are planned at a general, strategic level, and the strategy is validated and agreed prior to developing the detailed tactical approach. Once that is accomplished, the responses are expanded into actions at the tactical level and integrated into the relevant management plans. This activity may generate additional secondary risks, which need to be addressed at this time.

In addition to individual risk responses, actions may be taken to respond to overall portfolio, program, or project risk. All response strategies and actions are documented and communicated to key stakeholders and incorporated into the relevant plans.

4.6.1 PURPOSE OF PLAN RISK RESPONSES

The purpose of the Plan Risk Responses process is to determine the set of actions that provides the highest chance of success while complying with applicable constraints. Once risks have been identified, analyzed, and prioritized, plans are developed for addressing every risk that the team considers to be sufficiently important, either because of the threat it poses to the objectives or the opportunity it offers. The plans describe the agreed actions to be taken and the potential changes that these actions might cause.

Risk responses, when implemented, can have potential effects on the objectives and as such, can generate additional risks. These are known as secondary risks and are analyzed and planned for in the same way as those risks that were initially identified. There may be residual risks that remain after the responses are implemented. These residual risks are clearly identified, analyzed, documented, and communicated to all relevant stakeholders until they are satisfied.

4.6.2 KEY SUCCESS FACTORS FOR PLAN RISK RESPONSES

Success in achieving the objectives of the Plan Risk Responses process includes, but is not limited to:

- Clearly define risk-related roles and responsibilities;
- Specify the timing of risk responses;
- Provide resources, budget, and schedule for responses;
- Address the interaction of risks and responses taking into account secondary and residual risks;
- Ensure appropriate, timely, effective, and agreed responses; and
- Address both threats and opportunities.

4.7 IMPLEMENT RISK RESPONSES

Once the planning of risk responses is complete, all of the approved unconditional response actions are included and defined in the relevant management plans. These actions may be delegated to action owners as appropriate. The risk owner monitors actions to determine their effectiveness and to identify any secondary risks that may arise because of the implementation of risk responses.

The risk owners and risk action owners are briefed on any changes that may affect their responsibilities. Effective communications are maintained between the risk owners and the portfolio, program, or project managers so that the designated stakeholders (a) accept accountability for controlling the potential outcomes of specific risks, (b) apply their best efforts to track the associated trigger conditions, and (c) carry out the agreed responses in a timely manner.

In addition to the response actions and trigger conditions, a mechanism for measuring the effectiveness of the response is provided as part of the risk response planning. The risk action owner keeps the risk owner aware of the status of the response actions. The risk owner then decides whether the risk has been effectively dealt with, or whether additional actions need to be planned and implemented. This ensures that the agreed actions are carried out within the normal portfolio, program, or project execution framework.

4.7.1 PURPOSE OF IMPLEMENT RISK RESPONSES

The objective of the Implement Risk Responses process is to carry out the agreed risk response action should the risk occur. Proper attention to the Implement Risk Responses process helps to ensure that the agreed risk responses are executed accordingly.

4.7.2 KEY SUCCESS FACTORS FOR IMPLEMENT RISK RESPONSES

Success in achieving the objectives of the Implement Risk Responses process includes, but is not limited to:

- A risk owner is accountable for each risk,
- Stakeholders commit to implementing risk responses according to plan,
- Effective communications management is used,
- Cost of the risk responses is determined and calculated as part of the planning, and
- Contingency and management reserves are made available.

4.8 MONITOR RISKS

The Monitor Risks process enables the portfolio, program, or project management team to reevaluate the status of previously identified risks; to identify emergent, secondary, and residual risks; and to determine the effectiveness of the risk management processes.

The portfolio, program, or project environment may change as some risks occur, whether foreseen or unforeseen, and other risks become or cease to be relevant. The management team ensures that the planning documents are kept current as additional information becomes available. Periodic risk reassessment using the risk management life cycle is repeated at reasonable intervals or in response to relevant events.

In the event of major organizational changes, risk management planning may need to be revisited prior to performing risk reassessment.

In addition to regular status reviews, periodic risk audits are performed to determine strengths and weaknesses in handling risks within the portfolio, program, or project. This entails identifying any barriers to effectiveness or keys to success in risk management, the recognition of which could help to improve risk management of the current or future portfolios, programs, or projects.

At the end of the program or project, an integrated analysis of the risk management process is carried out with a focus on long-term process improvements. This analysis consolidates the findings of the periodic audits to identify lessons that are applicable to a large proportion of the organization's future programs or projects, such as appropriate levels of resources, adequate time for the analysis, use of tools, level of detail, etc.

The result of the risk management process audit is consolidated with specific information with respect to the experience of risk in the portfolio, program, or project. The results are highlighted, and potential actions are proposed for applying them in the future. This includes any generally applicable guidelines for the organization, and the results can lead to an update of the corresponding organizational process assets.

4.8.1 PURPOSE OF MONITOR RISKS

The primary objectives of the Monitor Risks process are to track identified risks and maintain viability of response plans. In addition to tracking and managing the risk response actions, the effectiveness of all of the risk management processes are periodically reviewed to provide improvements to the management of the current work as well as future work with an activity such as lessons learned.

For each risk or set of risks for which a contingent response has been defined, the corresponding set of trigger conditions are specified. It is the responsibility of the risk owner to ensure that these conditions are effectively monitored and that the corresponding actions are carried out as defined in a timely manner.

4.8.2 KEY SUCCESS FACTORS FOR MONITOR RISKS

Key success factors related to maintaining risk awareness throughout the life cycle include, but are not limited to:

- Integrated risk monitoring,
- Continuous monitoring of risk trigger conditions, and
- Maintaining risk awareness.

5

RISK MANAGEMENT IN THE CONTEXT OF PORTFOLIO MANAGEMENT

The purpose of risk management within the portfolio domain is to secure efficient and effective value delivery, which is pursued through the realization of the organization's strategic objectives. It is achieved by combining the management of opportunities and threats.

At the portfolio level, risk management takes into account the entire organizational framework. A portfolio is a collection of projects, programs, subsidiary portfolios, and operations managed as a group to achieve strategic objectives. Risk management in the portfolio domain ensures that all of the components implement effective processes to manage the entire risk management life cycle.

One of the main goals of portfolio management is to build a risk-efficient portfolio, where the organization chooses to take an appropriate amount of risk within the portfolio in order to achieve the required value in the overall organizational strategy. This is achieved by adding or removing portfolio components, based on their contributions to the overall risk exposure and strategic value.

5.1 PORTFOLIO RISK MANAGEMENT LIFE CYCLE

The life cycle of risk management as described in Section 4 generally applies to portfolio management. However, there are a number of additional considerations to the corresponding processes that need to be taken into account in this context.

5.1.1 PORTFOLIO RISK IDENTIFICATION

Risk identification at the portfolio level is focused on (a) identifying the risks that have an impact on the delivery of the expected business performance and (b) the ability of the organization to implement its strategy and achieve its strategic objectives.

There are two levels of risk:

- **Strategic risks.** Strategic risks are risks identified directly at the portfolio level and triggered by portfolio activities. Strategic risks include activities related to the generation of business performance by the portfolio components and those having an impact on the ability of the organization to achieve its strategic objectives.
- **Tactical risks.** Tactical risks are risks identified either by management processes at the portfolio level or escalated from the portfolio's components.

Risks that can impact portfolio components typically include the following categories:

- Changing business needs, environment, or context;
- Availability of resources;
- Interactions between components; and
- Conflicting component objectives.

5.1.2 PORTFOLIO RISK QUALITATIVE AND QUANTITATIVE ANALYSES

The evaluation of risks at the portfolio level is performed by taking into account the impact of risks on the realization of the expected business performance or the execution of the organizational strategy. One of the reasons these analyses are conducted is to evaluate whether the level of impact can be contained within the scope of the portfolio manager's accountability.

When the impact affects the portfolio's business performance or strategic objectives, then the impact is typically addressed at the portfolio level in an operational manner. When the impact affects the ability of the organization to execute strategy and realize the intended value, the risk and responsibility to respond to the risk is escalated to a higher governance level.

5.1.3 PORTFOLIO RISK RESPONSE STRATEGIES

In portfolio risk management, the focus of risk responses is oriented toward exploiting business opportunities and maximizing value creation for the organization and its stakeholders. It goes beyond treating threats, which, in the portfolio domain, are merely limitations to actions. Portfolio management also includes responding to risks escalated by its components in order to ensure that these are effectively and efficiently addressed at the appropriate level.

In principle, all of the potential responses listed in Section 4.6 can be used when responding to risks at the portfolio level.

The risk response strategies developed at the portfolio level consist of the activities documented in the portfolio risk management plan. In addition, some responses are developed as a result of escalation from the component level. These activities are budgeted accordingly and funded from the relevant sources. Examples of relevant funding sources are the portfolio's or component's budget for preventive responses, relevant contingency reserves for handling occurrences of known risks, or management reserves for handling unforeseen risk-related issues.

Risk responses can be planned as additional portfolio components such as projects, programs, subsidiary portfolios, or elements of the portfolio governance framework. These components are aimed at maximizing business performance or enhancing the execution of organizational strategy to achieve the strategic objectives. In some cases, the risk response can also lead to the removal of components from the portfolio.

5.1.4 IMPLEMENTING PORTFOLIO RISK RESPONSES

The implementation of risk responses within a portfolio includes:

- Triggering risk responses as they have been defined in the portfolio risk management plan,
- Transferring the corresponding budget from the contingency reserve into the budget at completion, and
- Updating the portfolio baselines accordingly.

The risk responses planned as new components become part of the portfolio and are subject to the application of the standard portfolio delivery and deployment processes.

Any formally approved risk response becomes an integral part of the portfolio management plan. The implementation of such a response is not a change to the portfolio that is initiated through a formal portfolio change management procedure. However, any new responses planned to address emergent risks become part of the portfolio change management procedure.

5.1.5 MONITORING PORTFOLIO RISKS

Monitoring the risks at the portfolio level is both a tactical and strategic activity, described as follows:

- **Tactical activity.** Oversees the aspects related to the execution of the anticipative and responsive actions undertaken to respond to identified risks. Also ensures that operational risks or systemic risks that could impact the portfolio are properly handled.
- **Strategic activity.** Addresses the evolution of the risk characteristics of each portfolio component, the overall portfolio risk profile, and the impact of that evolution on business performance. The focus is on development and implementation of the organizational strategy and the achievement of strategic objectives. These risk profiles are regularly analyzed in order to identify any potential trends that might indicate new risks or the inefficiency or ineffectiveness of the response strategies.

The monitoring of risk responses is conducted according to quantitative parameters and the use of qualitative assessments. These risk responses are intended to be effective at treating the specific risk they are addressing in order to enhance or maintain the realization of the expected business performance and the execution of the organizational strategy. The qualitative assessment is performed by revising the risk analysis to ensure these plans are efficient and effective.

Monitoring risks at the portfolio level includes ensuring that risk-related elements of the governance framework are properly implemented by the portfolio's components and are effective.

5.2 INTEGRATION OF RISK MANAGEMENT INTO THE PORTFOLIO MANAGEMENT PERFORMANCE DOMAINS

In order to achieve the portfolio objectives, there are a number of risk management practices that can be applied across the portfolio life cycle within all of the performance domains (see Figure 5-1). These practices typically cover the areas shown in Table 5-1.

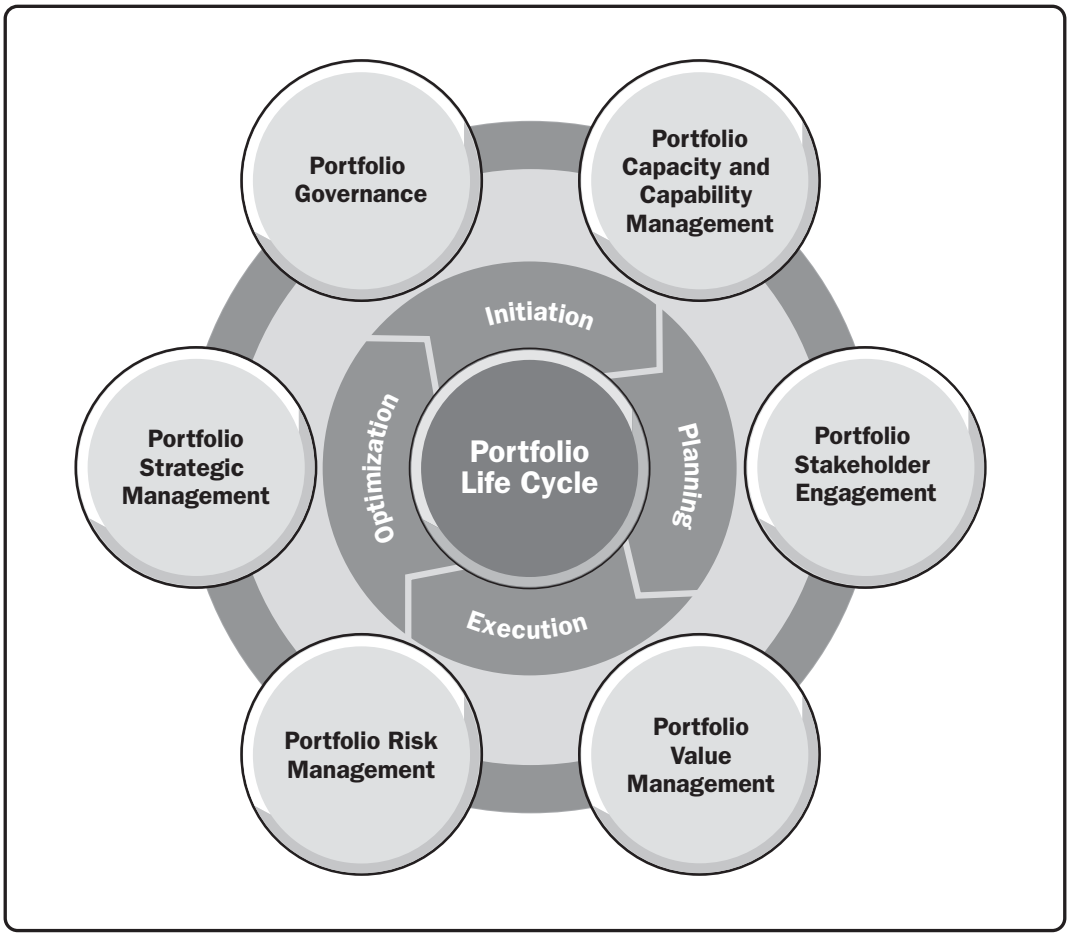


Figure 5-1. Portfolio Management Performance Domains (Source: *The Standard for Portfolio Management* [2])

Table 5-1. Areas of the Portfolio Management Performance Domains Typically Covered by Risk Management Practices

Performance Domain	Areas Covered by Risk Management Practices
Portfolio Strategic Management	• Alignment with organization's risk attitude and strategy • Quality of the organization's strategy • Impact of strategic changes within the organization • Interpretation of the portfolio mission, vision, strategic goals, and objectives • Impact of external opportunities and threats
Portfolio Governance	• Portfolio governance structures, policies, and procedures • Assignment of individuals to key governance roles • Risk-based audits • Use of audit reports
Portfolio Capacity and Capability Management	• Impact of the portfolio on other activities in the organization • Impact of the other activities of the organization • Key human, financial, and intellectual capital • Availability and fit for use of the key assets • Capacity required to manage risk • Impact of the organizational culture, structure, and key processes • Capacity of the partners and suppliers • Use of performance reports • Impact of portfolio optimization on value delivery
Portfolio Stakeholder Engagement	• Methods for stakeholder identification, categorization, and analysis • Attitude of key portfolio stakeholders • Interactions and conflicts of interests • Ways of engaging stakeholders • Scope, channels, techniques, and frequency of communications
Portfolio Value Management	• Opportunities to increase value delivery • Trends in the portfolio environment • Alignment of value targets with risk attitude • Impact of component risks on value delivery • Approach to the expected value negotiations
Portfolio Risk Management	• Risk management approach • General portfolio risks • Cumulative effects of component risks • Risk escalation policies

5.2.1 PORTFOLIO STRATEGIC MANAGEMENT

The essence of Portfolio Strategic Management is to ensure the enhancement/exploitation of strategic opportunities and the avoidance/mitigation of threats that could potentially prevent the organization from achieving its full potential. Therefore, risk management in the context of portfolio strategic management focuses on the identification and active management of those opportunities and threats that potentially have a substantial impact on the realization of the organizational strategy.

5.2.2 PORTFOLIO GOVERNANCE

The purpose of Portfolio Governance is to ensure that the portfolio is managed in an appropriate way. This includes meeting the legal, regulatory, and organizational governance requirements. The role of risk management within portfolio governance is to use the organization's potential to (a) efficiently secure adequate governance and management practices and (b) avoid or mitigate threats that could lead to misconduct or ineffective management of the portfolio.

5.2.3 PORTFOLIO CAPACITY AND CAPABILITY MANAGEMENT

Risk management in the context of Portfolio Capacity and Capability Management focuses on the mutual impact of the portfolio and related operations. In addition, risk management in the context of capacity and capability management ensures the proper use and development of capital and assets entrusted to the portfolio manager for the component programs and projects.

5.2.4 PORTFOLIO STAKEHOLDER ENGAGEMENT

Key stakeholders at the portfolio level typically include executive leaders and managers of the organization and their equivalents in the key partner, supplier, and customer organizations. Another key group of stakeholders is the component managers. From this perspective, portfolio risk management focuses on (a) opportunities to increase effectiveness in realizing the organization's strategy and (b) threats that could potentially lower the ability to do so.

5.2.5 PORTFOLIO VALUE MANAGEMENT

Portfolio Value Management focuses on ensuring that the investment in portfolio components leads to the delivery of expected value. Risk management, in this context, focuses on (a) maximizing opportunities to increase value delivered and (b) responding to threats that could potentially lower the value or probability of value delivery.

5.2.6 PORTFOLIO RISK MANAGEMENT

Portfolio Risk Management focuses on ensuring that risk at the portfolio and its component level is recognized and managed effectively. It is achieved through risk management and risk governance practices. Because these practices are essential for dealing with uncertainty at the portfolio level, they are also analyzed from the risk perspective. Adequate measures are then taken to ensure that the application of risk management is robust and effective.

6

RISK MANAGEMENT IN THE CONTEXT OF PROGRAM MANAGEMENT

The purpose of risk management within the program domain is to secure optimal realization of program benefits. This purpose is achieved by combining the management of opportunities and threats.

One of the key characteristics of a program is complexity, and risk management addresses this aspect. Risk management practices within a program use opportunities to reduce complexity and address threats that occur as a result of complexity.

Programs consist of related projects, subsidiary programs, and program activities managed in a coordinated manner to obtain benefits not available from managing them individually. Risk management ensures that all of these components have effective processes to manage the entire risk management life cycle.

6.1 PROGRAM RISK MANAGEMENT LIFE CYCLE

The life cycle of risk management as described in Section 4 generally applies to program management. However, there are a number of additional considerations for the corresponding processes that need to be taken into account in this context.

6.1.1 PROGRAM RISK IDENTIFICATION

Risk identification at the program level focuses on identifying the risks that could have an impact on the delivery of expected benefits. It also focuses on the ability of the organization to take over and use the results of the components that are part of the program scope.

There are three levels where risks relevant to the program can be identified:

- Risks cascading from the portfolio or enterprise level that can affect the achievement of program objectives;
- Risks identified directly at the program level and triggered by program activities, their interdependencies, and activities related to the integration of the components' results to generate the expected benefits; and
- Risks escalated from the program components.

The program domain risks are identified from their operational and contextual perspectives:

- **Operational risks.** Risks at the operational level are those risks directly triggered by program activities, such as integration of the results of projects and their related transition, change management, and triggering of operational activities. In addition, some operational risks may result from the escalation of the components' risks when these risks have an impact that expands beyond the perimeter of accountability of the component managers or their specific budgets.
- **Contextual risks.** Contextual risks are those risks resulting from the strategic and organizational environment of the program, from the stakeholders, and variations in the strategy or the evolution of the business environment or program's business case. Some contextual risks can also be escalated from the program components when their impact and treatment exceed the boundary of accountability of the components' managers.

Some risks identified at the program level or escalated from the project may need to be escalated to the enterprise or portfolio domain. These are the risks that have an impact on the business and operational performance generated through the exploitation of the business capabilities created by the program. Escalated risks follow the same processes of analyses as other risks identified at the program level (see Section 6.1.2).

6.1.2 PROGRAM RISK QUALITATIVE AND QUANTITATIVE ANALYSES

Evaluation of the risks at the program level is performed by taking into account the depth of each risk's impact on the realization of the expected benefits or the development of the expected organizational capability. The aim of these analyses is to evaluate whether or not the impact can be contained within the limits of the program budget.

When the impact affects the ability of the program to deliver its benefits or organizational capabilities, then the risk is addressed at the program level.

When the impact affects the ability of the organization to deliver the performance and value expected to be obtained from the benefits and capabilities created by the program, then the risk and its treatment are escalated to the enterprise or portfolio domain. In addition, the risk and its treatment are escalated when the risk affects the expected financial and operational performance anticipated from the new capabilities beyond the agreed thresholds.

6.1.3 PROGRAM RISK RESPONSE STRATEGIES

In principle, all potential responses listed in Section 4.6 may be used when responding to risks at the program level.

Strategies developed at the program level to deal with risks consist of the activities agreed to in the risk management plan and budgeted for in the program's budget or contingency reserve. Some of the responses are also developed as a result of escalation from the component level.

These risk responses consist of adding program activities or components, updating the program baselines, or removing components from the program.

These new components are intended to maximize the creation of further business benefits or further enhance the development of organizational capabilities. Alternatively, the intent may be to maintain or reinforce the contribution of the program to achieve related strategic objectives or minimize threats to the organization's objectives and strategy.

6.1.4 IMPLEMENTING PROGRAM RISK RESPONSES

Implementation of risk responses within a program consists of:

- Triggering the risk responses as they have been defined in the risk management plan,
- Transferring the corresponding budget from the reserves into the budget at completion, and
- Updating the program baselines accordingly.

When new components are added, they become part of the regular program scope and subject to the application of the standard program delivery and deployment processes.

Implementation of risk responses at the component level is aligned and performed in coordination with the responses that are implemented in the program domain. Any formally approved risk response becomes an integral part of the program management plan. The implementation of an approved risk response is not a change to the program that is initiated through a formal program change management procedure. However, any new responses planned to address emergent risks become part of the program change management procedure.

6.1.5 MONITORING PROGRAM RISKS

Monitoring the risks at the program level is both a tactical and strategic activity:

- **Tactical activity.** Oversees the aspects related to the execution of the anticipative and responsive actions undertaken to respond to identified risks.
- **Strategic activity.** Addresses the evolution of the risk characteristics of each program component individually, the overall program's risk profile, and the impact of that evolution on the business benefits or organizational capabilities it is intended to generate. These risk profiles are regularly analyzed in order to identify any potential trends that indicate new risks or the inefficiency or ineffectiveness of the response strategies.

The monitoring of risk responses is conducted according to their quantitative and qualitative parameters, as defined in the management plans with consideration of the overall impact from the component to the enterprise level.

These risk responses are intended to be effective at treating the respective, specific risks and contribute to enhancing or maintaining the realization of expected benefits. It is important to perform a qualitative assessment to ensure that the risk responses are efficient and effective.

Monitoring risks at the program level also includes ensuring that risk-related elements of the governance framework are properly implemented by the program's component managers and that they are effective.

