

NATO STANDARD

ARAMP-1

**NATO RISK MANAGEMENT GUIDE FOR
ACQUISITION PROGRAMMES**

Edition 1 Version 1

FEBRUARY 2012



NORTH ATLANTIC TREATY ORGANIZATION

ALLIED RISK ASSESSMENT MANAGEMENT PUBLICATION

**Published by the
NATO STANDARDIZATION AGENCY (NSA)
© NATO/OTAN**

INTENTIONALLY BLANK


NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION AGENCY (NSA)

NATO LETTER OF PROMULGATION

14 February 2012

1. The enclosed Allied Risk Assessment Management Publication ARAMP-1, RISK MANAGEMENT GUIDE FOR ACQUISITION PROGRAMMES, has been approved by the nations in the Life Cycle Management Group (AC/327), and is promulgated herewith.
2. ARAMP-1 is effective upon receipt.
3. No part of this publication may be reproduced, stored in a retrieval system, used commercially, adapted, or transmitted in any form or by any means, electronic, mechanical, photo-copying, recording or otherwise, without the prior permission of the publisher. With the exception of commercial sales, this does not apply to member nations and Partnership for Peace countries, or NATO commands and bodies.



Cihangir Aksit, TUR Civ
Director NATO Standardization Agency

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

[illegible]

INTENTIONALLY BLANK

RECORD OF SPECIFIC RESERVATIONS

[illegible]

INTENTIONALLY BLANK

TABLE OF CONTENTS

1	Introduction	1
1.1	Purpose	1
1.2	Applicability	1
1.3	Structure of this Document	1
1.4	NATO Framework for Risk Management	2
1.5	Risks: Threats and Opportunities	2
1.6	References	2
1.7	Abbreviations and Acronyms	2
1.8	Terms and Definitions	2
2	Risk Management Principles	3
2.1	History	3
2.2	Purpose and Benefits of Risk Management	4
2.3	Risk Management Critical Success Factors	5
2.4	Threats vs. Opportunities	5
2.5	Risk vs. Uncertainty	6
2.6	Risk vs. Issue	6
2.7	Enterprise, Programme and Project Risk Management	6
2.8	Project and Product Risks	9
2.9	Internal vs. External Risks	9
2.10	Probability, Impact, and Risk Rating	9
3	Risk Management within the NATO System Life Cycle Management Framework	12
3.1	System Life Cycle Stages	13
3.2	Programme / Project Management Process	17
3.3	Risk Management Process within NATO SLCM	19
3.4	System Life Cycle Processes	20
4	Risk Management Process	24
4.1	Risk Identification	26
4.2	Risk Analysis	31
4.3	Risk Response Planning	36
4.4	Risk Monitoring and Control	40
4.5	Risk Management Planning	42
5	Particularities of Risk Management to NATO	44
5.1	Risk Management between NATO Contracting Authorities and Contractors	44
5.2	Risk Management and Accelerated Fielding	46
	Annex A - Abbreviations and Acronyms	1
	Annex B - Terms and Definitions	1
	Annex C - Risk Management Plan Template	1
	Annex D - Risk Register	1
	Annex E - Risk Management as Part of the Contractual Process	1
	Annex F - Methods, Techniques and Tools	1
	Annex G - Suggested Literature	1

TABLE OF TABLES

Table 1-1: References	2
Table 2-1: RM organization: roles and responsibilities	8
Table 4-1: RM process: overview	25
Table 4-2: Risk identification tasks	28
Table 4-3: Example of risk identification checklist	29
Table 4-4: Risk analysis tasks	32
Table 4-5: Example of risk assessment checklist	33
Table 4-6: Example Risk response tasks.....	37
Table 4-7: Risk monitoring and control tasks.....	40
Table 4-8: Risk management planning tasks.....	43
Table 5-1: Solutions to documentation constraints	48
Table 5-2: COTS selection criteria	51
Table F-1: Overview of methods, techniques and tools	2

TABLE OF FIGURES

Figure 2-1: RM organization: levels and purpose	7
Figure 2-2: Example of probability rating	10
Figure 2-3: Example of impact rating	10
Figure 2-4: Example of basic probability and impact matrix	11
Figure 2-5: Example of probability and impact matrix for avoidance of risks with high impact ratings	11
Figure 3-1: RM framework: functional relations	12
Figure 3-2: RM framework: system life cycle stages	14
Figure 3-3: RM framework: programme / project management process.....	17
Figure 3-4: RM framework: risk management process	20
Figure 3-5: RM framework: system life cycle processes.....	21
Figure 4-1: RM process: flow diagram	26
Figure 4-2: Risk categorisation by functional area	31
Figure 4-3: Example of Monte Carlo statistical combination of risk and uncertainty.....	36

1 Introduction

This document provides guidance on how to apply Risk Management (RM) within the System Life Cycle Management (SLCM) framework used in NATO. RM is a systematic, proactive, and iterative endeavour that seeks to efficiently and effectively identify risks, prioritize them, develop response strategies and provide the necessary information at the appropriate time in order to minimize the impact of unfavourable events (threats) and maximize the benefit of favourable events (good risks), called opportunities.

It is NATO policy to maximize the use of industrial standards: while providing specific value for use with the NATO SLCM, this guide must be seen as a complement of the references listed in 1.6.

1.1 Purpose

This document provides a common understanding of RM and a common way of applying the related definitions, concepts, processes, tools and techniques for NATO Nations and Agencies applying the NATO Policy for SLCM.

It is a composite of agreed concepts, best practices and proven techniques for managing risks at all levels during all stages of projects and programmes. It is aimed at supporting acquisition programmes and projects objectives within the SLCM framework used in NATO.

It provides specific guidance on the use of tools and techniques for RM.

1.2 Applicability

This document is not mandatory for use but is principally focused toward NATO Nations.

Any NATO Nation or organization as well as industrial bodies, in their role as acquirer or supplier can use this document as a guide to perform Risk Management.

1.3 Structure of this Document

This document consists of 5 chapters, as follows:

- Chapter 1, Introduction, is a general introduction to the document presenting its purpose and applicability.
- Chapter 2, Risk Management Principles, provides some general information on Risk Management and its context of use.
- Chapter 3, Risk Management within the NATO System Life Cycle Management Framework, focuses on the place of this guidance within the general framework referring to the Life Cycle of Systems.
- Chapter 4, Risk Management Process, is an overview of the main activities involved and how they interrelate to each other. It provides specific guidance on their application within the scope of this document and for the target audience.
- Chapter 5, Particularities of Risk Management to NATO, provides recommendations about specific attention according to the NATO Life Cycle Management Policy like collaboration with contractors and rapid fielding.

Annexes provide complementary information.

1.4 NATO Framework for Risk Management

The purpose of System Life Cycle Management (SLCM) is to mitigate risk, reduce acquisition times to identify, quantify and control Life Cycle Cost, from the earliest possible opportunity”¹. One of the objectives of the NATO SLCM Policy is “to have a common understanding of all aspects of SLCM, including operational and logistic requirements, affordability, time, schedule, quality and risk”. The NATO SLCM Policy, therefore, provides the framework for the use of RM within NATO acquisition activities. Due to the particular importance of this aspect, the RM integration in the SLCM has been developed in chapter 3.

1.5 Risks: Threats and Opportunities

The “Guide to the Project Management Body Of Knowledge” (PMBOK) defines a risk as “*an uncertain event or condition that if it occurs has a positive or negative effects on a project’s objectives*”. According to this definition, the term “risk” covers both an opportunity and a threat. In fact, risks (opportunities and threats) may be managed in a similar manner (although differences in the risk quantification and response strategies exist). In this document, if there is a need to specifically address opportunities or threats, the word “opportunity” or “threat” will be used.

1.6 References

The following documents provided the foundation for many aspects of this document:

Table 1-1: References

	Document	Identifier
a.	NATO System Life Cycle Stages and Processes	AAP-48 (Edition 1)
b.	Handbook on the Phased Armaments Programming System (PAPS)	AAP-20
c.	Systems Engineering – System life cycle processes	ISO/IEC 15288 (First edition)
d.	A Guide to the Project Management Body of Knowledge	PMBOK (Third edition)

Other documents used in a more specific context have been referenced in the text.

In addition, Annex G - provides suggested readings.

1.7 Abbreviations and Acronyms

Refer to Annex A -.

1.8 Terms and Definitions

Refer to Annex B -

¹ NATO Policy for System Life Cycle Management, C-M (2005) 0108

2 Risk Management Principles

Following an informative summary of the history of risk management, this chapter presents a general description of key aspects provided for a better understanding of the rest of the guide.

2.1 History

Risk as a science was born in the sixteenth century Renaissance, a time of discovery. Up until that time there were great achievements in science and engineering but few thinkers ventured into forecasting the future. According to Bernstein², the concept of risk was a significant development in modern civilization:

“The revolutionary idea that defines the boundary between modern times and the past is the mastery of risk: the notion that the future is more than a whim of the gods and that men and women are not passive before nature. Until human beings discovered a way across that boundary, the future was a mirror of the past or the murky domain of oracles and soothsayers who held monopoly over knowledge of anticipated events.”

The word risk derives from the early Italian *risicare*, which means “to dare.”³ Games of chance led to the discovery of the theory of probability, the mathematical heart of risk which was first documented by Giralamo Cardano in his book on mathematics, *Ars Magna* (The Great Art) which appeared in 1545. After Cardano’s publication, mathematics and the understanding of probability and statistics had progressed at a rapid pace through France, on to Switzerland, Germany and England. One of the most significant contributions to the evolution of risk was Daniel Bernoulli’s paper in 1731 that argued that any decision relating to risk involves two distinct and yet inseparable elements; the objective facts and a subjective view about the desirability of what is to be gained, or lost by the decision.⁴ This paper became the basis of utility and decision theory. By 1760, the mathematical foundation had been laid with a several significant additions that included the 1875 discovery of regression to the mean, and in 1952 diversification is highly advantageous over a single option.

One of the first practical applications of risk was the development of marine insurance, started in 1688, in Lloyd’s coffee house, with the confluence of merchant seaman and businessman underwriting insurance policies against the safe shipment of goods, later to become the Lloyds of London. By 1720, the first formal insurance establishments emerged in England with the Royal Exchange Assurance and the London Assurance Corporations⁵. Since then, RM has become a prevalent discipline especially where the consequence of failure can be catastrophic to the stakeholders. In the modern world, the management of risk is all pervading but it is particularly prevalent in the following areas:

- Financial Institutions.
- Business Enterprises.
- Power/Nuclear Industry.
- Defence Sector.
- Aerospace Industry.

² Peter L. Bernstein, “Against the Gods: The Remarkable Story of Risk”, 1996

³ Elaine M. Hall, “Managing Risk: Methods for Software Systems Development”, 1997

⁴ Ibid., Bernstein, 1996

⁵ Ibid., Bernstein, 1996

2.2 Purpose and Benefits of Risk Management

The purpose of RM is to help ensure cost, schedule, and performance objectives are achieved at every stage in the lifecycle and to communicate to all stakeholders the process for uncovering, determining the scope of, and managing projects uncertainties. Without effective RM the programme or project managers may find themselves doing crisis management, a resource intensive process that is typically constrained by a restricted set of available options.

The benefits of RM are to support the realization of programme, project, but also System Of Interest (SOI) objectives throughout the life cycle, and support the following aspects:

- Programme/project as well as life cycle costs overrun are minimized.
- Schedules are met, reducing delays and allowing the investment they represent to be fully utilised.
- All deliverables meet their requirements, preventing costly repeats or top up activities that would otherwise be required to deliver the shortfall.
- The programme and project specific requirements (e.g. legal or statutory) are appropriately addressed.

The nature of defence related development programmes today are that they incur risk. These programmes have challenging missions, utilize new technologies, and have processes that typically involve multiple contractors and suppliers that may span across international boundaries. The risks that can emerge from these complex relationships need to be effectively managed. The essential question that must be asked is: "What can go wrong?" If the sum of the probability of occurrence and consequence of failure are high enough, response plans need to be implemented that will help ensure a successful outcome. Some examples of response plans may be to increase management reserve for budgets, conduct dual technology paths or hire additional engineers or Subject Matter Experts (SMEs). In all cases, the RM approach must be tailored to fully support the programme and project objectives within the environment (e.g. life cycle phase, statutory requirements, scope and complexity of the programme and project, engineering complexity of the system, etc).

In summary, RM provides a structured approach to support the accomplishment of programmes and projects objectives, within the SLCM framework, by adequately responding to threats and uncertainty.

2.3 Risk Management Critical Success Factors

The U.S. Department of Defence Risk Management Guide lists the following characteristics of a successful RM process:

- Feasible, stable, and well-understood user requirements and threats.
- A close relationship with user, industry, and other appropriate participants.
- A planned and structured risk management process, integral to the acquisition process.
- An acquisition strategy consistent with risk level and risk-handling strategies.
- Continual reassessment of programme and associated risks.
- A defined set of success criteria for all cost, schedule, and performance elements.
- Metrics to monitor effectiveness of risk-handling strategies.
- Effective Test and Evaluation Programme.
- Formal documentation.

Successful risk management depends on the knowledge gleaned from all aspects of the programme coupled with the appropriate responses applied to the specific root causes and consequences. This can only be effectively achieved with the involvement and collaboration of every team member and stakeholder on the programme, not just the managers.

2.4 Threats vs. Opportunities

Without understanding why risks encompass threat and opportunity, the risk management process will not be used to identify and capture opportunities. There are three main reasons why risk should include opportunity alongside threat:

1. **Conceptual** – Risk can be seen as a source of variability which is a two-sided construct. The double side nature of variability is captured in the definition of risk that includes both positive and negative consequences. An opportunity is also an uncertain event since it is a possible future event. So both threats and opportunities are covered by this same description of risk as “*uncertainty that matters*”.
2. **Practical** – Threats and opportunities are important and they both need to be managed. Dealing with them together in an integrated process could bring synergies and efficiencies. It is easy to implement a combined risk process to manage both threats and opportunities alongside each other: opportunities can be found by using standard risk identification techniques, they can be prioritized in the same ways as threats, opportunity response strategies mirror those used for threats and reporting formats such as a risk register can be simply adapted to include both threats and opportunities.

3. **Beneficial** – A structured approach to identify and capture opportunities is good for business and for projects in a way that it gives people a structured framework for working faster, smarter, cheaper, it supports innovation and creativity, it is very motivating for teams and will maximize the chances of hitting targets and achieve project objectives.

So, including opportunity within the definition of risk is not a theoretical or academic exercise driven by a misplaced desire for symmetry. It is a natural consequence of recognizing that businesses, projects and people are affected by uncertainty, some of which might be helpful.

2.5 Risk vs. Uncertainty

In Frank H. Knight's landmark book: "Risk, Uncertainty, and Profit"⁶, risks and uncertainties are explained as follows:

1. Risk is present when future events occur with measurable probability
2. Uncertainty is present when the likelihood of future events is indefinite or incalculable.

This document applies the same distinction between risks and uncertainties.

2.6 Risk vs. Issue

According to the PMBOK, a risk is: "*an uncertain event or condition that if occurs has a positive or negative effect on project objectives*". The word "issue" is used when the event or condition is realised. The alternative to RM is, therefore, issue or crisis management, a resource-intensive process that is typically constrained by a restricted set of available options.

2.7 Enterprise, Programme and Project Risk Management

2.7.1 RM organization: levels and purpose

The RM process may be performed at different interconnected levels in an organization. Generally, we can differentiate between the following levels:

- Enterprise: Enterprise risk management is a process, applied in a strategy setting and across the enterprise, to provide reasonable assurance that the enterprise's objectives are achieved.
- Programme: Programme risk management is a continuous process performed throughout the entire life cycle of a SOI (or throughout the entire programme duration).
- Project: Project risk management is a process aiming at increasing the probability that project's objectives will be met.

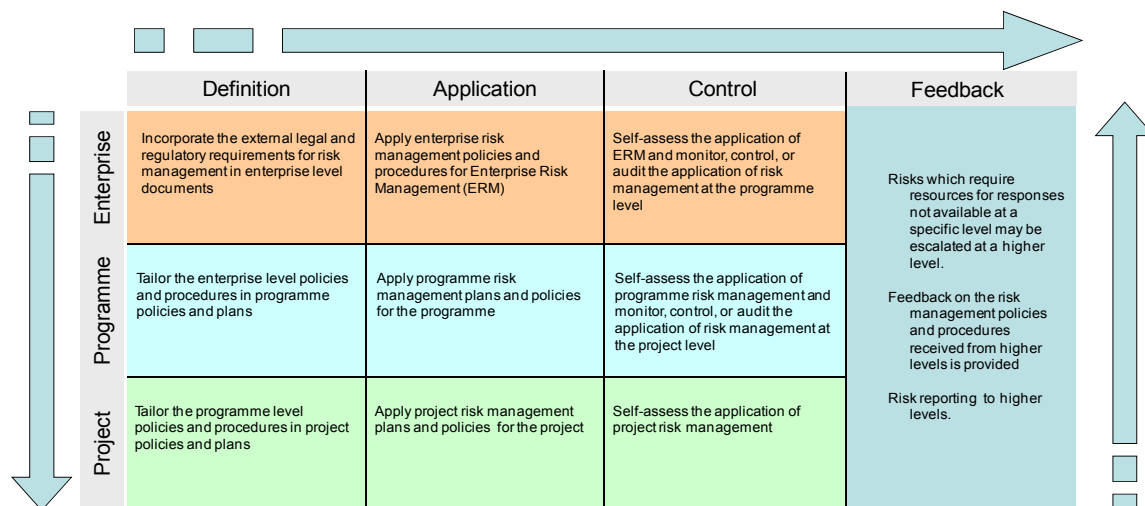
Depending on the organization, the three levels may be clearly differentiated and performed in different departments or be concentrated in a single office.

⁶ Frank H. Knight, Risk, "Uncertainty, and Profit", 1921

As shown in Figure 2-1, each level has four basic purposes:

1. A definition purpose to transform policies and procedures from higher echelons for use at the current and lower levels.
2. An application purpose to apply the transformed policies and procedures in order to achieve the objectives of risk management at the level.
3. A control purpose to self-assess and verify the application at the current and lower levels, respectively.
4. A feedback purpose to:
 - Escalate the need of resources for risk response actions.
 - Provide feedback on policies and procedures.
 - Report on risks.

