Foundations of the Platform Risk Analysis Process (PRAP)

Cyber Security Risk Analysis Process for Military Platforms of Canadian Armed Forces (CAF)

Eric Boivin

DRDC – Valcartier Research Centre

Defence Research and Development Canada

Scientific Report
DRDC-RDDC-2015-R016
February 2015

Abstract

The *Platform Risk Analysis Process* (PRAP) provides a generic methodology to conduct cybersecurity *risk analysis* (RA) for military platforms. This report describes foundations of PRAP designed by *Defence Research and Development Canada* (DRDC) – *Valcartier Research Centre* under the *Platform-to-Assembly Secured System* (PASS) project (2013-2018) (05aa). PASS project envisages to apply PRAP on three (3) military platforms of the *Canadian Armed Forces* (CAF), such as the *Aurora CP-140* of *Royal Canadian Air Force* (RCAF), the *Halifax-class Frigate* of the *Royal Canadian Navy* (RCN), and the *Land Combat Support System* (LCSS) of the *Light Amour Vehicle 6* (LAV) of the *Canadian Army* (CA). These platform assessments will contribute to validate concepts carried by PRAP.

Significance to defence and security

Introduction or background: Military platforms are now composed of a quantity and a variety of cyber components making a deep analysis and protection of each one unrealistic and useless for many of them. *Platform-to-Assembly Secured System* (PASS) (2013-2018) (05aa) project aims at managing cyber risks at a platform level by identifying critical personnel, process and technological components associated to the platforms, investigating attack vectors on these critical elements and study impacts of successful attacks. Such analyses will lead to some recommendations for improving *Canadian Armed Forces* (CAF) cyber security of specific platforms.

Results: This report throws the foundations of the *Platform Risk Analysis Process* (PRAP) to be used for assessing cyber risks of military platforms, and recommending fixes and/or control measures. PRAP provides a generic method inspired from the best practices of academic, governmental and international organizations in terms of cybersecurity risk assessment. This work has been conducted by *Defence Research and Development Canada* (DRDC) – *Valcartier* under PASS project.

Significance: PASS project envisages applying PRAP on three military platforms of CAF, such as the *Block IV systems* of the *Aurora CP-140* of *Royal Canadian Air Force* (RCAF), the *Combat Management System* (CMS-330) of the *Post-Frigate Life Extension* (FELEX) *of Halifax-class Frigate* of the *Royal Canadian Navy* (RCN), and the *Land Combat and Support System* (LCSS) of the *Light Amour Vehicle Upgrade* (LAV UP) of the *Canadian Army* (CA).

Future plans: This report presents a high-level description of PRAP. A detailed description of each step of PRAP and the result of its application to selected platforms will be published in subsequent reports to it.

Résumé

Le *processus d'analyse des risques de plateformes* PRAP (en anglais, *Platform Risk Analysis Process*) présente une méthodologie générique pour mener l'évaluation des risques cybernétiques de plateformes militaires. Ce rapport décrit les fondements du processus PRAP conçu par *Recherche et développement pour la défense Canada* (RDDC) – Centre de recherche *Valcartier* dans le cadre du projet *Platform-to-Assembly Secured System* (PASS) (2013-2018) (de 05aa). Le projet PASS envisage d'appliquer PRAP à trois plateformes militaires des *Forces armées canadiennes* (FAC) dont, le *CP-140 Aurora* de l'*Aviation royale canadienne* (ARC), la *Frégate Halifax* de la *Marine royale canadienne* (MRC), ainsi que le système de soutien au combat terrestre LCSS (en anglais, *Land Combat Support System*) de la nouvelle version du véhicule blindé léger LAV 6 (en anglais *Light Amour Vehicle*) de l'*Armée canadienne* (AC). L'analyse de ces plateformes contribuera à valider les concepts véhiculés par PRAP.

Importance pour la défense et la sécurité

Introduction ou contexte: Les plateformes militaires sont maintenant composées d'une quantité et d'une variété importante de composantes cybernétiques dont l'analyse et la protection totale sont quasi impossible. Le projet PASS (en anglais, *Platform-to-Assembly Secured System)* (2013-2018) (05aa) vise à gérer les risques cybernétiques au niveau d'une plateforme en identifiant le personnel critique, les processus opérationnels et les composants technologiques liés à celle-ci, en enquêtant sur les vecteurs d'attaques de ces éléments essentiels et en étudiant les effets d'attaques réussies. Ces analyses visent à formuler des recommandations visant à améliorer la sécurité cybernétique des plateformes militaires des *Forces armées canadiennes* (FAC).