6.2 INTEGRATION OF RISK MANAGEMENT INTO THE PROGRAM MANAGEMENT PERFORMANCE DOMAINS

There are a number of risk management practices that can be applied across the program life cycle within all of the performance domains in order to achieve their objectives (see Figure 6-1). These practices typically cover the areas shown in Table 6-1.

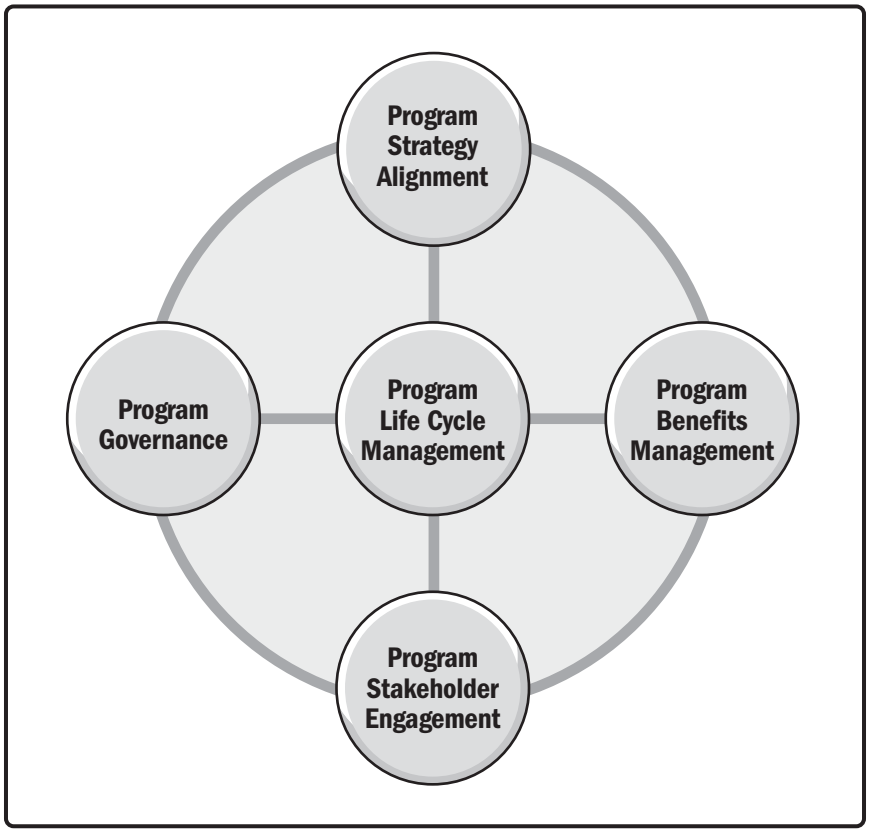


Figure 6-1. Program Management Performance Domains (Source: *The Standard for Program Management* [3])

Table 6-1. Areas of the Program Management Performance Domains Typically Covered by Risk Management Practices

Performance Domain	Areas Covered by Risk Management Practices
Program Strategy Alignment	• Program business case • Program risk management approach • Environmental assessments
Program Benefits Management	• Program objectives • Opportunities for new benefits • Efficiency and effectiveness of benefits realization • Sustainability of program benefits
Program Stakeholder Engagement	• Methods for stakeholder identification, categorization, and analysis • Attitude of key program stakeholders • Interactions and conflicts of interests • Ways of engaging stakeholders • Scope, channels, techniques, and frequency of communications
Program Governance	• Program governance structures, policies, and procedures • Assignment of individuals to key governance roles • Program complexity • Risk escalation policies • Effectiveness of risk management
Program Life Cycle Management	• Program definition phase activities • Component authorization and planning • Component oversight and integration • Component transition

6.2.1 PROGRAM STRATEGY ALIGNMENT

Program Strategy Alignment ensures that a program contributes to organizational strategy in the expected way. Risk management efforts in this domain address new strategic opportunities and threats. When necessary, these efforts lead to appropriate program redefinition or changes in the relevant program components.

6.2.2 PROGRAM BENEFITS MANAGEMENT

Program Benefits Management ensures that the program benefits described in the business case and other program governance documents are successfully realized. The main focus of risk management in this area is to (a) manage opportunities that could increase these benefits, (b) deliver opportunities more efficiently, and (c) manage threats that could potentially jeopardize the program's efforts to realize its benefits.

6.2.3 PROGRAM STAKEHOLDER ENGAGEMENT

Key stakeholders from the program perspective typically include program governance board members, the program manager, managers of program components, partners, key suppliers, and regulators impacting or being impacted by the program benefits. From this perspective, program risk management focuses on opportunities for increasing effectiveness in realizing program benefits and on minimizing threats that could potentially lower the ability to do so. It is realized by effective engagement of stakeholders at the program level and ensures consistency of stakeholder management strategies among program components.

6.2.4 PROGRAM GOVERNANCE

Program Governance uses the framework, functions, and processes by which a program is monitored, managed, and supported in order to meet organizational strategic and operational goals. Program Governance also addresses program complexity in an effort to reduce it. These activities are backed by risk management practices, focused on the analysis of various governance approaches from the risk perspective. In addition, the selection of individuals to perform key governance roles is supported by risk analysis.

A key element of Program Governance from the risk management perspective is the risk escalation process, which is integrated with processes within components and backed by program governance processes and structures.

6.2.5 PROGRAM LIFE CYCLE MANAGEMENT

Program Life Cycle Management ensures that program definition, delivery, and closure activities are effectively managed. This is accomplished to ensure program benefits are realized using the right set of components, in the right sequence, and with adherence to the program's business case and other governance documents.

Risk management in this area focuses on identifying and addressing program-level risks as early as possible. This is achieved by fully integrating risk identification, analysis, and response planning throughout all program and component activities.

6.2.6 SUPPORTING PROGRAM ACTIVITIES

Even though the management of program-level activities often differs significantly from the component level, risk management processes for the supporting program activities are similar in nature to the component projects.

Program Governance establishes policies on risk management between the program and its components, including escalation mechanisms. This ensures that there are no gaps between the component and program levels that are not covered by risk management practices.

7

RISK MANAGEMENT IN THE CONTEXT OF PROJECT MANAGEMENT

The purpose of risk management within the project domain is to support the optimal delivery of project results leading to the realization of benefits for which the project was undertaken. In addition, risk management helps to ensure that delivery of these results occurs within the identified project constraints.

Projects are aimed at creating a unique product, service, or result. Project risks are triggered by uncertainty in some of the operational activities and enterprise environmental factors. Project success is assessed and evaluated based upon the ability to deliver a tangible outcome. Therefore, risks that are managed at the project level are evaluated and considered according to their potential impact on the ability to deliver a tangible outcome. The evaluation and analysis of risks are focused at the tactical level, and every other consideration in terms of impact on expected value or benefit creation is escalated to the portfolio or program governance level.

Project teams need to have visibility into the strategic objectives that led to its authorization. This allows for effective, proactive project management and reporting of key opportunities and threats that could potentially impact the objectives.

7.1 PROJECT RISK MANAGEMENT LIFE CYCLE

The life cycle of risk management as described in Section 4 generally applies to project management. However, there are a number of additional considerations for the corresponding processes that need to be taken into account in this context.

7.1.1 PROJECT RISK IDENTIFICATION

Identification of risks at the project level is based on operational and contextual inputs. Operational inputs come from the activities of the project itself. Among these inputs are:

- **Project scope statement.** There are a number of risks related to the specifications and agreed methods of delivery for products, services, or other results that are expected to be delivered by the project.
- **Project life cycle.** Regardless of the life cycle selected, the life cycle itself introduces a number of risks.
- **Work breakdown structure (WBS), activity list, or backlog.** There are a number of risks directly connected to the decomposition of the project work and triggered by its execution.
- **Estimates.** Estimates are performed in terms of time, cost, effort, and resources. The target accuracy of an estimate is the level of risk tolerated for that estimate.
- **Dependencies and sequence of work.** Interdependencies and the resulting sequence of work are sources of risk. Special attention is paid to critical path and external dependencies created by the sharing of resources with other projects. If the critical path changes during the project life cycle, the criticality of the risks related to the elements on that critical path may also be dynamic.
- **Procurement plans.** Subcontracting parts of the project scope may be an action of risk transfer, but it may also trigger new risks.
- **Change requests.** Each time a change is implemented within a project, it may eliminate certain risks but also trigger new ones.
- **Historical data.** Based on past experience, it is important to identify systemic risks and automate their treatment.

Contextual risks result from the consideration of enterprise environmental factors and other strategic or organizational aspects shaping the environment of the project, such as:

- **Stakeholder analysis.** All key stakeholders can bring a number of opportunities to be exploited; however, when handled inadequately, they may introduce threats that need to be mitigated.
- **Business case.** The business case often implies a factor of profitability or positive return on investment that is exposed to a certain level of uncertainty or risk. The ability to achieve and sustain benefits after project completion is part of risk identification. Risks impacting the realization of benefits can be addressed during project execution.

- **Program or portfolio governance-level success factors.** These factors may vary over time and change the priority level of the project within the program or portfolio.
- **Enterprise environmental factors.** Factors such as the strategy of the organization, its structure, the dynamics of its business environment, and the variability of its regulatory environment are triggers of risks that directly impact the project.

7.1.2 QUALITATIVE AND QUANTITATIVE PROJECT RISK ANALYSES

The evaluation of risks at the project level is performed by taking into account the degree of impact on the project objectives and probability of occurrence. The purpose of these analyses is to evaluate whether or not the impact can be contained within the limits of the project budget and the boundary of accountability of the project manager. Risks that have an impact evaluated as containable within the limits of accountability of the project manager and team are dealt with in the project risk management plan and strategy. Every risk impact that exceeds the limits of accountability is escalated to the appropriate governance level.

When the impact of the risk is determined to be containable within the limit of the project budget and accountability of the project manager and team, it is addressed at the project level.

If the risk impacts the ability of the organization to obtain or sustain the expected benefits, then the risk and its treatment are escalated to the appropriate governance level.

7.1.3 PROJECT RISK RESPONSE STRATEGIES

In principle, all of the potential responses listed in Section 4.6 can be used when responding to risks at the project level.

The strategies developed to deal with risks at the project level consist of activities guided by the risk management plan, budgeted accordingly, and funded by the project's contingency reserve. Risk responses consist of additional activities or work packages to update the project's baselines or remove activities from these same baselines.

Whenever the project is part of a program or is managed as part of a portfolio, escalation of risks to a higher governance level is always one of the responses. Escalation increases the effectiveness or efficiency of dealing with specific risks that impact the program or portfolio or with risks that require funding in excess of the contingency reserves.

7.1.4 IMPLEMENTING PROJECT RISK RESPONSES

The implementation of risk responses within a project is performed according to the risk management plan, uses the corresponding budget from the reserves into the budget, and updates the project baselines accordingly. Together, these activities become part of the regular project scope and are subject to the application of project execution processes.

The implementation of a risk response plan is not initiated through a formal project change management procedure. A risk response is part of the project management plan and does not require a formal change control process because it has already been approved as part of the risk management plan.

7.1.5 MONITORING PROJECT RISK

Monitoring risks at the project level consists of:

- Checking the status of the risks that have already been identified,
- Verifying whether any known risk has not occurred or is not about to occur, and
- Monitoring the status of all actions implemented to respond to the detection or occurrence of a risk.

These activities typically lead to updates of plans, registers, and controlling documents. In addition, performance reports are regularly analyzed in order to identify any potential trends that could indicate new risks or the ineffectiveness of response strategies.

The risk responses implemented to anticipate and prevent the occurrence of threats or exploit and enhance the opportunities are conducted according to their quantitative parameters of time, cost, scope, and specifications. A qualitative assessment evaluates the effectiveness and efficiency of risk treatment for specific risks that have occurred.

7.2 INTEGRATION OF RISK MANAGEMENT INTO PROJECT MANAGEMENT PROCESS GROUPS

A Guide to the Project Management Body of Knowledge (*PMBOK® Guide*) [4] describes the Project Risk Management Knowledge Area. An analysis of the relationship between the processes in Project Risk Management and other Knowledge Areas is provided next. There are a number of general risk management practices that can be applied across the project life cycle. The following sections summarize these practices in a general way as they relate to the Process Groups and Knowledge Areas shown in Table 7-1.

Table 7-1. Areas of the Project Management Process Groups and Knowledge Areas Typically Covered by the Risk Management Practices

Knowledge Areas	Project Management Process Groups				
	Initiating Process Group	Planning Process Group	Executing Process Group	Monitoring and Controlling Process Group	Closing Process Group
Project Integration Management	• High-impact risks • Setting objectives and general scope • Selection of life cycle	• Integrity of planning processes • Quality of data	• Delivery processes • Risk-related knowledge transfer • Use of lessons learned and historical data	• Integrity of control • Risks related to changes	• Results transition • Sustainability of benefits
Project Scope Management		• Scope and requirements management approach • Decomposition approach		• Validation approach • Control approach • Use of work performance data	
Project Schedule Management		• Schedule management approach • Estimation		• Control approach • Use of work performance data	
Project Cost Management		• Financing • Cost management • Estimation		• Control approach • Use of work performance data	
Project Quality Management		• Quality management approach and metrics • Process improvement	• Quality culture	• Control approach • Use of work performance data	
Project Resource Management		• Resource management approach • Estimation	• Resource acquisition • Team development and management	• Control approach • Use of work performance data	
Project Communications Management		• Communication approach, scope, and frequency	• Communication channels and techniques	• Monitoring approach • Use of work performance data	
Project Risk Management		• Risk attitude • Risk management approach • Adaptation to life cycle • Integration with other project plans • Tolerances • Secondary and residual risks	• Accountability for risk management processes • Accountability for response implementation	• Monitoring approach • Use of work performance data • Continuous improvement of risk management	
Project Procurement Management		• Procurement management approach • Contract types	• Selection criteria • Negotiation approach	• Supplier capacity • Control approach • Use of work performance data	
Project Stakeholder Management	• Identification and categorization approach • Risk attitude of key stakeholders • Conflicts of interests	• Engagement strategies	• Consistency of strategy execution	• Monitoring approach • Use of work performance data	

7.2.1 INITIATING PROCESSES

Initiating processes are performed to define a new project or a new phase of an existing project by obtaining authorization to start the project or phase. An essential part of that work is related to understanding the high-level risks that might impact the realization of objectives specified in the business case. It is essential to address these risks prior to authorizing the project or phase.

During project initiation, the selection of the appropriate project life cycle is one of the first decisions supported by risk management. Each of the known project life cycles has an impact on all areas of project management by helping to enhance and exploit opportunities or introducing a number of threats.

Another important aspect of risk management during project initiation is the understanding of risks related to key stakeholders, their interests, and potential conflicts among them and with the project.

7.2.2 PLANNING PROCESSES

Planning processes establish the scope of the project, refine the objectives, and define the course of action required to attain the objectives that the project was undertaken to achieve.

The selection of the overall risk management approach is one of the key planning decisions. It involves the analysis of risks that could potentially impact the effectiveness of the risk management processes.

The key areas of planning that also include risk management practices are:

- Integrity of the planning processes and the resulting plans,
- Selection of the management approaches in all Knowledge Areas relevant to the project, and
- Estimation activities.

It is typical that processes in this Process Group lead to the identification of a high number of risks because these processes include analytical work necessary for planning. It is important to ensure that risk identification becomes a natural part of every process in this Process Group.

7.2.3 EXECUTING PROCESSES

Executing processes are performed to complete the work defined in the project management plan to satisfy the project requirements and achieve the objectives of the project. Successful risk management depends on the flow of knowledge within the project and the organizations involved in its execution.

Risk management practices are most effective when supported by a culture that embraces proactive behavior, open communication, organizational learning, and continuous improvement. This means that integration with team building and management, quality management, execution of stakeholder engagement strategies, and communication processes are essential.

7.2.4 MONITORING AND CONTROLLING PROCESSES

Monitoring and Controlling processes track, review, and regulate the progress and performance of the project, identify the areas in which changes to the plan are required, and initiate the corresponding changes.

Risk management supports efforts to ensure integrity and reliability of reporting. On the other hand, risk identification, risk analysis, and risk monitoring processes use the performance data and information as key inputs that help identify, analyze, and monitor risks.

7.2.5 CLOSING PROCESSES

Closing processes are performed to formally complete or close the project, phase, or contract. Where risk management is concerned, part of the closing practices involve securing knowledge that may be useful in future project phases, projects, or other activities of the organization. The remaining known risks that could impact the realization of benefits are handed over prior to project closure.

APPENDIX X1
DEVELOPMENT OF *THE STANDARD FOR RISK MANAGEMENT IN PORTFOLIOS, PROGRAMS, AND PROJECTS*

The *Practice Standard for Project Risk Management* was published in 2009. Its purpose was to (a) provide a standard for project management practitioners and other project stakeholders that defined the aspects of project risk management recognized as good practice on most projects most of the time and (b) provide a standard that is globally applicable and consistently applied.

The *Practice Standard for Project Risk Management* covered risk management for a single project. Section 11 of *A Guide to the Project Management Body of Knowledge* (*PMBOK® Guide*) – Fourth Edition formed the basis for the *Practice Standard for Project Risk Management*. Like the *PMBOK® Guide*, the practice standard did not cover risk in portfolios or programs.

In 2017, recognizing that risk management is a major consideration in portfolios and programs as well as projects, the PMI standards program team (SPT), which includes the PMI Standards Manager and the Standards Member Advisory Group, chartered the development of the principle-based *Standard for Risk Management in Portfolios, Programs, and Projects*. In addition to addressing risk in the purview of three of PMI's foundational standards (*PMBOK® Guide* – Sixth Edition, *The Standard for Program Management* – Fourth Edition, *and The Standard for Portfolio Management* – Fourth Edition), the charter directed the project team to identify the core principles and practices for risk management, describe the fundamentals of risk management, and write the standard to reflect current, accepted risk management good practices.

The project team formed in the fall of 2017. It consisted of eight PMI volunteers led by Gary Sikma, committee chair, and David Ross, vice chair. In addition to expanding the scope of risk management to cover portfolios, programs, and projects as directed by the charter, the project team submitted recommendations to PMI's Lexicon Team to enhance risk-related definitions to include all three domains. The first draft of the standard was completed on 12 March 2018 and distributed to subject matter experts (SMEs) for review and comment. Based on the SMEs' comments, the document was revised and released to the practitioner community on 2 July 2018 as a public exposure draft. The committee revised the draft and submitted the final draft and summary report of the public exposure draft actions to the PMI Standards Consensus Body for approval, leading to its subsequent publication.

APPENDIX X2
CONTRIBUTORS AND REVIEWERS OF *THE STANDARD FOR RISK MANAGEMENT IN PORTFOLIOS, PROGRAMS, AND PROJECTS*

The Project Management Institute is grateful to all of these individuals for their support and acknowledges their outstanding contributions to the project management profession.

X2.1 *THE STANDARD FOR RISK MANAGEMENT IN PORTFOLIOS, PROGRAMS, AND PROJECTS* CORE COMMITTEE

The following individuals were members of the Core Committee responsible for drafting the standard, including adjudication of reviewer comments.

Gary J. Sikma, PMP, PMI-ACP, Chair
David W. Ross, PMP, PgMP, Vice Chair
Kari Dakakni, PMI-RMP, PMP
Christopher Edwards, MBA, PMP
Nicki Kons, PMI-RMP, PMP
Olivier Lazar, PMI-RMP, PfMP
Grzegorz Szalajko, CISA, PMP
Te Wu, PhD, PgMP, PfMP

X2.2 SIGNIFICANT CONTRIBUTORS

In addition to the members of the Committee, the following individuals provided content and concepts as inputs to the document.

Nick Clemens, PMI-ACP, PMP
Joel Crook, PMP, PgMP
Valerie P. Denney, DBA, PMP
David Hillson, PhD, HonFAPM, PMI Fellow
Brian Williamson, PMI-RMP, PMP

X2.3 REVIEWERS

X2.3.1 SME REVIEW

The following individuals were invited subject matter experts who reviewed the initial draft and provided recommendations for improvement.

Ruan Almeida, MBA, PMP
Alfredo Armijos, PMI-RMP, PMP
Eric Biderbost, Ing Dipl EPF, PMP
Kiron D. Bondale, PMI-RMP, PMP
Robert G. Brown, PhD, PMP
Panos Chatzipanos, PhD, Dr Eur Ing
Nick Clemens, PMI-ACP, PMP
Joel Crook, PMP, PgMP
Valerie P. Denney, DBA, PMP
Tommy Dodson, MBA, PMP
John D. Driessnack,IPPM, PfMP
Vanessa Everhart, MBA
Akram Hassan, PhD, PMI-RMP
Piotr Hendzak, PMP
David A. Hilson, PhD, HonFAPM, PMI Fellow
Nicholas J. Holdcraft, PMI-RMP, PfMP
Cedrik Lanz
Alan C. Maltz, PhD, PE
Michael J. Marren, PMP
Debbie McKee
Rafal Nowak, MSc, PMP
Josef Oehmen, PhD
Andrew Resseguie, PMI-RMP
Dan Stelian Roman, PMI-ACP, PMP
Cindy Shelton
Dave Violette, MPM, PMP

X2.3.2 CONSENSUS BODY REVIEW

The following individuals are members of the Consensus Body, who provided final approval for publication of the standard.

Nigel Blampied, PE, PMP
Chris Cartwright, MPM, PMP
John Dettbarn, DSc, PE
Charles Follin, PMP
Michael Frenette, SMC, PMP
Dana Goulston, PMP
Brian Grafsgaard, PMP, PgMP
Dave Gunner, PMP
Dorothy Kangas, MS, PMP
Thomas Kurihara
Hagit Landman, PMI-SP, PMP
Tim MacFadyen, MBA, PMP
Vanina Mangano, PMI-RMP, PMP
Mike Mosley, PE, PMP
Nanette Patton, MSBA, PMP
Yvan Petit, PhD, PMP
Crispin ("Kik") Piney, PgMP PfMP
Mike Reed, PMP, PfMP
David Ross, PMP, PgMP
Paul Shaltry, PMP
C. Gabriela Spindola
Chris Stevens, PhD
Judi Vincent
David J. Violette, MPM, PMP

X2.3.3 PUBLIC EXPOSURE DRAFT REVIEW

The following individuals participated in the public review of the standard and provided recommendations for improvement.

