DEFENSE PROGRAMS RISK MANAGEMENT FRAMEWORK

Constantin PREDA

Risk Manager
NATO Alliance Ground Surveillance Management Agency (NAGSMA),
NATO HQ, Brussels, Belgium

For the past years defense programs have faced delays in delivering defense capabilities and budget overruns. Stakeholders are looking for ways to improve program management and the decision making process given the very fluid and uncertain economic and political environment. Consequently, they have increasingly resorted to risk management as the main management tool for achieving defense programs objectives and for delivering the defense capabilities strongly needed for the soldiers on the ground on time and within limited defense budgets. Following a risk management based decision-making approach the stakeholders are expected not only to protect program objectives against a wide range of risks but, at the same time, to take advantage of the opportunities to increase the likelihood of program success. The prerequisite for making risk management the main tool for achieving defense programs objectives is the design and implementation of a strong risk management framework as a foundation providing an efficient and effective application of the best risk management practices. The aim of this paper is to examine the risk management framework for defense programs based on the ISO 31000:2009 standard, best risk management practices and the defense programs' needs and particularities. For the purposes of this article, the term of defense programs refers to joint defense programs.

Key words: *objectives, risk management, framework, commitment, risk culture, governance, benchmark.*

1. DEFENSE PROGRAM GOVERNANCE

Defense program management is the centralized coordinated management to achieve programs' strategic objectives and benefits and to assure that suppliers deliver on time, within budget and in accordance with customer requirements. It also provides any other support, enablers (e.g. infrastructure, communication) needed for the defense capabilities to become operational.

For achieving defense programs objectives program governance is crucial. The latter can be defined as the process of developing, communicating, implementing, monitoring and assuring organizational structure and practices associated with a program.

The design of program Governance is highly specific to the program and organization. However, it has to fit for purpose. The role of program Governance is to *"ensure decision making and delivery management activities are focused on achieving program goals in a consistent manner, addressing appropriate risks and fulfilling stakeholder requirements"*[1].

The appropriate implementation of program Governance is critical for defense programs success, providing the appropriate organizational structure, policies, processes and procedures to manage, control and support the program. Program Governance should cover the entire defense programs life cycle phases.

Program Governance includes **(Fig.1)**:

- Organizational structure
- Policies
- Processes, procedures
- Roles and responsibilities:
  - –Sponsor
  - –Board (Steering Committee)
  - –Program Manager (PM)
  - –Program Management Office (PMO)
  - –Project Managers

Figure 1. Program Governance

Each of these entities plays an important role within the defense program risk management process. Program sponsors are ultimately responsible for the delivery of program benefits. They provide direction and oversight to the program and are the final decision makers. Their decisions should take into account program risks and opportunities.

Defense programs are typically large initiatives impacting strategic defense areas. To provide an opportunity for collaborative decision making and coordinated issue resolution, a program Board may be established. Such a board is mandatory for complex, high visibility and high risk exposure programs. The program Board approves release of funding and allocation of financial reserves, including contingency and management reserves. The Board also manages the escalated risks

that may impact program objectives and approves the prioritization of risk response strategies. The PMO defines program risk management policy, risk management plan, processes and procedures, provides coordination of risk assessment and response actions across the program and supports monitoring and tracking of program risks. A PM ensures that project deliverables are aligned with business strategy and interacts with senior management and sponsor in managing program strategic risks.

The program Governance is one of the most important factors for an effective and efficient defense programs risk management process. Strong and committed program Governance can provide the foundation for using the risk management as the main tool for managing the defense programs. Program Governance framework integrates the risk management within the organization processes and responsibilities and assists in managing defense programs risks. ISO 31000:2009 standard states very clearly that *"the success of risk management will depend on the effectiveness of the management framework providing the foundations and arrangements that will embed it throughout the organization at all levels"*[2].

Building a risk management based decision making process at program Governance level will be decisive for achieving program goals and objectives and for defining the importance of the defense programs risk management framework.

2. DEFENSE PROGRAMS RISK MANAGEMENT

Defense programs, known for their size, complexity and technological pursuits, are seen among the most challenging of programs. Large defense systems are very complex systems, consisting of hardware and software, multiple suppliers, rapid technology changes and obsolescence issues.

For the last decades, organizations have failed to manage successfully defense programs encountering significant delays in delivering the defense capabilities on time and overrunning the approved budgets. Consequently, some programs lost the political and financial support and became irrelevant for their end users. In addition, defense programs became more and more complex, not only due to the high political and strategic importance and economic implications, but also because of the cuts in defense budgets and schedule constraints. Moreover, it is worth reminding a common truth according to which a broad range of uncertainties and corresponding risks influences the acquisition of new equipment and defense capabilities.