Figure 2-1: RM organization: levels and purpose



2.7.2 RM organization : roles and responsibilities

This section identifies the primary roles and responsibilities that could be associated with the RM process. The structure in which the RM process has to be performed can vary in size (from a large group to a single person), in structure (from a separate organization to an integral part of the organization), in composition (from internal members only to a group that includes contractors and other external stakeholders), and in the approach (from a centralized unique team to a decentralized cross-organizational matrix). Since RM is never a standalone activity (it is performed in support of the enterprise, programme, or project management), its roles must also fit the level where it is performed.

The table below provides a notional description of the responsibilities associated with generic roles. The responsibilities are limited to the scope of the [level] where it applies.

The roles need to be tailored for the organization. For instance, any of the roles below may be assigned to existing functions and structures. As an example, the role of the risk board could be assigned to an existing Steering Committee or Management Board.

Table 2-1: RM organization: roles and responsibilities

Risk Board
<ul style="list-style-type: none"> •Coordinate risk management activities across internal departments and levels as well as with external stakeholders. •Provides and assigns resources required by a level when those resources are outside the manager's span of responsibility.
[Level] Manager
<ul style="list-style-type: none"> •Ultimately responsible for the achievement of the risk management. •Provides the required resources for the execution of the risk management process, plans, and actions. •Assigns ownership of risks to personnel of the level. •Reports to the hierarchy and risk board on risk management aspects.
[Level] Risk Manager
<ul style="list-style-type: none"> •Develops and maintains risk management policies, procedures, and plans. •Ensures, coordinates, and executes the risk management process. •Provides or arranges risk management training for personnel involved in risk management activities. •Provides the tools required for risk management (checklists, risk register, etc.). •Prepares risk management reports. •Ensures compliance with higher level policies and requirements. •Supports the level manager on all aspects of risk management, including advice on the use of resources and the assignment of risk ownership. •Escalates risk management issues to the manager. •Evaluates the application of risk management at the level and monitors, controls, or audits (eventually through independent assessors) the risk management at subordinate levels.
Risk Owner
<ul style="list-style-type: none"> •Executes the risk strategy for the owned risks. •Report the status of owned risk (for instance by updating the risk register) to the risk manager. •Proposes changes to the risk management policies, procedures, and plans.

2.8 Project and Product Risks

Objectives defined for a project will be defined in relation on how to execute the project and the “quality” of the product. Objectives related to project execution include schedule, cost, and project scope (the quality or compliance of activities performed within the project). Objectives related to the product focus on delivering the functional requirements (functions that the product must realize, such as “print a document”) and non-functional requirements (characteristics that the product must possess, such as availability, reliability, maintainability, testability, safety, security, but also Integrated Logistics Concepts aspects such as Total Cost of Ownership, etc) of the product.

Risk management must address both types to ensure that the “overall” project objectives as well as life cycle objectives are met.

2.9 Internal vs. External Risks

An internal risk is a risk of which the principal cause lies within the area of responsibility of the risk management process. The cause of external risks lies outside the area of responsibility of the risk management process

For instance, for a project, the risk of project member getting ill is an internal risk while the risk of a supplier not delivering on time is an external risk.

The categorization of risks as internal or external helps defining the necessary risk response actions at the appropriate level, and NOT why and how to manage those risks. It is the responsibility of each level to identify all risks (including those where the response lies outside) and trigger the right response, including addressing the risk at the right level of responsibility (the level best placed to manage the risk).

2.10 Probability, Impact, and Risk Rating

2.10.1 Probability Rating

Risk probability is one of the risk attributes. It is used to characterise the likelihood of occurrence of the risk. A probability (p) can take any discrete value strictly greater than zero and strictly smaller than one ($0 < p < 1$). Rules and guidelines to quantify and qualify probabilities (see Figure 2-2: Example of probability rating as an example) should be defined in the RM Plan (RMP). In this document, the word probability will be used to represent a probability value (between 0 and 1), a probability level (e.g. 1, 2, 3, 4, or 5), or a probability description (e.g. very unlikely).

Figure 2-2: Example of probability rating

Values	Ratings			
	Probability Descriptions		Probability Value	Probability Level
	Not Likely	Very Low	<20%	1
	Low Likelihood	Low	21% - 40%	2
	Likely	Moderate/Medium	41% - 60%	3
	Highly Likely	High	61% - 80%	4
	Near Certainty	Very High	>80%	5

2.10.2 Impact Rating

Risk impact is another risk attribute. It is used to characterise the effect of the risk (if it would happen). Impact should be assessed against the project objectives, and may be quantified in each of the following project areas: cost, schedule, and technical performances. Rules and guidelines to quantify and qualify impacts (see Figure 2-3: Example of impact rating as an example) should be defined in accordance with the RMP.

Figure 2-3: Example of impact rating

Risk Impact level	Impact Criteria		
	Technical Performance	Schedule	Cost
1	Minimal or no consequence to technical performance	Minimal or no impact	Minimal or no impact
2	Minor reduction in technical performance or supportability, can be tolerated with little or no impact on Programme objectives	Able to meet key dates. Slip < 1 month	<1% Over total estimated cost
3	Moderate reduction in technical performance or supportability with limited impact on Programme objectives	Minor schedule slip. Able to meet key Programme milestones with no schedule float. Slip < 3-6 months	< 5% over total estimated cost
4	Significant degradation in technical performance or major shortfall in supportability; may jeopardize Programme success	Programme critical path affected. Slip < 0.5-1 year	< 10% over total estimated cost
5	Severe degradation in technical performance; Cannot meet KPP or key technical/supportability threshold; will jeopardize Programme success	Cannot meet key Programme milestones.	> 10% over total estimated cost

2.10.3 Risk Rating

A risk rating is the combination of the probability and impact ratings. A probability and impact matrix determines a risk rating which expresses the overall risk assessment and is used to support the development of appropriate risk responses. In Figure 2-4, the combinations of 3 different probability and impact ratings lead to a risk being rated as “high”, “moderate”, or “low”.

Figure 2-4: Example of basic probability and impact matrix

		Probability rating		
		Unlikely	Likely	Very likely
Impact rating	Minor	Low	Low	Moderate
	Medium	Low	Moderate	High
	Major	Moderate	High	High

While the figure above provides a simple, balanced distribution of risk ratings, some projects will require a more specific approach in order to better calibrate the risk response. The table below shows a more elaborate matrix where four different risk ratings are defined (critical, high, moderate, and low) and where disastrous and major impacts are assessed to be critical even if they have low probabilities. This matrix could be used for instance for the technical risks of a safety critical product.

The organization or project must develop or adopt an appropriate probability and impact matrix with clear descriptions of impact ratings, for instance in terms of delay, costs, or quality.

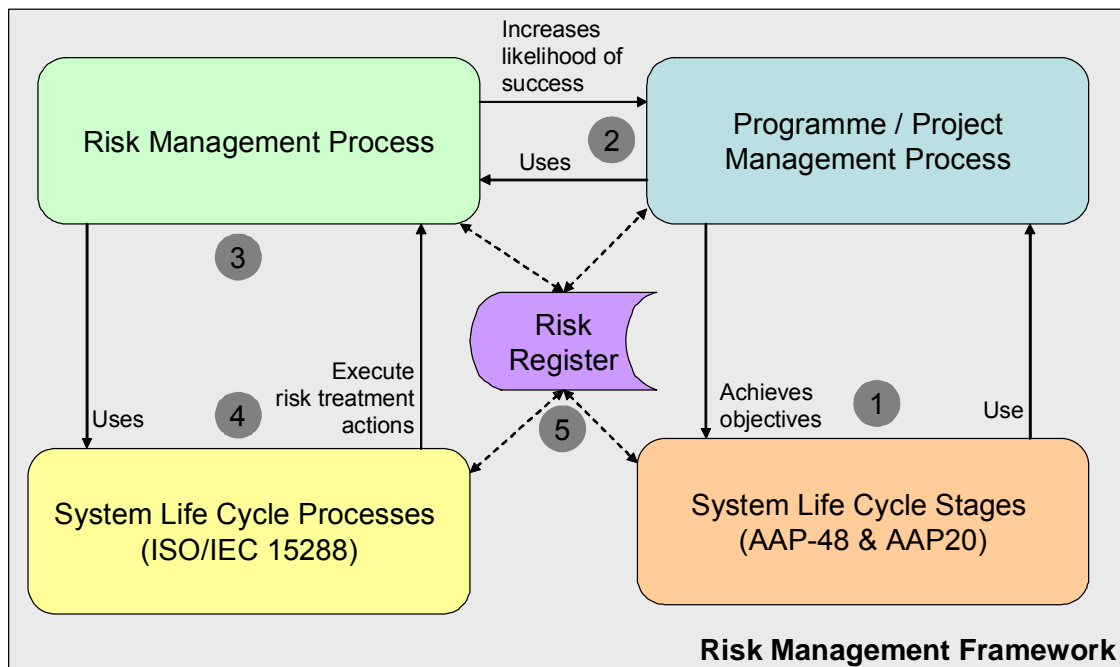
Figure 2-5: Example of probability and impact matrix for avoidance of risks with high impact ratings

		Probability rating				
		Extremely Unlikely	Very unlikely	Likely	Very likely	Extremely likely
Impact rating	Insignificant	Low	Low	Low	Low	Low
	Minor	Low	Low	Moderate	Moderate	Moderate
	Medium	Moderate	High	High	High	High
	Major	Critical	Critical	Critical	Critical	Critical
	Disastrous	Critical	Critical	Critical	Critical	Critical

3 Risk Management within the NATO System Life Cycle Management Framework

The RM framework presented in this chapter assembles the key elements needed for the successful application of a RM process (see chapter 4) across the system life cycle stages of a NATO armament system. Figure 3-1 below provides an overview of the principal functional relations among the main elements.

Figure 3-1: RM framework: functional relations



- 1 • **System Life Cycle Stages.** During its life, an SOI transitions through different life cycle stages. Within NATO, the AAP-48 and AAP-20, respectively define and employ the principles of life cycle stages. According to AAP-48, a SOI must meet specific criteria or requirements to leave stage x and enter stage y. These criteria, as well as global objectives such as minimal Total Cost of Ownership, or optimized Integrated Logistic Support, are achieved through programmes, projects, organizations, or any combination of these elements.
- **Accelerated fielding** uses specific options (fast tracking, use of Commercial-Off-The-Shelf (COTS), etc.) to shorten the time to delivery. This approach is likely to generate additional and/or different risks for the programme. RM under accelerated fielding is described in section 5.2.
- 2 • **Programme / Project Management Process.** The Programme / Project management process should utilize RM to help increase the likelihood of achieving the objectives related to the life cycle goals.

- 3 •Risk Management Process. RM uses an established process to execute risk response actions such as mitigation.
- 4 •System Life Cycle Processes. ISO/IEC 15288 system life cycle processes (also described in AAP-48) provide an articulated process structure and activities which contain potential risk responses.
- 5 •Risk Register. The risk register is the repository for all risks and their attributes (e.g. links to associated action item repository, statuses, etc.) A risk register will usually be a software application (specific tool, Excel sheet, database, etc.) but may also be a paper based registry for simple projects. It is central to the framework as each of the other framework elements may read or write information in this repository.

The next paragraphs will describe those elements in more details.

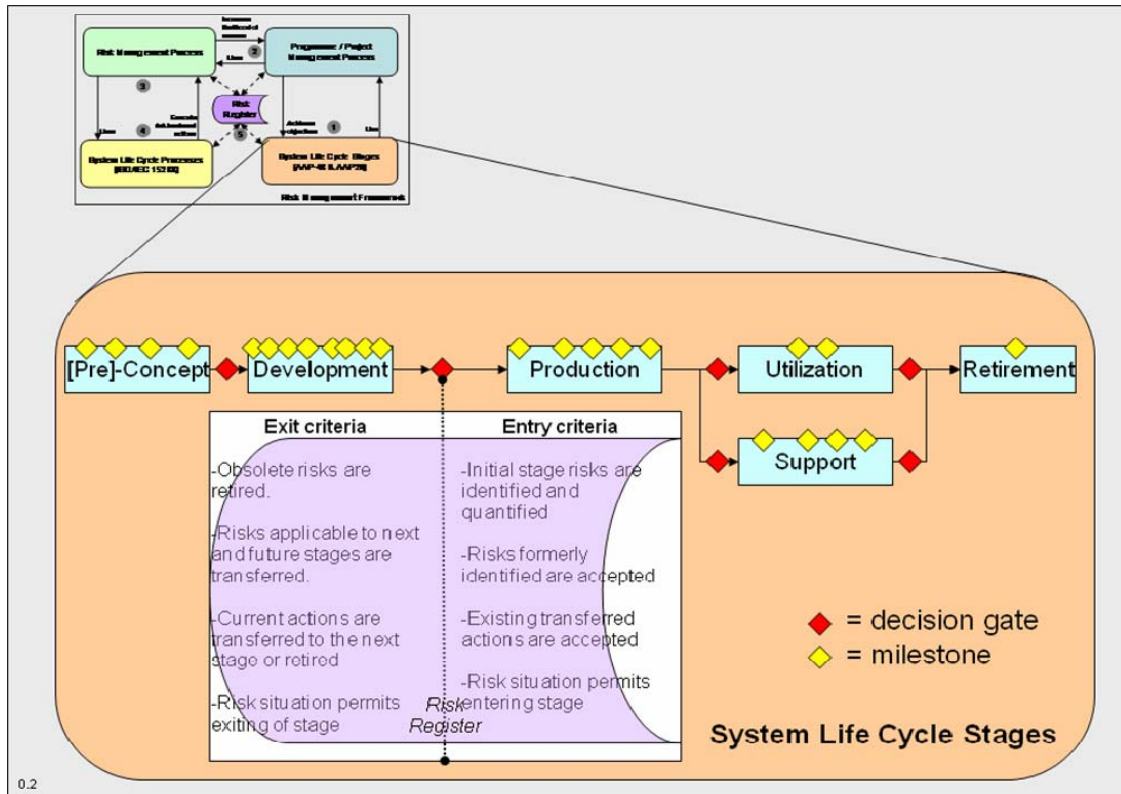
3.1 System Life Cycle Stages

The life cycle stages are the building blocks needed to define an overarching life cycle of an SOI. Stages are arranged in life cycle models where each stage represents a defined period (not always uninterrupted) of the life cycle.

The transition between the different stages is controlled by decision gates at the programme level. Within the stages, an SOI progresses through milestones (specific to each phase) at the project level. In other words, milestones control progress through a project while decision gates control progress through the programme. See also AAP-48 and AAP-20 for additional information on models, stages, and decision gates.

The RM framework described in this chapter is fully compatible with this approach and provides additional information to support the decision gates as shown in Figure 2 and described below.

Figure 3-2: RM framework: system life cycle stages



Understanding, coordinating and communicating risks among stakeholders throughout the life cycle are essential contributions to the success of the programme. The risk register is used to support this aspect.

3.1.1 Understanding Risks

Understanding the risks that are applicable to the current stage as well as those applicable to future stages contribute to the quality of the decisions to leave or enter a stage.

Risks must be identified as early as possible in the life cycle to allow early implementation of economical preventive actions (versus late implementation of expensive corrective actions). Risk identification will capture (in the risk register) various risk attributes so that when the risk information is provided accurately, completely and in a timely fashion at the decision gate, the decision authority has a better chance of making an appropriate decision.

3.1.2 Coordinating and Communicating Risks

The risk register is a repository where risk information is captured and managed, and also serves to coordinate and communicate the risks to all stakeholders. Maintaining the information in the risk register is an essential element of the RM process.

Typical activities to coordinate and communicate the risks and maintain the risk register at a decision gate include:

- **Retiring risks.** Various risks have been identified in the current and previous life cycle stages. These risks might no longer be applicable either because they were addressing the leaving stage (past risks) or because the actions performed in the leaving stage make them no longer applicable (future risks). To avoid transferring these obsolete risks to the next stages (and unnecessarily clutter the risk register), a careful review of the risk register must take place and the risks that are positively identified as no longer applicable must be retired. Any plan of actions, or actions being executed, for the treatment of these risks must also be terminated at the same time.
- **Transferring future risks.** If early identification of risks has taken place, the risk register may contain risks that were not yet applicable to the current stage but which may occur at future stages (next or further). The decision gate is an ideal time to coordinate the transfer of these risks to the next stage. It is also appropriate to transfer the control of any preventive actions that were already started to mitigate these risks.
- **Communicating** the lessons learned from past risk treatment actions to the stakeholders of the next stage will enhance risk management at the next stage.

3.1.3 Milestones and Decision Gates

Milestones and decision gates control the flow in and out of the life cycle stages (decision gates) and project phases (milestones), therefore providing a control mechanism. It is critical that the risk register be reviewed and updated before the milestone to ensure that risk information presented at this milestone or stage is accurate. In addition, a milestone review or stage meeting may be used to seek approval of new risks, obtain decisions on risk responses, and request resources for risk mitigation. It is also a perfect time to communicate the risks since the majority of internal and external stakeholders normally attend milestone reviews.

3.1.3.1 Milestone

A milestone is used within the perspective of a project. Every milestone represents a moment in the project life (or within a life cycle stage) where progress is measured and decisions are made. We can differentiate between **project milestones** (not necessarily related to the state of the product such as project planning or project closure reviews, see section 3.2) from **product milestones** (related to the state of deliverables such as technical reviews (SRR, CDR, etc.)), both types control the flow of the project.

3.1.3.2 Decision Gate

A decision gate is used within the programme perspective. At each decision gate, a twofold decision must be made: (a) to allow the programme to leave stage/phase x (current stage/phase), and (b) to allow the programme to enter stage/phase x+1.

Decision gates are extensively discussed in the AAP-48 and used in the AAP-20, stating:

“The decisions by national authorities at each decision gate must be taken with a thorough understanding of the objectives of the preceding and the following stages, as well as the overall programme goals. Successful completion of a programme is contingent upon coordination and communication between the appropriate stakeholders throughout the SLC.”