Habeeb Abdulla, MS, PMP
Charles D. Ackerman, PMI-ACP, PMP
Lipika Ahuja, MPA, PMP
Phill C. Akinwale, MSc, PMI-RMP
José Rafael Alcalá Gómez, PMP
Abdulrahman Alulaiyan, MBA, PMP
Charalampos Apostolopoulos, PhD, PfMP
Ondiappan Arivazhagan, PMI-RMP, PMP
Sharaf A. Attas, PMI-RMP, PMP
Kiron D. Bondale, PMI-RMP, PMP
Farid F. Bouges, PhD, PMP, PfMP
Armando Camino PMI-ACP, PMP
Tessore Carlos, PhD, PMI-RMP
Panos Chatzipanos, PhD, Dr Eur Ing
Nguyen Si Trieu Chau, PgMP, PfMP
Williams Chirinos, MSc, PMP
Jorge Omar Clemente, CPA, PMP
Dariusz Ciechan, PMI-RMP, PMP
Sergio Luis Conte, PhD, PMP
Adam D. Coombs, PEng, PE
Jeanine Cooper, PMI-SP, PMP
Helio R. Costa, DSc
Joel D. Crook, PMP, PgMP
William D'Souza, MBA, PMP
Panini Deshpande, MBS, PMP
Danil Dintsis, PhD, PMP, PgMP
Phillip Doyle, PMP
Vick Ekizian, PMI-RMP

Dimitrios M. Emiris, PhD, PMP
Fereydoun Fardad, PMI-RMP, PMP
Uriel Fliess, PMP
Luis Alberto Flores, PMI-RMP, PMP
Carlos Augusto Freitas, CAPM, PMP
Ivo Gerber, PMI-ACP, PgMP
Carl M. Gilbert, PMI-RMP, PMP
Theofanis C. Giotis, PhDc, PMP
Gabrielle Bonin Haskins, PMP
Sergio Herrera-Apestigue, P3O, PMP
David Hillson, PhD, HonFAPM, PMI Fellow
Suhail Iqbal
Dorothy L. Kangas, MS, PMP
Suhail Khaled, PMI-ACP, PMP
Aikaterini Kiafi, MSPM
Taeyoung Kim, PMP
Konstantinos Kirytopoulos, PhD, PMP
Maciej Koszykowski, PMI-RMP, PgMP
P. Ravikumar, PMP, PgMP
G. Lakshmi Sekhar, PMI-PBA, PMP
Jianyong Li
Lydia G. Liberio, JD, PMI-RMP
James Liu, PhD, PMP
Sivakumar Loganathan, MTech, MIIT Arb
Juan Carlos Flores López, SMC, PMP
Sergio O. Lugo, MBA, PMP
Frank M. Mangini, MSEE, PMP
Gaitan Marius, PMI-PBA, PMP
Atilio Mashini, SMC, PMP
Felipe Fernandes Moreira, PMP
Aleksei V. Nikitin, PMI-ACP, PMP
Josef Oehmen, PhD
Yelena Okonechnikova, MBA, PMP
Habeeb Omar, PgMP, PfMP
Zaid Omer, BSc ElecEng, M.IRMSA
David A. Borja Padilla, Msc, PMI-RMP
Crispin (“Kik”) Piney, PgMP, PfMP
Carl W. Pro, PMI-RMP, PMP
Norman Radatz, PMP
Gilberto Regal Rodríguez, PMI-SP, PMP
Dan Stelian Roman, PMI-ACP, PMP
Omar A. Samaniego, PMI-RMP, PMP
Parthasarathy Sampath, PMI-RMP, PMP
Pedro Sandoval
David Shrimpton, PMI-RMP, PMP
Ronald Zack Sionakides, MBA, PMP
Mauro Sotille, PMI-RMP, PMP
Gerhard J. Tekes, PMI-RMP, PMP
Mario Coquillat de Travesedo, PMI-RMP, PMP
Daniel Ubilla Baier, MBA, PMP
Juan Gabriel Gantiva Vergara, PMI-RMP, PMP
Dave Violette, MPM, PMP
Esteban Villegas, PMP
Kyriakos Vougiklakis, BSC, MA

X2.4 PMI STANDARDS PROGRAM MEMBER ADVISORY GROUP

The PMI Standards Program Member Advisory Group (SMAG) works under the leadership of the standards manager. We extend our sincerest thanks to them for their compelling and helpful guidance throughout the development process.

During the course of the committee's work, the following distinguished members of the PMI community served with distinction on the SMAG:

Maria Cristina Barbero, CSM, PMI-ACP, PMP
Michael J. Frenette, I.S.P., SMC, MCITP, PMP
Brian Grafsgaard, CSM, PMP, PgMP, PfMP
David Gunner, MSc, PMP, PfMP
Hagit Landman, MBA, PMI-SP, PMP
Vanina Mangano, PMI-RMP, PMP
Yvan Petit, PhD, MEng, MBA, PMP, PfMP
Carolina Gabriela Spindola, MBA, SSBB, PMP

X2.5 HARMONIZATION TEAM

The following served on the harmonization team to ensure consistency among the newly published standards:

X2.5.1 CORE TEAM:

Bridget Fleming
Greg Hart
Hagit Landman, PMI-SP, PMP
Vanina Mangano, PMI-RMP, PMP
Tim MacFadyen, MBA, PMP
Mike Mosley
John Post, PMP
David W. Ross, PMP, PgMP
Cindy Shelton, PMI-ACP, PMP
Gary Sikma, PMI-ACP, PMP
Dave Violette, MPM, PMP

X2.5.2 PMI STAFF:

M. Elaine Lazar, MA, AStd
Marvin R. Nelson, MBA, SCPM
Lorna Scheel, MSc
Roberta Storer
Kristin Vitello, CAPM
Ashley Wolski, MBA
John Zlockie, MBA, PMP

X2.6 PRODUCTION STAFF

Special mention is due to the following employees of PMI:

Donn Greenberg, Manager, Publications
Kim Shinners, Publications Production Associate
Roberta Storer, Product Editor
Barbara Walsh, Publications Production Supervisor

APPENDIX X3
PORTFOLIO RISK MANAGEMENT CONTROLS

X3.1 THE PURPOSE OF PORTFOLIO RISK MANAGEMENT CONTROLS

A portfolio is a collection of projects, programs, subsidiary portfolios, and operations managed as a group to achieve strategic objectives. At the portfolio level, projects, programs, and operations are aligned with the organization's investment strategy to assure achievement of strategic objectives through portfolio operations. The focus of portfolio management is on the alignment of programs, projects, and operations with the organization's strategy and balancing risks to achieve strategic objectives. Portfolio managers manage the resources, constraints, and interfaces between subordinate programs, projects, and operational activities.

The primary objective of portfolio risk management is to ensure portfolio components achieve the best possible success according to the organization's strategy and business model. From a risk perspective, this is accomplished through the balancing of positive and negative risks. Risk management controls help to achieve this by seamlessly integrating risk practices into the portfolio life cycle within all of the performance domains. This approach ensures that risk management becomes a natural part of portfolio management and helps achieve success in value delivery.

The selection, tailoring, implementation, and monitoring of particular controls in a given portfolio are a part of the oversight activities. Sections X3.2 through X3.7 provide risk management controls for portfolio risk management along with examples of factors to consider for some of the controls.

X3.2 RISK MANAGEMENT CONTROLS FOR PORTFOLIO STRATEGIC MANAGEMENT

Risk management controls and objectives for portfolio strategic management are provided in Table X3-1.

Table X3-1. Risk Management Controls and Objectives for Portfolio Strategic Management

Control ID	Control Objective
PF.STR.1	Organization's strategic risk attitude and appetite are regularly reassessed and reflected in the portfolio governance documents and other relevant portfolio process assets.
PF.STR.2	Criteria for selection of portfolio components reflect the organization's risk attitude and appetite.
PF.STR.3	Risks related to the correctness of the organizational strategy are identified and actively managed throughout the entire portfolio life cycle.
PF.STR.4	Risks related to strategic changes within the organization that could potentially impact the way that the portfolio or its components are managed, identified, and analyzed are reflected in the portfolio governance documents.
PF.STR.5	Risks related to the interpretation of the portfolio mission, vision, strategic goals, and objectives are identified, analyzed, and acted upon while developing or changing those elements.
PF.STR.6	Organization's environment is regularly monitored for opportunities and threats that could lead to changes at the portfolio level. Critical success factors (CSFs) for strategy realization are given special attention in this context.
PF.STR.7	When optimizing the portfolio, risks related to the realization of value expected from impacted programs and resulting from projects within the portfolio are identified, analyzed, and acted upon.

The following factors should be considered when reassessing the organization's strategic risk attitude and appetite and the selection of portfolio components based on organizational attitude and appetite (Control PF.STR.1 and Control PF.STR.2):

- Overall organization's strategic risk attitude, also considering its market, legal, and political context;
- Degree of uncertainty an organization is willing to accept in anticipation of a reward;
- Degree, amount, or volume of risk that an organization is willing to withstand; and
- Level of risk exposure above which risks are addressed and below which risks may be accepted.

The following factors should be considered when identifying risks related to the correctness of the organizational strategy (Control PF.STR.3):

- Experience and competence level of the team formulating the strategy;
- Reliability, applicability, and accuracy of models and data used for environmental analysis and forecasting;
- Clarity and completeness of strategic vision;
- Definition of strategic objectives;
- Comprehensiveness of the decision-making processes during strategy formulation; and
- Completeness of strategic dimensions taken into consideration (e.g., as suggested by the balanced scorecard technique).

The following factors should be considered when identifying risks related to strategic changes within the organization and when identifying risks related to analysis, execution, and change to portfolio mission, vision, and strategic goals and objectives (Control PF.STR.4):

- Ongoing and planned changes in the organization;
- Ongoing and planned changes in the organization's environment (legal, market, labor);
- Portfolio change control system and its interface with projects, programs, and operational components;
- Interface between other portfolios and entities external to the enterprise;
- Enterprise environmental factors and organizational process assets;
- Stakeholder engagement; and
- Portfolio interface with the organization's enterprise risk management processes.

The following factors should be considered when monitoring CSFs (critical success factors) and opportunities and threats (PF.STR.6):

- New technologies, materials, or tools;
- Availability of new types or increased amounts of resources;
- Changes in political, market, financial, or legal environments; and
- Balancing of opportunities and threats.

The following factors should be considered when identifying risks related to the realization of value contribution expected from programs, projects, and operations within the portfolio (PF.STR.7):

- Accuracy and continued applicability of the portfolio's business case and subordinate components' business cases,
- Linkages between portfolio value delivery and achievement of strategic objectives, and
- Linkages between and across any other portfolios and the managed portfolio.

X3.3 RISK MANAGEMENT CONTROLS FOR PORTFOLIO GOVERNANCE

Risk management controls and objectives for portfolio governance are provided in Table X3-2.

Table X3-2. Risk Management Controls and Objectives for Portfolio Governance

Control ID	Control Objective
PF.GOV.1	Risks related to portfolio governance structures, policies, and procedures are identified and actively managed throughout the entire portfolio life cycle.
PF.GOV.2	Risks related to the assignment of particular individuals to key governance roles within the portfolio are identified and actively managed throughout the entire portfolio.
PF.GOV.3	Audits conducted as part of portfolio governance are based on risk analysis in order to ensure the right focus and minimize impact on portfolio components.
PF.GOV.4	Audit reports are used as an input for portfolio and component-level risk identification.
PF.GOV.5	Audits conducted as part of portfolio governance are performed according to agreed standards by qualified personnel independent from the portfolio and component management roles.
PF.GOV.6	Risks related to the interface of the portfolio governance structure and policies and procedures with the enterprise risk management processes are identified and actively managed throughout the entire portfolio life cycle.

The following factors should be considered when identifying risks related to portfolio governance structure and policies and procedures (Control PF.GOV.1):

- For portfolio governance structures:
  - Complexity,
  - Clearness of accountability,
  - Level of interdependencies,

- Integration with other structures within the organization, and
- Degree of key stakeholders' representation.

◆ For portfolio policies and decision-making processes:

- Complexity,
- Transparency,
- Involvement of key stakeholders,
- Fairness,
- Time to make decisions, and
- Quality mechanisms.

The following factors should be considered when identifying risks related to assignment of particular individuals to key governance roles within the portfolio (Control PF.GOV.2):

◆ Competences,

◆ Level of power,

◆ Position in the organization,

◆ Reputation,

◆ Availability, and

◆ Shared and conflicting interests.

The following factors should be considered when planning and staffing audits as part of portfolio governance (Control PF.GOV.5):

◆ Competency of the auditing entity,

◆ Willingness of stakeholders to accept audit results,

◆ Applicability of audit results to portfolio and portfolio component processes, and

◆ Applicability of audit results to enterprise risk management processes.

The following factors should be considered when identifying risks related to the interface of portfolio governance structures and policies and procedures with enterprise risk management processes (Control PF.GOV.6):

◆ Governance processes defined by enterprise risk management,

◆ Applicability of enterprise risk management to specific portfolio processes and actions, and

◆ Linkages between portfolio governance and management processes with senior management and enterprise risk management.

X3.4 RISK MANAGEMENT CONTROLS FOR PORTFOLIO CAPACITY AND CAPABILITY MANAGEMENT

Risk management controls and objectives for portfolio capacity and capability management are provided in Table X3-3.

Table X3-3. Risk Management Controls and Objectives for Portfolio Capacity and Capability Management

Control ID	Control Objective
PF.CAP.1	Risks related to the impact of the portfolio on other activities of the organization and its partners are identified and actively managed throughout the entire portfolio life cycle.
PF.CAP.2	Risks related to other activities of the organization and its partners that impact the portfolio are identified and actively managed throughout the entire portfolio life cycle.
PF.CAP.3	Risks related to availability and performance of key human capital are identified and actively managed throughout the entire portfolio life cycle.
PF.CAP.4	Risks related to availability and stability of key financial capital are identified and actively managed throughout the entire portfolio life cycle.
PF.CAP.5	Risks related to availability and fit for use of the key assets are identified and actively managed throughout the entire portfolio life cycle.
PF.CAP.6	Risks related to the availability and development of key intellectual capital are identified and actively managed throughout the entire portfolio life cycle.
PF.CAP.7	Capacity required to manage risk at the portfolio and its component level is regularly identified, monitored, and (whenever needed) increased or reduced to maintain the optimal level.
PF.CAP.8	Risks related to the culture of the organization and its partners are identified and actively managed throughout the entire portfolio life cycle.
PF.CAP.9	Risks related to the structure of the organization and its partners are identified and actively managed throughout the entire portfolio life cycle.
PF.CAP.10	Risks related to key processes within the organization are identified and actively managed throughout the entire portfolio life cycle.
PF.CAP.11	Whenever partners or suppliers play a significant role in providing portfolio capacity, risks related to their involvement are identified and actively managed throughout the entire portfolio life cycle.
PF.CAP.12	Portfolio, program, and project performance reports, together with KPIs within the organization, are used to identify risks and recognize their potential impact on portfolio capacity and capability as early as possible.
PF.CAP.13	When optimizing portfolio capacity, risks related to the realization of value expected from impacted programs and resulting from projects within the portfolio are identified, analyzed, and acted upon.

The following factors should be considered when identifying risks related to both the impact of the portfolio on other activities of the organization and its partners, and risks related to other activities of the organization and its partners that impact on the portfolio (Control PF.CAP.1 and PF.CAP.2):

- Strategic plans of the organization and its partners,
- KPIs within the organization and its partners,
- Utilization level of organization's and partners' resources,
- Components within partners' portfolios that could impact the involvement of the partner in the organization's components realization,
- Governance across the enterprise,
- Management interfaces between portfolios,
- Management interfaces between the portfolio and senior management,
- Dealing with complexity across organizational structures,
- Dealing with product-, service-, or capability-related complexities as part of the portfolio's component processes, and
- Integration of operations with project and program actions within and external to the portfolio.

The following factors should be considered when identifying risks related to the availability and performance of key human capital (Control PF.CAP.3):

- **Opportunities:**
  - Learning new skills,
  - Personal growth,
  - Promotion, and
  - Development of successors.
- **Threats:**
  - Geographical distribution,
  - Cultural differences,
  - Learning curves,
  - Unavailability of key talent, and
  - Job market competition.

The following factors should be considered when identifying risks related to the availability and performance of financial capital (Control PF.CAP.4):

- Currency rate changes,
- Availability of cash at certain moments in time,
- Timing and results of decisions by key stakeholders providing financial capital,
- Financial condition of the key stakeholders providing financial capital, and
- Changing credit ability of the key stakeholders providing financial capital.

The following factors should be considered when identifying risks related to the availability and fit for use of the key assets (Control PF.CAP.5):

- Other users and priorities of their assignments,
- Procedures of sharing with other users,
- Availability,
- Fit for use, and
- Learning curves.

The following factors should be considered when identifying risks related to the availability and development of key intellectual capital (Control PF.CAP.6):

- Development of unique intellectual capital that could lead to competitive advantage,
- Protection of intellectual capital (e.g., patents, information security), and
- Use of intellectual capital to obtain additional benefits (e.g., selling licenses).

The following types of risk management-related activities should be considered when analyzing the capacity required to manage risk at the portfolio and its component level (Control PF.CAP.7):

- Risk identification, analysis, and monitoring at the portfolio level,
- Responses to risks escalated from components to the portfolio level,
- Responses to risks identified at the portfolio level, and
- Responses to unknown events that might occur for the portfolio and its components.

The following factors should be considered when identifying risks related to the culture of the organization and its partners (Control PF.CAP.8):

- Decision-making culture,
- Ways of working,
- Cooperation style, and
- Reporting culture and power distance.

The following factors should be considered when identifying risks related to the structure of the organization and its partners (Control PF.CAP.9):

- Location of the key portfolio governance and management roles within the organization's structure,
- Clarity of key decision-making roles,
- Conflicts and common objectives between portfolio roles and other roles within the organization,
- Clarity of ownership of the key resources, and
- Integration between the portfolio and operations divisions and roles.

The following process areas should be considered when identifying risks related to the key processes within the organization (Control PF.CAP.10):

- Strategic planning and decision making,
- High-level planning of operations,
- Resource allocation,
- Procurement, and
- Human resource management.

The following factors should be considered when identifying risks related to the involvement of partners and suppliers (Control PF.CAP.11):

- Strategic direction of their development,
- Ability to provide competitive advantage,
- Access to talent and intellectual property,
- Stability,
- Ability to scale,
- Mutual and conflicting objectives,
- Cooperation potential and conflicts with organization's internal structures, and
- Alternative suppliers or products/services.

The following indicators should be considered from the risk perspective when analyzing portfolio, program, and project performance reports, together with KPIs within the organization (Control PF.CAP.12):

- Resource utilization,
- Delivery velocity,
- Cost and schedule performance,
- Turnover ratio,
- Resource and service lead times,
- Amount of open sales leads, and
- Lead conversion ratio.

The following should be considered when identifying, analyzing, and responding to risks associated with optimizing portfolio capacity to realize value (Control PF.CAP.13):

- Balancing of portfolio projects, programs, and operational actions,
- Balancing of related opportunities and threats, and
- Relationship of program benefits or project deliverables to portfolio strategic objectives supporting the delivery of value to the enterprise.

X3.5 RISK MANAGEMENT CONTROLS FOR PORTFOLIO STAKEHOLDER ENGAGEMENT

Risk management controls and objectives for portfolio stakeholder engagement are provided in Table X3-4.

Table X3-4. Risk Management Controls and Objectives for Portfolio Stakeholder Engagement

Control ID	Control Objective
PF.STK.1	Risks related to key portfolio stakeholders are regularly identified and actively managed throughout the entire portfolio life cycle.
PF.STK.2	Decisions to engage certain stakeholders at the portfolio, program, or project level are evaluated from the risk perspective.
PF.STK.3	Risk appetite, attitude, and threshold of key portfolio stakeholders are assessed regularly. Whenever there are differences between the individual's factors just listed and the corresponding organizational factors, related risks are identified and actively managed.
PF.STK.4	Potential interactions and conflicts of interest among key portfolio stakeholders are taken into consideration when identifying risks.
PF.STK.5	Risks related to the selected approach to analysis, categorization, and grouping of stakeholders are identified and addressed when planning Portfolio Stakeholder Engagement.
PF.STK.6	Risks related to selected communication techniques and related communication infrastructure are identified and actively managed throughout the entire portfolio life cycle.
PF.STK.7	Risks related to the scope, frequency, and form of communications at the portfolio level are identified and actively managed throughout the entire portfolio life cycle.

The following factors should be considered when identifying risks related to key portfolio stakeholders (Control PF.STK.1):

- Risk appetite, attitude, and threshold;
- Interests aligned or conflicting with portfolio objectives;
- Personal views and preferences;
- Areas of accountability and related objectives;
- Impact of portfolio benefits on the stakeholder's objectives;
- Level of decision power;
- Ability to influence other stakeholders;

- Stakeholder culture, training, education, and experience;
- Stakeholder biases; and
- Trust between stakeholders.

The following factors should be considered when identifying risks related to decisions to engage certain stakeholders at the portfolio, program, or project level (Control PF.STK.2):

- Stakeholders' ability to influence portfolio capacity and capability,
- Ability to engage and manage a given stakeholder at the portfolio or component level,
- Opportunities and threats from dealing with a given stakeholder at the portfolio level, and
- Opportunities and threats from dealing with a given stakeholder at the component level.

The following factors should be considered when identifying risks related to disconnects between individual key stakeholders and organizational risk appetite, attitude, and threshold (Control PF.STK.3):

- Interests and goals of the stakeholders and organization,
- Key concerns of the stakeholders and organization,
- Key opportunities for the stakeholders and organization,
- Potential stakeholders' strategies to mitigate threats introduced by the portfolio that are unacceptable by them,
- Potential stakeholders' strategies to exploit their opportunities related to the portfolio that are not taken care of by portfolio components.

The following factors should be considered when identifying risks related to potential interactions and conflicts of interest among key portfolio stakeholders (Control PF.STK.4):

- Shared and conflicting objectives,
- Existing and potential coalitions, and
- Personal conflicts.

The following factors should be considered when identifying risks related to the selected approach to analyze, categorize, and group stakeholders (Control PF.STK.5):

- Accuracy and currency of stakeholder-related data,
- Accuracy and completeness of analytical techniques,
- Ability to adequately address all key stakeholders,
- Impact of assumptions, and
- Impact of biases.

The following factors should be considered when identifying risks related to the selected communication techniques and related communication infrastructure (Control PF.STK.6):

- Ability to transmit certain forms of information (e.g., visual, sound, or text),
- Noise level,
- Traceability of information,
- Authentication level,
- Familiarity of stakeholders to use the required techniques and related technology,
- Reliability and availability of the required technology,
- Stakeholder access to the required technology, and
- Stakeholder culture and communication preferences.

The following factors should be considered when identifying risks related to the scope, frequency, and form of communications at the portfolio level (Control PF.STK.7):

- Stakeholder culture and communications preferences;
- Stakeholder training, education, and experience;
- Stakeholder technical capabilities to receive, analyze, and respond to communication;
- Stakeholder bias;
- Management and governance approaches; and
- Trust between stakeholders.

X3.6 RISK MANAGEMENT CONTROLS FOR PORTFOLIO VALUE MANAGEMENT

Risk management controls and objectives for portfolio value management are provided in Table X3-5.

Table X3-5. Risk Management Controls and Objectives for Portfolio Value Management

Control ID	Control Objective
PF.VAL.1	Opportunities to increase value delivery are regularly identified and actively managed throughout the entire portfolio life cycle.
PF.VAL.2	Trends in enterprise environmental factors and changes to organizational process assets are regularly analyzed in order to identify risks that could potentially impact value delivery.
PF.VAL.3	Portfolio is regularly reassessed and balanced from the organizational risk appetite and attitude perspective in order to ensure the right set of portfolio components.
PF.VAL.4	Key portfolio component risks are regularly assessed from the perspective of their impact on delivering expected value.
PF.VAL.5	Techniques used for component performance optimization are assessed from the perspective of risks that can impact value contribution.
PF.VAL.6	Techniques and processes selected for expected value negotiations are evaluated from the risk perspective.

The following factors should be considered when identifying risks related to the opportunities to increase value delivery and the trends in enterprise environmental factors and changes to organizational process assets (Control PF.VAL.1 and Control PF.VAL.2):

- Balancing of threats and opportunities within the portfolio and its component elements,
- Market demand,
- Market share,
- Prices of related product categories,
- Costs of labor and materials, and
- Supply of key talent and materials.

The following factors should be considered when the portfolio is reassessed and balanced from an organizational risk appetite and attitude perspective in order to ensure the right set of portfolio components to maximize delivery of value (Control PF.VAL.3):

- Alignment of component and portfolio vision, goals, and objectives;
- Alignment of individual stakeholder and organizational risk appetite and attitude at the project, program, and portfolio levels; and
- Integration of operational risks into the balancing equation.