Résultats: Ce rapport jette les fondements du *Processus d'analyse des risques de plateformes* PRAP (en anglais, *Platform Risk Analysis Process*) destiné à évaluer les risques cybernétiques de plateformes militaires et à recommander l'application de correctifs et/ou de mesures de contrôles. PRAP présente une méthode générique basée sur les meilleures pratiques d'organisations universitaires, gouvernementales et internationales en matière d'évaluation des risques cybernétiques. Ce travail a été réalisé par *Recherche et développement pour la défense Canada* (RDDC) – *Valcartier* sous le projet PASS.

Importance: Le projet PASS envisage d'appliquer le processus PRAP à trois plateformes militaires des *Forces armées canadiennes* (FAC), tels le *Bloc système IV* du *CP-140 Aurora* de l'*Aviation royale canadienne* (ARC), le système de gestion de combat CMS-330 (en anglais, *Combat Management System*) de la *Frégate de classe Halifax* de la *Marine royale canadienne* (MRC), ainsi qu'au *Système de soutien au combat terrestre* LCSS (en anglais, *Land Combat Support System*) du *Véhicule blindé léger* LAV 6 (en anglais, *Light Amour Vehicle*) de l'*Armée canadienne* (AC).

Perspectives : Ce rapport présente une description de haut niveau des étapes du processus PRAP. Une description détaillée de chacune des étapes du processus PRAP, ainsi que les résultats issus de son application aux plateformes choisies seront publiés dans des rapports subséquents à celui-ci.

Table of contents

Abstract …….. i
Significance to defence and security i
Résumé …….. ii
Importance pour la défense et la sécurité ii
Table of contents iii
List of figures v
List of tables vi
1 Introduction 1
2 Requirements for cyber risk analysis on military platforms 2
Requirement 1: Apply project management concepts 2
Requirement 2: Adopt a risk model 2
Requirement 3: Embrace an iterative and flexible approach to conduct RA 2
Requirement 4: Develop a comprehensive understanding 3
Requirement 5: Initiate RA with an adverse impact analysis 3
Requirement 6: Provide comprehensive results 3
Requirement 7: Keep stakeholder informed 4
Summary 4
3 State-of-the-art : Risk management processes 5
Process 1: Risk assessment methodology of the NIST SP 800-30 standard 5
Process 2: Risk assessment process of the NIST SP 800-30 r1 standard 6
Process 3: Risk management process of the NIST SP 800-39 standard 7
Process 4: Cybersecurity Risk Management (CSRM) methodology 7
Process 5: Space systems risk management process of the ISO 17666:2003 standard 8
Process 6: Project Management Body of Knowledge (PMBoK) standard 9
Process 7: Information security risk management process of the ISO/IEC 27005:2011 standard 9
Process 8: Threat and Risk Assessment (TRA-1) methodology 11
Process 9: Information Operations Vulnerability / Survivability Assessment (IOVSA) 12
Process 10: Program Protection Planning (PPP) process 13
Summary 14
4 Platform Risk Analysis Process (PRAP) 17
Step 1: Plan 18
Step 2: Characterize 19
Step 3: Assess 20
Step 4: Mitigate 21
Step 5: Monitor 21
Communicate 22

Summary 23
5 Conclusion 25
References 27
Annex A Questionnaire for identifying PRAP requirements... 29
Annex B Risk model adopted by PRAP 31
List of symbols/abbreviations/acronyms/initialisms 33

List of figures

Figure 1 Risk assessment methodology flowchart extracted from NIST SP 800-30 standard.. 5

Figure 2 Risk assessment process extracted from NIST SP 800-30 r1 standard. . 6

Figure 3 Risk management process extracted from NIST SP 800-39 standard.. . 7

Figure 4 Cybersecurity Risk Management (CSRM) methodology. 8

Figure 5 Space systems risk management process of ISO 17666 standard. . . . 8

Figure 6 Project Management Processes based on the PMBoK guide 4th edition.. 9

Figure 7 Risk management process extracted from ISO 27005:2011 standard.. . 10

Figure 8 Risk treatment activity within the ISO 27005:2011 standard. 11

Figure 9 Harmonized Threat and Risk Assessment (TRA-1) methodology. . . . 11

Figure 10 Information Operations Vulnerability / Survivability Assessment (IOVSA) methodology. 12

