هيئة كفاءة الإنفاق والمشروعات الحكومية
Expenditure Efficiency & Projects Authority

EXPRO National Manual for Projects Management

Volume 13, Chapter 1

Introduction to Risk Management

Document No. EPM-EM0-GL-000001 Rev 003

Document Submittal History:

Revision:	Date:	Reason For Issue
000	19/10/2017	For Use
001	27/10/2018	For Use
002	12/02/2019	For Use
003	16/08/2021	For Use

THIS NOTICE MUST ACCOMPANY EVERY COPY OF THIS DOCUMENT

IMPORTANT NOTICE

This document, ("Document") is the exclusive property of Government Expenditure & Projects Efficiency Authority.

This Document should be read in its entirety including the terms of this Important Notice. The government entities may disclose this Document or extracts of this Document to their respective consultants and/or contractors, provided that such disclosure includes this Important Notice.

Any use or reliance on this Document, or extracts thereof, by any party, including government entities and their respective consultants and/or contractors, is at that third party's sole risk and responsibility. Government Expenditure and Projects Efficiency Authority, to the maximum extent permitted by law, disclaim all liability (including for losses or damages of whatsoever nature claimed on whatsoever basis including negligence or otherwise) to any third party howsoever arising with respect to or in connection with the use of this Document including any liability caused by negligent acts or omissions.

This Document and its contents are valid only for the conditions reported in it and as of the date of this Document.

Table of Contents

1.0 INTRODUCTION TO RISK MANAGEMENT

The purpose of Volume 13 in the EXPRO Projects White Book is to provide the reader with a preliminary introduction to the Risk Management discipline. Key concepts and ideas that are the fundamental building blocks for Risk Management will be introduced, and the benefits of Risk Management will be highlighted. Finally, the application of these concepts and ideas to the field of project Risk Management is described in the Procedures, Guidelines and Templates contained within Volume 13 as reflected in the table below.

Volume 13 RISK MANAGEMENT		Document Number
Chapter 1:	**Introduction to Risk Management**	
Chapter 2:	**Project Risk Management**	
	Project Risk Management Procedure	EPM-EM0-PR-000001
	Project Risk Management Plan Template	EPM-EM0-TP-000002
	Project Risk Register Template	EPM-EM0-TP-000001

Any initiative, such as implementation of a new Entity policy or delivery of an infrastructure project, is undertaken on the basis that it will satisfy some high-level objectives. These objectives will be related to the realization of specific benefits that may be policy driven in the case of governmental or public sector bodies, or financially driven in the case of a commercial enterprise. The guidance provided here is focused on government or public sector led initiatives. At the Entity level, every policy will have been developed with the aim of delivering social or societal benefits. For example, schools are built to improve education levels, hospitals are built to improve public health and roads or railways are built to improve public mobility. In all such cases, there are strategic or high level objectives that the initiative is trying to realize.

The objective of Risk Management is to understand all the ways in which these objectives can be threatened or compromised, and to undertake activities or implement controls that minimize the risk of this adverse outcome.

Risk Management should be undertaken at all stages of policy and associated program development. So, for example when a project is being developed as part of a program of initiatives to support a policy, Risk Management should be employed to ensure that alternative approaches to delivering the perceived benefits are considered and that the residual risks associated with any options are identified and assessed. As the business case for a project is developed in more detail, the risks to project costs and schedule should be assessed in more detail as should the risks to realizing the assumed benefits. The key thing is that Risk Management should be employed at every stage in a project development, delivery and execution, albeit at different levels of detail.

Volume 13 is structured to address the following:

- Defining risk
- Benefits of Risk Management
- Risk Management standards
- Risk Management Process
- Application of Risk Management process to projects
- Risk Registers
- Project Risk Management roles and responsibilities
- Project risk tolerance criteria
- Project risk governance

1.1 Risk Management Concepts and Application

At its heart, Risk Management is a formalization of what every decision maker does - either consciously or sub-consciously - when they consider alternative options as potential solutions to issues or problems. Bearing this in mind, the following hypothesis is postulated:

- Good management involves taking good decisions
- All decisions have inherent risks and uncertainties
- Decisions are therefore better informed by a better appreciation of these risks and uncertainties.