The following factors should be considered when key portfolio component risks are assessed from the perspective of their impact on delivering expected value (Control PF.VAL.4):

- Fit of the component scope to enable value realization,
- Continuity of the sponsorship throughout the entire component life cycle,
- Ability to deliver key component deliverables necessary to realize value,
- Timing of delivery at the component level in the context of value opportunity windows, and
- Overall costs at the component level in relation to the business case.

The following factors should be considered when techniques used for component performance optimization are assessed from the perspective of risks that can impact value contribution (Control PF.VAL.5):

- Impact on the value contribution,
- Applicability of techniques to the assessed items,
- Applicability and timeliness of data used in techniques, and
- Acceptance of techniques by stakeholders.

The following factors should be considered when identifying risks related to the techniques and processes selected for expected value negotiations (Control PF.VAL.6):

- Focus on the right value,
- Ability to match the strategic risk appetite and attitude, and
- Inclusion of the appropriate stakeholders.

X3.7 RISK MANAGEMENT CONTROLS FOR PORTFOLIO RISK MANAGEMENT

Risk management controls and objectives for portfolio risk management are provided in Table X3-6.

Table X3-6. Risk Management Controls and Objectives for Portfolio Risk Management

Control ID	Control Objective
PF.RSK.1	Risks related to the selection of a particular risk management approach within the portfolio are identified, analyzed, and considered when developing the portfolio risk management framework and management plans.
PF.RSK.2	Risk management at the portfolio level includes identification and management of general portfolio risks and cumulative effects of component risks.
PF.RSK.3	Risk escalation policies are in place in order to ensure the optimal management of portfolio and component risks and to ensure the correct visibility of component-level risks. This policy is reflected in the management plans at the component level.
PF.RSK.4	There are clear policies for integrating component risk activities with enterprise risk management.

The following factors should be considered when identifying risks related to the selection of a particular risk management approach within the portfolio (Control PF.RSK.1):

- Alignment with enterprise risk management processes,
- Ability to match the organization's strategic risk attitude,
- Ability to deal with expected portfolio complexity,
- Fit to the organizational culture,
- Level of risk transparency,
- Ability to follow the approach by the key stakeholders,
- Fit to the categories and level of risk expected in the portfolio,
- Clarity of integration with risk management approach at the component level, and
- Speed of key processes in comparison with the dynamics of the portfolio environment.

The following factors should be considered to ensure management of general portfolio risks and cumulative effects of component risks (Control PF.RSK.2):

- Management of risks that might occur as a result of the combination of individual component risks, and
- Management of risks that appear only at the portfolio level and are beyond the scope of individual components, even though these components may be within their impact.

The following factors should be considered for risk escalation policies at the level of portfolio (Control PF.RSK.3):

- Level of potential impact,
- Potential interdependencies between portfolio components,
- Risk categories in relation to competencies to handle certain types of risk, and
- Authorization levels of particular portfolio stakeholders.

The following factors should be considered when integrating component risk activities within enterprise risk management (Control PF.RSK.4):

- Placement of risk-related decision authorities,
- Stakeholder lines of communication,
- Risk governance processes, and
- Senior management processes and procedures.

APPENDIX X4
PROGRAM RISK MANAGEMENT CONTROLS

X4.1 THE PURPOSE OF PROGRAM RISK MANAGEMENT CONTROLS

The purpose of risk management within a program is to secure optimal realization of intended program benefits. Risk management controls help to achieve that by seamlessly integrating risk practices into the program life cycle and within all of the performance domains. This approach ensures that risk management becomes a natural part of program management and helps achieve success in benefits delivery by the program.

The selection, tailoring, implementation, and monitoring of particular controls in a given program are a part of the program governance activities. Sections X4.2 through X4.7 provide risk management controls for program risk management along with examples of factors to consider for some of the controls.

X4.2 RISK MANAGEMENT CONTROLS FOR PROGRAM STRATEGY ALIGNMENT

Table X4-1 provides risk management controls for program strategy alignment.

Table X4-1. Risk Management Controls for Program Strategy Alignment

Control ID	Control Objective
PG.STR.1	Overall risks that could have a substantial impact on the program's business case are identified early and addressed in the program business case.
PG.STR.2	Risks related to the program risk management approach are identified and actively managed throughout the entire program life cycle.
PG.STR.3	Environmental assessments are conducted regularly in order to identify program-level risks. Special attention is given to those elements of the environment that could impact the program's critical success factors (CSFs).

The following factors should be considered when identifying overall risks related to the program's business case (Control PG.STR.1):

- Market trends,
- Emergent technologies,
- Emerging products or services alternatives to those delivered by the program,
- Potential regulatory changes, and
- Trends in key cost elements, (e.g., labor, materials, or core services).

The following factors should be considered when identifying risks related to the program risk management approach (Control PG.STR.2):

- Ability to align with the organization's strategic risk appetite,
- Ability to deal with expected program complexity,
- Fit to the organizational culture,
- Level of risk transparency,
- Ability of key stakeholders to follow the approach,
- Fit to the organization's risk tolerance,
- Fit to the categories and level of risk expected in the program,
- Clarity of integration with the risk management approach at the component level,
- Clarity of integration with the risk management approach at the portfolio level, and
- Organization's decision cycle as it relates to the speed of change within the program environment.

X4.3 RISK MANAGEMENT CONTROLS FOR PROGRAM BENEFITS MANAGEMENT

Table X4-2 provides risk management controls for program benefits management.

Table X4-2. Risk Management Controls for Program Benefits Management

Control ID	Control Objective
PG.BNF.1	Opportunities for new benefits that help to meet program objectives are regularly identified and actively managed throughout the entire program life cycle.
PG.BNF.2	Opportunities to realize program benefits in a more efficient and/or effective way are regularly identified and actively managed throughout the entire program life cycle.
PG.BNF.3	Threats that could potentially affect realization of the program benefits are regularly identified and addressed as required before program closure.
PG.BNF.4	Threats that could potentially affect sustainability of the program benefits are regularly identified and addressed as required before program closure.

The following factors should be considered when identifying risks that could potentially affect realization and sustainability of the program benefits (Controls PG.BNF.1, PG.BNF.2, PG.BNF.3, and PG.BNF.4):

- Market conditions,
- Changes in political climate,
- Continuity in leadership after the component completion, and
- Availability of resources to perform operations or other components necessary to realize benefits.

X4.4 RISK MANAGEMENT CONTROLS FOR PROGRAM STAKEHOLDER ENGAGEMENT

Table X4-3 provides risk management controls for program stakeholder engagement.

Table X4-3. Risk Management Controls for Program Stakeholder Engagement

Control ID	Control Objective
PG.STK.1	Risks related to key program stakeholders are regularly identified and actively managed throughout the entire program life cycle.
PG.STK.2	Decisions to engage certain stakeholders at the program or component level are evaluated from a risk perspective.
PG.STK.3	Risks related to potential scope creep caused by key project stakeholders are regularly identified and actively managed throughout the entire program life cycle.
PG.STK.4	Risk attitude of key program stakeholders is regularly assessed. Whenever there are differences between the stakeholders' attitudes and expected program risk levels, related risks are identified and actively managed.
PG.STK.5	Risks related to potential interactions, conflicts of interest, and shared interests among key program stakeholders are regularly identified and actively managed throughout the entire program life cycle.
PG.STK.6	Risks related to the selected categorization approach and methods for stakeholder analysis are identified and addressed when planning Program Stakeholder Engagement.
PG.STK.7	Risks related to selected communication techniques and related communication infrastructure are identified and actively managed throughout the entire program life cycle.
PG.STK.8	Risks related to the scope, frequency, and form of communications at the program level are identified and actively managed throughout the entire program life cycle.

The following factors should be considered when identifying risks related to key program stakeholders and their potential influence on the program scope (Control PG.STK.1 and PG.STK.2):

- Interests aligned or conflicting with program objectives,
- Personal views and preferences,
- Areas of accountability and related program objectives,
- Impact of program benefits on stakeholders' objectives,

- Type and level of decision power, and
- Ability to influence other stakeholders.

The following factors should be considered when evaluating decisions to engage certain stakeholders at the program or component level from the risk perspective (Control PG.STK.3):

- Stakeholders' ability to influence the program's delivery of benefits,
- Ability to engage a given stakeholder at the program or component level,
- Opportunities and threats from dealing with a given stakeholder at the program level, and
- Opportunities and threats from dealing with a given stakeholder at the component level.

The following factors should be considered when identifying and dealing with differences between the stakeholder's risk attitude and expected program risk levels (Control PG.STK.4):

- Organization's and stakeholders' risk attitude,
- Business models of the organization and program stakeholders,
- Potential benefits and threats to the organization's and stakeholders' businesses, and
- Governance processes within and external to the program.

The following factors should be considered when identifying risks related to potential interactions, conflicts of interest, and shared interests among key program stakeholders (Control PG.STK.5):

- Shared and conflicting objectives,
- Existing or potential coalitions,
- Personal conflicts, and
- Organizational governance processes.

The following factors should be considered when identifying risks related to selected communication techniques and related communication infrastructure (Control PG.STK.7):

- Ability to transmit certain forms of information (e.g., visual, sound, or text),
- Noise level,
- Traceability of information,
- Authentication level,

- Familiarity of stakeholders regarding the use of required techniques and related technology,
- Reliability and availability of the required technology,
- Stakeholders' access to the required technology, and
- Organizational governance processes.

X4.5 RISK MANAGEMENT CONTROLS FOR PROGRAM GOVERNANCE

Table X4-4 provides risk management controls for program governance.

Table X4-4. Risk Management Controls for Program Governance

Control ID	Control Objective
PG.GOV.1	Risks related to program governance structures, policies, and procedures are regularly identified, reflected in the program's governance and management documents, and actively managed throughout the entire program life cycle.
PG.GOV.2	Risks resulting from program complexity are regularly identified, reflected in the program's governance and management documents, and actively managed throughout the entire program life cycle.
PG.GOV.3	All program components have effective risk management in place and its effectiveness is monitored on a regular basis.
PG.GOV.4	Clear risk escalation policies are in place in order to ensure the optimal management of program and component risks. These policies are reflected in the management plans at the component level.

The following factors should be considered when identifying risks related to the program governance structures, policies, and procedures (Control PG.GOV.1):

- For program governance structures:
  - Complexity of overall governance structure, including the number of oversight committees,
  - Clearness of accountability,
  - Level of interdependencies,
  - Integration with other structures within the organization, and
  - Degree of key stakeholders' representation.

- For program policies and decision-making processes:
  - Complexity of processes for making a final decision,
  - Transparency,
  - Involvement of key stakeholders,
  - Fairness,
  - Time to make decisions,
  - Information management systems, and
  - Quality mechanisms.

The following factors should be considered when identifying risks resulting from program complexity (Control PG.GOV.2):

- Governance and decision making;
- Amount and diversity of stakeholders and their interests;
- Geographical distribution;
- Amount, nature, and degree of agreement on the definition of benefits;
- Amount, nature, and dynamics of interdependencies;
- Amount, distribution, and dynamics of resources;
- Amount and nature of deliverables;
- Sophistication and dynamics of key processes; and
- Amount, nature, and dynamics of external factors influencing the program.

Risk escalation policies (Control PG.GOV.4) are typically based on:

- Level of potential impact,
- Potential interdependencies between program components,
- Risk categories in relation to competencies to handle certain types of risk, and
- Authorization levels of particular program stakeholders.

X4.6 RISK MANAGEMENT CONTROLS FOR PROGRAM LIFE CYCLE MANAGEMENT

Table X4-5 provides risk management controls for program life cycle management.

Table X4-5. Risk Management Controls for Program Life Cycle Management

Control ID	Control Objective
PG.LFC.1	Program definition phase includes program-level risk identification, analysis, and response planning. All significant risks identified at this stage are addressed by the program governance and management documents and are an integral part of decisions regarding formulation of the program, its objectives, and scope.
PG.LFC.2	Component authorization and planning activities include risk identification, analysis, and response planning. Major component risks are addressed at the earliest possible stage.
PG.LFC.3	Component oversight and integration activities include regular risk identification, analysis, response planning, and monitoring. Program risks potentially caused by the components are identified and addressed as early as possible.
PG.LFC.4	Component transition risks are addressed at the earliest possible stage, preferably before component closure.

The following factors should be considered when designing risk management policies, processes, and structures covering the program life cycle at all levels (Controls PG.LFC.1, PG.LFC.2, PG.LFC.3, and PG.LFC.4):

- Risks resulting from the decided program life cycle itself,
- Nature of risks that could emerge within the program and the ability of dealing with them at various program levels,
- Program complexity and ability to reduce it by dealing with risks at the most effective levels,
- Potential effectiveness of the program and component management in regard to dealing with risk,
- Potential for unknown-unknowns,
- Potential for residual and secondary risks, and
- Effect of high-impact, very low-probability (black swan) events.

X4.7 RISK MANAGEMENT CONTROLS FOR SUPPORTING PROGRAM ACTIVITIES

Table X4-6 provides risk management controls for supporting program activities.

Table X4-6. Risk Management Controls for Supporting Program Activities

Control ID	Control Objective
PG.SUP.1	There are clear policies regarding handling risks within all supporting program activities. As part of these policies, relevant management controls are established within each area of supporting activities.
PG.SUP.2	There are clear policies on what risks related to supporting activities are handled at the component versus the program level, including effective rules for risk escalation.
PG.SUP.3	There are clear policies for integrating program risk activities with enterprise risk management.
PG.SUP.4	There are clear policies for integrating program risk activities with operations risk management.

The following factors should be considered with regard to handling risks within all supporting program activities whether at the program or component level or within the enterprise risk management processes (Controls PG.SUP.1, PG.SUP.2, and PG.SUP.3).

It is important to establish effective policies on risk management within all supporting program activities. Special attention is given to the rules regarding risk handling between the program and its components, including escalation mechanisms. This ensures that there are no areas between the component and program level uncovered by the risk management practices.

Supporting program activities include:

- Program change management,
- Program communications management,
- Program financial management,
- Program information management,
- Program procurement management,
- Program quality management,

- Program resource management,
- Program risk management,
- Program schedule management, and
- Program scope management.

Even though the management of these activities at the program level often differs significantly from the way in which these are managed at the component level, the risk management controls for the supporting program activities are similar in nature to those within the corresponding Knowledge Areas of the project (see Appendix X5).

Although operations generally are not part of program management, the risks associated with operations are addressed as part of program risk management. The integration of operations with a program's component projects is an important part of the benefits realization equation and becomes critical when dealing with certain agile practices where component work and operational tasks overlap. This is especially true in a mixed development and operations environment.

The following factors should be considered when managing risks associated with operations (Control PG.SUP.4):

- Mutual impact of the program on operations and value creation within the organization,
- Integration of project work with the operations environment,
- Decision authority of the project team versus the operations manager, and
- Decision authority of the program manager versus the operations manager.

APPENDIX X5
PROJECT RISK MANAGEMENT CONTROLS

X5.1 THE PURPOSE OF PROJECT RISK MANAGEMENT CONTROLS

The purpose of risk management within projects is to secure the optimal delivery of the unique product, service, or result for which the project was undertaken. Risk management controls help to achieve optimal delivery by seamlessly integrating risk practices into the project life cycle and within all of the Knowledge Areas. This approach ensures that risk management becomes a natural part of project management.

The selection, tailoring, implementation, and monitoring of particular controls in a given project are a part of the governance activities. In all cases where the term risk is used, both residual and secondary risks should be considered when appropriate. Sections X5.2 through X5.11 provide risk management controls for project risk management along with examples of factors to consider for some of the controls.

X5.2 RISK MANAGEMENT CONTROLS FOR PROJECT INTEGRATION MANAGEMENT

Table X5-1 provides risk management controls for Project Integration Management.

Table X5-1. Risk Management Controls for Project Integration Management

Control ID	Control Objective
PR.INT.1	Overall project risks are identified when initiating the project and are taken into consideration when setting the project objectives and scope. This usually occurs as part of the business case analysis and includes analysis of the enterprise environmental factors and trends related to them. Lessons learned from past and current projects are also taken into consideration.
PR.INT.2	Organization of the planning processes is analyzed to identify potential risks resulting from inconsistent or incomplete project management planning and/or inaccurate or incomplete baselines.
PR.INT.3	Opportunities to continuously improve the delivery of project deliverables are regularly identified at all project levels.
PR.INT.4	When making decisions on change requests, risks related to implementing or rejecting a change are taken into consideration.
PR.INT.5	When making decisions on change requests, risks related to implementing certain sets of changes at the same time or implementing them separately are taken into consideration.
PR.INT.6	Whenever approval or denial of change requests introduces new risks into the project, these risks are handled in accordance with agreed processes for project risk management.
PR.INT.7	Before closing a project, risks related to the ability to realize the business case are reevaluated and their management is ensured to continue after project closure.

The following factors should be considered when identifying risks related to organization of the planning processes and opportunities to continuously improve the delivery of project deliverables (Controls PR.INT.2 and PR.INT.3):

- Use of a continuous process improvement effort as part of an integrated quality program,
- Reaction of stakeholders,
- Experience level of team members,
- Maturity of project teams,
- Project life cycle approach (i.e., predictive, iterative, incremental, or agile), and
- Ability to address project complexity.

The following factors should be considered when identifying risks related to implementing or rejecting a change (Control PR.INT.4):

- Reaction of stakeholders,
- Impact on further deliverable approvals,
- Impact on other work,
- Unexpected additional costs or possibilities of cost reduction,
- Contractual consequences, and
- Regulatory consequences.

The following factors should be considered when identifying risks related to implementing certain sets of changes at the same time or implementing them separately (Control PR.INT.5):

- Interaction between changes,
- Impact on project complexity,
- Resource availability and capability, and
- Ability to manage multiple changes at once.

X5.3 RISK MANAGEMENT CONTROLS FOR PROJECT SCOPE MANAGEMENT

Table X5-2 provides risk management controls for Project Scope Management.

Table X5-2. Risk Management Controls for Project Scope Management

Control ID	Control Objective
PR.SCP.1	Risks related to the project life cycle are taken into consideration when planning Project Scope Management.
PR.SCP.2	Risks resulting from environmental factors are taken into consideration when planning Project Scope Management and developing the scope baseline.
PR.SCP.3	Risks related to the approach and methods used for collecting, documenting, and updating requirements are taken into consideration when planning requirements management.
PR.SCP.4	Risks related to the approach and method selected for product and project scope definition, decomposition, validation, and control are taken into consideration when planning Project Scope Management.
PR.SCP.5	Work performance information from scope control activities is regularly analyzed in order to identify potential new risks and detect materialization of previously identified risks.

The following factors should be considered when identifying risks related to the project life cycle (Control PR.SCP.1):

- For predictive life cycles:
  - Level of expertise to specify scope,
  - Predictability of the scope,
  - Ability to anticipate future requirements,
  - Ability to predict or control enterprise environmental factors,
  - Impact on ability to react to new opportunities that might arise during project execution, and
  - Use of planning packages and "rolling wave" planning.
- For iterative and incremental life cycles:
  - Stakeholders' readiness to operate with limited scope definition,
  - Availability of decision makers to make scope decisions regularly,
  - Ability to react timely to the results and lessons learned from previous iterations,
  - Readiness of stakeholders to receive partial results,
  - Ability to decompose scope into work packages that could be executed within agreed cycles, and
  - Impact on ability to react to new opportunities that might arise during project execution.
- For adaptive life cycles, in addition to those for iterative and incremental life cycles:
  - Ability to actively manage ongoing scope definition,
  - Readiness for accepting frequent major changes as the project progresses, and
  - Ability to deal with interdependencies in progressively developed scope.

The following factors should be considered when identifying risks resulting from environmental factors (Control PR.SCP.2):

- Changing market conditions,
- Changing political climate, and
- Changing regulatory requirements.

The following factors should be considered when identifying risks related to the approach and method used for collecting, documenting, and updating requirements (Control PR.SCP.3):

- Level of engagement of particular stakeholders,
- Stakeholders' availability and willingness to cooperate,
- Stakeholders' experience in the area,

- Stakeholders' ability to predict their future needs,
- Stakeholders' ability to express their needs,
- Impact of the requirements collection process on stakeholders' expectations,
- Cognitive biases,
- Limitations of the chosen form of documentation,
- Ability to confirm the requirements by relevant stakeholders once they are documented,
- Ability to understand the requirements by those planning and executing project work, and
- Fundamental difference between high-level user or operational requirements and lower-level design or engineering requirements.

The following factors should be considered when identifying risks related to the approach and method selected for product and project scope definition, decomposition, validation, and control (Control PR.SCP.4):

- Impact of the scope decomposition approach on the ability to accomplish the following:
  - Delegation work,
  - Aggregation work,
  - Cooperation,
  - Optimization of resource usage, and
  - Monitoring other aspects of the project, such as time and cost.
- Impact of the documentation approach on the ability to accomplish the following:
  - Respond to changes,
  - Describe product and work in accurate and unambiguous way, and
  - Distribute up-to-date scope documents to relevant stakeholders.
- Ability to understand the scope by those who will execute project work,
- Ability to monitor progress objectively and unambiguously, and
- Ability to prevent scope creep and gold plating.

The following factors should be considered when identifying risks related to work performance information from scope control activities (Control PR.SCP.5):

- Report tailoring, and
- Information and data delivery channels.

X5.4 RISK MANAGEMENT CONTROLS FOR PROJECT SCHEDULE MANAGEMENT

Table X5-3 provides risk management controls for Project Schedule Management.

Table X5-3. Risk Management Controls for Project Schedule Management

Control ID	Control Objective
PR.SCH.1	Risks related to the project life cycle are taken into consideration when planning Project Schedule Management.
PR.SCH.2	Risks resulting from environmental factors are taken into consideration when planning Project Schedule Management and developing the project schedule baseline.
PR.SCH.3	Risks related to the approach and method selected for estimation of activities' duration are taken into consideration when planning Project Schedule Management.
PR.SCH.4	The risks related to the approach and method selected for sequencing activities are taken into consideration when planning Project Schedule Management.
PR.SCH.5	The risks related to the approach and method selected for schedule development and control are taken into consideration when planning Project Schedule Management.
PR.SCH.6	Work performance information from the schedule control activities is regularly analyzed in order to identify potential new risks and detect materialization of previously identified risks.

The following factors should be considered when identifying risks related to the project life cycle (Control PR.SCH.1):

- For predictive life cycles:
  - Predictability of the scope,
  - Ability to estimate duration and resource needs of the future activities,
  - Ability to predict availability and capability of resources,
  - Ability to predict and control enterprise environmental factors, and
  - Use of planning packages and "rolling wave" planning.

- For iterative and incremental life cycles:
  - Stakeholders' readiness to operate on the general milestone schedule,
  - Availability of decision makers to make decisions regularly and on time,
  - Ability to deliver meaningful increments within the agreed duration of the life cycle,
  - Ability to react in a timely manner to the results and lessons learned from previous iterations,
  - Ability of key stakeholders, including suppliers, to keep sustainable pace, and
  - Ability to handle tasks that, due to their nature, take longer than the agreed life cycle.
- For adaptive life cycles, in addition to those for iterative and incremental life cycles:
  - Stakeholders' readiness to operate within a changing environment, and
  - Ability to deal with interdependencies in a progressively developed schedule.

The following factors should be considered when identifying risks resulting from environmental factors (Control PR.SCH.2):

- Natural environment conditions,
- Availability of key resources,
- Timeliness of external decision making,
- Conflicts with other components of the program or portfolio, and
- Conflicts with external events.