3.1.3.3 Entry Criteria

The authority responsible for the decision gate ensures that:

- **Initial stage risks are identified.** The decision to enter the stage must consider the risks. Some of the risks applicable to that stage may have been identified earlier in the life cycle and transferred from previous stages; however, identifying new risks will allow the new stage’s authorities, not only to make a better risk based decision, but also to gain additional knowledge about the programme and SOI. The use of risk identification checklists will greatly facilitate this activity.
- **Former risks are accepted.** The risks previously identified must be accepted in the new stage. Whether they are applicable to this stage or not they must be managed throughout the stage.
- **Existing actions are accepted.** The actions started in previous stages must be accepted if they correspond to the risk strategy of the stage.
- **The risk situation permits entering stage.** One element of the decision to enter the stage is to recognize that the risk situation allows the successful entry into the stage.

3.1.3.4 Exit Criteria

The authority responsible for the decision gate ensures that:

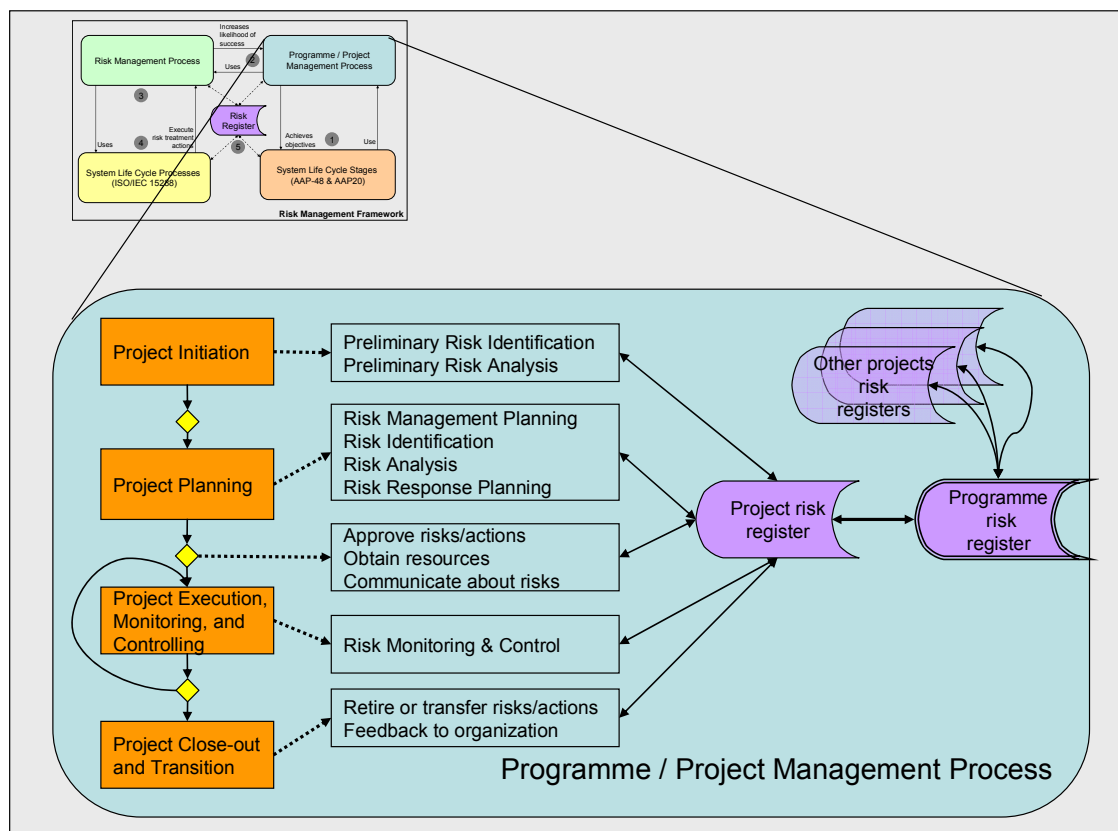
- **All obsolete risks are retired.** The risk register has been maintained and that non-applicable risks have been removed.
- **The valid risks are transferred.** The responsibility for risks is transferred to the next stage.
- **The current actions are transferred or abandoned.** If risk response actions are still in progress, they must be either transferred under the responsibility of the next stage (if they are to be continued) or be retired (if they are no longer needed).
- **The risk situation permits leaving stage.** One element of the decision to leave the stage is to recognize that no major risk response actions are required to be performed at this stage.

3.2 Programme / Project Management Process

The achievements of programme and project objectives allow the realization of the goals of a life cycle. By convention within AAP-20, a programme represents the management of the whole life cycle of one or more SOI(s) while a project represents a smaller size endeavour, within a programme, aimed at achieving one or more objectives. In other words, projects can generally be seen as the place where deliverables are produced in order to achieve the programme objectives.

The RM framework recognizes that RM is a key element of project management and incorporates the risk aspects in the project management structure. Figure 3 shows that risk management activities are performed at the various phases of the project. This is explained further in the following paragraphs. Details on the specific RM process activities can be found in chapter 4. Milestone reviews have been discussed above.

Figure 3-3: RM framework: programme / project management process



3.2.1 Project Initiation

At project initiation the project is defined and authorized. RM supports this phase by ensuring that major risks to the project are identified and analyzed (quantified). The following project initiation outputs must be supported by the preliminary risk identification and analysis:

- **Formal authorization of the project.** The decision to undertake a project must consider the risks. If too many high value risks are identified or if no risk identification has taken place, project authorization should be reconsidered.

- **Establish project scope.** The project charter and/or project scope statement should provide early indications that RM must be considered in the project. The details of the RM process will be defined later during RM planning.
- **Provide funding.** While it is recognized that RM increases the overall return on investment in projects, it must be funded to be effective. Obtaining funds at project initiation is essential since extensive RM activities and responses will be performed in the planning phase and the return of these activities and responses will only be capitalized in later phases.

The RM output of this stage may be captured in an existing risk register since no formal risk management infrastructure has been established yet.

RM needs to be closely linked and coordinated with other key project documents such as: plans (e.g. project management plan, test plan), schedules (project schedule), Work Breakdown Structure (WBS).

3.2.2 Project Planning

The project planning phase follows project initiation. At that time the major project management resources are available and may be used to perform RM activities.

- **RM planning.** RM planning is performed in parallel with project planning and uses, as much as possible, the tools, techniques and documents produced by the project, or available at the programme or organizational level. The risk register will be established and the RMP (or a chapter in the project management plan) will be written. The resources required for effective RM must be requested. These resources include principally tool support (risk register) and skilled personnel.
- **Risk identification.** Effective RM depends on early identification and analyses of risks. The list of risks in the risk register should grow with the evolution of the project plan; the more detailed the plan, the more accurate the list of risks. Risk identification for the project can be supported not only by the tools and techniques but also by an analysis of risks originating from other projects, or from the programme. The identification of risks in project planning should also include the risks inherent to this phase.
- **Risk analysis.** Similarly to risk identification, risk analysis is performed throughout project planning. The accuracy of probabilities and impacts also increases as the maturity of the planning increases.
- **Risk response planning.** Although not all resources needed to mitigate risks are available at this time, responses to risks should be documented early. It is generally recognized that project planning is the earliest and most efficient time to start arranging risk responses: indeed the development of the WBS may already include many preventive actions in response to risks.

3.2.3 Project Execution, Monitoring and Controlling

During project execution, the entire set of RM activities is performed in a continuous manner: new risks are identified and managed, existing risks are updated, risk responses are implemented, etc. Project monitoring and control involves monitoring the RM process and initiating corrective and preventive action to control its performance.

3.2.4 Project Close-Out and Transition

The value of the project close-out and transition phase should not be underestimated, especially if the project is an element of a larger programme. If the project is standalone, the major risk related activity in this phase is to provide feedback to enterprise RM by:

- Feeding historical data in to the risk register and thereby improve future risk identification, analysis, and responses.
- Providing improvements proposals for the corporate risk management process.
- Providing lessons learned to peers.

If the project or the risk register are part of a larger programme, the following activities are taken in addition to those above.

- The obsolete and non-applicable risks have been retired from the risk register and all other risks have been updated.
- The responsibility for risks is ready to be transferred to another project or is transmitted to the programme manager.
- If risk responses were initiated (but not completed) in the project they must be either transferred to another project, placed under the responsibility of the programme manager, or be retired (if they are no longer required).

3.3 Risk Management Process within NATO SLCM

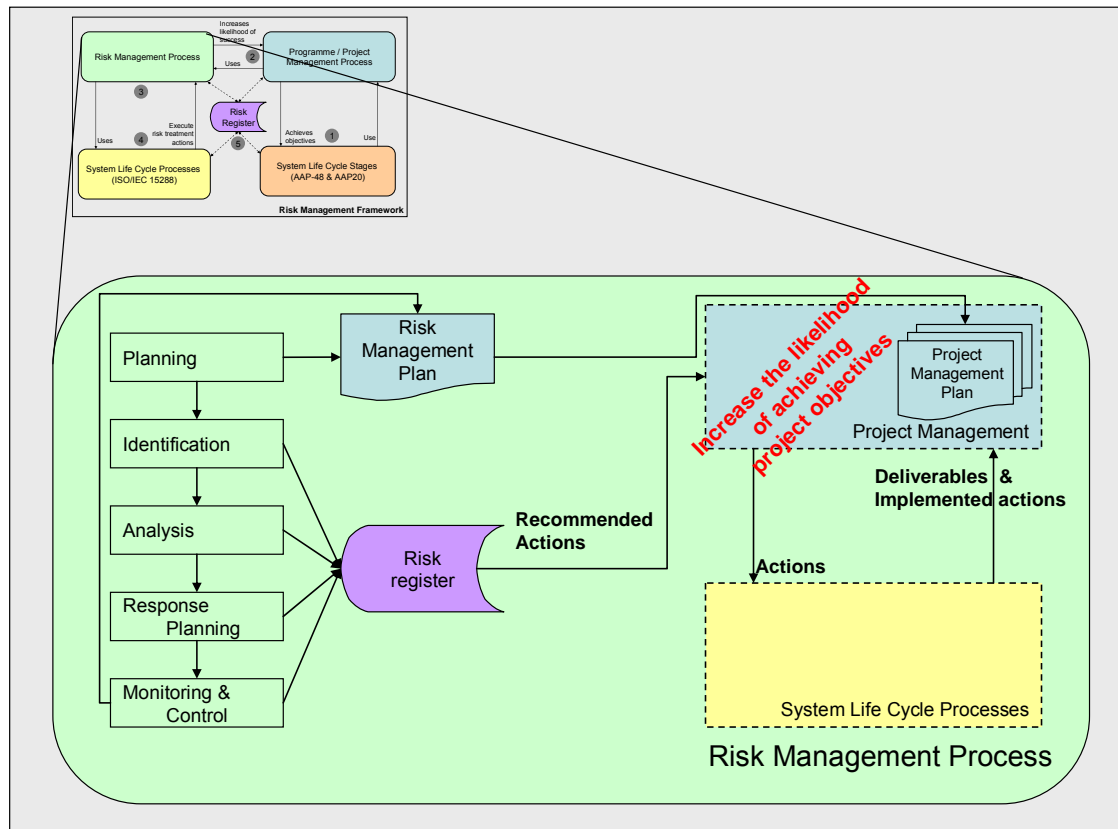
The RM process is the key element of the RM framework. It first establishes the environment required to execute RM (during risk planning), documented in the RMP. It then identifies risks, analyses them, and plans risk responses. The results of these activities are captured in the risk register. This sequence is repeated continuously to ensure that risks and plans remain current.

Actions planned as responses to risks are monitored by the RM process and executed under the direction of project management. Project management takes the recommended actions from the risk register, prioritizes them, provides the resources, and directs their execution. The system life cycle processes (implemented by the project or available through the organization) provide the means to execute the risk responses which result in deliverables and implemented actions. For instance, adequate responses to the risk that a key engineer would leave the project could be handled by the resource management process.

Ultimately, the mechanism shown in Figure 4 leads to the realization of the RM process goal: increasing the likelihood of achieving the project objectives.

The RM process is fully described in chapter 4.

Figure 3-4: RM framework: risk management process



3.4 System Life Cycle Processes

ISO/IEC 15288 and AAP-48 describe four process groups:

- Agreement processes
- Enterprise processes
- Project processes
- Technical processes

The role of the enterprise and project processes is to achieve the project goals within the applicable life cycle stages to satisfy an agreement.

Enterprise processes provide enabling resources and infrastructure that are used to create, support, and monitor projects and to assess project effectiveness. Project processes ensure that adequate planning, assessment, and control activities are performed to manage processes and life cycle stages. Appropriate processes are selected from the Technical processes and used to populate projects in order for the project to perform life cycle related work.

Within the risk management framework, those processes acquire a specific role: the one of performing risk treatment actions. Risk strategies such as mitigation (reducing the probability of occurrence or the impact) are performed, under the authority of project management, by system life cycle processes. Which process is used to mitigate a risk depends of many

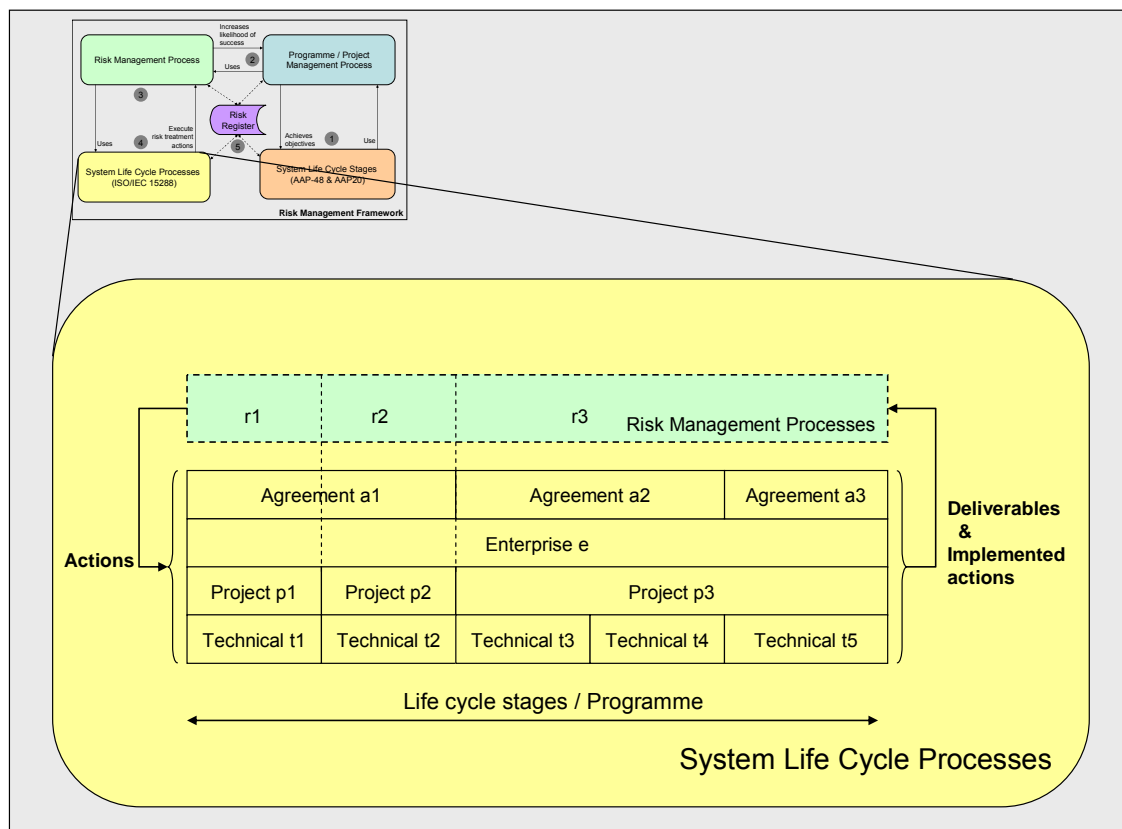
factors such as the availability of the process, the type of mitigation action, the level of mitigation required, etc.

For instance, the risk that a key design engineer would leave the project could be handled by the resource management process. In this case, the risk responses will be at the enterprise resource level and could be to secure a better contract with the existing engineer (reducing the probability) or hire another engineer as fall back solution (reducing the impact). The same risk could also possibly be handled by the architectural design process. In this case, the responses will be technical and could include ensuring that the design is simple or using standard methods (e.g. using Unified Modelling Language). This mitigation reduces the impact of the key engineer leaving by facilitating the transfer of work to another designer.

The complexity of the interrelationships between the different processes is shown in Figure 5. This figure shows an example implementation of a programme through three projects (p1, p2, p3). Those three projects contain three different instantiations of the risk management process (r1, r2, r3). This basically means that each project uses a different risk management plan, but they may share the same data or tools (e.g. risk register). Those projects use different [groups of] technical processes (t1, t2, t3, t4, t5), agreement processes (a1, a2, a3), and a common enterprise process (e) to implement risk response actions.

This figure shows the need to have a complete view at the programme level to ensure that, from the start, projects are aware of potential risk responses that may be exercised by whom.

Figure 3-5: RM framework: system life cycle processes



The chosen risk response action will condition the process that will execute it. Therefore, the selection of a risk response should also verify that a process suitable to perform the action exists and that it is available and can perform the action. If the process is not under the control of the project, the action has to be contracted (tasked) and funded.

The sections below provide an overview of the general purpose of life cycle processes to perform risk actions.

3.4.1 Agreement Processes

Agreement processes establish agreements between two organizations. For risk management, the processes in this category may be used to transfer entire risks to third parties by means of contract or insurance. It may also be used to contract the execution of risk responses, such as mitigation. The transfer of risk or risk response nearly always involves the payment of a premium to the party accepting the risk.

From a life cycle point of view, the transfer of risks through agreement processes can also happen between different life cycle stages. For instance warranties and guarantees following the production stage prevent some financial risk in the support stage.

In addition, risks related to the selection of suppliers, the definition of acceptance criteria for products and services, the payment of goods, etc could be handled through these processes.