Figure 11 Program Protection Planning (PPP) process.. 14

Figure 12 Platform Risk Analysis Process (PRAP). 17

Figure 13 Platform Risk Analysis Process – Step 1: Plan. 18

Figure 14 Platform Risk Analysis Process – Step 2: Characterize.. 19

Figure 15 Platform Risk Analysis Process – Step 3: Assess. 20

Figure 16 Platform Risk Analysis Process – Step 4: Mitigate.. 21

Figure 17 Platform Risk Analysis Process – Step 5: Monitor.. 22

Figure 18 Platform Risk Analysis Process – Communication plan. 23

Figure A.1 Questionnaire used for identifying PRAP requirements. 29

Figure B.1 Cybersecurity risk model adopted by PRAP. 31

List of tables

Table 1 Retained RA processes. 14

Table 2 PRAP steps vs RA requirements.. 24

Table B.1 Concepts of the risk model used by PRAP. 31

1 Introduction

This document introduces the foundations of *Platform Risk Assessment Process* (PRAP) which wants to provide a comprehensive methodology aiming to identify cyber risks, and support platform's stakeholders into their actions to lower them. It is part of the *Platform-to-Assembly Secured Systems* (PASS) tacking place under the *Defence research & Development Canada* (DRDC) *Science and Technology* (S&T) Cyber program. Such a methodology for military platforms is a new area and very few people appear to address it: Almost all cyber risk analyses have been tackling software systems.

Originally, military platform has few similarities with corporate *information technology* (IT) systems. Military platforms are lightly connected systems exploiting proprietary solutions. However, planned platform revisions are likely to replace proprietary solutions by standard computers, operating systems and network protocols, which increase the likelihood of cyber incidents. Gradually, platforms are starting to resemble to common IT solutions. Therefore, their cyber risks are growing making their physical interaction with the environment more worrying.

Following the current *Section 1 Introduction*, the document is organized in five (5) sections:

- *Section 2 Requirements* lists RA requirements which PRAP should implement;
- *Section 3 State-of-the-Art* provides a general overview of current RA processes and methodologies used for managing risks;
- *Section 4 Process* describes the 5-step process PRAP integrating the RA requirements and the best RA practices into its design; and
- *Section 5 Conclusions* summaries the definition of PRAP and future R&D efforts.

2 Requirements for cyber risk analysis on military platforms

Conducting a cybersecurity RA for a military platform is more likely to present a high level of complexity than for a typical corporate IT system. Even if military platforms are starting to resemble to common IT solutions, the remaining heterogeneity of hardware and software solutions challenge any assessment efforts. Based on this observation, this section presents a set of requirements to consider for mastering complexity when conducting a cybersecurity RA for military platforms.

Requirements have been identified by using a questionnaire (see Annex A) to solicit ideas about what should be included into a hypothetical platform risk analysis report. The questionnaire was submitted to project team members, and up to twenty-five (25) requirements where gathered. Proposed requirements were analysed and regrouped into seven (7) major requirements presented below. Consulted team members included experts in defence & security, information technology and human factors.

Requirement 1: Apply project management concepts

This requirement suggests adopting recognized project management technics and processes for conducting cybersecurity RA. In fact, cybersecurity RA could be managed as a typical project. For instances, objectives have to be defined, resources should be allocated to activities, risks should be identified, and so on. Project management technics and processes help to bring standardization and interoperability within the RA. It allows simplifying communication exchanges between stakeholders and RA team.

Project management theory integrates a wide range of tools for supporting a RA. For instance, the *Project Management Body of Knowledge* (PMBOK) guide (PMI Standard, 2013), a recognized standard, provides processes for *Initiating*, *Planning*, *Executing*, *Monitoring* and *Closing* a project. Therefore, even if project management processes are likely to strongly support initial activities of a RA (i.e., mandate and work plan definitions), they could be used for supporting execution of the whole spectrum of a RA.

Requirement 2: Adopt a risk model

This requirement suggests adopting a risk model in order to develop a mutual understanding of cybersecurity concepts and theory during stakeholders and RA team discussions. The risk model defines keys terms, risk factors and relationships among factors that support the foundations of the RA process. Annex B presents the risk model adopted by PRAP for assessing military platforms (Nécaille, 2014).

Requirement 3: Embrace an iterative and flexible approach to conduct RA

In the earliest stage of a RA, it could be difficult producing accurate and crystal clear deliverable content for each step of the RA. Many constraints could impede the accomplishment of them. For instance, the definition of the RA scope could be influenced by a lack of information coming from inaccurate technical documents or unavailable subject matter experts. Unless stakeholders have a clear idea of what should be assessed first, an iterative cycle of scope definition and assessment efforts should be adopted to gradually determine the optimal focus of the RA. Therefore, the RA team has to deal with these constraints by embracing an iterative approach for conducting the RA.