When analysing the effectiveness of risk management within defense programs, a number of pitfalls can be identified:

- the lack of the management commitment in applying the best risk management practices;
- the reactive behaviour of management instead of promoting

and implementing a proactive attitude in managing programs risks;

• the decision making process is not based on the results of risk analysis and evaluation;

• the lack of a risk culture and organization risk appetite;

• the lack of a risk management lessons learned system leading to repetitive mistakes.

Managing risk has been inherent to any type of activity within defense programs. But now, more than ever, and given the recent results of global and local financial crises, the need for a coordinated and systematic approach to managing defense programs risks has emerged. Consequently, the importance of risk management has increased and more and more organizations have made significant investments in using the best risk management practices, expertise and software tools. Organizations have begun to perceive risk management as the main management tool used for protecting stakeholders' investments and for delivering defense capabilities on time, within budget and in accordance with customer and end user demands.

The publication of the ISO 31000 standard in 2009 has provided the organizations a reference guidance and common ground for applying risk management in a more coherent and efficient way. Even if the standard is not mandatory and cannot be used for certification purposes, more and more organizations rely on it, recognizing its value and benefits. The public and private sectors should share a common approach to risk management. However, the need for public accountability and transparency results in some differences between the two sectors. Thus, there are issues which make the public sector risk context quite specific. For example, all employees are required to act in accordance with government regulations, public service values, ethical principles and codes of conduct. Risk management in the public sector must meet strict legal requirements. There is a significant pressure on defense management agencies to be more risk averse in the current uncertain environment. As a result, strong risk management coupled with stronger defense programs governance can improve the decision making process and avoid future delays and budget overruns in providing defense capabilities.

3. RISK MANAGEMENT FRAMEWORK

3.1. Definition

The framework is a structure to guide the management of program risks. ISO Guide 73:2009 defines the risk management framework as *"a set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring reviewing and continually improving risk management throughout the organization"* [2]. The risk management framework proposed by this paper takes into account the concept and definition proposed by

ISO 31000:2009, as well as the best practices in the risk management area of the defense programs (**Fig.2**).

3.2. Role

The risk management framework *"is not intended to prescribe a management system, but rather to assist organization to integrate risk management into its overall management system"* [2]. The framework provides the foundation for *"managing risks effectively through the application of the risk management process at varying levels and within specific context of the organization"*[2]. It also assists the organization in the integration of risk management into the overall organization management system. With a risk management framework in place as a foundation for mutual understanding, all parties involved in defense programs management will be able to speak a common language and communicate more effectively. Throughout the framework the risk management will be adopted by all program staff as inherent part of the everyday way to manage the program. The introduction of a risk management framework is to help organizations to set up a higher standard of program management: the framework *"ensures that information about risks derived from the risk management process is adequately reported and used as a basis for decision making and accountability at all relevant organizational levels"*[2].

3.3. Components

The program risk management framework includes a set of interrelated components. The core components, defined as the risk management foundation, are found in all risk management frameworks, regardless of the type of organization and complexity of the program. Over time frameworks for risk management have evolved and improved as more and more applications of risk assessment and risk based approaches have been implemented within program management. This evolution involves the addition of new components to the framework core components. For example, the addition of the component concerning the risk communication with stakeholders was an essential framework improvement in the 1990s as part of the Canadian Guideline for Decision-Makers (CAN/CSA-Q850-97). In accordance with ISO Guide 73:2009 [3], the risk management framework includes the foundation and organizational arrangements. The foundation includes:

- Mandate
- Commitment
- Policy
- Objectives

The organizational arrangements include:

- Plans
- Relationships
- Accountabilities
- Resources
- Processes and activities

3.3.1. FOUNDATION

A program Sponsor should make a clear statement through a mandate that program risk management is considered an important tool for achieving program objectives and that all program decision-making processes will be risk management based. By giving a clear mandate the sponsor conveys, in a strong and clear message, his interest for risk management and his continuous preoccupation for supporting the program risk management area and for overseeing program management.

Before a program is started, high-level strategic objectives should be defined and made very clear for the management agency. These will have a number of levels of detail including program risk management. According to ISO 31000 a risk is an *"effect of uncertainty on Objectives"*[2]. Defining clear program Objectives will guide the management agency and program staff in identifying and mitigating the risks. But even having a clear mandate program risk management cannot be effective without a clear and strong management commitment at all organization levels. Management commitment provides the motivating force and resources for any organization. Without gaining the TOTAL support from the top program management the risk management process will fail and program staff will not support its implementation. It is very difficult to implement an effective risk management if management, particularly at senior level, do not have a mature understanding of risk and how it can be managed.