3.4.2 Enterprise Processes

The Enterprise processes manage the initiation, support and control of projects and provide resources and infrastructure for the projects.

Depending on the projects environment, enterprise processes can be provided by the programme, the organization, or both.

The first role of the enterprise processes for RM is to provide the project with existing organizational assets. Depending on the risk maturity of the organization, a project could get an important head start if inheriting the following elements:

- Organizational RM processes, standards, policies, guidelines, templates, and other work instructions. The availability of standard risk categories, probability, impact, and severity definitions will allow the project to fit into the organization and more easily exploit existing information as well as more easily share data.
- Historical information. Historical risk data of similar projects in the organization plays a crucial role in more accurately estimating likelihood and occurrences, and also in helping to select the best responses based on those that have succeeded before. The availability of this data (e.g. in the risk register) will increase both the effectiveness and efficiency of risk management.
- Communication lines with other projects, programmes, and organization. When a project is established, the project leader will benefit from existing horizontal or vertical RM related communication lines. RM will benefit from the ability to immediately start providing visibility to higher management, to benefit from information of other projects, or to take advantage from organizational resources.
- Enterprise RM responsibilities. Established roles and responsibilities for RM will support the communication of risks and execution of responses.

- Risk register. This tool is valuable not only because it allows the capture of risks but also because it can support the execution of processes and instructions, link to checklists, contain historical information, sustain communication, etc. The risk register is often the glue which assembles the different risk elements into practical and usable information.

3.4.3 Project Processes

As already discussed above, the project management process is responsible to manage RM responses. In addition, it may also be used to perform risk responses related to:

- Project planning. For instance, risk avoidance can be done by extending the schedule to meet some high value objectives.
- Project assessment. If needed, the project assessment process may support RM by evaluating RM effectiveness as part of the project performance measures. Project assessment may also be used to monitor risks related to:
 - Deviations between project plans and actual cost, schedule and quality.
 - Performance of quality assurance.
 - Effectiveness of project team structure, roles and responsibilities.
 - Adequacy and availability of the project's supporting infrastructure.

by:

- Including risk management in the reviews, audits and inspections.
- Monitoring the risk management process.
- Analyzing the results of risk management actions to identify deviations or variations from expected results make appropriate recommendations.
- Providing periodic status report as required.
- Project control. The project control process may be used to direct RM execution. This process will also ensure that risks are considered in the decision gates and milestones.
- Decision-making. The process may support RM by providing the framework to select the most appropriate risk treatment. It responds to a request for a decision for risk responses encountered during the system life cycle, in order to reach specified, desirable or optimized outcomes. Alternative risk actions are analyzed and a risk response is selected and directed. Decisions and their rationale are recorded in the risk register to support future decision-making.
- Configuration Management. Configuration management maintains the integrity of all identified RM outputs such as the RMP or the risk register.
- Information Management. Information management supports the relevant, timely, complete, valid and, if required, confidential dissemination of risk related information (e.g. the risk register) to interested parties. It ensures the transmission of appropriate risk data to other projects, the programme, customers and suppliers.

3.4.4 Technical Processes

In summary, the technical processes are those required to define, design, build, employ, maintain, and retire a SOI. With such a large scope, they offer many opportunities to be used for risk responses. Because any different programme/project/product/SOI combination may implement different technical risk responses, defining precise risk responses for all technical processes would not be helpful. Furthermore, the description of the processes itself are normally sufficient to match them with risk responses. Therefore, some general guidelines on how to use these processes are provided below.

Guidelines on the use of technical processes for RM:

- The timeliness of use of technical processes must correspond to specific project or programme phases or stages. For instance, the requirements analysis process will be used mainly during the requirements definition phase of the project. Also, the maintenance process will be exercised during the support stage of the SOI. This does not mean that those technical processes can only provide risk responses during their matching phase. For instance, the verification and validation processes may provide risk responses to requirements that cannot be adequately tested or verified.
- In general, risks should be identified as early as possible in the life cycle of the programme or SOI to increase the probability that the most effective and efficient risk response can be implemented at lowest costs. For instance, the majority of risks related to product retirement need to be identified during design to yield the best risk responses.
- When the chosen risk response has to be executed by a technical process in another life cycle stage, it will have to be coordinated at the programme level or contracted through the agreement process.
- Several tools and techniques, available through NATO or other means, facilitate the selection of the most appropriate technical process for risk response. These tools and techniques, many of which are used during acquisition, include, but are not limited to: Life Cycle Costing, Integrated Logistic Support, Continuous Acquisition and Life-cycle Support, etc.

4 Risk Management Process

The RM process aims principally at increasing the likelihood of success of a project. A structured RM process is required to facilitate open communication and cost effective management of risks. The process also ensures that all project personnel use a disciplined approach to reduce risk to an acceptable, manageable level. The RM process should be managed at each stage of the project and integrated within the project management process. The notional RM process is described in Table 4-1: RM process: overview

The process described is a five step process in which each step interacts with each other. Although the steps are presented as discrete steps, in practice they will overlap and interact most of the time.

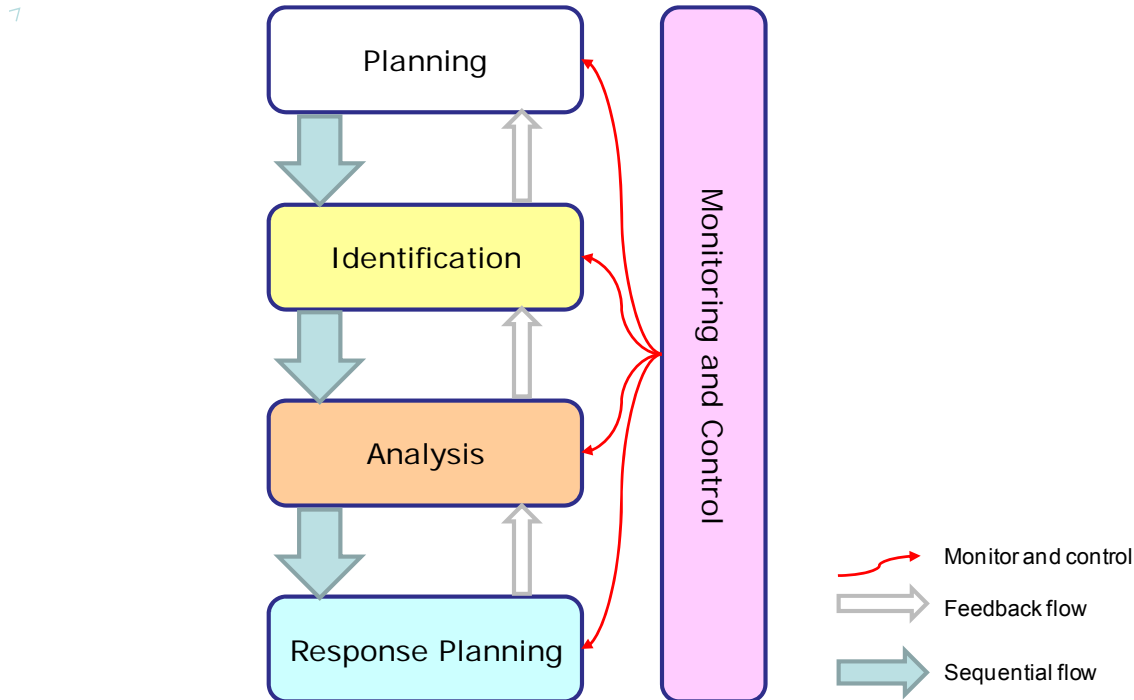
The first step, RM Planning, has to address how the other steps have to be handled. This step will be explained at the end of the chapter (section 4.5) in order to take into account the principles associated with the other steps.

Table 4-1: RM process: overview

Step No	Step		Section	Actions	
1	Risk Management Planning		4.5	Determining how to approach and plan the RM activities for a project, who will be involved and procedures to be used.	
2	Risk Assessment	Risk Identification		4.1	Determining which risks might affect the project and documenting their characteristics.
3		Risk Analysis	Qualitative Risk Analysis	4.2	Performing a qualitative analysis of risks and prioritise them.
			Quantitative Risk Analysis		Numerically estimating the probability and risks impact on project objectives.
4	Risk Response Planning		4.3	Developing risk response strategies and actions to enhance opportunities and to reduce threats to the project's objectives.	
5	Risk Monitoring and Control		4.4	Executing risk response plan. Evaluating its effectiveness throughout the project life cycle. Monitoring residual risks, identifying new risks.	

A flow diagram version of the RM process model is presented in Figure 4-1.

Figure 4-1: RM process: flow diagram



The RM process is a continuous process throughout the project life. Each RM process step may be performed at any project phase. For instance, risk identification will occur during project planning, but might also be performed during project execution and control, as changes are made and problems discovered. Each step of the process will be done as completely as possible and then fine-tuned through iterations.

The following sections describe each of the RM process steps applying a common structure that includes: inputs, tasks, outputs, and toolbox. The toolbox section describes the tools most commonly used; additional tools are described in Annex F -.

4.1 Risk Identification

Risk identification might be the most important step of the RM process. Timely identification and visibility of risks are necessary to ensure that risks are assessed and brought to management attention in time to preclude any adverse impacts and foster the development of opportunities.

Risk identification deals with examining all elements of the project (including the environments) to detect and document risks and their associated root causes. It essentially answers the question: “What can go wrong (threats) or right (opportunities)?”

Risk identification should begin as early as possible in the project life cycle and should continue throughout the project life cycle with regular project reviews. Risk identification focuses on identifying both the threats and opportunities to the projects’ objectives and documenting some of their characteristics.

This step should involve all stakeholders from the project, programme, or SOI because risks need to be identified from all perspectives. The RMP should identify the procedures for identifying and documenting risks. Risk identification starts as soon as a project is initiated and may be applied throughout the whole project. The majority of risks are uncovered during the initial risk identification which also represents the major risk identification effort.

The specific objectives of risk identification are to:

- Make a list of risks (threats and opportunities) by examining all relevant elements/areas of the project and product.
- Understand the root causes associated to the risks and provide clear risk statements.
- Define or maintain the required risk attributes in the risk register.

Risk statements must be prepared once the risk has been identified and must include both a risk event (or condition) and an impact. They may also include a (root) cause. The three components of a risk statement (risk definition) are:

- **Risk event or condition:** The context of the risk time frame, the concerns or doubts about the risk, the circumstances, the conditions under which the risk could occur, the interrelationships within the project, etc.
- **Impact:** A single phrase or sentence that describes the key possible outcome(s) on the objectives. It focuses on the intermediate and long-term impacts of the risk. Understanding the depth and breadth of the impact is useful information in determining how much time, resources, and effort should be allocated to the mitigation.
- **Cause:** A single phrase or sentence briefly describing the key elements that are causing the risk. It provides information about the risk root causes that is useful when determining how to mitigate a risk.

Risk statements may be written:

- Using a “cause-risk-impact” format (As a result of (X), (Y) may occur which would/could/may lead to (Z)).
- Using an “if-then” format (if a certain event or condition occurs, then a certain impact is the result).

The examples below are based on a situation where a radar system is being developed and includes a circuit card component procured from a single source vendor.

- Given that XYZ is the only vendor source for the transceiver circuit card (cause), and XYZ could discontinue production of the card making it unavailable during the radar system production (risk), deliveries of the radar system could be delayed (impact).
- The single source vendor of the transceiver circuit card could discontinue production of the card (cause), so that the circuit card becomes unavailable during the radar system production (risk), resulting in delays in the radar system deliveries (impact).
- If the transceiver circuit card is not available during the radar system production (if), then deliveries of the radar system could be delayed.

Risk identification should also identify risk triggers. A risk trigger is an unambiguous event recognized as a warning sign that announces the imminence of a risk and may lead to a re-assessment of a risk or the need to implement some specific risk responses. Examples of

risk triggers may be a financial report of a key supplier that may have potential impact on future commitments, or positive economic changes that may have negative impacts on human resource requirements (e.g. retirement and staff turnover).

Again, it is important to emphasize that if the identified event or condition has already occurred or is certain to occur, it is not a risk, it is an issue, and should be resolved accordingly.

4.1.1 Inputs

The main inputs to risk identification include, but are not limited to:

- The outputs from the project management process (charter, objectives, plans, scope statement, contracts, etc.)
- The Risk Management Plan (including risk categories).
- Historical information (risks from similar projects).
- Interviews of experts (list of technical or financial risks)

4.1.2 Tasks

Risk identification is an iterative process, meaning that it will be repeated throughout the life cycle, because not all risks can be identified at any given point in time. During this step, the following tasks will be performed:

Table 4-2: Risk identification tasks

#	Tasks
1.	Create a list of risks (include opportunities as required) with the stakeholders considering assumptions.
2.	Develop risk statements (potentially including risk causes) and document the required risk attributes such as the risk category.
3.	Identify the risk triggers.
4.	Repeat tasks 1 to 3 until the team is confident that the major risks and triggers have been identified.
5.	Document the identified risks in the risk register and ensure that key personnel is informed of any new or changed risk.

4.1.3 Outputs

The main output from risk identification is the [updated] risk register with [new] risks (including the risk statement, triggers, and required attributes). In addition, feedback from this step could also lead to updated risk categories and proposed changes to the project's assumptions.

4.1.4 Toolbox

Risks within the project could be identified using different approaches, which will complement each other:

- Top – Down Approach:** The Top – Down approach begins with an overall project view and details the risks stepwise to lower levels of the project.
- Bottom – Up Approach:** The Bottom – Up approach represents the core of risk identification, because the risks will be identified at the work package level in addition to the project level.
- Top – Down combined with Bottom – Up Approach:** In order to ensure the completeness of the risk identification the top down and the bottom up approaches will be merged.

The toolbox elements below can be used with any approach.

4.1.4.1 Delphi Technique

Delphi technique can be used to obtain a consensus of expert opinion, which participate anonymously, on what risks exist in the project through a facilitated process. The facilitator forwards questionnaires (a request for information) to the experts requesting inputs on project risks; the responses are compiled and summarized, and then returned to the participants for additional comments and further review until consensus is reached. The process of forwarding, compiling, summarizing and returning can continue for several rounds until a consensus is reached. Important: this technique helps reduce bias in the data and keeps any one person from having undue influence on the outcome.

4.1.4.2 Checklists

Checklists are quick and simple tools for risk identification. A checklist gives a listing of general risks that is applicable for all projects or a list of typical risks for a specific technology or project environment. A checklist will never be exhaustive; therefore one should also explore other items that do not appear on the list.

Table 4-3: Example of risk identification checklist

D	Scope of Programme, project or procurement
D.1	Is the 'project' scope well defined and agreed in terms of what the project should deliver?
D.2	Is the 'project' well defined and understood by the project team and all stakeholders?
D.3	Does the scope of the 'project' include all of the business areas affected?
D.4	Does the scope of the 'project' address modular and/or incremental delivery, each with clear business scope and business case, where appropriate?
D.5	If the project fails to deliver the expected outcome, will the business be able to continue?
D.6	Does the 'project' have some flexibility on delivery dates?
D.7	Are the business processes being supported or enabled by the technical infrastructure (solution) well understood, well defined and formally documented by the project team?
D.8	Do all the people who have a stake in the project agree on what the project should deliver and how it will benefit the business?
D.9	Is there a business case that clearly states why the changes are needed, what the changes are, how the business will benefit and how benefits will be measured?
D.10	Has the necessary funding been approved and allocated, with budget holder/s identified?
D.11	Have you considered how changes will be dealt with in the future?
E	'Project' organisation and control
E.1	Are the stakeholders committed in their support of the 'project' and its objectives?
E.2	Are customers and/or users able to commit sufficient time to the 'project'?

E.3	Is the 'project' plan complete and considered to be achievable?
E.4	Are good relationships established between the project team, customers and suppliers?
E.5	Are the project management approach and milestones approach understood by all parties?
E.6	Is there adequate budget provision (risk allowance) for contingency actions?
E.7	Are the project interfaces defined and being managed effectively?
E.8	Is the project fully under control, in terms of progress against milestones, budget and deliverables?
E.9	Are there appropriate processes for managing change to requirements?
E.10	Are there established and effective communications between the project and all stakeholders?
E.11	Are the project dependencies clearly identified and being managed effectively?
F	Team capability, experience and support
F.1	Are the necessary project skills available within the project team?
F.2	Are team members able to commit sufficient time to the project?
F.3	Is there sufficient fall back for critical resources?
F.4	Has the team access to the specialist expertise needed, when required?
F.5	Is the team adequately supported in terms of accommodation, administrative support and tools?
F.6	Is there enough time and resource within the schedule for necessary information gathering?
F.7	Has the team access to people who understand the business domain and the business needs?
F.8	Is there a good mix of leadership and other key attributes within the project team?
F.9	Are roles and responsibilities clearly defined both within the team and third party interfaces?
F.10	Are the customer &/or user roles clearly defined and understood?

4.1.4.3 Historical Information

Examination of existing information such as lessons learned, risk registers and categories from previous, similar projects help identify risks. This is based on the premise that every system or product will be established through a combination of some existing system(s), components, and/or concepts. Another good source of information is test results from previous, similar programmes; particularly test failures.