The iterative approach is not limited to the definition of the RA scope. For instance, the list of identified risks or the recommended mitigation plan is likely to evolve with time. Modern RA process should embrace this vision by fostering iteration and deliverable updates when deemed necessary.

Requirement 4: Develop a comprehensive understanding

Mentioned bellow, military platforms are usually much more complex than typical IT systems. In order to develop a comprehensive understanding of how the platform works, the RA team should develop views, matrix and tables expressing various facets of its architecture and its behavior. The *Department of National Defence / Canadian Armed Forces Architecture Framework* (DNDAF) guides (DEA 4, 2013a) (DEA 4, 2013b) (DEA 4, 2013c) provides a structured approach that address this challenge. The DNDAF framework provides a series of commonly understood stakeholders' views and sub-views that could be used for representing complex aspects of a military platform. This requirement suggests using DNDAF views and sub-views when suitable.

Requirement 5: Initiate RA with an adverse impact analysis

Typically, it exists three approaches to initiate a cybersecurity RA (NIST SP 800-30, 2002): (1) *Identify threat sources*; (2) *Identify system vulnerabilities*; and (3) *Conduct an adverse impact analysis*. The first two requires a significant level of effort to accomplish when used for military platforms. In one hand, military platform is designed to deal with a wide range of operational context environments where threat sources are various and/or unwell known. In other hand, military platform includes proprietary hardware and software solutions which make difficult the identification of vulnerabilities.

Initial assessment efforts could be optimized by privileging first an adverse impact analysis. This requirement contributes to limit the RA scope by identifying critical systems or sensitive information to consider first.

Requirement 6: Provide comprehensive results

Essentially, this requirement focuses on delivering comprehensive results for stakeholders. In one hand, the RA team should take care to deliver comprehensive results by using graphics, charts, graphs and tables that express clearly how and which risks have been identified, which treatment options are suggested and what are expected results of mitigation actions.

In other hand, this requirement suggests supporting comprehension by fostering stakeholders to follow basic trainings on cybersecurity (if required). In addition to facilitating the interpretation of results, cybersecurity trainings could raise the level of awareness of platform operators, and thereby reduce the level of some identified risks. For instance, the *SANS Institute* (www.sans.org) provides a wide spectrum of training courses that could help to meet this requirement.

Requirement 7: Keep stakeholder informed

This requirement suggests adopting a communication strategy to keep inform stakeholders about RA progress. The strategy should include a deliverable schedule for each accomplished step of the analysis. The idea is to continuously inform stakeholders about any findings which could threaten the integrity of the military platform. Even if results are preliminary, it is critical to communicate them in order to quickly put in place mitigation strategies when deemed necessary.

Summary

Essentially, PRAP should foster the establishment of effective communication channel between stakeholders and the RA team. Whatever requirement, communication is a key concern to satisfy which will help to maximize the application of the RA.

The following section presents an overview of current RA processes and methodologies developed by the risk management community.

3 State-of-the-art : Risk management processes

This section presents various risk assessment processes that inspired the design of PRAP. Retained processes were extracted form academic, governmental and international organizations. A brief description of each process was produced in order to identify positive characteristics witch have to be included to PRAP. The accomplished work of this section was jointly conducted with the *National Research Council Canada* (NRC) under the agreement number DRDC-SRE07-01-038. Full report content could be retrieved under the following reference (Senay, 2014).

Process 1: Risk assessment methodology of the NIST SP 800-30 standard

In 2002, *National Institute of Standards and Technology* (NIST) published the *Risk Management Guide for Information Technology Systems* (NIST SP 800-30, 2002) witch presents the 9-step *Risk assessment methodology* (Figure 1). The guide provides *a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems*. The process was designed for experienced or inexperienced, technical and non-technical personnel who support RA activities into their organization. The nine (9) steps provide a comprehensive and structured methodology that helps to identify appropriate controls for reducing or eliminating risk associated to IT systems.