The following factors should be considered when identifying risks related to the approach and methods selected for estimation of activities' duration (Control PR.SCH.3):

- Selection and competence level of experts,
- Availability and credibility of data sources,
- Familiarity with selected tools and techniques of estimation,
- Adequacy of estimation models,
- Historical accuracy of similarly estimated durations, and
- Estimating approach.

The following factors should be considered when identifying risks related to the approach and method selected for sequencing activities (Control PR.SCH.4):

- Level of interdependencies,
- Stakeholders' risk appetite and attitude levels,
- Likelihood of changes,
- Impact of potential delays and accelerated deliveries,
- Impact of the resource constraints,
- Impact of increasing work backlogs, and
- Impact of work in progress.

The following factors should be considered when identifying risks related to the approach and method selected for schedule development and control (Control PR.SCH.5):

- Ability to cover relevant aspects of scheduling in the particular project such as:
  - Planning in time,
  - Managing interdependencies,
  - Managing resource allocation,
  - Managing logistics, and
  - Handling reserves.
- Familiarity with the tools used, as measured by the following:
  - Ability to address project complexity,
  - Ability to use the tools to optimize the schedule,
  - Ability to integrate planning efforts with other key stakeholders,
  - Ability to deliver in a timely manner relevant performance data for key stakeholders, and
  - Ability to visualize schedule and progress.

X5.5 RISK MANAGEMENT CONTROLS FOR PROJECT COST MANAGEMENT

Table X5-4 provides risk management controls for Project Cost Management.

Table X5-4. Risk Management Controls for Project Cost Management

Control ID	Control Objective
PR.CST.1	Risks related to project life cycle are taken into consideration when planning Project Cost Management.
PR.CST.2	Risks resulting from environmental factors are taken into consideration when planning Project Cost Management and developing the cost baseline.
PR.CST.3	Risks related to the approach and method selected for cost estimation are taken into consideration when planning Project Cost Management.
PR.CST.4	Risks related to the approach and method selected for determining budget and cost control are taken into consideration when planning Project Cost Management.
PR.CST.5	Work performance information from cost control activities is regularly analyzed in order to identify potential new risks and detect materialization of the previously identified risks.

The following factors should be considered when identifying risks related to the project life cycle (Control PR.CST.1):

- For predictive life cycles:
  - Predictability of the scope,
  - Ability to estimate duration and resource needs of the future activities,
  - Stakeholders' readiness to provide financing without immediate benefits,
  - Ability to predict and control enterprise environmental factors, and
  - Use of planning packages and "rolling wave" planning.
- For iterative and incremental life cycles:
  - Stakeholders' readiness to provide financing for partially met customer or user requirements during an incremental development,
  - Availability of decision makers to make decisions regularly and on time,
  - Unequal level of funding required in specific iterations or increments, and
  - Ability to react timely to the results and lessons learned from previous iterations or increments.

- For adaptive life cycles, in addition to those for iterative and incremental life cycles:
  - Stakeholders' readiness to provide financing within a changing environment, and
  - Ability to deal with unexpected expenses in a progressively developed budget.

The following factors should be considered when identifying risks resulting from environmental factors (Control PR.CST.2):

- Partners' and suppliers' need for financing,
- Market conditions,
- Costs of materials and resources,
- Currency rates,
- Stakeholders' ability to provide financing,
- Policies of financing organizations, and
- Contractual conditions.

The following factors should be considered when identifying risks related to the approach and methods selected for cost estimation (Control PR.CST.3):

- Selection and competence level of experts,
- Availability and credibility of data sources,
- Familiarity with selected tools and techniques of estimation,
- Adequacy of estimation models, and
- Historical accuracy of similarly estimated costs.

The following factors should be considered when identifying risks related to the approach and methods selected for determining budget and cost control (Control PR.CST.4):

- Ability to cover relevant aspects of financial management in the particular project, such as:
  - Planning for, monitoring of, and allocating costs to particular work packages or planning packages;
  - Planning, monitoring, and allocating expenses in time;
  - Planning, monitoring, and allocating of cash flow;
  - Handling settlements;
  - Handling multi-currency operations; and
  - Handling reserves.

- Ability to match costs with scope and schedule performance,
- Familiarity with the tools used,
- Ability to address project complexity,
- Ability to use the tools to optimize the budget,
- Ability to integrate planning efforts with other key stakeholders,
- Ability to deliver in a timely fashion the relevant performance data for key stakeholders, and
- Ability to visualize the budget and its condition in key areas.

X5.6 RISK MANAGEMENT CONTROLS FOR PROJECT QUALITY MANAGEMENT

Table X5-5 provides risk management controls for Project Quality Management.

Table X5-5. Risk Management Controls for Project Quality Management

Control ID	Control Objective
PR.QLT.1	Risks related to project life cycle are taken into consideration when planning Project Quality Management.
PR.QLT.2	Risks resulting from environmental factors are taken into consideration when planning Project Quality Management.
PR.QLT.3	Risks related to the approach and method selected for managing quality are taken into consideration when planning Project Quality Management.
PR.QLT.4	Risks related to the approach and method selected for quality control are taken into consideration when planning Project Quality Management.
PR.QLT.5	Opportunities for continuous process improvement are identified and actively managed throughout the entire project life cycle, including implementation of accessible and effective decision-making processes in this area.
PR.QLT.6	Work performance information from quality control activities is regularly analyzed in order to identify potential new risks and detect materialization of the previously identified risks.

The following factors should be considered when identifying risks related to the project life cycle (Control PR.QLT.1):

- For predictive life cycles:
  - Predictability of the scope,
  - Ability to determine stakeholders' quality requirements,
  - Ability of decision makers to make quality-related decisions supporting the project's change management system,
  - Ability to deliver within the agreed quality metrics,
  - Ability to determine or predict regulatory requirements on quality, and
  - Use of planning packages and "rolling wave" planning.
- For iterative, incremental, and adaptive life cycles:
  - Ability to define quality requirements while having a limited predictability of the scope,
  - Availability of decision makers to make quality-related decisions regularly and on time,
  - Ability to deliver within the agreed quality metrics and delivery cycles,
  - Ability to timely determine regulatory requirements on quality of evolving deliverables,
  - Ability to ensure that regulatory requirements regarding results are met whenever deliverables are handed over for use, and
  - Ability to react timely to the results and lessons learned from previous iterations or increments.

The following factors should be considered when identifying risks resulting from environmental factors (Control PR.QLT.2):

- Potential changes to regulations, norms, and standards;
- Natural environment conditions potentially impacting quality (fitness for use);
- Ability of third parties to deliver quality and adapt to potential changes; and
- Availability of independent third parties to control quality.

The following factors should be considered when identifying risks related to the approach and methods selected for managing quality (Control PR.QLT.3):

- Distribution of attention between prevention (assurance), detection (control), and corrective actions;
- Extent to which stakeholders are involved in quality efforts;
- Motivation or mobilization means used to drive quality efforts;
- Availability and correctness of data for data-driven quality management; and
- Availability of quality visualization tools and techniques.

The following factors should be considered when identifying risks related to the approach and methods selected for managing quality (Control PR.QLT.4):

- Ability to select and measure key quality metrics,
- Accuracy of measurements,
- Effectiveness of sampling,
- Ability to observe trends in quality metrics, and
- Existence and effectiveness of root-cause identification methods.

The following techniques should be used for identifying opportunities for process improvement (Control PR.QLT.5):

- Plan-Do-Check-Act (PDCA) cycle,
- Quality circles,
- Regular project retrospectives,
- Lessons learned,
- Lean management, and
- Theory of constraints.

X5.7 RISK MANAGEMENT CONTROLS FOR PROJECT RESOURCE MANAGEMENT

Table X5-6 provides risk management controls for Project Resource Management.

Table X5-6. Risk Management Controls for Project Resource Management

Control ID	Control Objective
PR.RES.1	Risks related to project life cycle are taken into consideration when planning Project Resource Management and resource needs.
PR.RES.2	Risks resulting from environmental factors are taken into consideration when planning Project Resource Management and resource needs.
PR.RES.3	Risks related to the approach and method selected for resource estimation are taken into consideration when planning Project Resource Management and resource needs.
PR.RES.4	Risks related to the approach and method selected for resource acquisition are taken into consideration when planning Project Resource Management and resource needs.
PR.RES.5	Risks related to the approach and method selected for team development and management are taken into consideration when planning Project Resource Management and are managed throughout the entire project life cycle.
PR.RES.6	Work performance information from resource control activities is regularly analyzed in order to identify potential new risks and detect materialization of previously identified risks.

The following factors should be considered when identifying risks related to the project life cycle (Control PR.RES.1):

- For predictive life cycles:
  - Predictability of the scope,
  - Ability to predict resource needs,
  - Ability to predict resource availability,
  - Ability to predict resource capability,
  - Ability to change resource ability or capability in response to potential changes, and
  - Use of planning packages and “rolling wave” planning.

- For iterative, incremental, and adaptive life cycles:
  - Stakeholders' readiness to engage resources flexibly,
  - Availability of decision makers to make resource decisions regularly,
  - Readiness of the project team to operate in a changing environment, and
  - Ability of the project team to maintain a sustainable pace.

The following factors should be considered when identifying risks resulting from environmental factors (Control PR.RES.2):

- General availability of resources needed,
- Historical resource availability cycles,
- Other initiatives that might impact resource availability,
- Market conditions for key resources such as talent, materials, and equipment, and
- Competition over key resources.

The following factors should be considered when identifying risks related to the approach and method selected for resource estimation (Control PR.RES.3):

- Selection and competence level of experts,
- Availability and credibility of data sources,
- Familiarity with selected tools and techniques of estimation,
- Adequacy of estimation models, and
- Historical accuracy of similarly estimated durations.

The following factors should be considered when identifying risks related to the approach and method selected for resource acquisition (Control PR.RES.4):

- Effectiveness of the acquisition techniques under given conditions,
- Impact of project's acquisition efforts on resource costs,
- Ability to verify key resource characteristics,
- Project information security in the context of acquisition communications,
- Ability to sustain knowledge and intellectual property in the context of contractual conditions, and
- Acquisition lead times.

The following factors should be considered when identifying risks related to the approach and method selected for team development (Control PR.RES.5):

- Degree to which team members already know each other,
- Existing relations in the team,
- Psychological characteristics of the team members,
- Management style of the project manager and organization stakeholders,
- Corporate climate and organizational process assets,
- Natural motivators of the team members,
- Mobilization systems in the organization,
- Time and resources available for team building,
- Geographical distribution of the team,
- Amount of time the team will spend together,
- Available communications technologies,
- Ability to effectively deal with conflicts, and
- Cultural differences.

X5.8 RISK MANAGEMENT CONTROLS FOR PROJECT COMMUNICATIONS MANAGEMENT

Table X5-7 provides risk management controls for Project Communications Management.

Table X5-7. Risk Management Controls for Project Communications Management

Control ID	Control Objective
PR.COM.1	Risks related to the project life cycle are taken into consideration when planning Project Communications Management.
PR.COM.2	Risks resulting from environmental factors are considered when planning Project Communications Management.
PR.COM.3	Risks resulting from the potential impact of certain information or data being delivered or withheld from certain stakeholders are taken into consideration when planning Project Communications Management.
PR.COM.4	Risks related to approach and method selected for communications management and monitoring are taken into consideration when planning Project Communications Management.
PR.COM.5	Work performance data from communications monitoring activities are regularly analyzed in order to identify potential new risks and detect materialization of previously identified risks.

The following factors should be considered when identifying risks related to the project life cycle (Control PR.COM.1):

- For predictive life cycles:
  - Ability to predict communications needs of the stakeholders,
  - Ability to respond to unexpected events and changes, and
  - Stakeholders' readiness to receive and respond to communications as agreed.
- For iterative, incremental, and adaptive life cycles:
  - Ability to continuously adapt communications to the changing project environment, and
  - Stakeholders' readiness to regularly receive and respond to communications in line with the dynamics of the delivery cycle.

The following factors should be considered when identifying risks resulting from environmental factors (Control PR.COM.2):

- Communication of other key stakeholders, including:
  - Competition,
  - Government,
  - Nongovernment organizations, and
  - Local community leaders.
- Background information and noise, and
- Impact of media.

The following factors should be considered when identifying risks resulting from the potential impact of certain information or data being delivered to or withheld from certain stakeholders (Control PR.COM.3):

- Importance of provided information or data from the stakeholders' perspectives,
- Scope of information or data necessary for stakeholders to engage in a desired way,
- Importance to deliver a given piece of information or data from the project's perspective,
- Consequences of withholding information or data and immediate delivery of information,
- Consequences of hiding and communicating information or data, and
- Regulatory and contractual requirements and consequences.

The following factors should be considered when identifying risks related to the approach and methods selected for communications management and monitoring (Control PR.COM.4):

- Scope of information or data necessary for the stakeholder to engage in a desired way;
- Cultural differences and preferences to use certain styles and methods of communication;
- Available communication technologies and expected technological advancement;
- Advantages and limitations of certain communication channels, techniques, and tools;
- Communication competencies of key project stakeholders;
- Availability of information or data when needed by stakeholders; and
- Possibility of information or data overload, taking into consideration communications from other simultaneous projects.

X5.9 RISK MANAGEMENT CONTROLS FOR PROJECT RISK MANAGEMENT

Table X5-8 provides risk management controls for Project Risk Management.

Table X5-8. Risk Management Controls for Project Risk Management

Control ID	Control Objective
PR.RSK.1	Risks related to project life cycle are taken into consideration when planning Project Risk Management.
PR.RSK.2	Risks related to the ability to determine the level of key stakeholders' risk appetite or attitude and the levels of their appetite or attitude are taken into consideration when planning Project Risk Management.
PR.RSK.3	Risks related to approach and methods selected for risk identification, analysis, and monitoring are taken into consideration when planning Project Risk Management.
PR.RSK.4	Lessons learned from past and current projects are taken into consideration when identifying project risks and ways to respond to them.
PR.RSK.5	Work performance reports are used continuously to identify potential new risks and reevaluate risks identified previously.
PR.RSK.6	Secondary and residual risks are identified, analyzed, and addressed when planning risk responses.
PR.RSK.7	Risk responses are reflected in all relevant project management plans and baselines.
PR.RSK.8	Work performance information from risk monitoring activities is regularly analyzed in order to evaluate effectiveness of the risk management, identify potential new risks, and reevaluate or detect the materialization of previously identified risks.
PR.RSK.9	Outputs from risk monitoring activities are used to continuously improve the project's approach and methods used for risk management.
PR.RSK.10	Risk information and data for effective decision making are available and adequate to the complexity of the project.

The following factors should be considered when identifying risks related to the project life cycle (Control PR.RSK.1):

- For predictive life cycles:
  - Predictability of scope,
  - Ability to predict and control enterprise environmental factors,
  - Ability to identify and manage risks in key project areas,
  - Stakeholders' willingness to invest in uncertain elements of the project that are expected to be predictable, and
  - The use of planning packages and "rolling wave" planning.
- For iterative and incremental life cycles:
  - Availability of decision makers to make risk-related decisions regularly and on time,
  - Stakeholders' readiness to provide financing for risks identified as the project progresses, and
  - Ability to react in a timely manner to the results and lessons learned from previous iterations.
- For adaptive life cycles, in addition to those for iterative and incremental life cycles:
  - Stakeholders' readiness to deal with largely unpredictable risks, and
  - Stakeholders' readiness to operate without detailed, long-term risk analysis.

The following factors should be considered when identifying risks related to the approach and method selected for risk identification, analysis, and monitoring (Control PR.RSK.3):

- Ability to identify risks in all key areas;
- Ability to focus on the right risks;
- Accuracy of risk information or data from the perspective of the ability to plan precise risk responses;
- Expertise needed to effectively identify, analyze, and monitor risks in certain areas;
- Accountability for managing risks in key areas of the project; and
- Continuity and regularity of the identification, analysis, and monitoring processes.

X5.10 RISK MANAGEMENT CONTROLS FOR PROJECT PROCUREMENT MANAGEMENT

Table X5-9 provides risk management controls for Project Procurement Management.

Table X5-9. Risk Management Controls for Project Procurement Management

Control ID	Control Objective
PR.PRO.1	Risks related to the project life cycle are taken into consideration when planning Project Procurement Management.
PR.PRO.2	Risks resulting from environmental factors are taken into consideration when planning Project Procurement Management.
PR.PRO.3	Make-or-buy decisions include risk identification and analysis. The risks resulting from these decisions are managed according to the risk management plan.
PR.PRO.4	Risks related to the proposed supplier selection criteria are taken into consideration when planning Project Procurement Management.
PR.PRO.5	Risks related to the proposed contract types are taken into consideration when planning Project Procurement Management. The risks resulting from the final agreements are managed according to the risk management plan.
PR.PRO.6	Risks related to the approach and method selected for conducting procurements are taken into consideration when planning Project Procurement Management.
PR.PRO.7	Risks related to approach and method selected for controlling procurements and nature of proposed potential follow-up strategies are taken into consideration when planning Project Procurement Management.
PR.PRO.8	Work performance information from procurement control activities, especially the suppliers' performance and the nature of claims, is regularly analyzed in order to identify potential new risks and detect materialization of previously identified risks.

The following factors should be considered when identifying risks related to the project life cycle (Control PR.PRO.1):

- For predictive life cycles:
  - Predictability of the scope,
  - Use of planning packages and "rolling wave" planning, and
  - Ability to predict and control enterprise environmental factors, especially market conditions, availability of the suppliers when needed, and availability of goods and services when needed.

- For iterative, incremental, and adaptive life cycles:
  - Ability to purchase long-lead-time goods and services,
  - Ability to purchase goods and services while having limited scope information in advance,
  - Availability of decision makers to make procurement-related decisions regularly and on time,
  - Ability to evaluate and use new suppliers on short notice,
  - Ability to conduct procurements in a timely manner to ensure the execution of the project is not slowed by the process,
  - Flexibility of the supplier contracts, and
  - Ability to react in a timely manner to the results and lessons learned from previous iterations.

The following factors should be considered when identifying risks resulting from environmental factors (Control PR.PRO.2):

- General availability of goods and services needed,
- Availability of sellers,
- Historical goods and services availability cycles,
- Other initiatives that might impact goods and services availability,
- Market conditions for key goods and services to acquire,
- Competition over key goods and services, and
- Regulatory requirements when purchasing certain goods and services.

The following factors should be considered when identifying risks related to and resulting from make-or-buy decisions (Control PR.PRO.3):

- Competence and intellectual property needs,
- Availability of capability and capacity,
- Degree of control over delivery,
- Impact on other project activities and deliverables, and
- Risks related to specific third parties considered in the process.

The following factors should be considered when identifying risks related to the proposed supplier selection criteria (Control PR.PRO.4):

- Ability to balance cost and quality requirements,
- Ability to address supplier's willingness and ability to tighten cooperation,
- Ability to recognize historical performance of the supplier,
- Ability to integrate into team-level actions to support small team work in near real time,
- Ability to recognize supplier's culture, and
- Degree to which criteria cover risk areas that are planned to be transferred to the supplier.

The following factors should be considered when identifying risks related to the contract types (Control PR.PRO.5):

- Willingness and ability of customer and supplier to manage certain types of risks,
- Level of risk balance between parties,
- Adequacy of the contract scope to the project needs,
- Secondary risks of transferring certain risks contractually,
- Residual risk on the customer side after transferring some part of the risk contractually, and
- Adequacy of the contract to the project life cycle, especially considering responsibilities, approach to scope management, and performance metrics.

The following factors should be considered when identifying risks related to the approach and methods for conducting procurements (Control PR.PRO.6):

- Ability to create a level playing field between suppliers,
- Ability to finalize procurements on time,
- Ability to attract the right suppliers,
- Flexibility to address opportunities and threats arising during the process,
- Opportunity to use suppliers' expertise to provide optimal solution,
- Ability to recognize actual quality of purchased goods or services, and
- Ability to meet regulatory requirements when purchasing given goods or services.

The following factors should be considered when identifying risks related to the approach and methods selected for controlling procurements and nature of proposed potential follow-up strategies (Control PR.PRO.7):

- Criticality of goods or services from the project perspective;
- Experience and competence level of the supplier;
- Nature of control with a focus on the balance between preventive, detective, and corrective actions;
- Adequacy of the performance metrics to the selected project life cycle;
- Level of trust; and
- Impact on relations.

X5.11 RISK MANAGEMENT CONTROLS FOR PROJECT STAKEHOLDER MANAGEMENT

Table X5-10 provides risk management controls for Project Stakeholder Management.

Table X5-10. Risk Management Controls for Project Stakeholder Management

Control ID	Control Objective
PR.STK.1	Risks related to project life cycle are taken into consideration when planning Project Stakeholder Management.
PR.STK.2	Risks resulting from environmental factors are taken into consideration when planning Project Stakeholder Management.
PR.STK.3	Risks related to the approach and method selected for monitoring and managing stakeholder engagement are taken into consideration when planning Project Stakeholder Management.
PR.STK.4	Information from Project Stakeholder Management control activities is regularly analyzed in order to identify potential new risks and detect materialization of previously identified risks.

The following factors should be considered when identifying risks related to the project life cycle (Control PR.STK.1):

- For predictive life cycles:
  - Ability to identify and engage key stakeholders early,
  - Stakeholders' ability and willingness to predict their future requirements,

- Stakeholders' readiness to invest time in planning efforts,
- Stakeholders' ability and willingness to deal with potential mistakes in the planning stage of the project, and
- Stakeholders' understanding and willingness to deal with potential risks that could disturb predictability.

◆ For iterative and incremental life cycles:

- Stakeholders' willingness to accept an incomplete definition of product scope,
- Stakeholders' readiness to work with partially defined and incomplete deliverables, and
- Stakeholders' ability to react to the results and lessons learned from previous iterations in a timely manner.

◆ For adaptive life cycles, in addition to those for iterative and incremental life cycles:

- Ability to deal with unexpected new stakeholders appearing as the project evolves,
- Stakeholders' readiness to work with largely undefined deliverables, and
- Stakeholders' readiness to operate without a predictive long-term budget and schedule tied to specific deliverables.

The following factors should be considered when identifying risks resulting from environmental factors (Control PR.STK.2):

◆ Potential mutual impact of key external stakeholders, including:

- Suppliers,
- Competition,
- Government,
- Nongovernment organizations,
- Local community leaders, and
- Media.

◆ Organizational structures;

◆ Organizational risk tolerance, capacity, and appetite;

◆ Trends in market conditions;

◆ Trends in political climate; and

◆ Trends in regulatory requirements.

The following factors should be considered when identifying risks related to the approach and methods selected for monitoring and managing stakeholder engagement (Control PR.STK.3):

- Stakeholders' willingness to engage in a desired manner,
- Impact on stakeholders' ability to deliver,
- Cooperation culture,
- Impact on overall relations,
- Level of trust,
- Maturity of individuals,
- Team maturity,
- Risk attitude and appetite of individuals,
- Cultural differences,
- Advantages and limitations of certain engagement methods, and
- Availability of personnel to manage stakeholder engagement.

APPENDIX X6
TECHNIQUES FOR THE RISK MANAGEMENT FRAMEWORK

Many techniques are in widespread use to support risk management processes. This appendix provides examples and highlights some of the most common and effective techniques that support the risk management life cycle. This information is not intended to explain the techniques in detail but to list their most important characteristics. Those who are interested in learning more are encouraged to seek additional sources of information.

There are three major types of techniques: templates and lists, process techniques, and quantitative techniques. Templates and lists are designed to reflect industry and internal benchmarks and best practices as well as lessons learned. Process techniques make it easier to manage the risk management process and range from basic documents and spreadsheets to automated processes. Quantitative techniques support the analytical aspect of considering options and consequences in definitive terms.