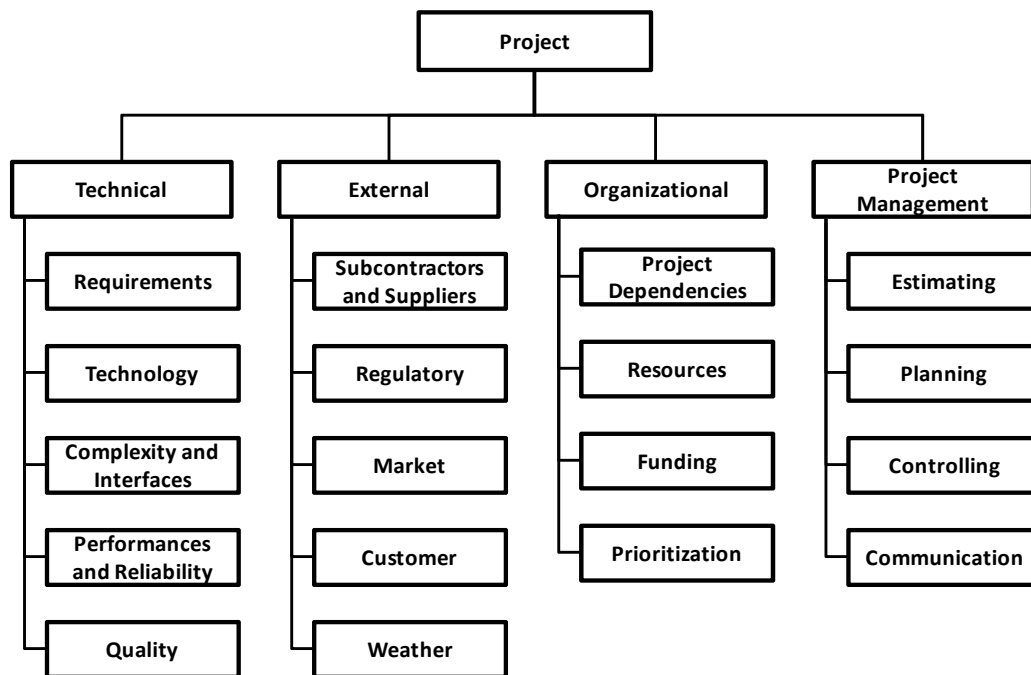
4.1.4.4 Risk Categorization

Risks may be categorized by source, area of project and organized in a useful breakdown (see Figure 4-2 Risk vs. Issue) often called Risk Breakdown Structure (RBS). These categories support risk identification by providing a way to verify that all relevant areas have been covered during the risk identification.

Categorisation of project risks could be accomplished through:

- Decomposition into relevant elements or areas. Decomposition may be oriented to requirements, processes, functional areas, technical baselines, or acquisition phases.
- Create a WBS (product-oriented tool) as early as possible in a programme, which is particularly useful in identifying product oriented risks.
- Use a process-oriented framework, to determine the process-based risks root causes, which could be tracked via the WBS structure to view impacts to schedule, cost, and performances.

Figure 4-2 : Risk categorisation by functional area



4.2 Risk Analysis

Risk analysis is the process of examining identified risks and determining the risk exposure based on estimated probability and impact values. Risks should be prioritised by considering other factors such as the time frame for response.

Qualitative risk analysis is usually a rapid and cost-effective means of establishing priorities for risk response planning or for the quantitative analysis, if required. Quantitative risk analysis is conducted on selected risks to show how the combined effects of those risks may impact objectives.

Many risk management models split the risk analysis into qualitative and quantitative risk analysis tasks. Considering that many of the same inputs, tasks, tools and techniques, outputs, and associated resources are needed for each type of analysis, this document describes risk analysis in one step, but ensures that the key differences between qualitative and quantitative analysis are highlighted in the description below.

4.2.1 Inputs

The inputs to risk analysis include:

- List of risks within the risk register.
- Scales to qualify and quantify risk probability and impact levels.
- Probability and impact matrix to determine risk exposure.
- Historical records showing how similar risks were qualified in the past.
- For quantitative risk analysis, a selection of meaningful interdependent risks.

4.2.2 Tasks

Table 4-4: Risk analysis tasks

#	Tasks
1.	Determine probability, impact, and exposure based on the given scales and matrix.
2.	Prioritize risks based on exposure and other factors.
3.	Decide whether to perform quantitative risk analysis on selected risks.
4.	Perform quantitative risk analysis if required.
5.	Refine probability, impact, and exposure based on outputs from quantitative risk analysis. Re-prioritize risks based on updated values.
6.	Update the risk register with newly obtained risk attributes and ensure that key personnel are informed of the updated risk situation.

4.2.3 Outputs

The output of the risk analysis is the updated risk register.

4.2.4 Toolbox

The toolbox elements below rely heavily on judgment and educated guesses but may be the most suitable approach to qualitative analysis.

- Apply judgment to rate probability and impact using matrixes as shown in 2.10.
- Delphi technique
- Risk Assessment Checklist

The toolbox elements below rely more on technical, historical, or statistical data and are more prone to be used in a quantitative analysis.

- Calculate actual cost/time impact
- Use historical records
- Monte Carlo simulation

Both approaches (qualitative and quantitative) are complementary. In all cases a qualitative analysis has always to be done prior an eventual quantitative one in order to reduce the effort requested to apply the quantitative analysis.

The Monte Carlo simulation is described below due to its prevalent use in many different industry sectors.

4.2.4.1 Risk Assessment Checklist

Checklists can also be used for assisting in assessing the risks. Like for risk identification checklists, one should also explore other items this approach has to be completed by a more exhaustive one.

Table 4-5: Example of risk assessment checklist

Risk Assessment Checklist				
Characteristics		Low risk	Medium risk	High risk
A. Scope				
A1.	The scope of the project is:	Well defined & understood	Somewhat defined, but subject to change	Poorly defined and/or likely to change
A2.	The requirements of the project are:	Understood and straightforward		Very vague or very complex
A3.	The total estimated effort hours are:	Less than 5,000		Greater than 50,000
B. Schedule				
B1.	Are the project's major milestones and operational dates:	Flexible - may be established by the project team and recipient personnel	Firm - pre-established and missed dates may affect the business	Fixed - pre-established by a specific operational commitment or legal requirements beyond the team's control
B2.	Project duration is estimated at:	Less than 1 year	1 year to 2 years	Greater than 2 years
C. Budget/Cost				
C1.	The project budget is based upon use of a proven successful cost estimation process used by personnel with estimation experience:	Yes – Proven estimation process with experienced personnel	Some experience or process	No – Estimates not established by personnel with any experience nor any proven process
C2.	Project funding matches or exceeds the estimated cost and is stable.	Funding is greater than estimated need and/or is expected to be stable.	Funding is marginally adequate and expected to remain relatively stable.	Funding is less than estimated need and/or its stability is highly uncertain.
D. Project interdependencies				
D1.	This project's dependencies on linkage projects could best be described as:	Slightly dependent, can be successful without linkage project deliverables	Somewhat dependent, without linkage project deliverables, schedule delays possible	Highly dependent, cannot proceed without deliverables from linkage projects
E. Human Resources				
E1.	The Project Manager's experience and training is:	Recent success in managing projects similar to this one	Recent success in managing a project not similar to this one or trained and no actual experience	No recent experience or project management training
E2.	Describe the experience of project personnel with the tools and techniques to be used.	Experienced in use of tools and techniques	Formal training in use of tools and techniques but little or no practical experience	No formal training or practical experience in use of tools and techniques

Risk Assessment Checklist				
Characteristics		Low risk	Medium risk	High risk
E3.	The project team is:	Located together		Dispersed at multiple sites
F. Management/Senior Leadership Support				
F1.	The project sponsor is:	Identified, committed, and enthusiastic		Not identified or not enthusiastic
G. Organizational Impacts				
G1.	The project participant(s) providing content knowledge on the project:	Are not required on the project or are very knowledgeable	Are somewhat inexperienced	May not be available as needed or are unknown at this time
G2.	Operational processes, procedures, policies require:	Little or no change	Occasional to frequent changes	Substantial change
G3.	How would you rate the readiness level within the project recipient and stakeholder organizations for changes this project will create?	High readiness (Passionate and enthusiastic)	Moderate readiness	Low readiness (Passive and hard to engage)
H. Technology				
H1.	The technology being utilized is:	Mature	Emerging	Leading Edge
H2.	The technical requirements are:	Similar to others in the company		New and complex
H3.	The subject matter is:	Well known by the project team		Not well known by the project team
I. Supplier				
I1.	If development is required	The vendor is familiar in this market		The vendor is new to this market
J. Other (Add as appropriate to project)				
J1.				

4.2.4.2 Monte Carlo Simulation

With regards to project management, Monte Carlo simulation is “a technique that computes or iterates the project cost or schedule many times using input values selected at random from probability distributions of possible costs or durations, to calculate a distribution of possible total project cost or completion dates. ” (PMBOK, 2004).

Monte Carlo simulation is primarily (but not only) useful in the areas of cost and time management to quantify the risk level of a project's budget or planned completion date, taking into account both the risks as already identified and qualitatively assessed and the uncertainty associated with both the baseline of project schedules and/or budgets and the risks themselves.

Monte Carlo simulation aids the project manager in answering questions such as, "Taking into account the uncertainty and the risks, what is the probability of meeting the project due date?" and, "What is the 90 per cent confident project duration?"

In time management, Monte Carlo simulation may be applied to project schedules to quantify the confidence the project Mgr should have in the target project completion date or total project duration. Project Mgr.

In cost management, the project Mgr can use Monte Carlo simulation to better understand project budget and estimate final budget at completion. Instead of assigning a probability distribution to the project task durations, project manager assigns the distribution to the project costs. These estimates are normally produced by a project cost expert, and the final product is a probability distribution of the final total project cost. Project managers often use this distribution to set aside a project budget reserve, to be used when contingency plans are necessary to respond to risk events.

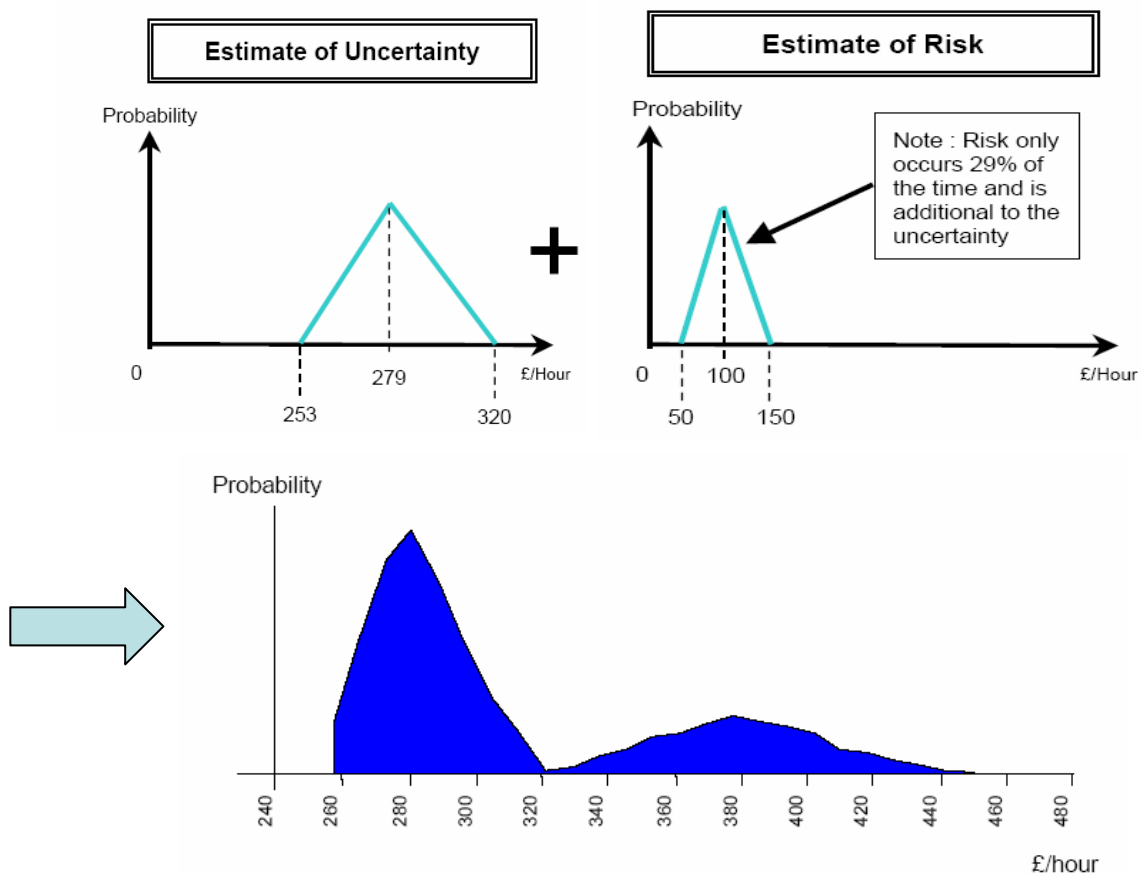
Monte Carlo simulation can certainly be an extremely powerful tool that allows project Mgrs to incorporate both uncertainty and risk in their project plans and set reasonable expectations on their projects, with respect to schedule and budget.

The results of simulation are quantifiable, allowing project Mgrs to better communicate their arguments when management is pushing for unrealistic project expectations. Recent advancements in computing capability and Monte Carlo simulation software allow project managers to implement the method more easily.

However, Monte Carlo simulation is still not a popular tool in current project management practice considering the practical usefulness of the method in project schedule, cost, and risk management. This is primarily due to its statistical nature, which many project managers are reluctant to tackle. More project management education and training programs that demonstrate the simulation and hands on experience with the Monte Carlo Simulation techniques to current and potential project managers are needed to overcome

For more explanation of the use of Monte Carlo simulation, we refer to the UK MoD process guide for risk practitioners called "three point estimates and quantitative risk analysis, a process guide for risk practitioners".

Figure 4-2: Example of Monte Carlo statistical combination of risk and uncertainty



4.3 Risk Response Planning

The objective of the risk response planning is to determine what can be done to increase the project's likelihood of success. The following strategies may be used:

- Avoidance
- Mitigation
- Transfer
- Exploit
- Enhance
- Sharing
- Acceptance
 - Active acceptance
 - Passive acceptance

Those strategies are further detailed in 4.3.4.

A strategy represents a general approach to handle a risk, this strategy is determined based on the type and rating of the risk. The project must consider the guidance for risk response strategies identified in the RMP, for example the RMP could recommend that all risks rated “low” be handled by passive acceptance. The strategy must be translated into concrete plans and actions, and documented in the risk response plan or as action items.

4.3.1 Inputs

The inputs to risk response planning include:

- Recommended strategies in the RMP
- List of prioritised and analysed risks within the risk register
- Historical records about risks responses from the past projects and common risk causes

4.3.2 Tasks

Table 4-6: Example Risk response tasks

#	Tasks
1.	Examine each risk and determine the most appropriate risk strategy.
2.	List alternative risk responses and actions to implement the strategy.
3.	Determine the most appropriate alternative based on cost effectiveness, or any other factor (regulatory, availability of resources, etc.). This task will also look at potential “global” risk strategies to handle multiple risks (i.e. handling the common root cause rather than separate effects).
4.	Determine residual and secondary risks that would result from the application of the selected alternative.
5.	Perform limited risk identification and analysis for residual and secondary risks.
6.	Repeat steps 1 to 5 until the risk responses provide an acceptable solution to reduce the risks to an acceptable level.
7.	Update the risk register with newly obtained risks and attributes and ensure that key personnel are informed of the updated risk situation.
8.	Risk owners develop detailed risk response plan as required.
9.	Gain approval from management and other stakeholders for the risk response plans which may impact any other plan (e.g. financial plan, quality management plan, schedule, test plan, etc.) or project documents (WBS, schedule, etc.)

Different skills are needed for risk response planning. Whereas risk identification use experience and qualitative and quantitative risk analysis use analytical and mathematical skills, the risk response planning uses creativity.

The effectiveness of the response plans and actions should be evaluated by means of objective indicators. These indicators should consist of cost and schedule data, technical performances measures and project metrics.

A secondary risk is a new risk that is generated by a response to another risk.

A residual risk is what remains from an existing risk after the risk response has been successfully implemented.

4.3.3 Outputs

The outputs of risk response planning are:

- Approved risk response plans which identify impact to other plans and project's artefacts. Risk response plans basically describe the actions to be taken to implement the risk strategy, the resources required, the timeline of implementation, the associated costs, the other plans and project documents impacted, and the expected outcome. The exact contents and format of the risk response plan will have to be determined and tailored for the project.
- Residual risks
- Secondary risks

4.3.4 Toolbox

The risk strategies explained below support the realization of the risk response plan.

4.3.4.1 Risk Strategies

Options for risk response planning are often referred, in their entirety, as risk handling, mitigation, or simply risk strategies. Options to select from may be different for threats and opportunities.

Risk strategies for threats include:

- **Avoidance:** eliminating the risk by eliminating its cause (modifying the scope of the project or of the product, adapt the project objectives, adapt the schedule, etc.).
- **Mitigation:** reducing the probability and/or the impact of the risk. The following mitigation options could be considered:
 - Change in approach to execute a task.
 - Multiple development efforts.
 - Trade studies.
 - Early prototyping.
 - Incremental development.
 - Technology maturation efforts.
 - Robust design.
 - Design of experiment.
 - Open systems.
 - Reviews, walkthrough, and inspections
 - Government Quality Assurance activities
 - Use less complex processes.
 - Increase redundancy.
 - Add or change resources or suppliers.

- Manufacturing screening.
- Demonstration.
- Outsource.

- Transfer:** making another party responsible for the risk. This can be done through purchasing of insurance, performance bond, warranties, guarantees or contracting (e.g. fixed price strategy). Transfer does not eliminate the risk but simply transfers the responsibility to a third-party.

Response strategies for opportunities include:

- Exploit:** increasing the opportunity by making it happen. Directly exploiting responses include assigning more talented resources to the project or to use new techniques to reduce the time to completion, or to provide better quality than originally planned. Caution: as an opportunity like this one often leads to secondary risks (threats), a proper balance cost/effectiveness has to be made before adopting this strategy.
- Enhance:** increasing the probability or impact values of the opportunity. For example, the project manager could propose a good incentive to the project team so that they get motivated to reduce the project time to completion.
- Share:** sharing a positive risk involves allocating ownership to a third party who is best able to capture the opportunity for the benefit of the project. Examples of sharing actions include forming risk-sharing partnerships, teams.

Response strategies for both threats and opportunities include:

- Acceptance:** accepting that the risk materializes. A strategy that is adopted because it is seldom possible to eliminate all risk from a project. This strategy indicates that the project team has decided not to change the project management plan to deal with a risk, or is unable to identify any other suitable response strategy. It may be adopted for either threats or opportunities. This strategy can be either passive or active
 - Active acceptance:** preparing contingency plans to be executed when the risk occurs. The most common active acceptance strategy is to establish a contingency reserve, including amounts of time, money, or resources to handle known-or even sometimes potential, unknown-threats or opportunities.
 - Passive acceptance:** leaving actions to be determined as needed after the risk occurs.