Risk management policy represents *"a statement of the overall intentions and directions of an organization related to risk management"* [3]. The policy statement is a formal acknowledgment of management commitment to effectively manage program risks, including risk management objectives, roles and responsibilities and to support risk management plan, process and procedures. The risk management policy must be implemented at all levels of the organization.

3.3.2. Organizational Arrangements

Organizational arrangements define the framework components which are specific for each organization and program. All these components are to be tailored to program needs in accordance with the risk management policy provisions. The framework design will consider all defense program particularities, characteristics, goals and objectives, organization risk attitude, stakeholders and resources.

3.4. Design

The framework design takes into account defense programs' needs, objectives, as well as their political, strategic, internal and external context. However, the framework for all organizations, whatever their

size or purpose, should still contain certain essential elements (core components), for risk management to be effective. The framework should reflect current best practices for risk management and should allow for a clear and easy understanding and implementation on behalf of all stakeholders. The framework should be embedded in all organization practices and process in a way that is relevant, effective and efficient. Through program governance the risk management framework and process should be treated as an integral part of organizational processes. The PMO is responsible for designing the policy, plans, processes, activities and for providing templates, tools and techniques.

A key framework design component defines the resources needed for implementing the risk management policy and process. Consequently the program contingency and management reserves should be sized in accordance with program risk level, organization risk tolerance and program Objectives.

The framework should allow for quicker and better communication between the decision-maker and all stakeholders, avoiding excessive cost and complexity in the process. Establishing internal and external communication channels and reporting mechanism are of the great importance for the risk framework success.

Clause 5 of ISO 31000 contains full advice on how the framework should be designed and implemented.

3.5. Implementation

This paper supports the implementation of the risk management framework based on the ISO 31000 standard provisions. A structured and comprehensive risk management framework should be implemented using a top-down incremental approach where risk management should become a key process to enable the organization to determine and achieve its objectives.

The program governance provides guidance and oversees the framework implementation strategy. The program management should ensure that the decision making process is aligned with the risk management process outcomes. Implementing the risk management framework involves trained people, consultation with program stakeholders, discipline and appropriate tools.

3.6. Monitoring & Review

The risk management framework should adapt to program changes generated by organizations' external and internal context. From this point of view, the PMO should periodically review the effectiveness of the risk management framework and whether the risk management framework, policy and plan are still appropriate. Monitoring and review involves confirmation that the various risk management elements and activities actually work effectively and in line with expectations.

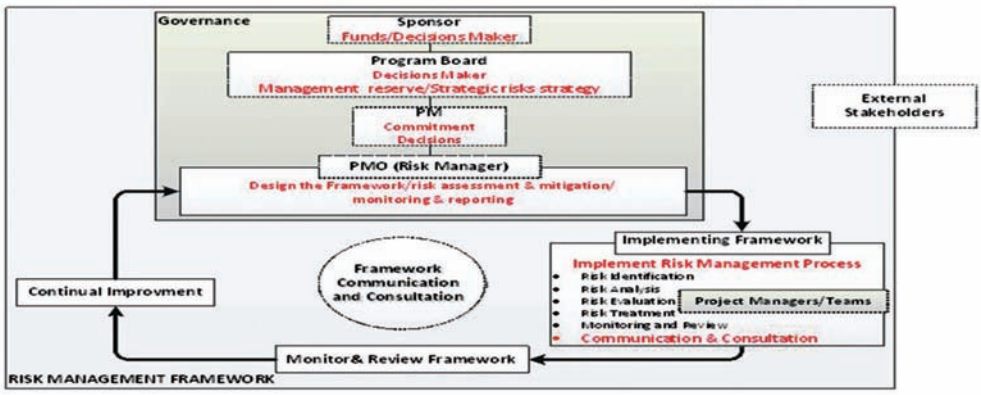

Figure 2. Risk Management Framework

3.7. Continuous Improvement

Based on the results of the monitoring and review processes, the PMO should make proposals to program management on how the risk management framework can be improved. Any change to the risk management framework should lead to improvements. Moreover, it should be timely communicated so that all program stakeholders' buy-in is thus obtained.

4. BENCHMARK FRAMEWORK

Organizations can and should use ISO 31000 principles and attributes of good practices as a means to benchmark their risk management framework. ISO 31000 should be used as a *"health check"* of the maturity of risk management framework and process. ISO 31000/ Annex A shows an informative list of the attributes representing a high level performance in managing risks and some tangible indicators for each attribute:

• Continuous improvement - Continual improvement of the risk management framework based on the risk management performance assessment as part of organization performance measurement.