The following sections describe some of the more popular techniques for each stage of the risk management framework. This list is not exhaustive, and several techniques are useful for more than one stage. Section X6.8 maps techniques to risk management stages where they may be useful. Some techniques are useful for more than one stage.

X6.1 RISK MANAGEMENT PLANNING

Plan Risk Management defines the approach to be followed for managing risks throughout the life cycle of the corresponding portfolio, program, or project. Planning sessions are recommended in order to build a common understanding of the risk approach between stakeholders and to gain agreement on the techniques to be used for managing risk. The risk management planning phase is usually supported by templates. The results of risk management planning are documented in the risk management plan. An overview of the key areas of focus is provided in Figure X6-1.

People	Tools	Business
Attitudes	Toolbox	Constraints
Roles, responsibilities, authority	Parameters	Amount of detail and effort
Communications	Definitions	

Figure X6-1. Key Areas of Focus for Plan Risk Management

Depending upon the size and complexity of the work, some or all of the following elements are present in a risk management plan:

- Introduction,
- Portfolio, program, or project description,
- Risk management methodology,
- Risk management organization,
- Roles, responsibilities, and authority,
- Stakeholder risk appetite,
- Criteria for success,
- Risk management techniques and guidelines for use,
- Thresholds and corresponding definitions,
- Templates,
- Communications management plan,
- Strategy, and
- Risk breakdown structure.

There are several software tools available to assist with risk management planning. While not discussed here, many of the techniques listed in the following sections are incorporated in risk management software.

X6.2 IDENTIFY RISKS

Risk identification is carried out in order to develop a comprehensive list of all known uncertainties that could have an effect on the portfolio, program, or project. All risk identification techniques have strengths and weaknesses. Best practices suggest using more than one technique to identify risks to compensate for any one technique's shortcomings and to increase risk identification rates. The main assumption in identifying risks is that biases and an array of human behavior patterns stand in the way of identifying unknown risks, identifying the wrong risks, or emphasizing or prioritizing the wrong risks. Some risk identification techniques are more helpful in identifying threats than opportunities or vice versa. It is important to balance the techniques used to target both threats and opportunities.

Whichever risk identification techniques are used, it is important that identified risks are unambiguously described in order to ensure that the risk process is focused on the actual risks and not distracted or diluted by nonrisks. Use of structured risk descriptions can ensure clarity. Risk metalanguage offers a useful way of distinguishing a risk from its cause(s) and effect(s) by describing each risk using a three-part statement in the following form: "As a result of *cause*, risk may occur, which would lead to *effect*." The relationship between cause, risk, and effect is shown in Figure X6-2.

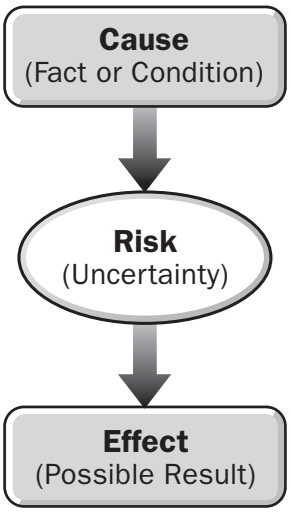


Figure X6-2. The Relationship between Cause, Risk, and Effect

Risks can be identified based on checklists and templates, individual assessments, group risk assessments, external risk identification, etc. Individual assessments are performed by a single individual, whether an expert, stakeholder, or other participant. Individual risk assessments can be combined to create the overall risk register. Outside risk assessments can be generated by the enterprise risk management (ERM) function within the organization or provided by an outside source, such as a customer or supplier.

Sections X6.2.1 through X6.2.14 describe some of the common techniques for risk identification. Refer to Section X6.8 for other risk management framework stages where the technique may prove useful as well.

X6.2.1 ASSUMPTIONS AND CONSTRAINTS ANALYSIS

Assumptions are used to determine risk impact. They are statements accepted as true but need to be validated and continually reviewed during the iteration process and throughout the risk management work related to portfolio, program, and project life cycles. This technique requires three steps: (1) list; (2) test the validity; and (3) identify impacts on project, program, or portfolio. An example is shown in Figure X6-3.

Assumption or Constraint	Could this assumption/constraint prove false? (Y/N)	If false, would it affect project? (Y/N)	Convert to a risk?

Figure X6-3. Example of a Constraint Analysis with Fields for Description and Analysis Results

Another way of approaching assumption and constraint analysis is to use the following logic sequence:

- List the assumption or constraint.
- Test the assumptions or constraint by asking two questions:
  - Could the assumption/constraint be false?
  - If it were false, would one or more objectives be affected (positively or negatively)?
- Where both questions are answered "Yes," generate a risk, for example, in the form: <*Assumption/constraint*> may prove false, leading to <*effect on objective(s)*>.

X6.2.2 BRAINSTORMING

Brainstorming is a technique for generating spontaneous ideas either individually or from a group of people. When brainstorming is used as a group risk identification method, the ideas and thoughts of one individual serve to stimulate ideas in the other participants.

X6.2.3 CAUSE AND EFFECT (ISHIKAWA) DIAGRAMS

The cause and effect diagram or fishbone diagram (see Figure X6-4) is used to display root causes of risk visually, allowing deeper understanding of the source and likelihood of potential problems. The content is organized into a branching diagram where the causes may themselves have multiple potential sources so that the overview on risk stimulates additional thinking. The cause and effect diagram is also used to identify quality-related problems.

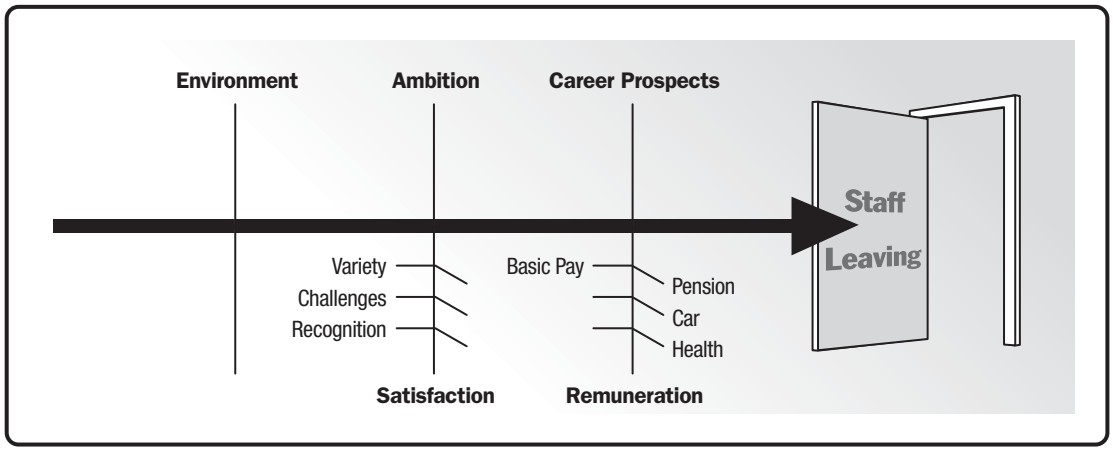


Figure X6-4. Example of a Cause and Effect or Ishikawa Diagram

X6.2.4 CHECKLISTS

Risk identification checklists can be developed based on historical information and knowledge that has been accumulated from previous, similar portfolios, programs, or projects and from other sources of information. The lowest level of a risk breakdown structure can also be used as a risk checklist. An example of a checklist is shown in Figure X6-5.

RISK CATEGORY	SUBCATEGORY	EXAMPLE RISKS	Could this risk affect our project? **Yes, No Don't know, Not applicable**
1. TECHNICAL RISK	1.1 Scope definition	Scope changes may arise during project.	
		Redundant scope may be discovered.	
		Etc...	
	1.2 Technical interfaces	Etc...	

Figure X6-5. Example (Partial) of a Checklist with Typical Structure of Category, Subcategory, Specific Risks, and Effect

While a checklist can be quick and simple, it is impossible to build an exhaustive one. Care should be taken to explore items that do not appear on the checklist. The checklist should be reviewed during closure to improve it for use in the future.

X6.2.5 DELPHI TECHNIQUE

The Delphi technique uses a facilitated anonymous polling of subject matter experts to identify risks in their area of expertise. The facilitator gathers the experts' initial responses and circulates them without attribution to the entire group. The group members may then revise their contributions based on those of others. The process often generates a consensus of the experts after a few iterations.

X6.2.6 DOCUMENT REVIEW

A structured review may be performed of documentation, including plans, assumptions, prior portfolio, program, or project files, and other information. The quality of the plans, as well as consistency between those plans and the assumptions, can be indicators of risk.

X6.2.7 EXPERT JUDGMENT

Expert judgment is the contribution provided to risk identification based on expertise in a subject area, industry segment, organizational processes, etc.

X6.2.8 FACILITATION

Facilitation is the ability to effectively guide a group event to a successful decision, solution, or conclusion. A facilitator ensures that there is effective participation and that all contributions are considered.

X6.2.9 HISTORICAL INFORMATION

Historical records and data from past projects, programs, and portfolios help to identify common risks and prevent repeating mistakes.

X6.2.10 INTERVIEWS

Interviewing experienced project, program, or portfolio participants, stakeholders, and subject matter experts can identify risks. Interviews are one of the main sources of risk identification data gathering.

X6.2.11 PROMPT LISTS

Prompt lists enumerate risk categories with the purpose of detecting the most relevant to the project, program, or portfolio. A prompt list can be useful as a framework for brainstorming and interviews. Categories of risks include:

- Technical risks,
- Organizational risks, and
- External risks.

There are different types of prompt lists. Figure X6-6 provides examples of some of the better-known ones.

PESTLE	TECOP	SPECTRUM
Political	**T**echnical	**S**ocio-cultural
Economic	**E**nvironmental	**P**olitical
Social	**C**ommercial	**E**conomic
Technological	**O**perational	**C**ompetitive
Legal	**P**olitical	**T**echnology
Environmental		**R**egulatory/legal
		Uncertainty/risk
		Market

Figure X6-6. Three Well-Known Examples of Prompt Lists That Can Be Useful for Risk Identification

X6.2.12 QUESTIONNAIRE

Questionnaire techniques encourage broad thinking to identify risks; however, it requires quality questions to be effective.

X6.2.13 ROOT-CAUSE ANALYSIS

Root-cause analysis helps to identify additional, dependent risks. The identified risks may be related because of their common root causes. Root-cause analysis can be the basis for development of preemptive and comprehensive responses and can serve to reduce apparent complexity. One way of diagramming root cause is shown in Figure X6-7.

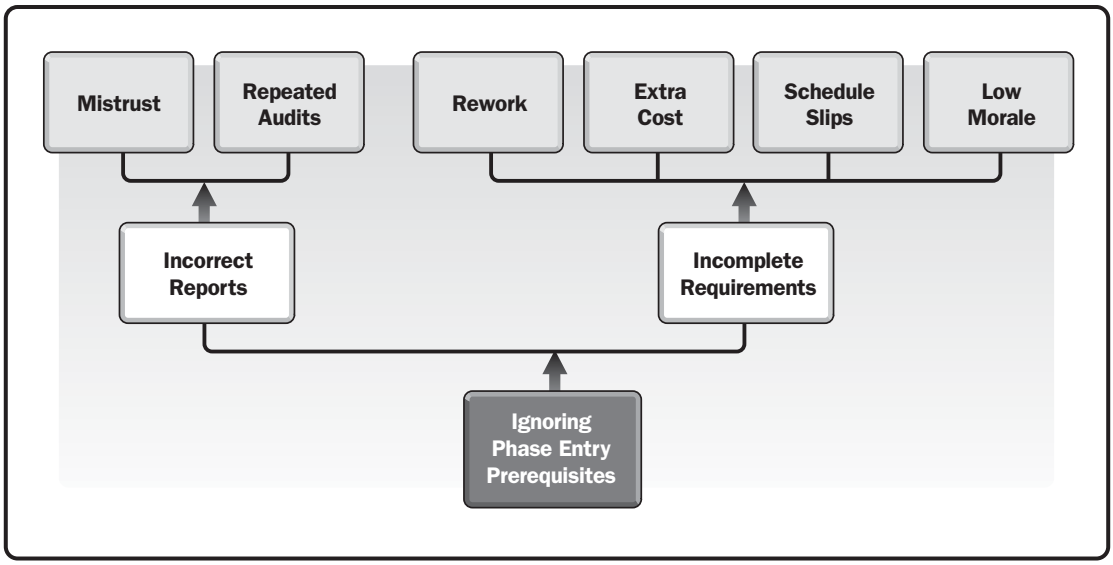


Figure X6-7. Example of a Root-Cause Analysis

X6.2.14 SWOT ANALYSIS

SWOT (strength, weakness, opportunity, and threat) is a technique that examines the initiative from each of the SWOT perspectives to increase the breadth of considered risks. It ensures equal focus on both threats and opportunities. This technique focuses on internal (organizational strengths and weaknesses) and external (opportunities and threats) factors. A method for structuring the results of a SWOT analysis is shown in Figure X6-8.

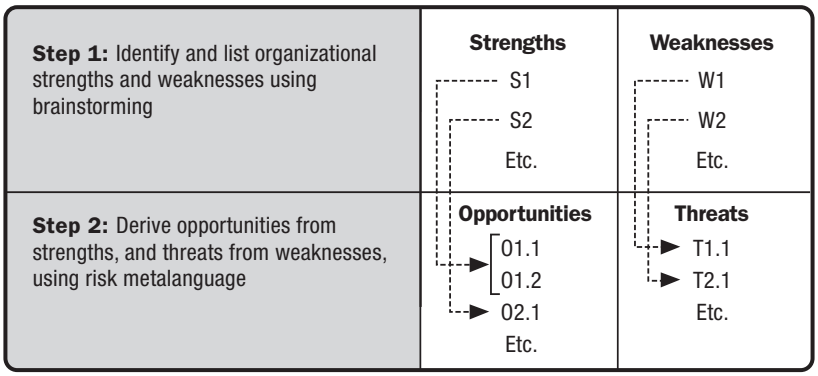


Figure X6-8. Example of a SWOT Analysis Structure

X6.3 QUALITATIVE RISK ANALYSIS

Qualitative risk analysis prioritizes the undifferentiated list of risks that have been identified in the Identify Risks process for further evaluation or for handling. Organizations tend to apply resources to those designated as *high risk* based on their priority, often indicated by the risks' probability and impact characteristics. Qualitative risk analysis techniques are usually based on probability and impact but can also include additional prioritization variables. It is recommended to have a consistent, well-defined prioritization technique to maintain consistency among raters. An example of a rating definition schema is shown in Figure X6-9.

SCALE	PROBABILITY	± IMPACT ON PROJECT OBJECTIVES		
		TIME	COST	QUALITY
VHI	61–99%	>40 days	>US$200K	Very significant impact on overall functionality
HI	41–60%	21–40 days	US$101K–US$200K	Significant impact on overall functionality
MED	21–40%	11–20 days	US$51K–US$100K	Some impact in key functional areas
LO	11–20%	6–10 days	US$11K–US$50K	Minor impact on overall functionality
VLO	1–10%	1–5 day	US$1K–US$10K	Minor impact on secondary functions
NIL	<1%	No change	No change	No change in functionality

Figure X6-9. Example of Definitions for Levels of Probability and Impact on Three Specific Objectives Used to Evaluate Individual Risks

Sections X6.3.1 and X6.3.7 describe some common techniques for qualitative risk analysis.

X6.3.1 AFFINITY DIAGRAMS

An affinity diagram is used to organize specific ideas or factors that contribute to a risk. It helps to sort risks by similarities or generic risk categories.

X6.3.2 ANALYTIC HIERARCHY PROCESS

Analytic hierarchy process (AHP) is a matrix method-based technique used to support a multicriteria decision-making process. It can also be used to identify risks. Even though there is an objective ranking where the subjectivity is minimized, the grouping is arbitrary. An example is shown in Figure X6-10.

Preference Factors	
1	Equally Preferred
2	Mildly Preferred
3	Moderately Preferred
4	Greatly Preferred
5	Always Preferred

Input Matrix (Preference Factors)				
	Cost	Time	Scope	Quality
Cost	1.00	0.25	0.33	0.20
Time	4.00	1.00	1.00	0.25
Scope	3.00	1.00	1.00	0.25
Quality	5.00	4.00	4.00	1.00

Note: Preference Factors input into the Dark Gray Area. Principal Diagonal is 1.0 by definition.
Other cells calculated as 1 / preference factor for same objectives.

Calculated Factors (Preference Factor/Column Total)					Weighting Factors
	Cost	Time	Scope	Quality	Average of Row
Cost	0.08	0.04	0.05	0.12	0.1
Time	0.31	0.16	0.16	0.15	0.2
Scope	0.23	0.16	0.16	0.15	0.2
Quality	0.38	0.64	0.63	0.59	0.6
Sum	13.00	6.25	6.33	1.70	1.0

Figure X6-10. Example of Analytic Hierarchy Process Computations to Determine the Relative Weighting of Four Objectives Related to a Project

X6.3.3 INFLUENCE DIAGRAMS

An influence diagram is a diagrammatic representation of a situation showing the main entities, decision points, uncertainties, and outcomes, indicating the relationships (influences) between them. When combined with sensitivity analysis or Monte Carlo simulation, the influence diagram can identify risks to reveal their sources.

X6.3.4 NOMINAL GROUP TECHNIQUE

The nominal group technique is an adaptation of brainstorming where participants share and discuss all issues before evaluation, with each participant participating equally in evaluation.

X6.3.5 PROBABILITY AND IMPACT MATRIX

A probability and impact matrix allows the user to prioritize risks for further analysis or responses. It helps to distinguish between those risks that will have a minor impact on business activities and those that will have a major impact. It usually classifies risks according to their impact probability, such as very high, high, moderate, low, and very low. An example of a probability and impact matrix is shown in Figure X6-11.

Probability and Impact Risk Ranking											
Probability	**Threats**					**Opportunities**					**Probability**
VH	L	M	M	H	H	H	H	M	M	L	VH
H	L	L	M	H	H	H	H	M	L	L	H
M	L	L	M	H	H	H	H	M	L	L	M
L	L	L	L	M	H	H	M	L	L	L	L
VL	L	L	L	L	M	M	L	L	L	L	VL
	VL	L	M	H	VH	VH	H	M	L	VL	
	Impact (Threats)					**Impact (Opportunities)**					

Figure X6-11. Example of Probability-Impact Matrix Used to Sort Risks into Very High (VH), High (H), Moderate (M), Low (L), and Very Low (VL) Classes

X6.3.6 RISK DATA QUALITY ANALYSIS

Results of the risk analysis are only as good as the data collected. Review of the reliability and sufficiency of the data ensures that the analysis is based on high-quality information. Data that are deemed to be of lesser quality may be further researched or excluded from the risk analysis. Care should be taken when excluding poor quality data to avoid a less-than-robust qualitative analysis.

X6.3.7 ASSESSMENT OF OTHER RISK PARAMETERS

Other characteristics of risk (in addition to probability and impact) can be considered when prioritizing risks for further analysis and action. These characteristics may include but are not limited to:

- **Urgency.** The period of time within which a response to a risk is to be implemented in order to be effective. A short period indicates high urgency.
- **Proximity.** The period of time before a risk might have an impact on one or more objectives. A short period indicates high proximity.
- **Detectability.** The ease with which the results of a risk occurring, or being about to occur, can be detected and recognized. When the risk occurrence can be detected easily, detectability is high.
- **Dormancy.** The period of time that may elapse after a risk has occurred before its impact is discovered. A short period indicates low dormancy.
- **Manageability.** The ease with which a risk owner (or owning organization) can manage the occurrence or impact of a risk. When management is easy, manageability is high.
- **Controllability.** The degree to which a risk owner (or owning organization) is able to control the risk's outcome. When the outcome can be controlled easily, controllability is high.
- **Connectivity.** The extent to which a risk is related to other individual risks. When a risk is connected to many other risks, connectivity is high.
- **Strategic impact.** The potential for a risk to have a positive or negative effect on the organization's strategic goals. When a risk has a major effect on strategic goals, strategic impact is high.
- **Stakeholder impact.** The degree to which a risk is perceived to matter by one or more stakeholders. When a risk is perceived as very significant, stakeholder impact is high.

X6.3.8 SYSTEM DYNAMICS

System dynamics (SD) is a particular application of influence diagrams and can be used to further identify risks within a given situation. The SD model represents entities and information flows, and analysis of the model can reveal feedback and feed-forward loops that lead to uncertainty or instability. In addition, the results of an SD analysis can show the impact of risk events on overall results. Analyses of changes in the model or assumptions can indicate the system's sensitivity to specific events, some of which may be risks.

System dynamics exposes unexpected interrelationships between elements (feedback and feed-forward loops). It can generate counterintuitive perspectives not available through other techniques. The result is a view of the overall impact of all included risks.

X6.4 QUANTITATIVE RISK ANALYSIS

Quantitative risk analysis is used to determine the overall risk to objectives when all risks potentially operate simultaneously. Techniques used appropriately for quantitative risk analysis have several characteristics: comprehensive risk representation, overall risk impact calculation, probability models, data-gathering capabilities, effective presentation of quantitative analysis results, and iteration capabilities. Quantitative risk analysis techniques enable representation of both opportunities and threats to the objectives.

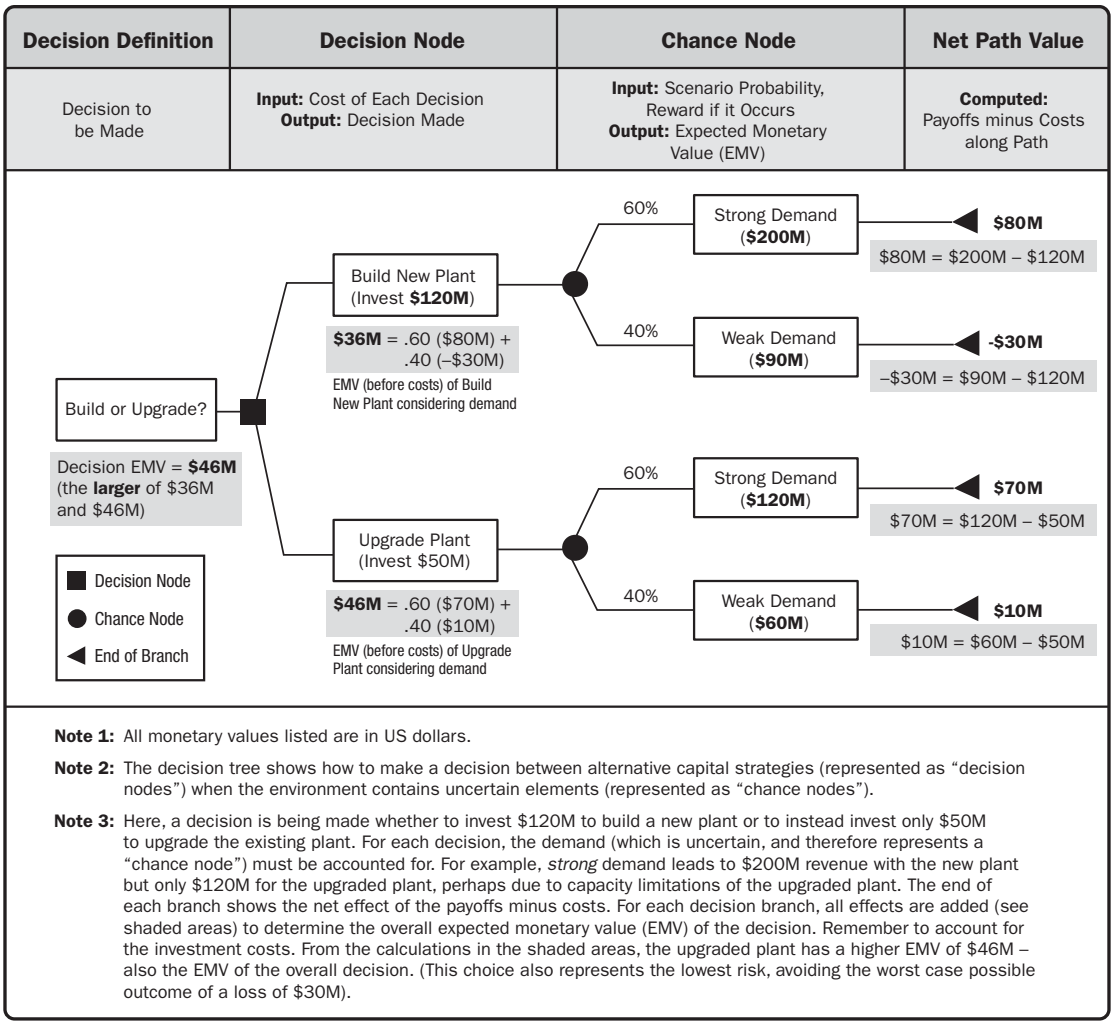
Sections X6.4.1 through X6.4.7 describe some common techniques useful for quantitative risk analysis.