The latter point is realized by application of a ***Risk Assessment*** process - which is about identifying and understanding the impact of the risks and uncertainties. Armed with this information and understanding, ***Risk Management*** is employed to maximize the chances of realizing the benefits of the selected decision.

These concepts and ideas are discussed in more detail in the subsequent sections.

1.1.1 Defining Risk

If a group of people are asked to list different types of risk, they will typically draw up a list that will look something like the following:

- Safety
- Environmental
- Technological
- Time
- Reputation
- Security/ terrorism
- Health
- Fraud
- Corruption
- Political
- Socio-demographic
- Data integrity / loss
- Cyber attack
- Legal / regulatory
- Cost
- Quality
- Climate change
- Extreme weather (flood, storm)

However, a closer review of this list illustrates an important point. It contains a mixture of risk ***sources*** as well as risk ***impacts***. The list shown above has been rearranged to demonstrate this:

Risk Sources

- Technological
- Security/ terrorism
- Political
- Socio-demographic
- Cyber attack
- Legal / regulatory
- Corruption
- Climate change

Risk Impacts

- Safety
- Health
- Cost
- Time
- Quality
- Data integrity / loss
- Reputation
- Fraud
- Extreme weather (flood, storm)
- Environmental

Distinguishing between these aspects is important from a Risk Management perspective because this understanding help to inform thinking about how best to intervene to manage or control the risks. For example, understanding what the source of the risk is helps us to explore means of eliminating the risk altogether, understanding the potential impact of the risk helps us to explore means for reducing the potential impact or implementing controls to mitigate the potential impact.

There are a wide range of risk sources and risk types. Unsurprisingly, the nature or characteristics of the risks which are important in different circumstances, can differ widely. This means that approaches to Risk Management has developed in different ways in order to address specific and emerging industrial, sectoral or regulatory needs. This point is discussed further in Section 1.1.3 below, but one of the main consequences of this is that the literature contains many different definitions of ‘risk’ and a selection of these is presented in Table 1 below.

Table 1 – Selection of Risk Definitions from Different Standards

'Effect of uncertainty on objectives' ISO 3100:2009 Risk Management - Principles and Guidelines	*'The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.'* The Institute of Internal Auditors - https://na.theiia.org/certification/Public%20Documents/Glossary.pdf
'Uncertainty of outcome, whether positive opportunity or negative threat, of actions and events. It is the combination of likelihood and impact, including perceived importance.' UK HM Treasury, The Orange Book, 2004	*'… a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. '* The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management - Integrated Framework, 2004.
'The likelihood, measured by its probability, that a particular event will occur.' UK HM Treasury, The Green Book, July 2011	
'A hazard is the potential for harm arising from an intrinsic property or disposition of something to cause detriment.' *'Risk is the chance, high or low, that somebody or something could be harmed by these and other hazards, together with an indication of how serious the harm could be.'* UK Health and Safety Executive - www.hse.gov.uk/risk/index.htm	*A risk is an uncertain event or condition that, if it occurs, has a positive or negative effect on at least one of the project's objectives. Risks can be threats (negative) or Opportunities (positive).'* Project Management Institute, Practice Standard for Project Management (https://www.pmi.org/)

It should be clear from the examples that there are different emphases on aspects of the definitions, which reflect the origins and application of the definition. The Society for Risk Analysis recently undertook an exercise (*http://www.sra.org/sra-glossary-draft*) to construct a glossary of risk terms and definition but concluded that:

'…experience has shown that to agree on one unified set of definitions is not realistic - the several attempts made earlier have not achieved success.'