One or more choices above may be selected for each risk.

4.4 Risk Monitoring and Control

Risk monitoring and control is initiated after the initial risk management planning, identification, analysis, and response planning. It is executed to:

- monitor and control the execution of response plans (including the measurement the progress associated with its implementation),
- monitor the project environment (deliverables, schedules, regulatory requirements, etc.) to maintain situational awareness,
- initiate subsequent risk management planning, identification, analysis, and response planning activities, and
- transfer historical data and lessons learned at the end of the project.

During this step of the process, the investment in the previous risk management activities is capitalized. The monitoring process systematically tracks and evaluates the effectiveness of risk response actions. Monitoring results may also provide a basis for developing additional risk response options and/or approaches, or updating existing risk response strategies, and/or re-analyzing known risks. In some cases monitoring results may also be used to identify new risks and revise some aspects of risk planning. In summary, risk monitoring and control evaluates the effectiveness of the whole risk management process and triggers corrective and preventive actions as required (eventually through the project management process).

4.4.1 Inputs

- RMP.
- Risk response plans.
- Work results (deliverables, meetings, testing results, etc.).
- Technical performance measurement (for example obtained using Earned Value Analysis).
- Updates to plans, project, and product documents.
- Changes in the environments.

4.4.2 Tasks

Table 4-7: Risk monitoring and control tasks

#	Tasks
1.	Verify and ensure that the adequate conditions exist for the process (e.g. configuration management of risk register and RMP, resource management, etc.).
2.	Monitor and control the execution of risk response, contingency and fallback plans.
3.	Watch for triggers.
4.	Trigger the execution of contingency and fallback plans.
5.	Watch the environments by attending project status meetings.
6.	Perform risk reviews and risk audits.

7.	Identify and analyse new risks. Develop response plans for those risks.
8.	Revise existing risks. Eventually adapt existing response plans.
9.	Collect and communicate the risk status in accordance with the measures planned in the RMP.
10.	Update the RMP.
11.	Produce lessons learned.

Risk monitoring and control is described as a control function, yet the function contains element of execution phase as well as control. During this step, the risk owners will execute and risk response plans and respond to risk triggers by implementing contingency and fall back plans.

4.4.3 Outputs

- Actions executed as results of the execution of risk response plans.
- Risk register updates.
- Updates to the risk response plans.
- Updates to the PMP.
- Lessons learned.
- Communication of risk status.

4.4.4 Toolbox

The concepts explained below support the realization of outputs.

4.4.4.1 Risk Reviews

Risk review meetings are conducted at regular intervals, ideally in conjunction with project review meetings to ensure the availability of all major stakeholders and reduce administrative overhead. Risk reviews are mainly used to communicate the status of risks, monitor the status of response plans' execution, and eventually identify new risks. The information gathered during the risk review supports the steering of the risk management process. The conduct of risk reviews should follow the best practices for review meetings: agreed agenda, capturing meeting minutes, producing reports, etc.

4.4.4.2 Risk Audits

Risk audits may be performed on risk response plans and the risk management process. Independent risk audits are performed by auditors not immediately involved in the project (e.g. risk manager from other projects, consultants, etc.) The independency of the auditors helps eliminate the biases and provides different perspectives on risk responses and process.

The output of the audit should contain corrective and preventive actions to be taken (e.g. risk owners might be changed or contingency and fallback plans for risks might be adjusted). Based on the risk audit results the lessons learned are included in the lessons learned repository.

4.5 Risk Management Planning

Risk management planning prepares the execution of the four other RM steps (identification, analysis, response planning, and monitoring and control). RM planning “sets the tone” for the rest the RM activities; ensuring that they are adequate to the project and that all conditions are met to ensure the successful execution of the process. The key to successful risk management is early planning with all stakeholders, resourcing and integration with the other project management processes.

Risk management planning includes:

- Developing and documenting an organized, comprehensive risk management strategy (including tolerance and appetite) and process;
- Determining the methods, tools and techniques to be used to execute the risk management strategy;
- Identifying and planning for adequate resources (including competencies and training) for the process; and;
- Ensuring that the communication of risks (risk assessments, reports. trends) is considered.

The risk management planning process should begin as early as possible in the project life cycle and should be completed early during project planning. The main output of RM planning is the RM Plan. This plan should basically answer the questions: “who, what, where, when and how”.

4.5.1 Inputs

The inputs listed below are the key inputs used for risk management planning:

- Enterprise level inputs
 - Historical records.
 - Organizational process assets (such as risk categories, common definitions and terms, standard templates).
 - Organizational environmental factors (risk tolerance of the enterprise as expressed in policies).
- Project level inputs
 - Project information (charter, scope statement).
 - Project environmental factors (risk tolerance and acceptance of the project manager and team members).
- Strategies and management plans (procurement, schedule, cost, staffing, communication).
- WBS.
- Stakeholders.

4.5.2 Tasks

The following activities are performed during RM planning.

Table 4-8: Risk management planning tasks

#	Tasks
1.	Collect and organize the required inputs as well as any other background information.
2.	Identify all appropriate stakeholders to support the task.
3.	Utilize appropriate toolbox items (methods, tools and techniques) based on recommendation in the RMP and as described in Toolbox.
4.	Train stakeholders on the use of the toolbox items as required.
Note: The tasks above are to be performed before every RM process step. One of the purposes of the RMP is to ensure that these tasks are adequately planned.	
5.	Obtain authority to establish the RM process in the project.
6.	Define how RM integrates with project management and other business management activities (including cost aspects) to avoid overhead.
7.	Complete and staff the RMP. Obtain approval of the RMP.
8.	Ensure that sufficient configuration management processes are in place to support the RM process (primarily RMP and risk register).

4.5.3 Outputs

The RMP is the main output of the RM planning step. For small projects, with limited RM scope, the RMP may be contained within the Project Management Plan (PMP) as discussed in the AAP-20, annex 3. For larger projects and programmes, the RMP will be a separate document and will be referenced in the PMP.

4.5.4 Toolbox

The concepts explained below support the realization of outputs.

4.5.4.1 Risk Management Plan Template

Annex C -, **Risk Management Plan Template**, contains a suggested structure for the RMP that can be easily tailored for a given project or programme. Each chapter of the template contains:

- Description and rationale: The contents and need of a given chapter.
- Example text, in italics: This will aid the author in writing the introductory text for each paragraph that will be modified or extended for a particular project or programme.
- Applicable references. This will aid the author to easily find detailed guidance on a given RM subject.

As mentioned earlier, the RMP is expected to be tailored for a given project or programme. The following bullets provide suggested RMP development recommendations and tailoring considerations:

- Copy and paste Annex C, RMP template, into a new file. This will save the author having to retype the chapter outline.
- Review the applicability of each of the RMP template paragraphs. If a paragraph is not applicable to the project, document the paragraph as “Not Applicable” and provide a justification of the non-applicability. Try to avoid deleting the paragraph all together. This will avoid reviewer comments questioning the completeness of the RMP in accordance with the template.
- Keep paragraphs simple and to the point. . If a particular subject is detailed and lengthy, consider moving the information into its own annex. Avoid duplication of information by referencing the sources in the RMP. For example, , if an organization has already implemented an Enterprise RM process, and you are developing a Programme RM process, there is no need to re-document the Enterprise RM process in the Programme RM process. Only those areas that are different and then reference the Enterprise RM Process document..
- Finally, delete the provided template guidance and reference information in the final RMP.

4.5.4.2 Risk Register

The risk register is the place where most of risk information is kept. The risk register is a repository for the whole RM process that will be constantly updated with information as risk identification and other steps of the RM process are performed. The risk register is used to generate the required risk reports. The risk register is normally managed by the risk manager and made available to the project team.

Depending on the organization, the risk register may be unique for a single project or be shared by multiple projects. Applications supporting risk registers may vary from simple spreadsheets, word processors, databases, to complex dedicated software tools. The choice of the risk register for a project will depend largely of the availability of existing software and of the requirements of the project.

Annex D -, Risk Register, provides basic fields to be included in a risk register as well as the steps of the RM process when these fields should be initially filled.

Like other project artefacts, it is essential that the risk register be kept under configuration management.

5 Particularities of Risk Management to NATO

5.1 Risk Management between NATO Contracting Authorities and Contractors

Although there will be separate risk management effort/processes on the parts of both NATO Contracting Authorities/Governments and the Contractor(s), it is a good practice to establish a collaborative risk management relationship. By doing this, NATO Contracting Authorities/Governments share the programme risks with the contractor (as opposed to transferring all or most of the risk to him). Since NATO Contracting Authorities/Governments

ultimately have the responsibility to provide a capable and supportable system to the NATO/Governments system user, all programme risks, regardless of who is assigned primary ownership, are a concern to the NATO Contracting Authorities/Governments project Mgr and must be addressed and managed by it.

While there is a need for collaborative risk management work between NATO Contracting Authorities/Governments and Contractor(s), each party views risk from a different perspective. Contractors typically divide risk into two basic types as shown below:

- **Business Risk:** This involves the inherent chance of making a profit or incurring a loss on any given contract.
- **Program Risk:** This includes uncertainties in technical requirements, design, development, integration, cost, funding, scheduling, etc.

NATO Contracting Authorities/Governments typically focuses on project type risks, and the negative aspects associated with them. Although NATO Contracting Authorities/Governments do not dictate how the Contractor should manage risk, some characteristics of good NATO Contracting Authorities/Governments - Contractor interaction include:

- Flexibility for assignment of common project risk management responsibilities among NATO Contracting Authorities/Governments – Contractor, e.g. NATO Contracting Authorities/Governments - Contractor collaborative teams
- Clearly identifying and analyzing risks and their root causes, and assigning responsibility or ownership for identifying, selecting, implementing and tracking their mitigation plans
- Evaluate risk root causes and their cost, schedule and performance impacts and the use of resources to mitigate them
- Use of the best management practices which, if followed, avoid unnecessary risk
- Use (partially or not) of a common RMP and Risk Register
- Conducting event-based systems engineering technical reviews
- Commitment concerning planning and executing a successful risk management programme

Other steps that the NATO Contracting Authorities/Governments can take to promote a collaborative NATO Contracting Authorities/Governments - Contractor RM program are:

- Conduct an initial meeting with the Contractor to describe the programme's objectives and the approach to managing risk (including the RMP and Risk Register)
- Train members of NATO Contracting Authorities/Governments and contractor's organizations on NATO programmes risk management basics
- Review the programme's contractual documentation (e.g. RFP) requirements with the contractor. Ensure that the NATO Contracting Authorities/Governments and Contractor personnel understand the purpose, format and contents of various risk reports
- Work with the Contractor to refine risk tracking plans and procedures
- Establish programme risk reporting requirements with the Contractor
- Work with the Contractor to develop appropriate measures to track moderate and high risk items

The project Manager always has a responsibility to the system user to develop a capable and supportable system and can not absolve itself of that responsibility. Therefore, all project risks, whether primarily managed by the project Mgr or by the development/support contractor, are of concern and must be assessed and managed by the project Mgr. Once the project Mgr has determined which risks and how much of each risk to share with the contractor, he must then assess the total risk assumed by the developing contractor (including subcontractors).

Both NATO Contracting Authorities/Governments and the Contractor must have a common view on risk management process and data. More explanation about the specific risk management contractual process can be found in annex D. Successful risk strategy requires that government and the contractor communicate all programme risks for mutual adjudication. Both parties may not always agree on risk probability, and the government Project Mgr maintains ultimate approval authority for risk definition and assignment. A common risk register available and open to the government and the contractor is an extremely valuable tool. Successful risk strategy involves selection of the option that best provides the balance between performance and cost. Recall that schedule slips generally and directly impact cost. It is also possible that throughout the system life cycle there may be a need for different near-term and long-term risk strategy approaches.

An effective risk management process requires a commitment on the part of the PM, the programme office and the contractor to be successful. Many impediments exist to risk management implementation, however, the programme team must work together to overcome these obstacles. One good example is the natural reluctance to identify real programme risks early for fear of jeopardizing support of the programme by decision makers. Another example is the lack of sufficient funds to properly implement the risk management process. However, when properly resourced and implemented, the risk management process supports setting and achieving realistic cost, schedule, and performance objectives and provides early identification of risks for special attention and handling. The risk management plan should address industry involvement in dealing with programme risks.

5.2 Risk Management and Accelerated Fielding

Accelerated fielding (a.k.a. rapid acquisition) is a specific approach to deliver an urgent or immediate capability and, therefore, saves time over a traditional approach such as the one documented in the AAP-20. Accelerated fielding is recognized to significantly increase project risks and potentially increase costs. The sections below list some of the solutions chosen to enable accelerated fielding, describe potential effects and propose solutions.

5.2.1 Reduced documentation

Because the immediate benefits (clearer communication, familiarization, record of decisions, knowledge base, etc.) of properly documenting the project (project, test, risk management plans) or the product (requirements, designs, tests) are not always visible, many project managers will decide on reducing, simplifying, delaying, and/or cancelling project and product artefacts. These decisions might be planned or the result of delays in the project. It is true that producing, reviewing, and approving artefacts that meet specific standards (Mil-Std, IEEE ...) is resource and time intensive, especially when the documents have to be authored and reviewed in a non-native language. The following sections list the most common risks linked to reduced documentation and provide solutions, which need to be adapted for the project.

5.2.1.1 Risks

The potential effects of reduced documentation may be far ranging and include:

- Effects caused by reduced project documents
 - Degraded communication.
 - Undocumented decisions leading to uncontrolled actions.
 - Lack of available information leading to incorrect decisions.
 - Rework or redundancy caused by unclear plans.
 - Fines or penalties for not meeting legal obligations.
 - Reduced ability to control the process.
 - Etc.
- Effect caused by reduced product documents
 - Faulty (or lengthy) technical implementation at stage x caused by undocumented stage x-1 solutions.
 - Increased costs of having to reverse engineer technical implementations at later stages.
 - Increased costs of maintainability or reduced maintainability.
 - Unclear product status (e.g. caused by reduced test documentation) leading to non-fact based decisions.
 - Increased difficulties to obtain certification (security, safety, quality management, etc.).

5.2.1.2 Solutions

The solution described below should be executed at the beginning of the project and involve all stakeholders.

- List all formal (contractual) and informal (best practices or organizational) requirements related to the documentation. The list should detail at least: which documents need to be produced, in which format and by when.
- For each documentation requirement, list the negative consequences, the benefits and risks of not meeting the requirement. Consider the negative consequences and benefits across the whole lifecycle and not only for a particular stage.
- For each requirement, list potential alternative solutions (see below) to this requirement and include its negative consequences, benefits, and risks.
- Choose a solution and document the decision.

Table 5-1: Solutions to documentation constraints

Constraint	Alternatives
Artefact required contractually, legally, or by corporate processes	<ul style="list-style-type: none"> • Discuss contractual requirement and propose alternative solutions or decreased costs. • Request for waiver. • Outsource production of the artefact.
Artefact required to be in specific format	<ul style="list-style-type: none"> • Tailor the standard (Data Item Description) to the minimum required. • Propose alternative industry standard or own template.
Artefact implied by best practice	<ul style="list-style-type: none"> • Do not produce the artefact but ensure that the purpose of the artefact is met.
Any constraint	<ul style="list-style-type: none"> • Reject the constraint and register an associated risk.

5.2.2 Reduced lifecycle activities

Another mechanism often used to implement accelerated fielding is to reduce the activities in a given life cycle (e.g. the system life cycle proposed in the PAPS). Not fully implementing all activities in the life cycle is considered as one of the most important risk linked to the life cycle. However, not choosing an appropriate life cycle should be considered to be the greatest risk. As clearly documented in the PAPS: *“PAPS provides a systematic and coherent, yet flexible, framework [...] and should not be regarded as a set of formal and mandatory steps [...]”*. Therefore, the first responsibility of the project manager is to select, develop, or tailor a life cycle that supports the realization of the project objectives.

5.2.2.1 Risks

The top-level risk of adopting an inappropriate life cycle for the project is its inability to efficiently, effectively, and coherently manage the activities. This risk is enhanced in accelerated fielding where a standard life cycle will rarely be appropriate and where the project manager will have to combine different life cycles to obtain the maximum effect. An insufficient knowledge of the life cycles and their application may lead to an “apprentice sorcerer” approach to life cycle management.

The section below documents the approach to select the most appropriate life cycle model for your project.

5.2.2.2 Solutions

The solution described below should be executed at the beginning of the project and involve all stakeholders.

- Know the differences between life cycles. The majority of the development lifecycles originate from the software industry and are articulated around the following steps

(building blocs): requirement, design, code, integration, test, and production/delivery. A life cycle arranges and combines those building blocs in patterns. The patterns can be serial (e.g. waterfall or V models), iterative (e.g. spiral), incremental (e.g. staged delivery), or agile (e.g. SCRUM, XP).

Programme life cycles can be arranged in similar patterns but the building blocs will be different. According to the PAPS, the building blocs would be: pre-concept, concept, development, production, utilisation, support, and retirement.

- Select and tailor the life cycle. Not all those models lend themselves to accelerated fielding. Typically, serial and iterative models are not good candidates because they cannot easily function with changing or incomplete requirements, in addition, serial models only deliver the final products at the very end of the life cycle. Incremental models, on the other hand, function well when not all requirements are known at the beginning of the project or when requirements are volatile. Those models may also deliver intermediate products (fully tested or prototypes) and deal with project risks (schedule and costs) or product risks (functionalities). Incremental models are risky to implement for complex or large systems because, since not all requirements are defined at the start of the project, the chosen initial architecture may not be adequate to support later requirements and require major rework.

In many cases, the programme manager will have to define a new model adapted to the requirements of the programme. For accelerated fielding, this model is likely to have an incremental top-level model (the tree of the programme) with serial development branches (for sub-products). Each increment will deliver a specific Level Of Capability (LOC).