X6.4.1 CONTINGENCY RESERVE ESTIMATION

All of the conditional response plans, as well any of the residual risks will, if they occur, have an effect on objectives. An amount (time and cost) needs to be set aside to allow for these eventualities. This amount is made up of two components: (1) amounts to cover specific, approved conditional responses (e.g., contingency plans) and (2) amounts to address unspecified or passively accepted risks. Quantitative methods can be used to determine the amounts that should be set aside. These reserves are tracked and managed as part of the Monitor Risks process.

X6.4.2 DECISION TREE ANALYSIS

Decision tree analysis is used to determine partial and global probabilities of occurrence. It is a tree-like model that calculates the expected monetary value (see Section X6.4.4) of different possibilities by probability of occurrence. A simple example of a decision tree is shown in Figure X6-12.



Note 1: All monetary values listed are in US dollars.

Note 2: The decision tree shows how to make a decision between alternative capital strategies (represented as "decision nodes") when the environment contains uncertain elements (represented as "chance nodes").

Note 3: Here, a decision is being made whether to invest $120M to build a new plant or to instead invest only $50M to upgrade the existing plant. For each decision, the demand (which is uncertain, and therefore represents a "chance node") must be accounted for. For example, *strong* demand leads to $200M revenue with the new plant but only $120M for the upgraded plant, perhaps due to capacity limitations of the upgraded plant. The end of each branch shows the net effect of the payoffs minus costs. For each decision branch, all effects are added (see shaded areas) to determine the overall expected monetary value (EMV) of the decision. Remember to account for the investment costs. From the calculations in the shaded areas, the upgraded plant has a higher EMV of $46M – also the EMV of the overall decision. (This choice also represents the lowest risk, avoiding the worst case possible outcome of a loss of $30M).

Figure X6-12. Example of a Decision Tree Diagram (Source: *PMBOK® Guide* [4])

X6.4.3 ESTIMATING TECHNIQUES APPLIED TO PROBABILITY AND IMPACT

The probability of a risk occurring can be specified in several different ways. One common way is to assign levels of risk probability by ranges of probability. One benefit of this approach is that the subject matter experts only need to assess a risk's probability within a range rather than as a specific value.

Examples of impact-level definitions are very work specific. The values used to specify the level of impact from very low to very high (if a 5×5 matrix is being used) should be:

- Designated as higher impact for threats or opportunities as they move from very low to very high for a specific objective,
- Defined by the organization as causing the same amount of pain or gain for each level across objectives, and
- Tailored or scaled by stakeholders to the specific work. The definitions, appropriately tailored, can be used for opportunities and threats.

If a risk's impact is uncertain and could be assigned to more than one level of impact (e.g., from moderate to high), the analyst may choose to assign the risk to the impact level that represents the expected or average impact. Alternatively, the risk may be flagged for extra analysis in order to reduce the range of uncertainty to fit within a single range.

X6.4.4 EXPECTED MONETARY VALUE

Expected monetary value (EMV) is a statistical technique that is used to quantify risks, which in turn assists the manager in calculating the contingency reserve. EMV is a calculation of a value, such as weighted average or expected cost or benefit, when the outcomes are uncertain. All reasonable alternative outcomes are identified. Their probabilities of occurring (summing to 100%) and their values are estimated. The EMV calculation is made for the entire event by weighting the individual possible outcomes by their probabilities of occurring. The formula is:

Expected monetary value (EMV) = Probability × Impact

X6.4.5 FMEA/FAULT TREE ANALYSIS

Failure modes and effects analysis (FMEA) or fault tree analysis uses a model structured to identify the various elements that can cause system failure by themselves, or in combination with others, based on the logic of the system. Fault tree analysis is often used in engineering contexts. It can be adapted for use to identify risks by analyzing how risk impacts might arise, or the probability of failure (or of reliability, mean time between failure, etc.) of the overall system, indicating the level of quality of the system or product. If the level of reliability is not acceptable, the fault tree can indicate where the system can be made more reliable; therefore, it is useful in the design and engineering phase of a program or project.

Failure-mode effect analysis assesses and analyzes the potential reliability of a system and/or products. It is used together with failure-mode effect and criticality analysis as part of the general program to assess reliability of a system and potential failure modes.

Using historical data, the analysis of similar products/services, warranty data, customer data complaints, and any other information available may lead to the use of inferential statistics, mathematical modeling, simulations, concurrent engineering, and reliability engineering to identify and define possible failures.

Failure-mode effect and criticality analysis (FMECA) is the logical extension of FMEA. It evaluates the criticality and probability of occurrence of the failure modes.

X6.4.6 MONTE CARLO SIMULATION

Monte Carlo simulation is a technique to simulate probability distribution for a risk on an objective. The statistical method samples events to determine the average behavior of a system.

Monte Carlo simulation is a statistical analysis technique that can be applied in situations in which there are uncertain estimates, with the aim of reducing the level of uncertainty through a series of simulations. In this sense, it can be applied in the analysis of risks associated with a particular objective. For each of the variables, Monte Carlo simulations do not provide a single estimate, but a range of possible estimates associated with each estimate and the level of probability that that estimate is accurate (confidence level) as shown in Figure X6-13.

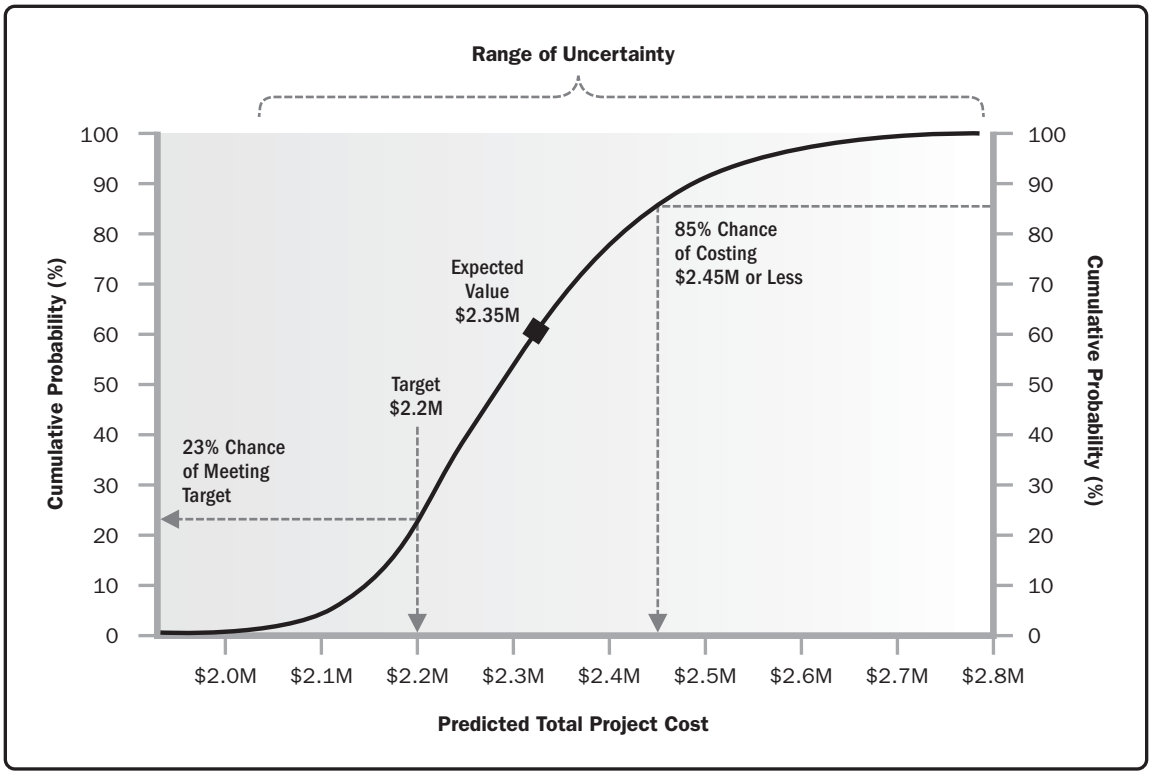


Figure X6-13. Example Histogram from Monte Carlo Simulation of a Project Schedule (Note—all monetary values are given in US dollars)

X6.4.7 PERT (PROGRAM OR PROJECT EVALUATION AND REVIEW TECHNIQUE)

A time-based technique that can be used to quantify risks at a given point in the development of a project or program.

X6.5 PLAN RISK RESPONSES

Plan Risk Responses develops the set of actions required to consider the risks and their characteristics and integrates them into corresponding plans and budgets. The resultant plan should satisfy the risk appetites and attitudes of the key stakeholders. There are three categories of techniques, as follows:

- Creativity techniques to identify potential responses,
- Decision-support techniques for determining the optimal potential response, and
- Implementation techniques designed to turn a risk response into action.

Respectively, these categories of techniques can be used to identify potential responses, select the most appropriate response to translate strategy into planning, and assign corresponding actions.

Identifying potential responses by a variety of creativity techniques are quite similar to risk identification techniques (see Section X6-2). Decision-support techniques assist in examining the trade-off between risk response strategies. Such techniques also assist in choosing between preemptive prevention and contingency responses based on triggers.

Sections X6.5.1 through X6.5.5 describe a few decision-support techniques that may be used for the Plan Risk Response process.

X6.5.1 CONTINGENCY PLANNING

For specific (normally high-impact) risks, the risk owner may choose to assemble a team to develop a response as if the risk had genuinely happened. The corresponding plan, with the supporting information, is then documented and approved by management or the sponsor. This approval includes authorization to deploy the corresponding resources if the predefined trigger conditions arise.

X6.5.2 FORCE FIELD ANALYSIS

Force field analysis is typically used in the change management context. It can be adapted for risk response planning by identifying driving forces (forces for change) and restraining forces (forces against change) which currently affect achievement of an objective. Risk responses can then be modeled based on the net result of the forces as shown in Figure X6-14.

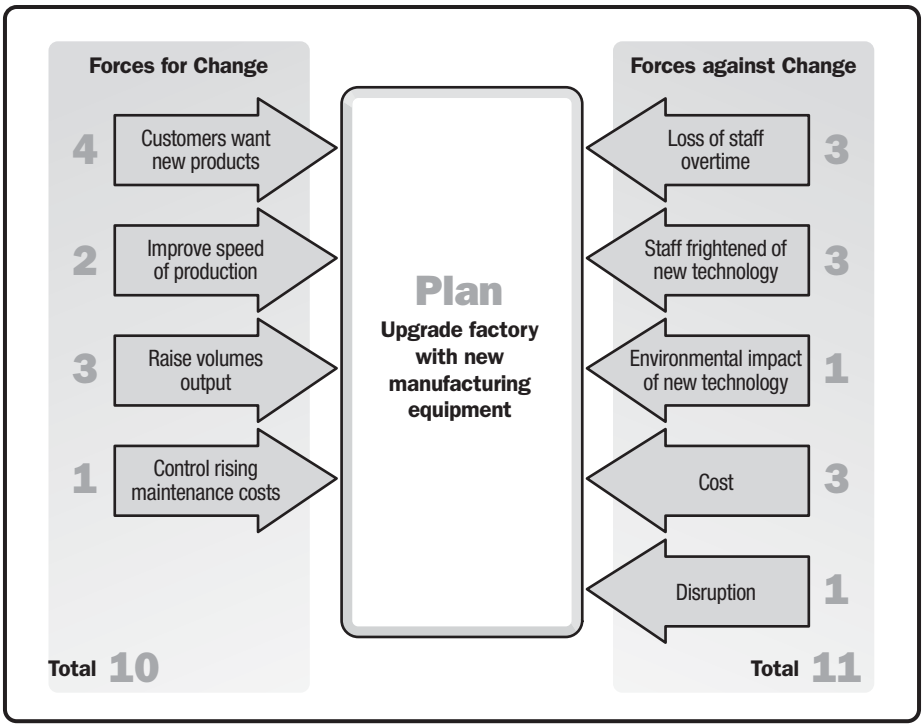


Figure X6-14. Example of a Force Field Analysis and the Balance of Forces for and against Change

X6.5.3 MULTICRITERIA SELECTION TECHNIQUE

Criteria for deciding whether to choose a specific risk response from among several options include cost, schedule, technical requirements, etc., as well as the risk attributes, such as the type of risk, magnitude of probability, and impact. Multicriteria selection could be weighted to reflect the importance of various criterion as shown in Figure X6-15.

Criterion	Weight	Option A		Option B	
		Rating	Points	Rating	Points
Price	9	8	72	10	90
Functionality	9	5	45	8	72
Ease of use	6	9	54	7	42
Lead time	7	9	63	6	42
Scores			**234**		**246**

Figure X6-15. Example of Multicriteria Weighting and Analysis

X6.5.4 SCENARIO ANALYSIS

Scenario analysis for risk response planning involves defining several plausible alternative scenarios. Each scenario may require different risk responses that can be described and evaluated for their cost and effectiveness. If the organization can choose between several scenarios, the alternatives, including responses, can be compared. If the scenarios are out of the control of the organization, the analysis can lead to effective and necessary contingency planning.

Scenarios usually include optimistic, most likely, and pessimistic assessments. The representation of optimistic and pessimistic scenarios can be useful in providing managers with a certain sensitivity to the upside and downside potential associated with a portfolio, program, or project.

X6.5.5 SIMULATION

Simulation is a technique to estimate the benefits and implications of different response plans versus the efforts and costs required to implement them. Simulations can also help analyze the possible implications to the critical chain in projects when implementing different risk response options.

X6.6 RESPONSE PLAN IMPLEMENTATION

The most common technique to turn preventative response plans into action is adding them to the portfolio, program, or project management plan. While some planning techniques can keep track of and differentiate between tasks and actions that originated from response plans, some planning techniques will not differentiate between risk response tasks and other tasks.

X6.7 MONITOR RISKS

Monitor Risks provides the assurance that risk responses are being applied, verifies whether they are effective, and, as necessary, initiates corrective actions. Sections X6.7.1 through X6.7.10 describe techniques for monitoring risks during the entire portfolio, program, or project life cycle.

X6.7.1 DATA ANALYTICS

Data analytics supports the exploration of known risk types by analyzing related documentation and related data for applicability to a specific portfolio, program, or project. In direct data analytics, the question and types of risks explored are predefined, as are the relationships between different types of risks and cause and effect. The use of big data, advanced analytics, or artificial intelligence capabilities to explore unknown types of risks are forms of advanced data analytics.

X6.7.2 RESERVE ANALYSIS

Reserve analysis is an analytical technique to determine the essential features and relationships of components in the work management plan to establish a reserve for the schedule duration, budget, estimated cost, or funds. Tracking the state of the reserve through execution provides summary information as to the evolution of the status of the corresponding risks. This information can be useful when reporting up the organization management structure. In addition, once a risk occurs or ceases to be current (i.e., when it can no longer impact), the corresponding reserve needs to be reviewed to assess whether it still provides the agreed-upon level of confidence.

X6.7.3 RESIDUAL IMPACT ANALYSIS

Response plan implementation could lead to residual risks or an emergent risk. Residual impact analysis is used to identify side effects of implementing a response plan.

X6.7.4 RISK AUDIT

Risk audits are carried out in order to evaluate the following:

- Risk management rules are being carried out as specified, and
- Risk management rules are adequate for controlling the work.

Appendixes X3, X4, and X5 discuss metrics useful for developing and defining management controls for portfolio, program, and project risk management governance. These management controls then become criteria against which an audit is conducted.

X6.7.5 RISK BREAKDOWN STRUCTURE

The risk breakdown structure (RBS) is a hierarchical framework of potential sources of risk. An organization may develop a generic or specific RBS. The RBS helps to identify specific risks in relation to its category and offers a framework for other risk identification techniques such as brainstorming. An RBS helps to ensure coverage of all types of risk and tests for blind spots or omissions. An example of a generic RBS for a project is shown in Figure X6-16.

RBS LEVEL 0	RBS LEVEL 1	RBS LEVEL 2
ALL SOURCES OF PROJECT RISK	1. TECHNICAL RISK	1.1 Scope definition
		1.2 Requirements definition
		1.3 Estimates, assumptions, and constraints
		1.4 Technical processes
		1.5 Technology
		1.6 Technical interfaces
		Etc.
	2. MANAGEMENT RISK	2.1 Project management
		2.2 Program/portfolio management
		2.3 Operations management
		2.4 Organization
		2.5 Resourcing
		2.6 Communication
		Etc.
	3. COMMERCIAL RISK	3.1 Contractual terms and conditions
		3.2 Internal procurement
		3.3 Suppliers and vendors
		3.4 Subcontracts
		3.5 Client/customer stability
		3.6 Partnerships and joint ventures
		Etc.
	4. EXTERNAL RISK	4.1 Legislation
		4.2 Exchange rates
		4.3 Site/facilities
		4.4 Environmental/weather
		4.5 Competition
		4.6 Regulatory
		Etc.

Figure X6-16. Example of a Generic Risk Breakdown Structure for a Project

X6.7.6 RISK REASSESSMENT

Risk reassessment requires the following activities to be estimated and validated again to assure effective control:

- Identifying new risks,
- Evaluating current risks,
- Evaluating the risk management processes, and
- Closing risks.

X6.7.7 SENSITIVITY ANALYSIS

Sensitivity analysis is the evaluation of the effect on a variable by one or more influencing variables. Often used as a technique in monitoring risks, it serves to identify the possible impact on a given objective should one or more risks materialize.

X6.7.8 STATUS MEETINGS

Status meetings include the review of all open risks and trigger conditions that have occurred, leading to risks becoming issues. Risks responded to in the past period, effectiveness of the actions taken, impacts on the portfolio, program, or project, and lessons learned are formally recorded in a knowledge management system.

X6.7.9 TREND ANALYSIS

Trend analysis evaluates how the risk profile changes over time, whether or not the previous actions resulted in the expected effect, and whether or not additional actions are required.

X6.7.10 VARIANCE ANALYSIS

The analysis of variances compares planned versus actual results. When the variances are increasing, there is increased uncertainty and risk. Outcomes from this analysis may forecast any potential for future deviation from the baseline plan prior to completion. Deviation from the baseline plan may indicate the potential impact of threats or opportunities.

X6.8 RISK MANAGEMENT TECHNIQUES RECAP

Table X6-1 lists techniques for carrying out risk management in portfolios, programs, and projects. The list is not exhaustive, and it is not necessary to use all of the techniques.

The column headings list the risk management processes discussed in Section 4 of the standard and indicate a few of the strengths and weaknesses of each technique. Within each cell, the letters indicate a subjective evaluation of the relevance of each technique for the risk management process. In Table X6-1, the "C" stands for *core* and means that the use of that technique is recognized as useful in the context of a given process; the "S" stands for *supportive* and means that the technique can provide some useful information for a given process.

Table X6-1. Matrix of Risk Management Techniques Mapped to Risk Management Life Cycle Stages

Technique	Risk Identification	Qualitative Analysis	Quantitative Analysis	Response Planning	Risk Monitoring	Strengths	Weaknesses
Affinity diagrams		S		S		• Allows for grouping of ideas by common attributes	• May miss nuances of individual risks
Analytic hierarchy process		C	S			• Assists in developing a relative weighting for objectives that reflects the organization's priorities • Assists the creation of an overall priority list of risks created from the risks' priority with respect to individual objectives	• Organizational decisions are often made by committees, and individuals may not agree on the relative priority among objectives • Difficult to gather the information about pair-wise comparison of the objectives from high-level management
Assessment of other risk parameters		C		S	S	• Gives additional perspectives on risks • Helps to plan actions in the right time • Helps to identify additional needs for monitoring mechanisms	• Might make the qualitative analysis more complicated
Assumptions and constraints analysis	C	S			S	• Simple, structured approach • Can be based on assumptions and constraints already listed in the charter • Generates work-specific risks	• Implicit/hidden assumptions or constraints are often missed
Brainstorming	C			S		• Allows all participants to speak their mind and contribute to the discussion • Can involve all key stakeholders • Creative generation of ideas	• Requires attendance of key stakeholders at a workshop; therefore, can be expensive and difficult to arrange • Prone to groupthink and other group dynamics • May produce biased results if dominated by a strong person • Often not well facilitated • Generates nonrisks and duplicates; requires filtering
Cause and effect (Ishikawa) diagrams	C	S		S		• Visual representation; promotes structured thinking	• Diagram can quickly become overly complex
Checklists	C	S		S	S	• Captures previous experience • Presents detailed list of risks	• Checklist can grow to become unwieldy • Risks not on the list will be missed • Often only includes threats and misses opportunities

(continued)

Table X6-1. *(Continued)*

Technique	Risk Identification	Qualitative Analysis	Quantitative Analysis	Response Planning	Risk Monitoring	Strengths	Weaknesses
Technique	Risk Identification	Qualitative Analysis	Quantitative Analysis	Response Planning	Risk Monitoring	Strengths	Weaknesses
Contingency planning		S	S	C		• Ensures that actions are available to address significant events before their occurrence • Allows rapid and focused response • Improves image of professionalism of the way in which the work is managed	• Can give a false feeling of confidence—as if the risk has been avoided
Contingency reserve estimation			C	S	S	• Provides a rationale for reserves • Basis for constructive discussion with sponsor	• Makes the reserve visible and therefore liable to be reduced arbitrarily
Data analytics	S		S		C	• Enables complex analysis • Provides insights that might otherwise be missed	• Requires significant investment of resources to build • Relies on consistency of data input
Decision tree analysis		S	C	C		• Causes the organization to structure the costs and benefits of decisions when the results are determined in part by uncertainty and risk • Solution of the decision tree helps select the decision that provides the highest expected monetary value or expected utility to the organization	• Sometimes difficult to create the decision structure • Probabilities of occurrences can be difficult to quantify in the absence of historical data • The best decision may change with plausible changes in the input data, meaning that the answer may not be stable • The organization may not make decisions based on a linear expected monetary value basis, but rather on a nonlinear utility function; utility functions are difficult to specify • Decision tree analysis of complicated situations requires specialized software • There may be some resistance to using technical approaches to decision making
Delphi technique	C	S		S		• Captures input from technical experts • Removes sources of bias	• Limited to technical risks • Dependent on actual expertise of experts • May take longer time than available due to iterations of the experts' inputs
Document review	C					• Exposes detailed risks • Requires no specialist tools	• Limited to risks contained in documentation