• Full accountability for risks - Fully defined and fully accepted accountability for risks, controls and risk treatment tasks. For this, designated people must have appropriate skills, training, authority and adequate resources.

• Application of risk management in all decision making - Explicit consideration of risks and application of risk management within the decision making process at all levels of an organization.

• Continuous Communications - Ongoing communication with external and internal stakeholders, establishing a two-way channel and including appropriate reports.

• Full integration in the organization's governance structure -

Risk management is central to the organization management processes especially if risks are evaluated in terms of uncertainty and inherent effects on program objectives. In such a case, the governance structure and process are based on the management of risk.

Taking into account defense programs' particularities and the criticality of the decisions that are to be made about them, two other attributes are of equal importance for an enhanced risk management framework: risk culture and stakeholders' management.

4.1. Risk Culture

Defense programs involve people from different countries with different levels of knowledge of risk management. This makes the implementation of a risk management process quite difficult and requires a significant culture change. Some changes can happen quickly but it does require prolonged effort and management focus to make risk management become self-sustaining. One solution is to form and use a community of practice of risk champions who represent parts of the organization. Thus, risk management practices within a program can be approached as a whole instead of delegating responsibility solely to the risk management department. A risk management culture needs to be supported by top level management by developing a clear risk policy and process and by involving all staff in risk training and education. The challenge of changing the organization's culture to ensure risk management should be management first priority and must be applied to every activity at every level with an impact on organizational goals and objectives.

Some of the means to ensure that risk management becomes an integral part of the general culture of the organization are: raising risk awareness, organization-wide dialogues/discussions, formal training, recognition of risk qualification levels and assigning management responsibilities for risk communication. An effective risk management framework must be based on a comprehensive, systematic and coordinated approach and on a culture recognising risk management as everyone's responsibility and as a feature of the way of doing things.

4.2. Stakeholder Management

International defense programs involve a significant number of stakeholders with different power, culture, position and interests within the program. Program risk management covers all risks that might affect program objectives, including the risks originating from external stakeholders. Consequently, management should identify all program stakeholders' concerns and involve them within the program risk management process for risk identification and mitigation. Stakeholders' involvement within risk management process is vital for program success.

5. CONCLUSIONS

Most of the defense programs management agencies face problems in delivering the defense capabilities on time and within limited budgets. The defense programs risk management encounters challenges which could negatively impact the defense programs decision making process. The management should be aware of these challenges and take the appropriate actions. Some of the management agencies have implemented a risk management framework based on the best risk management practices and more and more agencies seek to improve their risk management by implementing ISO 31000:2009 standard.

However, unless management, especially senior management, values the new paradigm for risk as an effect of the inherent uncertainties of program objectives, and the value of risk management, then no real progress can be made in designing and implementing an enhanced risk management framework. ISO 31000 is already a well-recognized and accepted standard which should be followed for significant improvements in the defense programs risk management.

REFERENCES

[1] Program Management Governance Course, http://cstudies.ubc.ca/a/Course/Program-Management-Governance/IQ200/, last retrieved 13.06.2012.

[2] *** (2009) International Standard: ISO 31000:2009, Risk Management Principles and Guidelines, http://calmap.gisc.berkeley.edu/dwh_doc_link/Technical_Background/RAM_documents/ISO+31000-2009.pdf, pp. 8-9, last retrieved 13.06.2012.

[3] *** (2009) ISO Guide 73:2009, Risk Management Vocabulary, http://www.pqm-online.com/assets/files/standards/iso_iec_guide_73-2009.pdf, last retrieved 13.06.2012.

[4] Australian Defense Risk management Framework: A Comparative Study, Svetoslav Gaidow and Seng Boey, Land Operations Division Systems Sciences Laboratory, Australia, 2005.

[5] Benchmark Framework for Risk Management, Contributed by J.H. Shortreed, L.Craig and S.McColl, 2000.

[6] Canadian Standards Association, 1997-Risk management: Guideline for Decision-Makers (CAN/CSA-Q850-97).

[7] How to bring your ERM framework into line with ISO31000 - Grant Purdy, Chairman of Standards Australia and New Zeeland Joint Technical Committee on Risk Management, Broadleaf Capital International Pty Ltd, 2008.

[8] PMI-The Standard for Program Management, Second Edition, 2008

[9] PMI-Practice Standard for Project Risk Management, 2009.