Despite this conclusion from an authoritative, learned organization, there are some common themes that can be highlighted. The first of these is that many of the definitions highlight the importance of understanding the potential impact or scale of the risk. Secondly, several of the definitions make it clear that there is a need to understand the chance or likelihood that this risk impact will be realized. Finally, several of the definitions emphasize the link between risk and the impact on achievement of objectives.

In summary, it is important to understand the **impact** and **likelihood** risk characteristics and these should be considered in terms of how they may affect **objectives**. We therefore define risk as follows:

Anything that can threaten successful achievement of objectives.

It should be noted that the emphasis here is on managing 'threats'. Good practice would encourage consideration of 'risks' as well as 'opportunities' as part of risk management. At this time the general level of risk management maturity across the Kingdom is not judged to be high. Therefore, and on the basis that the concept of 'opportunity' is often misunderstood and applied incorrectly, the risk management focus is required to be on 'threats'.

1.1.2 Benefits of Risk Management

It is not unusual for senior managers to ask:

“What value does Risk Management add to my organization?”

This is often asked when an organization has experienced an extended period where few or no risks have been realized. Many institutions have undertaken research to provide some answers to this question but often it is more useful to think not in terms of ‘value added’, but rather in terms of ‘value erosion avoided’, i.e. what potential risks were we able to avoid experiencing? This way of thinking highlights the point that effective Risk Management is about the prevention of bad things from happening, or limiting the potential damage when things do go wrong (and they will at some point).

If we consider the application of Risk Management to projects, there are many examples in the literature of major infrastructure projects that have gone wrong. A selection of these are presented here from the following source: *(http://www.architectureanddesign.com.au/features/list/world-s-most-over-budget-projects-sydney-opera-hou).*

Original Budget	$56m
Final Cost	$819m
Overspend	× 14
Project Start	1959
Planned Completion	1963
Actual Completion	1973
Years Late	10

Original Budget	$92m
Final Cost	$954m
Overspend	× 10
Project Start	1999
Planned Completion	2001
Actual Completion	2004
Years Late	3

Original Budget	$443m
Final Cost	$2,007m
Overspend	× 5
Project Start	2004
Planned Completion	2012
Actual Completion	2014
Years Late	2

The National Audit Office in the UK has analyzed the causes of UK Government project failures and identified common causes of project failure which include the following:

- Starting badly - a project that does not start well is always struggling to catch-up
- Residual uncertainties associated with the following can put a project at risk:
  - Size
  - Timescale
  - Ambition / Scope
  - Complexity.

A good and effective approach to project Risk Management can save time, reduce costs and can therefore be a significant contributor to project success. The Project Risk Analysis and Management (PRAM) Guide (2004) – published by the Association of Project Management (APM), lists the following ‘hard’ and ‘soft’ benefits that can be expected from an effective project Risk Management system:

'Hard' (Tangible) Benefits	'Soft' (Intangible) Benefits
• Enables better informed and more believable plans, schedules and budgets • Increases the likelihood of a project adhering to its schedules and budgets • Leads to the use of the most suitable type of contract • Allows a more meaningful assessment of contingencies • Discourages the acceptance of financially unsound projects • Contributes to the build-up of statistical information to assist in better management of future projects • Enables a more objective comparison of alternatives • Identifies, and allocates responsibility to, the best risk owner	• Improves corporate experience and general; communication • Leads to a common understanding and improved team spirit • Helps distinguish between good luck / good management and bad luck / bad management • Helps develop the ability of staff to assess risks • Focuses project management attention on the real and most important issues • Facilitates greater risk-taking, thus increasing the benefits gained • Demonstrates a responsible approach to customers • Provides a fresh view of the personnel issues in a project.