Estimating techniques applied to probability and impact		C	C	S		• Addresses both key dimensions of a risk, namely its degree of uncertainty (expressed as probability) and its effect on objectives (expressed as impact)	• Difficult to calibrate if there is no historical database of similar events • Terms for probability (e.g., probable, almost certain) and for impact (e.g., insignificant, major) are ambiguous and subjective • Impacts can be uncertain or represented by a range of values that cannot be put into a specific impact level such as "moderate impact on time"
Expected monetary value			C			• EMV allows the user to calculate the weighted average (expected) value of an event that includes uncertain outcomes • Well suited to decision tree analysis • EMV incorporates both the probability and impact of the uncertain events • EMV is a simple calculation that does not require specialized software	• Assessment of probability of risk events occurring and of their impact can be difficult to make • EMV provides only the expected value of uncertain events; risk decisions often require more information than EMV can provide • EMV is sometimes used in situations where Monte Carlo simulation would be more appropriate and provide additional information about risk
Expert judgment	C	C	S	S	S	• Provides experiential perspective • Multiple experts increase breadth and depth	• Can be subject to biases based on experience • Potential for limited perspective
Facilitation	C			S		• Enables broad participation and diverse perspectives	• Can be time consuming • Subject to groupthink bias
FMEA/FMECA fault tree analysis	C		C	S		• Structured approach; well understood by engineers • Produces an estimate of overall reliability using quantitative tools • Good tool support	• Focuses on threats, not so useful for opportunities • Requires expert tools not generally available to others
Force field analysis	C	S		S		• Creates deep understanding of factors that affect objectives	• Time-consuming and complex technique • Usually only applied to a single objective, so does not provide whole view
Historical information	C	C	C	C	S	• Leverages previous experience • Prevents making the same mistakes or missing the same opportunities • Enhances the organizational process assets	• Limited to those risks that occurred previously • Information is frequently incomplete: lacks detail of past risks and may not include details of successful resolution; ineffective strategies are rarely documented
Influence diagrams	C	C		S		• Exposes key risk drivers • Can generate counterintuitive insights not available through other techniques	• Requires disciplined thinking • Not always easy to determine appropriate structure
Interviews	C				C	• Addresses risks in detail • Generates engagement of stakeholders	• Time consuming • Raises nonrisks, concerns, issues, worries, etc.; therefore, requires filtering

(continued)

Technique	Risk Identification	Qualitative Analysis	Quantitative Analysis	Response Planning	Risk Monitoring	Strengths	Weaknesses
Monte Carlo simulation			C	S		• Used primarily for project schedule and cost risk analysis in strategic decisions • Allows all specified risks to vary simultaneously • Calculates quantitative estimates of overall risk; reflects the reality that several risks may occur together • Provides answers to questions such as (1) How likely is the base plan to be successful? (2) How much contingency in time and cost do we need to achieve our desired level of confidence? (3) Which activities are important in determining the overall risk?	• Schedules are not simple and often cannot be used in simulation without significant debugging by an expert scheduler • Quality of the input data depends heavily on the expert judgment and the effort and expertise of the risk analyst • Simulation is sometimes resisted by management as being unnecessary or too sophisticated compared to other, more traditional techniques • Monte Carlo simulation requires specialized software, which must be acquired and learned, causing a barrier to its use • Produces unrealistic results unless input data include both threats and opportunities
Multicriteria selection technique		S		C		• Provides a means of selecting the responses that best supports the full set of objectives	• Can give counterintuitive results
Nominal group technique	S	C				• Encourages and allows all participants to contribute • Allows for different levels of competence in common language • Provides ideal base for affinity diagramming (grouping by risk categories for use in the risk breakdown structure and root-cause analysis)	• Can lead to frustration in dominant members who feel it is moving slowly
PERT (program or project evaluation and review technique)			C	S		• Provides a time-based view of risks • Useful for observing the degree to which a risk takes on greater significance at a given point in time	• Does not have a defined measure of impact
Probability and impact matrix		C		S	S	• Allows the organization to prioritize the risks for further analysis (e.g., quantitative) or risk response • Reflects the organization's level of risk tolerance	• Does not explicitly handle other factors such as urgency or manageability that may partly determine a risk's ranking • Range of uncertainty in the assessment of a risk's probability or impact may overlap a boundary
Prompt lists	C			S		• Ensures coverage of all types of risk • Stimulates creativity	• Topics can be too abstract

Questionnaire	C	S				• Encourages broad thinking to identify risks	• Success depends on the quality of the questions • Limited to the topics covered by the questions • Can be a simple reformatting of a checklist
Reserve analysis		C	C	C	S	• Provides a means of tracking spend and releasing contingency amounts as risks expire; can be applied to schedule reserves in the same way • Gives early warning of the need to communicate with sponsor	• Could lead to unwarranted focus on cost dimension • Attention to overall measure of reserve depletion may hide detailed risks
Residual impact analysis	C			S	S	• Provides for further analysis of potential risks after initial treatment is applied	• May promote focusing on risks that do not have substantial impact potential
Risk audit	S				C	• Provides a formal assessment of the compliance with the approach specified in the risk management plan	• Can be disruptive and taken as too judgmental to the team
Risk breakdown structure	C	S	S	S	S	• Offers a framework for other risk identification techniques such as brainstorming • Ensures coverage of all types of risk • Tests for blind spots or omissions	• Can lead to complacency where the fact that the risk is recorded is deemed adequate risk management
Risk data quality assessment		C				• Promotes consideration of the validity of risk characteristics	• May be difficult to quantify the accuracy of the data
Risk reassessment				S	C	• Forces a review of the risks when it becomes necessary so that the risk register remains current	• Takes time and effort
Root-cause analysis	C	S	S	C		• Allows identification of additional, dependent risks • Allows the organization to identify risks that may be related because of their common root causes • Basis for development of preemptive and comprehensive responses • Can serve to reduce apparent complexity	• Most risk management techniques are organized by individual risk; this structure is not conducive to identifying the root causes • Can oversimplify and hide existence of other potential causes • There may be no valid strategy available for addressing the root cause once it has been identified
Scenario analysis	C	S	S	C		• Provides view of the potential effect of the relevant risk and the corresponding response strategy • Forces the participants to analyze the effect of any strategy • Helps to identify secondary risks	• Adds to the list of assumptions • Can be time consuming
Sensitivity analysis			C	S	S	• Enables a structured approach to evaluating potential impact of risks	• Suggests that the results are absolute because they have been given a quantified measure

(continued)

Table X6-1. *(Continued)*

Technique	Risk Identification	Qualitative Analysis	Quantitative Analysis	Response Planning	Risk Monitoring	Strengths	Weaknesses
Simulations	S		C	S		• Allows for analysis of multiple forces around a given risk or set of risks	• Can be difficult to build a comprehensive model • Often expensive to implement
Status meeting	S				C	• Provides a means of verifying information about the status of risks (active, occurred, retired) and maintaining team understanding	• Can seem unnecessary to some participants
SWOT analysis	C	S		S		• Ensures equal focus on both threats and opportunities • Offers a structured approach to identify threats and opportunities • Focus on internal (organizational strengths and weaknesses) and external (opportunities and threats)	• Focuses on internally generated risks arising from organizational strengths and weaknesses, excludes external risks • Tends to produce high-level, generic risks
System dynamics	C	C		S		• Exposes unexpected interrelations between elements (feedback and feed-forward loops) • Can generate counterintuitive insights not available through other techniques • Produces overall impacts of all included risks	• Requires specialized software and expertise to build models • Focuses on impacts, but difficult to include the concept of probability
Trend analysis	S				C	• Provides an indication of the effectiveness of earlier responses • Can provide trigger conditions for responses	• Requires understanding of significant vs. nonsignificant variation
Variance analysis	S				C	• Allows comparison between forecast and actual risk impacts • Can provide trigger conditions for responses • Provides data for earned value analysis, which can be compared to quantitative risk analysis results	• Does not show relationship with earlier data • Values can be taken out of context

APPENDIX X7
ENTERPRISE RISK MANAGEMENT CONSIDERATIONS FOR PORTFOLIO, PROGRAM, AND PROJECT RISK MANAGEMENT

Enterprise risk management (ERM) considers all of an organization's risks as an interrelated collection. It is a systematic, organized, and structured methodology of examining and measuring all risks facing an organization, developing suitable responses, and communicating, monitoring, and managing these to align with the strategic objectives of the organization. For ERM to deliver maximum benefits, it is essential that a common approach to risk management be used across the enterprise.

A common risk management approach allows for all risks, whether portfolio, program, or project risks, to be normalized and aggregated. Risk aggregation allows for a risk position to be stated for any part of the organization. This is essential for understanding the organization's proximity to its stated risk appetite and tolerance.

The risk management process that is employed at each level of the organization should be appropriate, scalable, and tailorable. In other words, the process should have a graded approach to risk. At the lowest levels of the organization or for very small organizations, the risk management process may be very simple and entirely qualitative. At the highest levels of the organization, the risk management process may need to be quite sophisticated, because of the risk-based decisions that are made at this level. As different as these two contexts may appear, it is possible for them to use a common process which is scaled and tailored to their needs.

For larger organizations, ERM is usually a top-down and bottom-up process, with risk review boards operating at multiple levels in the organization. Each level is chartered with established escalation criteria to determine which risks are escalated to the next level. Escalation is usually implemented for one of two reasons: situational awareness or to activate a help chain that is necessary to address the risk. For example, this could happen if one of a program's projects experiences a risk that not only threatens the project's planned output, but also has the potential to affect the program's benefits. Conversely, risk may cascade from the top of the organization to its lower levels through the same communication channels.

Portfolios, programs, and projects reflect core aspects of ERM as it supports the setting and management of strategies and business objectives. Risks from portfolios, programs, and projects should be reflected as ERM risks that may result in changes to business objectives or even strategies. The alignment process between ERM and the portfolio of programs and projects could result in elevating the portfolio or program and project risks to the ERM level or result in additions of ERM top-down risks to the portfolio of programs and projects. Interprogram and interproject risks could also be the outcome of the alignment process. The prioritization, probabilities, and impacts of risks escalated, cascaded, or identified during the alignment process may vary from one level to the other, and could decrease, increase, or stay the same. Alignment between ERM and portfolio, program, and project risks should be reexamined as changes are made to ERM, to the portfolio of programs and projects, and as part of the risk controls processes.

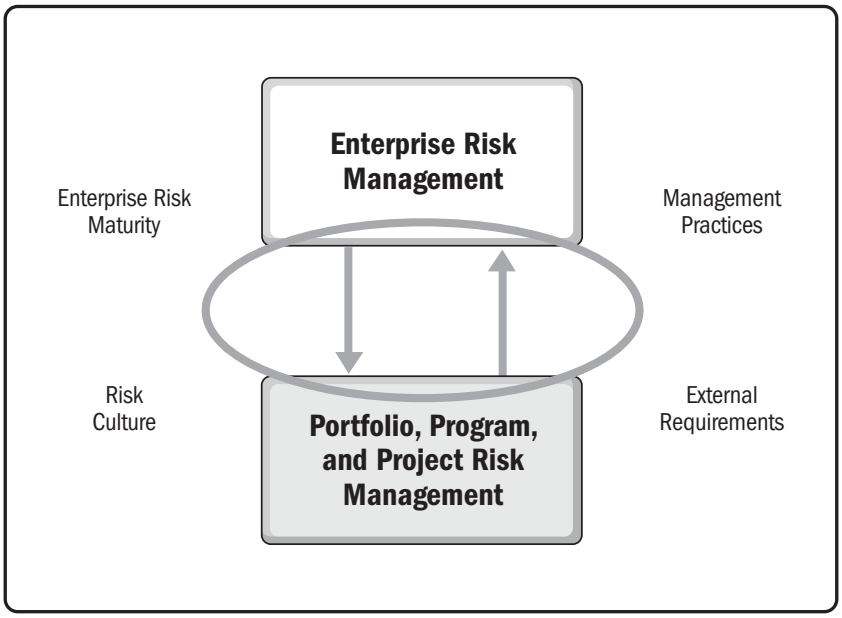


Figure X7-1. Elements Contributing to the Degree of Alignment between ERM and Portfolio, Program, and Project Risk Management

The connection between ERM indicators and portfolio, program, and project risk indicators depends on the degree of integration and alignment. Indicators reflecting strategy and business goals could be cascaded to the portfolio risks to promote integration of ERM indicators and connection to enterprise targets and goals.

ERM is an approach to managing risk that reflects the organization's culture, capability, and strategy to create and sustain value (Figure X7-1). Many of the benefits of ERM are common to the benefits of portfolio risk management. ERM supports the organization's mission, vision, core values, and strategy. ERM is based on the organization's risk appetite and supports broad aspects of the strategy and objectives as well as specific targets and goals that may be relevant to the organization's success. Other objectives of ERM include, but are not limited to:

- Prioritization of resources,
- Shaping of strategy,
- Protecting strategic objectives,
- Protecting existing value,
- Driving profitability and growth by using risk management techniques to generate value, and
- Ensuring regulatory compliance, which protects the organization from negative regulatory intervention and avoids penalties.

ERM emphasizes the trade-offs between benefits and their associated level of risk exposure. ERM examines different scenarios and their associated level of risks. The ERM view of portfolios, programs, and projects is a chosen scenario between a variety of risk result options, each with its own confidence level and associated risks. When ERM is fully integrated into the management of the organization and its culture, it brings clarity to the organization, addressing all of its uncertainty.

APPENDIX X8
RISK CLASSIFICATION

Potential risks can be classified into one of four quadrants based on the degree of available information, ambiguity, and variability (see Section 3.3.1 and Figure 3-3). Organizations work to reduce the degree of unknown factors so they can be progressively converted to known-knowns or at least known-unknowns. This appendix details this concept, which was introduced in Section 3 of this standard.

- **Known-known.** A known-known is a fact, not a risk. These are typically identified as part of requirements and scope. The entity working on the endeavor is aware of these facts, which are incorporated in the portfolio, program, or project scope.
- **Known-unknown.** A known-unknown is an identified risk. The entity working on the endeavor is aware of the uncertain event and the potential consequences. Known-unknown risks are identified and proactively managed.
- **Unknown-known.** An unknown-known is a hidden fact. Knowledge about the fact might exist; however, the entity may not be aware of it at the time of the endeavor. An example of an unknown-known is a hidden or ignored assumption. The identification, assessment, and development of a strong understanding of unknown-known risks occur over time. For complex and innovative activities, there is a high degree of guesswork in which risks can be identified, but with limited visibility. Unknown-knowns are typically addressed through progressive risk elaboration integrated with execution of the endeavor.
- **Unknown-unknown.** Unknown-unknown risks may be emergent risks that are essentially unknowable within the context of portfolio, program, and project management. That lack of knowledge makes any type of evaluation or exploration impossible. Unknown-unknowns can be managed through organizational resilience. Due to the unpredictability, resilient organizations encourage research, raise awareness, encourage teams to question the status quo, and increase the flow of information. These actions stretch the boundaries of influence and prepare organizations to better respond to and recover from such events.

REFERENCES

[1] Project Management Institute. 2015. *Pulse of the Profession® Report: Capturing the Value of Project Management*, p. 15. Newtown Square, PA: Author.

[2] Project Management Institute. 2017. *The Standard for Portfolio Management* – Fourth Edition. Newtown Square, PA: Author.

[3] Project Management Institute. 2017. *The Standard for Program Management* – Fourth Edition. Newtown Square, PA: Author.

[4] Project Management Institute. 2017. *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)* – Sixth Edition. Newtown Square, PA: Author.

[5] Project Management Institute. 2014. *Navigating Complexity: A Practice Guide*. Newtown Square, PA: Author.

GLOSSARY

Assumption. A factor in the planning process considered to be true, real, or certain, without proof or demonstration.

Cause. Events or circumstances that currently exist or are certain to exist in the future, which might give rise to risks.

Component. A predetermined element of a portfolio or program that is work related to the achievement of the portfolio's or program's strategic objectives.

Constraint. A factor that limits the options for managing a project, program, portfolio, or process.

Contingency Plan. A document that describes actions to take if predetermined trigger conditions occur.

Contingency Reserve. Time or money allocated in the schedule or cost baseline for known risks with active response strategies. See also *management reserve*.

Emergent Risk. A risk that arises which could not have been identified earlier on.

Enterprise Risk Management. An approach to managing risk that reflects the organization's culture, capability, and strategy to create and sustain value.

Identify Risks. The process of determining and documenting the risks that might affect the intended outcomes.

Impact. A measure of the effect of a risk on one or more objectives if it occurs.

Issue. A current threat that may have an impact on one or more objectives. See also *opportunity*, *risk*, and *threat*.

Management Reserve. Time or money that management sets aside in addition to the schedule or cost baseline and releases for unforeseen work that is within the scope of the project. See also *contingency reserve*.

Opportunity. A risk that would have a positive effect on one or more objectives. See also *issue*, *risk*, and *threat*.

Organizational Project Management. A framework in which portfolio, program, and project management are integrated with organizational enablers in order to achieve strategic objectives.

Overall Risk. The effect of uncertainty on the portfolio, program, or project as a whole.

Portfolio. Projects, programs, subsidiary portfolios, and operations managed as a group to achieve strategic objectives. See also *program* and *project.*

Portfolio Management. The centralized management of one or more portfolios to achieve strategic objectives. See also *program management* and *project management.*

Probability. A measure of how likely an individual risk is to occur.

Program. Related projects, subsidiary programs, and program activities managed in a coordinated manner to obtain benefits not available from managing them individually. See also *portfolio* and *project*.

Program Management. The application of knowledge, skills, and principles to a program to achieve the program objectives and to obtain benefits and control not available by managing program components individually. See also *portfolio management* and *project management.*

Project. A temporary endeavor undertaken to create a unique product, service, or result. See also *portfolio* and *program.*

Project Management. The application of knowledge, skills, tools, and techniques to project activities to meet the project requirements. See also *portfolio management* and *program management.*

Qualitative Risk Analysis. The consideration of a range of characteristics such as probability of occurrence, degree of impact on the objectives, manageability, timing of possible impacts, relationships with other risks, and common causes or effects.

Quantitative Risk Analysis. The combined effect of identified risks on the desired outcome.

Residual Risk. The risk that remains after risk responses have been implemented. See also *secondary risk*.

Response Strategy. A high-level approach to address an individual risk or overall risk, broken down into a set of risk actions.

Risk. An uncertain event or condition that, if it occurs, has a positive or negative effect on one or more objectives. See also *issue, opportunity,* and *threat*.

Risk Acceptance. A risk response that involves acknowledging the risk and taking no action unless it occurs. See also *risk avoidance*, *risk enhancement*, *risk exploiting*, *risk mitigation*, *risk sharing*, and *risk transference*.

Risk Action. A detailed task that implements, in whole or in part, a response strategy in order to address an individual risk or overall risk.

Risk Action Owner. The person(s) responsible for carrying out the approved risk actions when responding to a given risk. Also known as *response owner.*

Risk Analysis. The activities related to defining the characteristics of a risk and the degree to which it can impact objectives.

Risk Appetite. The degree of uncertainty an organization or individual is willing to accept in anticipation of a reward. See also *risk threshold* and *risk tolerance*.

Risk Assessment. The process of identifying, analyzing, and determining the probability of occurrence of a risk.

Risk Attitude. A disposition toward uncertainty, adopted explicitly or implicitly by individuals and groups, driven by perception, and evidenced by observable behavior.

Risk Avoidance. A risk response that involves eliminating the threat or protecting the project, program, or portfolio from its impact. See also *risk acceptance*, *risk enhancement*, *risk exploiting*, *risk mitigation*, *risk sharing*, and *risk transference*.

Risk Enhancement. A risk response that involves increasing the probability of occurrence or impact of an opportunity.

Risk Escalation. A risk response that involves transferring the ownership of the risk to a relevant party in the organization because the risk is outside of scope or the team does not have sufficient authority to address it.

Risk Exploiting. A risk response that involves ensuring that an opportunity occurs. See also *risk acceptance*, *risk avoidance*, *risk enhancement*, *risk mitigation*, *risk sharing*, and *risk transference.*

Risk Exposure. An aggregate measure of the potential impact of all risks at any given point in time in a project, program, or portfolio.

Risk Identification. The process of locating and profiling the characteristics of risks related to work objectives.

Risk Management. The process that shapes decision making across the organization and within each of the domains and involves identifying, analyzing, responding to, and monitoring risks.

Risk Management Framework. A structure that organizes the process and activities of managing risks in an iterative fashion.

Risk Management Life Cycle. A structured approach for undertaking a comprehensive view of risk throughout the enterprise, portfolio, program, and project domains.

Risk Management Plan. A component of the project, program, or portfolio management plan that describes how risk management activities will be structured and performed.

Risk Mitigation. A risk response that involves decreasing the probability or impact of a threat. See also *risk acceptance*, *risk avoidance*, *risk enhancement*, *risk exploiting*, *risk sharing*, and *risk transference*.

Risk Owner. The person responsible for monitoring the risk and for selecting and implementing an appropriate risk response strategy.

Risk Register. A repository in which outputs of risk management processes are recorded.

Risk Response. An action, planned or implemented, to address particular threats and opportunities.

Risk Sharing. A risk response that involves allocating ownership of an opportunity to a third party who is best able to capture the opportunity or absorb the impact of the threat. See also *risk acceptance*, *risk avoidance*, *risk enhancement*, *risk exploiting*, *risk mitigation*, and *risk transference*.

Risk Threshold. The measure of acceptable variation around an objective that reflects the risk appetite of the organization and stakeholders. See also *risk appetite* and *risk tolerance*.

Risk Transference. A risk response that involves shifting the impact of a threat to a third party, together with ownership of the response. See also *risk acceptance*, *risk avoidance*, *risk enhancement*, *risk exploiting*, *risk mitigation*, and *risk sharing*.

Secondary Risk. A risk that arises as a direct result of implementing a risk response. See also *residual risk*.

Stakeholder. An individual, group, or organization that may affect, be affected by, or perceive itself to be affected by a decision, activity, or outcome of a project, program, or portfolio.

Threat. A risk that would have a negative effect on one or more objectives. See also *issue*, *opportunity*, and *risk*.

Trigger Condition. An event or situation that indicates that a risk is about to occur.

INDEX

F

G

I

K

L

M

N

O

P

Q

R

S

T

U

V

The Standard for Risk Management in Portfolios, Programs, and Projects

The Standard for Risk Management in Portfolios, Programs, and Projects is an update and expansion upon PMI's popular reference, *The Practice Standard for Project Risk Management*.

Risk management addresses the fact that certain events or conditions—whether expected or unforeseeable during the planning process—may occur with impacts on portfolio, program, and project objectives. These impacts can be positive or negative and may cause deviation from the intended objectives. Risk management processes allow for proactive planning to capture opportunities and limit threats.

This standard:

- Identifies the core principles of risk management
- Describes the fundamentals of risk management and the environment within which it is carried out
- Defines the risk management life cycle
- Applies risk management principles to the portfolio, program, and project domains within the context of an enterprise risk management approach

This standard focuses on the "what" of risk management (i.e., the key considerations for effective risk management). It is primarily written for portfolio, program, and project managers, but is a useful tool for leaders in risk management, business consumers of risk management, and other stakeholders in the portfolio, program, and project management professions.

Project Management Institute
GLOBAL**STANDARD**

Project Management Institute
Global Operations Center
14 Campus Blvd
Newtown Square, PA 19073 USA
Tel: +1 610 356 4600
PMI.org

ISBN: 978-1-62825-565-2 U.S. $63.95
56395
9 781628 255652