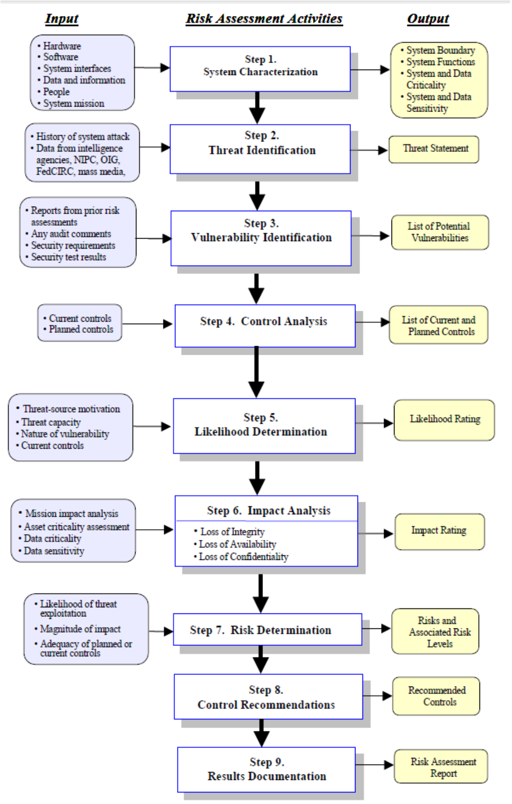


Figure 1: *Risk assessment methodology flowchart extracted from NIST SP 800-30 standard.*

NIST sees ***risk*** as a function of the ***likelihood*** of a given ***threat***-source's exercising a particular potential ***vulnerability***, and the resulting ***impact*** of that adverse event on the organization (NIST SP 800-30, 2002, p. 8). PRAP endorses this vision and has developed a risk model strongly inspired from that definition to support stakeholder discussions (Nécaille, 2014). This view of risk has been integrated to PRAP, and generalized at a platform level.

NIST states that steps *2-Threat identification*, *3-Vulnerability identification*, *4-Control analysis*, and *6-Impact analysis* can be conducted in parallel after Step *1-System characterization* has been completed. This feature allows the RA team to conduct an adverse impact analysis first, as suggested by *Requirement 5* of the previous chapter.

Process 2: Risk assessment process of the NIST SP 800-30 r1 standard

In 2012, NIST published the *Guide for Conducting Risk Assessments* (NIST SP 800-30 r1, 2012) which presents the *Risk Assessment Process, and* superseded its 2002 version (see Process 1). This new version presents the concept of risk assessment at a higher level. Steps 2 to 7 of its previous version were merged into a larger one, called *Conduct Assessment* (Step 2), while *Preparation* (Step 1), *Communication* (Step 3) and *Recommendations* (Step 4) were maintained separately (Figure 2).

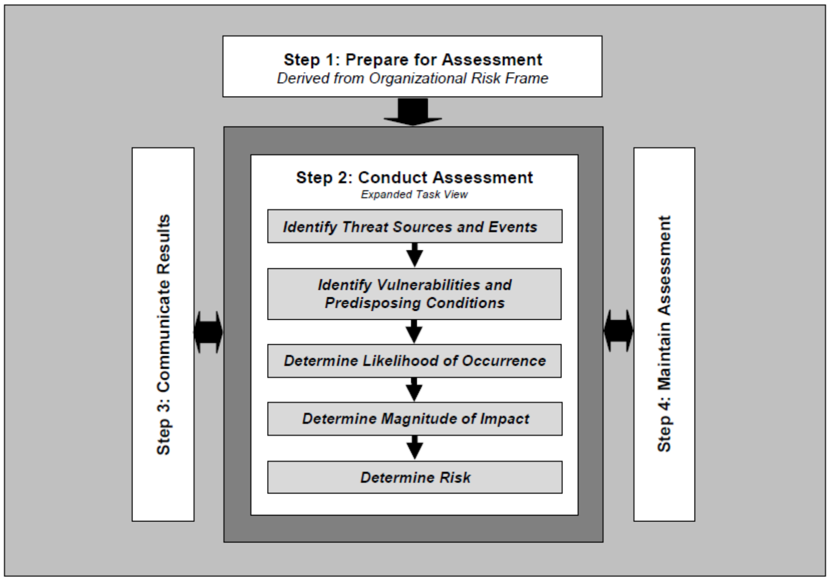

Step 1: Prepare for Assessment
Derived from Organizational Risk Frame
Step 2: Conduct Assessment
Expanded Task View
Identify Threat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurrence
Determine Magnitude of Impact
Determine Risk
Step 3: Communicate Results
Step 4: Maintain Assessment

Figure 2: *Risk assessment process extracted from NIST SP 800-30 r1 standard.*

The *Risk Assessment Process* of NIST SP 800-30 r1 standard shows a strong level of maturity. Three positive changes are observed and integrated to PRAP:

1. *Step 1: Preparation for Assessment,* previously named *Step 1: Characterization* in 2002's version, shows particular status. It is exclusively dedicated to gather information about IT system. No opinion is formulated about the security and no change is applied to the IT system. This step focusses on understanding the IT system has is.