5.2.3 Reuse of existing products

With the aim of reducing NATO resources, overall life cycle costs, implementation risk and timescale, the NATO Software Management Policy edition 1⁷ states that proven off the-shelf software should be utilised whenever possible and certainly for all common user, non specialist applications. Off-The-Shelf (OTS) software includes:

- COTS: Commercial OTS. This term pertains to a commercially marketed product which is normally used without modification. For COTS software, source code is not made available and maintenance is provided by the vendor under license.
- NOTS: NATO OTS. NOTS products are provided by a NATO organization to meet specific user needs. NATO exercises partial or full ownership and maintenance of the products and may make them available to other NATO bodies as required. NOTS application software may be made available with or without its source code.
- GOTS: Government OTS. GOTS products are provided to meet specific user needs. A government exercises partial or full ownership and maintenance of the products and may make them available on mutually agreed terms. GOTS application software may be made available with or without its source code.

Open Source Software (OSS) is software made available to all users together with its source code; this provision distinguishes it from 'proprietary' COTS software which is supplied in

⁷ NATO Software Management Guidance, EAPC(AC/322-SC/5)N(2003)011

object form only, the source code rights being retained by the vendor. OSS may be used, copied and further distributed with or without modifications, and may be offered either with or without a fee. If an end-user makes any changes to the software, they can either be retained for his specific application use or be returned to the wider community to be included in future product releases if desired. The OSS community consists of individuals, groups of individuals and organisations who contribute to a particular open source product or technology.

Using COTS or OSS products has several advantages:

- Standardised usable functions and capabilities come out of the box.
- Operational products can readily be deployed in a cost effective way.
- Resources can be focused on user driven and mission-directed applications development.
- Interoperability and portability can be guaranteed.
- Re-use of computerised applications across heterogeneous networks is facilitated.
- Standardisation of data management subsystems can be achieved, making applications independent from data base physical implementation.
- Users need minimum training to become familiar with the user's interfaces.

5.2.3.1 Risks

The risks and drawbacks of reusing COTS or OSS are:

- The implementation of COTS makes the final NOTS product highly dependent on the commercial packages, especially when these packages constitute the pillars for the whole application (operating systems, network protocols, etc.).
- A poor choice of COTS could result in the inability of the final product to fulfil all users' requirements. An excessive amount of glue code might then be required to implement the missing functions, making the final product cumbersome and unstable;
- Final system performance might be degraded by the poor performance of COTS, with no possible action except costly improvement of surrounding elements, like hardware upgrades, allocation of more bandwidth, etc.
- Manpower and material resources must be retained for testing COTS upgrades before they are deployed, for identifying compatibility.
- Difficulty to integrate with other products or interoperate. The use of proprietary interfaces (non standard) and architectures will result in integration of interoperability difficulties.
- Long-term maintenance. The use of typically short-lived products or product versions will increase the difficulty to maintain the system. The management of obsolescence of these products will be a major challenge.
- Costs of licenses. The use of COTS is not free. License costs may represent a large percentage of the total operational costs of the systems.
- Difficulty to obtain certification. The necessary certifications (safety, security, environmental, etc.) of a system using OTS may be more difficult to obtain if, for instance, the source code is not available.

5.2.3.2 Solutions

The choice of integrating COTS or OSS products into a system must consider risks and benefits. A risks/benefits analysis should be performed using the criteria shown in Table 5-2.

Table 5-2: COTS selection criteria⁸

Product selection		Vendor selection	Stakeholder acceptability
Security	Performance suitability	Reputation	Project engineering familiarity with product
Safety	Transparency	Technical support	Open attitude to new technology offered by product
Quality	Functional match	Willingness to negotiate changes	Training requirements to develop product expertise
Maintainability	Update cycle	Training support	
Reliability	Upward compatibility of revisions	Competitive standing	
Portability	Architectural compatibility	Match between vendor release dates/cycle and system release dates/cycles	
Interoperability	Efficiency of resource utilization	References with national or NATO organizations	
Maturity	Maintenance and operations costs / fees		

An evaluation matrix may be used to support the decision. A candidate product is weighted (e.g. on a scale from 0 to 5) to indicate the importance of the criterion and scored (e.g. on a scale from 0% to 100%) to show the match between the criterion and the product characteristics.

⁸ Space and Naval Warfare Systems Center, "COTS evaluation, selection, and qualification process", 2002

INTENTIONALLY BLANK

Annex A -Abbreviations and Acronyms

Abbreviations	Description
CDR	Critical Design Review
CWBS	Contractual Breakdown Structure
ERM	Enterprise Risk Management
IPT	Integrated Product Team
OSS	Open Source Software
OTS	Off-The-Shelf
PAPS	Phased Armament Programme System
PM	Project Management
PMgr	Project Manager
PMI	Project Management Institute
PMO	Project/Programme Management Office
PMP	Project Management Plan
RFP	Request For Proposal
RM	Risk Management
RMgr	Risk Manager
RMP	RM Plan
SLCM	System Life Cycle Management
SME	Subject Matter Expert
SOI	System Of Interest
SRR	System Requirements Review
WBS	Work Breakdown Structure

INTENTIONALLY BLANK

Annex B -Terms and Definitions

Term	Definition	Reference
Assumptions	Assumptions are factors that, for planning purposes, are considered to be true, real, or certain without proof or demonstration.	PMBOK (2008)
Criteria	Standards, rules, or tests on which a judgment or decision can be based, or by which a product, service, result, or process can be evaluated.	PMBOK
Decision gate	Life cycle elements controlling the flow in and out of the stages and providing a control mechanism.	Derived from AAP-48
Delphi Technique	An information gathering technique used as a way to reach a consensus of experts on a subject. Experts on the subject participate in this technique anonymously. A facilitator uses a questionnaire to solicit ideas about the important project points related to the subject. The responses are summarized and are then re-circulated to the experts for further comment. Consensus may be reached in a few rounds of this process. The Delphi technique helps reduce bias in the data and keeps any one person from having undue influence on the outcome.	PMBOK (2008) Reference to Tools and tech?
External risk	A risk of which the principal cause lies outside the area of responsibility of the risk management process.	
Internal risk	A risk of which the principal cause lies within the area of responsibility of the risk management process.	
Issue	A point or matter in question or in dispute, or a point or matter that is not settled and is under discussion or over which there are opposing views or disagreements.	PMBOK (2008)
Life-cycle model	A framework of processes and activities concerned with the life cycle, which also acts as a common reference for communication and understanding.	ISO/IEC 15288:2002(E)
Master schedule	A summary-level project schedule that identifies the major deliverables and work breakdown structure components and key schedule milestones.	PMBOK (2008)
Monte Carlo Simulation	A process which generates hundreds or thousands of probable performance outcomes based on probability distributions for cost and schedule on individual tasks. The outcomes are then used to generate a probability distribution for the project as a whole.	PMBOK (2008) Reference to Tools and tech?
Opportunity	A condition or situation favourable to the project, a positive set of circumstances, a positive set of events, a risk that will have a positive impact on project objectives, or a possibility for positive changes. Contrast with <i>threat</i> .	PMBOK (2008)
Organization	A framework of processes and activities concerned with the life cycle, which also acts as a common reference for communication and understanding.	ISO 9000:2000
Parent risk	The cause of a secondary risk.	

Term	Definition	Reference
Process	Set of interrelated or interacting activities which transform inputs into outputs.	ISO 9000:2000
Project life-cycle	A collection of generally sequential project phases whose name and number are determined by the control needs of the organization or organizations involved in the project. A life cycle can be documented with a methodology.	PMBOK (2008)
Residual risk	A risk that remains after risk responses have been implemented.	PMBOK (2008)
Risk	An uncertain event or condition that, if it occurs, has a positive or negative effect on a project's objectives.	PMBOK (2008)
Risk avoidance	A risk response planning technique for a threat that creates changes to the project management plan that are meant to either eliminate the risk or to protect the project objectives from its impact.	PMBOK (2008)
Risk breakdown structure	A hierarchically organized depiction of the identified project risks arranged by risk category and subcategory that identifies the various areas and causes of potential risks. The risk breakdown structure is often tailored to specific project types.	PMBOK (2008)
Risk category	A group of potential causes of risk. Risk causes may be grouped into categories such as technical, external, organizational, environmental, or project management. A category may include subcategories such as technical maturity, weather, or aggressive estimating.	PMBOK (2008)
Risk impact	The potential effect of a risk on objectives.	Derived from PMBOK (2008)
Risk management plan	The document describing how project risk management will be structured and performed on the project. It is contained in or is a subsidiary plan of the project management plan. Information in the risk management plan varies by application area and project size. The risk management plan is different from the risk register that contains the list of project risks, the results of risk analysis, and the risk responses.	PMBOK (2008)
Risk probability	The likelihood that a risk will occur.	Derived from PMBOK (2008)
Risk rating	A risk attribute determined based on an assessed risk probability and impact.	Derived from PMBOK (2008)
Risk register	The document containing the results of the qualitative risk analysis, quantitative risk analysis, and risk response planning. The risk register details all identified risks, including description, category, cause, probability of occurring, impact(s) on objectives, proposed responses, owners, and current status.	PMBOK (2008)
Risk response	Option or action to enhance opportunities and to reduce threats to project objectives.	Derived from PMBOK (2008)

Term	Definition	Reference
Risk strategy	A plan of action designed to achieve the risk management goal.	Derived from definition of strategy in wiki
Risk transference	A risk response planning technique that shifts the impact of a threat to a third party, together with ownership of the response.	PMBOK (2008)
Secondary risk	A risk that arises as a direct result of implementing a risk response.	PMBOK (2008)
Stage	A period within the life cycle of a system that relates to the state of the system description or the system itself.	ISO/IEC 15288:2002(E)
System life cycle	The evolution with time of a system-of-interest from conception through to retirement.	ISO/IEC 15288:2002(E)
System-of-interest	The system whose life cycle is under consideration.	ISO/IEC 15288:2002(E)
Threat	A condition or situation unfavourable to the project, a negative set of circumstances, a negative set of events, a risk that will have a negative impact on a project objective if it occurs, or a possibility for negative changes. Contrast with <i>opportunity</i> .	PMBOK (2008)
Threshold	A cost, time, quality, technical, or resource value used as a parameter, and which may be included in product specifications. Crossing the threshold should trigger some action, such as generating an exception report.	PMBOK (2008)
Triggers	Indications that a risk has occurred or is about to occur. Triggers may be discovered in the risk identification process and watched in the risk monitoring and control process. Triggers are sometimes called risk symptoms or warning signs.	PMBOK (2008)

INTENTIONALLY BLANK

Annex C -Risk Management Plan Template

C-1 Introduction

C-1-1 Purpose

The section explains the reasons why an RMP was created for the project⁹ and documents the objectives of the RMP. The description should be concise and not simply just list the contents of the RMP.

If the RMP applies to a programme, the section will mention the applicability of this RMP to subordinate projects.

Example Text:

Project XYZ was established within the Industrialization Agency (IndA) to industrialize a state-of-the-art prototype based on new technologies, called the FastEnOut, developed by the Prototyping Agency (ProtA). The industrialization includes reverse engineering requirements and designs to develop requirement statements and design documents as well as producing blueprints for production. Only a few of the project XYZ members were involved in the development of the prototype at ProtA. Under these circumstances, it is recognized that risk management plays a crucial role in the support of the project management activities.

This RMP is used to:

- Tailor the risk management process documented in the organization directive IndA-001;*
- Specify the project specific responsibilities for risk management;*
- Provide an understanding of the project's risk management aspects to internal and external stakeholders.*

References:

- Section 2.7.1 RM organization: levels and purpose
- Section 5 Particularities of Risk Management to NATO

C-1-2 Administration

The section describes all aspects regarding the initial and further approval of the document, the revisions, the relation with other plans, and other administrative aspects. It is expected that the RMP will apply and be supported by existing document management processes. Generic contents such as approval page, revision history, references, definitions, etc. are not covered by this template.

Example Text:

The RMP will be updated as required by changes in the environment or the process and as a minimum annually. It will follow standard revision and approval procedures for project documents as documented in IndA-002.

⁹ The RMP template may be applied to projects and programmes. Therefore the word "project" may be substituted by "programme" throughout the template. Any information applicable only to a project or a programme will be clearly indicated.

References:

- No references in this guide.

C-2 Enterprise/Programme/Project Description

The chapter provides information (or references to information) about the project. It should focus on the information that is used for the management of risks such as the project objectives (that are impacted by the risks) or the different environments (that may be the source of risks).

Example Text:

For the XYZ Project, the prototype developed by the ProtA is already in operation, therefore, the delivery date is not an essential objective. However, because of high costs of the production and future maintenance of the product, the completeness and accuracy of the documentation produced in the project is of high importance. The competitive labour environment in which IndA and ProtA co-exist presents a threat to the availability of key HR technical resources.

References:

- No Reference in this guide.

C-3 Organization

The chapter defines the risk management organization for the project and situates it within its context (organizational or programmatic), it includes the definition of roles and responsibilities that are not already documented in other project or organization documents. If the RM structure is complex (including a risk management board reporting to a higher programme or part of the organization), the chapter maybe be broken down in sections. It is highly advisable that the relations between the risk management organization and other project or organization structure be (also) documented in the PMP. The chapter should also include the definition of stakeholders of the process and the required qualifications of internal members which may lead to additional training (e.g. on tools).

Example Text:

The risk management organization of project XYZ applies the structure and responsibilities described in IndA-001. In summary, the Project Manager (PMgr) and Risk Manager (RMgr) report to the Corporate Risk Management Board to share information on project risks to other projects and to the organization, to obtain resources for the project risk responses that are outside of the project scope and to assign ownership of project risks to members of the organization outside the project.

Within the project, the RMgr maintains the RMP, prepares for the Risk Management Board, maintains the risk register by closely following-up on all project risks and associated actions.

The PMgr assigns resources and schedule activities resulting from the risk responses.

Both PMgr and RMgr are familiar with the tools used in the process and no specific training is required at this time.

References:

- Section 2.7 Enterprise, Programme and Project Risk Management
- Section 2.7.2 RM organization : roles and responsibilities
- Section 5.1 Risk Management between NATO Contracting Authorities and Contractors

C-4 Process

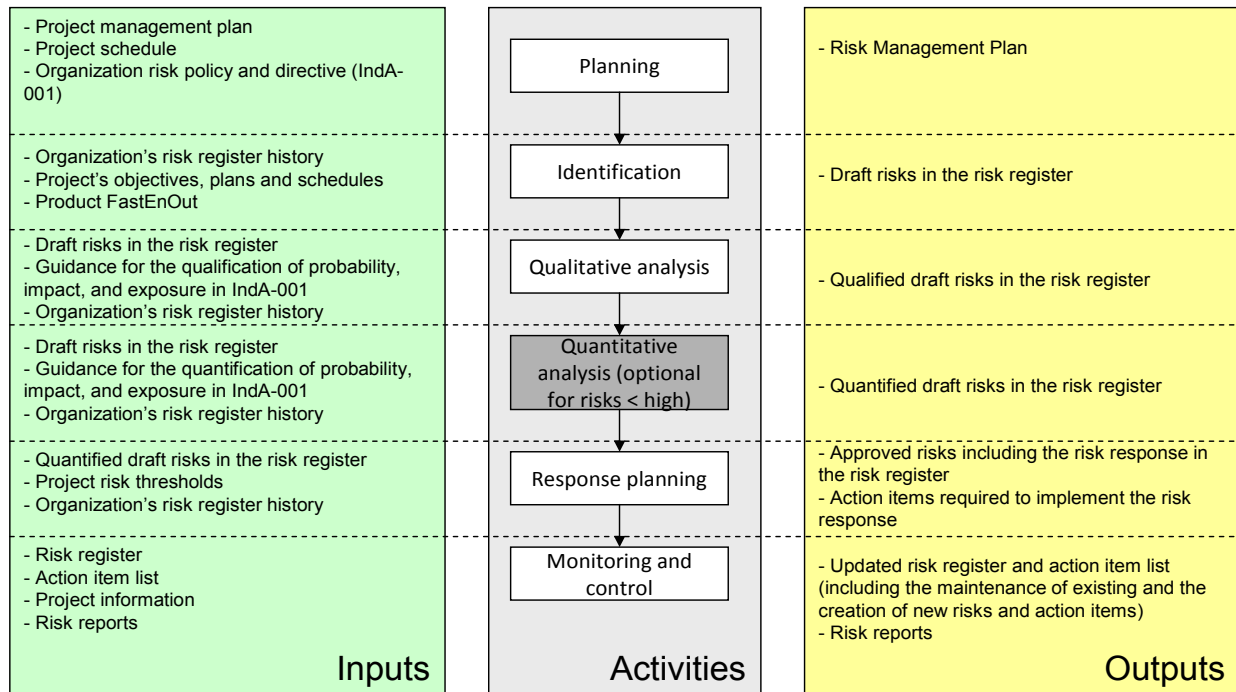
This chapter is the core of the RMP. It provides the details of the risk management process which aims at minimizing the impact of unfavourable events (threats) and maximizing the benefit of favourable events (opportunities). Whether documented in an organizational directive or in the RMP, the following should be defined:

- An explanation on how the process integrates within the Programme Plan (or higher level plans), and supports project management.
- A risk process flowchart that defines the activities, roles (who performs the activities) and decision logic for the given risk process. (
- For each activity: a description of key inputs, outputs, tools, and activities.
- Definitions of each of the risk levels and associated probabilities, impact estimation values.
- Criteria and thresholds for each risk to determine the need of a risk response as well as risk strategies to be applied (e.g. accept, avoid, mitigate, transfer)
- A repository of current documented risks with key attributes (also called the risk register).
- A method to assign and track action items for the each risk response.

Depending on the needs and maturity of the project and organization, additional information such as: objectives of the activities, checklists for risk identification, metrics, tools, control points, etc. may be included in the chapter.

Example Text:

The risk management process used by project XYZ applies and tailors the process described in IndA-001. The standard process is tailored (simplified) by making the risk quantification optional for low or medium risks, as shown in the figure below.



The scales for the qualification and quantification of the risk probabilities, impact, and exposure are defined in IndA-001.

During the execution of the project, the PMgr and RMgr will ensure that the project risks are captured, maintained, and actioned (a) through a reserved mandatory agenda item at all project review meeting and (b) by coordinating the risks with the Risk Management Board at the organizational level.