1.1.3 Risk Management Standards

As indicated in Section 1.1.1 there is a range of Risk Management standards to pick from. The most commonly cited or referenced standards are:

- ISO 31000:2009 - Risk Management Principles and Guidelines
- BS31000:2008 – Code of Practice for Risk Management
- COSO: 2004 – Enterprise Risk Management – Integrated Framework
- Federation of European Risk Management Associations (FERMA): 2002 – A Risk Management Standard
- Open Compliance and Ethics Group (OCEG) 'Red Book' 2.0 2009 – Governance, Risk and Compliance (GRC) Capability Model
- Solvency II: 2012 – Risk Management for the Insurance Industry.

This begs the question ***"How have we got here, and why are there so many different standards?"*** Answering this question requires an understanding of the historical evolution and understanding of risk, which has been informed by specific events, and the regulatory responses (sometimes at an international level) to the public outcry following these events. So, for example, in the 1980s there were a series of large scale, and high profile safety related disasters which included:

- Chernobyl nuclear power plant explosion (52 deaths + latent cancers, 1986)
- Herald of Free Enterprise ferry disaster (193 deaths, 1987)
- The Piper Alpha offshore platform explosion in the North Sea (167 deaths, 1988).

In the 1990s, there were a series of financial management scandals including:

- Polly Peck International was a small British textile company which grew to a Financial Times Stock Exchange (FTSE) 100 company before collapsing in 1991 with debts of £1.3 billion
- Robert Maxwell developed a publishing empire in the UK but after his death in 1991, huge discrepancies in his companies' finances were revealed, including fraudulent use of £100s of millions from the Mirror Group pension fund to support his other businesses.
- The Bank of Credit and Commerce International (BCCI) was forced to go into liquidation in 1991. Subsequent investigations in the US and the UK revealed that BCCI had been set up deliberately to avoid regulatory review and that its officers were committing fraud on a massive scale.
- In 1996, Nick Leeson lost £827 million and brought down Barings Bank.

In the 2000s, there were a series of Corporate scandals including:

- Enron filed for bankruptcy in 2001 following claimed revenues of over $100 billion in 2000 which were found to be derived via a complex set of fraudulent accounting systems.
- In 2002 Worldcom filed for Chapter 11 bankruptcy protection following an Internal Audit that revealed $3.8 billion of accounting fraud.
- Lehman Brothers filed for Chapter 11 bankruptcy protection in 2008. This remains the largest bankruptcy filing in U.S. history, with Lehman holding over $600 billion in assets.

The result of these events was that in the 1980s there was a lot of regulatory attention paid to development of safety risk and operational Risk Management standards. In the 1990s, there was a lot of focus on Governance of organizations, and the roles and responsibilities of Board members – especially between Executive Directors and Non-Executive Directors. In the 2000s and the subsequent global financial crisis, there has been a lot of attention and scrutiny of how financial institutions should demonstrate to financial regulators the financial risk exposure that their financial assets and shareholders are exposed to.

This historically diverse experience of risk types and exposure in different sectors illustrates the challenges associated with employing a uniform and consistent Risk Management approach. As a result, it is unsurprising that a multitude of different Risk Management standards have emerged. An important corollary through is that there is a potential danger in thinking that a Risk Management standard that has been developed to address a certain set of problems in a specific sector, can be employed at a general level - in other areas.

1.1.4 Risk Management Process

Notwithstanding the fact that Risk Management has evolved for application in different areas, there are common principles and themes that each sectoral application addresses. In all cases, the Risk Management approach is generally intended to address or answer the following questions:

- Risk of what?
- Risk to whom or what?
- How big or bad is the risk?
- Should we do something about it?
- What can be done about it?
- How can we implement this effectively?

These questions can be generalized by recognizing that every organization, initiative, policy, program, or project has specific goals and objectives that it wants to realize. In this case, the challenge is to understand:

How can realization of these goals and objectives be compromised?

Answering this question will require a comprehensive and thorough identification of the events and /or uncertainties that could contribute to these compromises. If it is accepted that good management is about taking decisions and intervening where appropriate to maximize the chance of realizing these goals and objectives, then it should also be accepted that all management decisions or interventions will be better informed if we understand the following:

- What can go wrong?
- What are the key uncertainties?

These aspects are all pulled together in the Risk Management process that has been developed for ISO:31000 and is described in (http://www.ferma.eu/guide-iso-31000). Figure 1 illustrates this in schematic form.

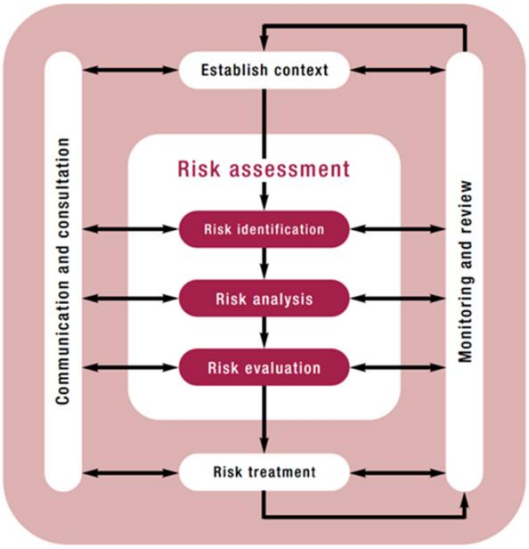


Figure 1 – The Risk Management Process

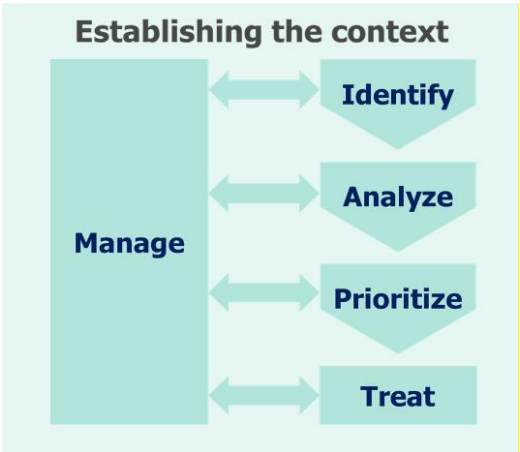
Key activities that form part of every Risk Management system are as follows:

- Risk identification
- Risk analysis (or assessment)
- Risk evaluation (or prioritization)
- Risk treatment

These activities are wrapped up in the monitoring, review, engagement, and communication activities that complete the overall Risk Management system.

The activities that constitute these individual stages for project Risk Management are described in more detail in Section 1.1.5.

1.1.5 Application of Risk Management Process to Projects



The schematic shown above summarizes how the general approach to Risk Management has been adopted for project Risk Management. The main steps in the project Risk Management process can be summarized as follows:

- **Identify** risks via risk elicitation, draft their risk statements, and assign Risk Owners. All risks will be captured in a project risk register.
- **Analyze** risks through an examination and documentation of causes (sources) and effects (impacts), categorize the risks by their sources, and determine potential impact dates.

- **Prioritize** risks based on estimation of likelihood and impacts, determine the current risk ranking on the risk matrix, and recommend Risk Management intervention options based on its risk priority.
- **Treat** risks where the Risk Management interventions are judged to be practicable and result in tolerable residual risk, regularly evaluate the effectiveness of these risk treatments.
- **Manage** risks by undertaking regular monitoring and review activities, ensuring project risk register data quality, ensuring alignment with functional interfaces, executing risk response plans, providing reports and metrics, interfacing with other relevant project related processes and procedures, closing risks, and completing lessons learned.

A **Project Risk Management Procedure** has been developed for use and implementation by the Entities and provides much more detail around each of these stages. The procedure describes ***what*** should be done. ***How*** the procedure will be implemented for any given project will be described in the **Project Risk Management Plan**.