The risks will be captured in the project's risk register maintained in the project folder by the RMgr. Action items resulting from the risk response will be entered and maintained in the project's action item list in the project folder. Standard metrics defined in IndA-001 will be maintained by the RMgr.

References:

- Chapter 4 Risk Management Process
- Annex F Methods, Techniques and Tools

Annex D -Risk Register

The risk register supports all steps of the RM process by capturing, processing, and centralizing risk attributes. It can link risks to risk responses (action items), it can be used as a means to communicate risk information, and supports the transitions between programme/project stages/phases, etc.

This annex provides a non exhaustive list of risk attributes that are subject to be captured in a risk register (D-1) and a short list of typical reports that can be produced with data from the risk register (D-2). The description, format and values must be tailored and adapted to the organization, programme, or project.

D-1 Risk Register Contents

D-1-1 Title

The <title> can be either a short textual description of the risk (e.g. “Lack of stable requirements”) or a scheme specific to the risk register (e.g. a combination of project identifier and sequential number\such as Risk PRJ_XYZ/001). The <title> does not have to be unique if the <number> (see below) is used in conjunction with this field.

This field is filled at risk identification.

D-1-2 Number

The <number> is a unique identifier for the risk within the risk register. It can be composed of a number or alphanumeric combination allowing to uniquely identifying the risk within the risk register. For instance, Risk PRJ_XYZ/001. The <number> may be optional if the <title> (see above) is unique.

This field is filled at risk identification.

D-1-3 Parent

If the risk is a secondary risk (see Annex B -), the reference to the unique identifier (<title> or <number>) of the risk which caused this new risk.

This field is filled at risk identification.

D-1-4 Project

The reference of the project to which the risk belongs.

This field is filled at risk identification.

D-1-5 Programme

The reference of the programme to which the risk belongs.

This field is filled at risk identification.

D-1-6 SOI

The reference of the SOI under which the parent project/programme is managed. This information may be useful to extract a product view of the risks managed in different projects or programmes.

This field is filled at risk identification.

D-1-7 Objectives

The project objectives impacted by the risk. Each project or programme has to meet specific objectives which generally include a time, cost, and quality aspect. A risk may affect one or sometimes more than one objectives. This field is used to list which of the project objectives are impacted. This field can be further explained in <effects> below.

This field is filled at risk identification.

D-1-8 RGQA

The reference of the Delegator RGQA number. Mutual Government Quality Assurance is the process by which NATO Nations provide each other and NATO organisations Quality Assurance services on defence products, to establish confidence that the contractual requirements relating to quality are met. GQA is performed on those contractual requirements either posing risks to or required by law of the acquiring Nation (Reference AQAP 2070). This field allows a risk to be linked to the RGQA process.

D-1-9 Owner

The owner of the risk. The owner of the risk is a person or a department responsible to the project manager for all actions related to this risk. The owner should have sufficient authority and resources to execute the risk response actions.

The owner may be assigned at risk identification.

D-1-10 Description

The description is a long, full description of the risk. The description may include impact statements, causes, and other information specific to this risk. The description is often used to summarise and communicate general risk information and may contain the risk statement (see 4.1).

This field is filled at risk identification.

D-1-11 Causes

The causes of the risk. The causes (root causes) of the risk describe the conditions why the risk exists. The field can be used to elaborate on the <category> and provide additional information and analysis. This field may be used to elaborate on the risk statement (see 4.1).

This field is filled at risk identification.

D-1-12 Impacts

The impacts of the risk. The impacts of a risk will generally effect one or more objectives. The field can be used to elaborate on those effects and provide any additional description such as impacts on other plans (budget, development, etc.). This field may be used to elaborate on the risk statement (see 4.1).

This field is filled at risk identification.

D-1-13 Stage detected

The programme stage when the risk was first detected. In accordance with reference b, programme stages are: pre-concept, concept, development, production, utilization, support, and retirement

This field is filled at risk identification.

D-1-14 Phase detected

The project phase when the risk was first detected. In accordance with reference a, project phases are: initiation, planning, execution, and monitoring and control.

This field is filled at risk identification.

D-1-15 Stages applicable

The programme stage(s) when the risk may occur. See <stage detected> for a list of stages.

This field is filled at risk identification.

D-1-16 Phases applicable

The programme phase(s) when the risk may occur. See <phase detected> for a list of phases.

This field is filled at risk identification.

D-1-17 Category

The category (and eventually, sub-category) that this risk belongs to (see 4.14.1.4.4).

This field is filled at risk identification.

D-1-18 Probability rating

The probability rating as defined in the probability and impact matrix (see 2.10).

This field is filled at risk analysis.

D-1-19 Impact rating

The impact rating as defined in the probability and impact matrix (see 2.10).

This field is filled at risk analysis.

D-1-20 Risk rating

The risk rating as defined in the probability and impact matrix (see 2.10).

This field is filled at risk analysis.

D-1-21 Residual probability rating

The residual probability rating represents the future probability rating estimated once all currently defined actions are successfully completed.

This field is filled at risk analysis and is continuously updated as actions are executed.

D-1-22 Residual impact rating

The residual impact rating represents the future impact rating estimated once all currently defined actions are successfully completed.

This field is filled at risk analysis and is continuously updated as actions are executed.

D-1-23 Residual risk rating

The residual risk rating represents the future risk rating obtained once all currently defined actions are successfully completed.

This field is filled at risk analysis and is continuously updated as actions are executed.

D-1-24 Strategy

The type of risk response chosen for the risk (see 4.3.4.1).

This field is filled at risk response planning.

D-1-25 Actions

The references to action items created to implement the risk strategy. The implementation of a strategy requires actions to be executed. This field is used to capture the references to action items or plans managed in another repository.

This field is filled at risk response planning.

D-1-26 Status

The risk status represents the evolution of the risk through the risk management process. Statuses may include:

- Created
- Identified
- Analyzed
- Open
- Closed: issue
- Closed: retired

This field is first filled during risk identification and updated continuously.

D-1-27 Date updated

The date when the risk was last updated in the risk register.

This field is first filled during risk identification and updated continuously.

D-1-28 Date status

The date when the risk achieved the new status. The risk register does not capture historical data in specific fields. This is a responsibility of the tool or configuration management data.

This field is first filled during risk identification and updated continuously.

D-2 Risk Register Reports

- Top 5 risks by risk rating (absolute)
- Top 5 risks increase (since last report)
- Top 5 risks decrease (since last report)
- Top 5 volatile risks (most changes in)
- Top 5 categories/sub-categories with highest Σ risk rating
- Top 5 risks with oldest update
- Etc.

INTENTIONALLY BLANK

Annex E -Risk Management as Part of the Contractual Process

E-1 Overview

Risk should be considered in each step of the contractual process in order to establish the relationship needed to share programme risks between the contractual partners. Best practices in contracting are outlined below for each phase of the contracting process.

E-2 Risk Management: Pre-Contract Award

The contractor's developmental and manufacturing processes and tools, the availability and skill of their personnel and the previous experience of the NATO and contractor team all influence their ability to handle the proposed system development and subsequent production. Therefore, an effective risk management process includes an evaluation of the capabilities of the potential contractors.

E-3 Early Industry Involvement: Industrial Capabilities Review

An industrial Capabilities Review is a powerful tool available to PMs for determining general industrial capabilities. To avoid potential problems in the subsequent competitive process and to ensure that a "level playing field" is maintained and announcement in the Commerce Business Daily (or NATO equivalent) should be made to inform all potential offerors that the NATO plans to conduct an Industrial Capabilities Review and to request responses from all interested parties. Below is general approach that PMOs may find readily adaptable to any type of capability review. The basic steps in the process are:

- Obtain Source Selection Authority's approval to conduct the review
- Establish the criteria for the capability review
- Identify the potential contractors who will participate in the review
- Provide an advance copy of the review material to those contractors
- Select the review team on the purpose of the review and review criteria
- Conduct the review and evaluate the results
- Provide feedback to each contractor on the results of their review and assessment
- Provide the results to the PM.

The review is an appraisal of general industrial capabilities. It is used to support identification of potential program risks and best practices rather than to evaluate specific contractors.

Regardless of the approach, the PMO should determine what specific information is needed. The questions generally focus on two areas:

- What is the state-of-the-art of the technology proposed for use in the system?
- What are the general developmental/manufacturing capabilities of the potential contractors (including experience, tools, processes, etc.) as compared to industry best practices?

The answers to these questions help to develop the final programme acquisition strategy and the risk sharing structure between the NATO and industry. The PMO can also use the results to adjust the RFP to the next phase of the programme.

E-4 Developing the Request for Proposal

The RFP should communicate to all offerors the concept that risk management is an essential part of the NATO's acquisition strategy.

Before the draft RFP is developed, the PMO should conduct a risk assessment to ensure that the programme described in the RFP is executable within the technical, schedule and budget constraints. Based on this assessment, the preliminary Contract Work Breakdown

Structure (CWBS) and CWBS dictionary, a revised program plan and integrated master schedule and an updated Life-Cycle Cost (LCC) estimate can be prepared. The technical, schedule, and cost issues identified should be discussed in the pre-proposal conference(s) before the draft RFP is released. In this way, the critical risk inherent in the programme can be identified and addressed in the RFP. In addition, this helps to establish key risk management contractual conditions. Offerors should be encouraged to extend the CWBS to reflect how the work will be performed, and to identify all elements at any level that are expected to be high cost or high risk. Offerors also should be encouraged to identify any elements of the CWBS provided in the draft RFP that are not consistent with their planned approach.

In the solicitation, PMgrs may ask offerors to include a risk analysis and risk management plan and develop a supporting programme plan and an integrated master schedule in their proposals. These proposals will support the NATO's source selection evaluation and the formulation of a most probable cost estimate for each proposal. In addition, the RFP inputs to the PMgr's risk assessment and monitoring processes, and ensures that risks are continuously assessed.

E-5 The Offeror's Proposal

The offeror's proposed programme planning must be developed and documented at an adequate level to identify risk and define risk-management activities to be used throughout the programme. Resources, technical performance measures, and schedule should be integrated in the proposed program planning. This program planning should extend the CWBS to reflect the offeror's approach and provide in the CWBS dictionary the supporting activities, critical tasks, and processes. The associated schedules for each should be incorporated into the integrated master schedule. The planning should also include an estimate of the funds required to execute the program, with a particular focus on the resource requirements for the high risk areas.

The information required and the level of detail will depend on the acquisition phase, the category, and criticality to the programme, as well as on the contract type and value. However, the detail submitted with the proposal must be at a sufficiently low level to allow identification of possible conflicts in the schedule and to support the Government's proposal evaluation. Generally, the CWBS should be defined below level 3, by the contractor, only to the extent necessary to capture those lower level elements to be high cost, high risk, or high management interest.

E-6 Basis for Selection

NATO acquisition management must focus on balancing performance, schedule, and cost objectives by selecting the contractor team that provides the best value to the user within acceptable risk limits. Therefore, the RFP/Source Selection process must evaluate each offeror's capability for meeting product and process technical, schedule, and cost requirements while addressing and controlling the risks inherent in a programme.

The evaluation team should discriminate among offerors based upon the following:

- Product and process approach and associated risk determined by comparison with the best practices baseline
- Ability to perform with a focus on the critical risk elements inherent in the programme
- Adherence to requirements associated with any mandatory legal items
- Past performance on efforts similar to the proposed program being evaluated.

The process of choosing among offerors is significantly enhanced if the evaluation team includes risk management as a "source selection discriminator" to be used in making the selection decision. Risk management then becomes an important factor in the Source Selection Authority determination of who provides the most executable program.

E-7 Source Selection

The purpose of a source selection is to select the contractor whose performance can best be expected to meet the Government's requirements at an affordable price. To perform this evaluation, the Government must assess both *proposal risk* and *performance risk* for each proposal. These risk assessments must be done entirely within the boundaries of the source selection process. Previous assessments of any of the offerors may not be applicable.

Proposal risk refers to the risk associated with the offeror's proposed approach to meet the NATO's requirements. The evaluation of proposal risk includes an assessment of proposed time and resources and recommendations adjustments. This assessment should be performed according to the risk definitions and evaluation standards developed for the source selection.

The technical and schedule assessments are primary inputs to the most probable cost estimate for each proposal. It is important to estimate the additional resources needed to control any risks that have "moderate" or "high" risk ratings. These resource requirements may be defined in terms of additional time, manpower loading, hardware, or special actions such as additional tests. However, whatever the type of the required resources, it is essential that cost estimates be integrated and consistent with the technical and schedule evaluations.

A performance risk assessment is an evaluation of the contractor's past and present performance record to establish a level of confidence in the contractor's ability to perform the proposed effort.

E-8 Risk Management: Post-Contract Award

Post-contract award risk management builds on the work done during the pre-contract award phase. With the award of the contract, the relationship between the NATO the contractor changes as teams are formed to address programme-associated risk. These teams should validate pre-contract award risk management plans by reviewing assessments, risk-handling plans, and risk-monitoring intentions. The extent of assessments increases as the contractor develops and refines his design, test and evaluation, and manufacturing plans. The NATO PMO should work with the contractor to refine risk-handling plans.

The process begins with the Integrated Baseline Review (IBR) (or NATO equivalent) to ensure reliable plans and performance measurement baselines are established that capture the entire scope of work, are consistent with contract schedule requirements, and have adequate resources assigned o complete program risks. The IBR could be conducted in a way to incorporate other steps identified below. These steps suggest an approach that the PMO might take to initiate the program's risk management plans and activities after contract. They are intended to be a starting point and the PMO should tailor the plan to reflect each program's unique needs.

- Conduct initial meeting with the contractor to describe the programme's objectives and approach to managing risk. The PM may also present the risk management plan.
- Train members of PMO and contractor's organization on risk-management basics, incorporating the programme's risk-management plan and procedures into the training.
- Review the pre-contract award risk plan with the PMO and contractor, revise it as necessary, and share results with the contractor.
- Conduct in-depth review of the pre-contract award risk assessments and expand the review to include any new information obtained since the award of the contract.
- Review and revise risk-handling plans to reflect the reassessment of the risks.
- Review the programme's risk documentation requirements with the contractor. Ensure that the PMO and contractor understand the purpose, format, and contents of the various risk reports.
- Initially, it may be necessary to establish a formalized PMO-contractor risk management organization for the programme, consistent with the terms of the contract.
- Working with the contractor, refine the risk-monitoring plans and procedures.
- Establish the programme reporting requirements with the contractor. Describe the risk management information system that the programme has established, including procedures for providing information for data entry, and identify reports for the PMO and contractor.
- In conjunction with the contractor, identify other risk-management activities that need to be performed.
- Manage the programme risk in accordance with the risk management plan.

- Working with the contactor, refine the risk-monitoring plans and procedures and develop appropriate measures and metrics to track medium and high risk items (e.g., technical performance measures).

INTENTIONALLY BLANK

Annex F - Methods, Techniques and Tools

F-1 Introduction

The methods, techniques and tools presented in this annex are instruments used by the various actors of the risk management process in all stages of the risk management process to help perform the various activities and produce the outputs.

A method is a way of doing something in a systematic way, i.e. in an orderly logical sequence of steps or tasks. A technique is a specific approach to efficiently accomplish these steps and tasks in a manner that is adapted to the particulars of the task or specific to the person executing it. A tool provides a mechanical or mental advantage in accomplishing this task. A tool can be a physical object (e.g. a flip-chart), a technical object (e.g. a software programme).

This annex is a summary of methods, techniques, tools and mentioned and explained within this guide. The methods, techniques and tools shown in Table F-1 are a limited set chosen for their practicality, ease of implementation or common industry practice. However, some of these methods, techniques and tools may not be a best choice for a specific application. For a more exhaustive set of methods, techniques and tools, the reader is referred to ISO/IEC 31010.

Table F-1: Overview of methods, techniques and tools

Method/Technique/Tool	Planning	Identification	Analysis	Response Planning	Monitoring and Control	Guide Reference
RMP Template	X					Annex A
Risk Register Data Model		X	X	X		Annex B
Interview Method		X	X			
Risk Statement Preparation Methods Cause-Risk-Impact Format If –Then Format		X				4.1
Delphi Technique		X	X			4.1.4.1
Checklists		X	X			4.1.4.2 and 4.2.4.1.
Historical Information		X				4.1.4.3
Risk Categorization		X				4.1.4.4
Monte Carlo Simulation			X			4.2.4.2
Probability and Impact Matrix			X			2.12
Risk Exposure Method			X			4.2
Risk Strategies				X		4.3.4.1
Risk Reviews					X	4.4.4.1
Risk Audits					X	4.4.4.2

Annex G - Suggested Literature

Enhancing Risk Management with an efficient risk identification approach.

Barati, S.: Mohammadi, S.: Management of Innovation and Technology, 2008 JCMIT 2008, 4th IEEE International Conference on 21-24 Sept. 2008 Page(s): 1181-1186

An integrated risk management tool and process

Perera J. Holsomback. :Aerospace Conference, 2005 IEEE 5-12 March 2005 Page(s): 129-136

The Application of Risk Matrix to Software Project Risk Management.

Li Xiaoson; Liu Shushi, Cai Wenjun; Feng Songjiang; Information Technology Applications, 2009. IFITA '09. International Forum on Volume 2, 15-17 May 2009 Page(s): 480 – 483

Robust Derivation of Risk Reduction Strategies.

Richardson, J.: Feather, M: Port, D.: Aerospace Conference, 2007 IEEE 3-10 March 2007 Page(s) 1-10

Managing in an uncertain world: risk analysis and the bottom line.

Rowley. I.: Systems Engineering Contribution to Increase Profitability, IEEE Colloquium on 31 Oct 1989 Page(s): 3/1-3/8

Risk Management in R&D Projects.

Kasap.D.: Asyali, I.S.: Elci, K.: Management of Engineering and Technology, Portland International Center for 5-9 Aug. 2007 Page(s): 2287-2290

Policy, information and guidance on the Risk Management aspects of UK MOD Defence Acquisition version 4.0.3 - October 2009

<http://aof.mod.uk/aofcontent/tactical/risk/index.htm>