1.1.6 Risk Registers

Risk Registers are at the heart of every Risk Management system. Amongst other things, they provide the mechanism for identifying and recording risks, ensuring they are scored or rated in a consistent manner, and tracking Risk Management intervention activities. A **Project Risk Register Template** has been provided to support execution of the Project Risk Management Procedure.

1.1.7 Project Risk Tolerance Criteria

When a risk has been identified, it is important to assess the risk. This is typically undertaken by consideration of the potential scale or impact of the risk and the associated chance or likelihood that this impact will be realized. There are a range of methods that can be employed in undertaking this assessment especially qualitative, semi-quantitative and quantitative methods. More detail about the application of these methods to projects is provided in the Project Risk Management Procedure.

The following examples illustrate how a qualitative risk impact and likelihood scales can be tailored for specific circumstances and audiences.

London Underground - Operations Managers	
Scale	Impact
High (H)	Partial Line Closure (or worse)
Medium High (MH)	Station closure
Medium Low (ML)	Journey delay > 2 mins
Low	Journey delay < 2 mins

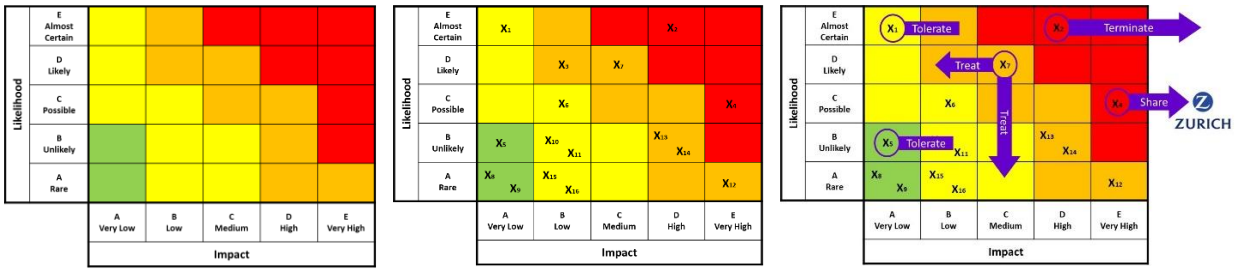
Battery Manufacturer - Board	
Scale	Impact
High (H)	Threatens business survival
Medium High (MH)	Long term damage to business
Medium Low (ML)	Short term damage to business
Low	Trivial

London Underground - Operations Managers	
Scale	Likelihood
High (H)	Greater than once per day
Medium High (MH)	Greater than once per week
Medium Low (ML)	Greater than once per month
Low	Greater than once per year

Battery Manufacturer - Board	
Scale	Likelihood
High (H)	Once a month
Medium High (MH)	Once a year
Medium Low (ML)	Once every five years
Low	Once every 20 years

When a risk register has been populated, it is normal to map all the risks onto a Risk Matrix constructed from the risk impact and likelihood scales - as shown in (a) in the following schematic. It is normal for a Risk Matrix to have the individual cells categorized in some way (typically 'red', 'amber', 'green') as also illustrated in (a) of the following schematic. The distinction between 'red', 'amber' and 'green' risks should reflect the risk tolerance limits (often called risk appetite) that will be employed when making decisions.

Risk tolerability limits will be driven by a range of factors including: regulatory obligations; financial or contractual constraints; organizational goals and values; client requirements. In any case, the rationale for establishing the risk tolerance criteria should be recorded in the Project Risk Management Plan.



(a) Risk Matrix **(b) Risk Profile** **(c) Risk Management Interventions**

When all the risks are plotted onto the Risk Matrix, the results define the Risk Profile as shown in (b) of the schematic above.

The Risk Management response or intervention level that should be employed for risks that fall into different risk categories, should be a policy decision that is recorded in a manner such as illustrated in the following schematic and this should also be recorded in the Project Risk Management Plan. The associated risk management interventions fall into one of four categories: Terminate; Share; Treat; and Tolerate. These are illustrated in (c) in the schematic above.

	Risk Matrix Category			
	Red Priority 1	**Amber Priority 2**	**Yellow Priority 3**	**Green Priority 4**
Risk Tolerance	Risks that significantly exceed the risk tolerance threshold	Risks that exceed the risk tolerance threshold	Risks that lie on the risk tolerability threshold	Risks that are below the risk tolerability threshold
Risk Response	Requires urgent and immediate attention	Requires proactive management	Requires active monitoring	Do not require active management

Example of Risk Management Intervention Levels

1.1.8 Project Risk Management Roles and Responsibilities

As indicated earlier, all of these general Risk Management steps need to be wrapped up in an overall set of activities that determine who does what, what information is shared between different parties, in what form, and how often. This completes the establishment of Risk Management system.

An important aspect of this is to establish who is responsible for what and this is particularly true for infrastructure projects which may be of extended durations, and it is therefore not unusual for individuals in key project roles to change. The following schematic highlights the key project roles that are critical for successful project Risk Management.

The Project Risk Management Procedure describes the main responsibilities of these roles in detail and the Project Risk Management Plan will confirm named individuals against the key roles. The key roles are summarized here:

Project Manager (PM)

- To provide overall direction for the project, including project Risk Management activities
- To support all internal and external interface and resource requirements.

Risk Manager

- To support the PM by managing the project Risk Management process
- To engage with all internal and external stakeholders and facilitate all communication requirements
- To manage the interfaces with all other relevant project management processes
- To maintain the project risk, register and facilitate all data collation in support of this.

Project Team

- To participate in and contribute to the execution of the project Risk Management process throughout the complete project life cycle
- To provide expert input on the allocation of Risk Owners for all identified project risks
- To provide guidance and expert input on any decisions about Risk Management intervention options.

Risk Owner

- These are nominated by the project team against individual risks, and approved by the PM
- Responsible for the management of any risks allocated to them – and are answerable to the PM
- Provide suggestions to the project team on the Risk Management interventions that could be employed to help manage specific risks.

Risk Treatment Owners

- These are nominated by the Risk Owner
- Responsible for the implementation and execution of agreed Risk Management interventions - and are answerable to the Risk Owner
- Responsible for monitoring and reporting effectiveness of the Risk Management interventions that they are responsible for.

1.1.9 Project Risk Governance

As indicated in the previous section, it is the responsibility of the Risk Manager to administer the project Risk Management process. The project Risk Management activities that are managed and overseen by the Risk Manager will be undertaken according to a predetermined management cycle that will be agreed and approved by the Project Manager, and will be formalized in the Project Risk Management Plan.

The following table presents an example of the form that such an engagement and management plan may take:

Date	Activity to be Undertaken
1st of the Month	• Risk Owners review their risks for update and action using reports and metrics provided by the Risk Manager
2nd to 22nd of each Month	• Risk Manager, Risk Owners and other risk stakeholders update risks in the project risk register, and evaluate risk response plans as required by risk review requirements • From stakeholder discussions, consideration is given to the potential for new risks for consideration by the project management team at the monthly risk meeting, or sooner if a high-level risk is foreseen

Date	Activity to be Undertaken
23rd of each Month	• The risk register is frozen at month-end for report development and for a copy to be archived
25th of each Month	• The Risk Manager issues reports and metrics to the PM, project team (or project risk review group), Risk Owners, and other stakeholders (e.g. the customer) • Risk Manager ensures data archival requirements are complied with
28th of each Month	• The monthly project risk review meeting is held with the project team (or project risk review group)
Quarterly	• Project team (or project risk review group) undertake a full review of the project risk register • Review of overall effectiveness of project Risk Management plan and associated activities with the project management team
Semi-Annually	• Project risk identification workshop with the project team (or project risk review group) and other risk stakeholders • Health check of project Risk Management process, either as part of Stage Gate Process, by the project team (or project risk review group), or independently initiated