2. *Step 3: Communication results*, previously named *Step 9: Results Documentation* in 2002's version, includes the possibility to deliver intermediate results when conducting the RA. Sharing intermediate results with stakeholders are essential to develop quick response plans.

3. *Step 4: Maintain Assessment*, absent from 2002's version, helps to reconfirm the purpose, the scope and the assumptions of the RA. The RA is no more see as a single assessment task, but more as continuous one adaptable to emerging threats or organizational changes.

Process 3: Risk management process of the NIST SP 800-39 standard

In 2011, NIST published the *Managing Information Security Risk* (NIST SP 800-39, 2011) standard which introduces a structured approach to risk management in information security. This high level process presents four actions: *Frame*, *Assess*, *Respond* and *Monitor* (Figure 3).

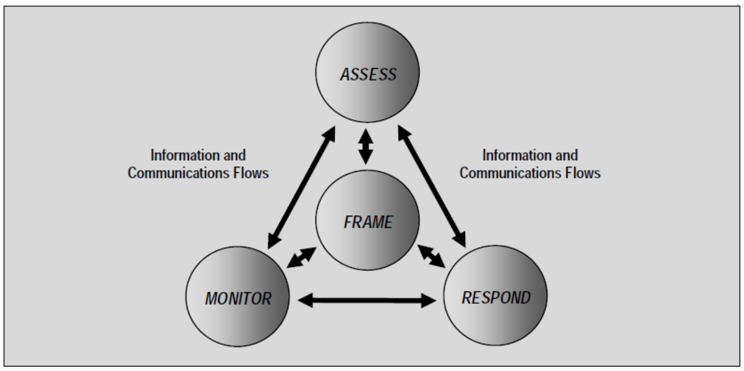

ASSESS
Information and Communications Flows
Information and Communications Flows
FRAME
MONITOR
RESPOND

Figure 3: *Risk management process extracted from NIST SP 800-39 standard.*

Assess, *Respond* and *Monitor* actions are intuitive to understand, while *Frame* needs explanations. *Frame* tries to establish how organizations manage risk regarding various aspects such as assumptions, constraints, risk tolerances, and priorities used within organizations for making investment and operational decisions. Military platforms are highly exposed to organizational and external risk factors. A comprehensive understanding of platform context could contribute to narrow scope and develops a mutual understanding of the RA expectations.

Process 4: Cybersecurity Risk Management (CSRM) methodology

In 2010, the firm *Booz Allen Hamilton* published the *Cybersecurity Risk Management* (CSRM) *methodology* (Figure 4) which ensures that assurance and resilience are built into mission systems as they progress through the acquisition and systems development lifecycle and continuing during system operations (Peter Katsumata, Judy Hemenway, & Wes Gavins, 2010). CSRM methodology has been designed for *Department of Defence* (DoD) mission systems.

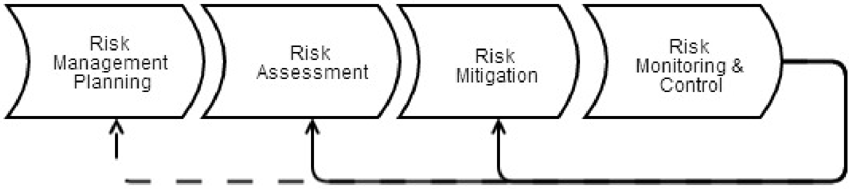


Figure 4: *Cybersecurity Risk Management (CSRM) methodology.*

The methodology includes some of the steps described in NIST 800-30 process (NIST SP 800-30, 2002), risk management concepts from the ISO 17666:2003 *Space Systems – Risk Management* standard (ISO 17666, 2003), *DoD risk management guidance* (DoD, 2006), and some of the processes described in the PMBOK guide. CSME methodology combines risk and project management methodologies to support its approach.

Process 5: Space systems risk management process of the ISO 17666:2003 standard

In 2003, the *International Organization for Standardization* (ISO) published the *Risk Management Process for Space Systems* (ISO 17666, 2003) which presents an iterative risk management process. The four-step process is illustrated in Figure 5.

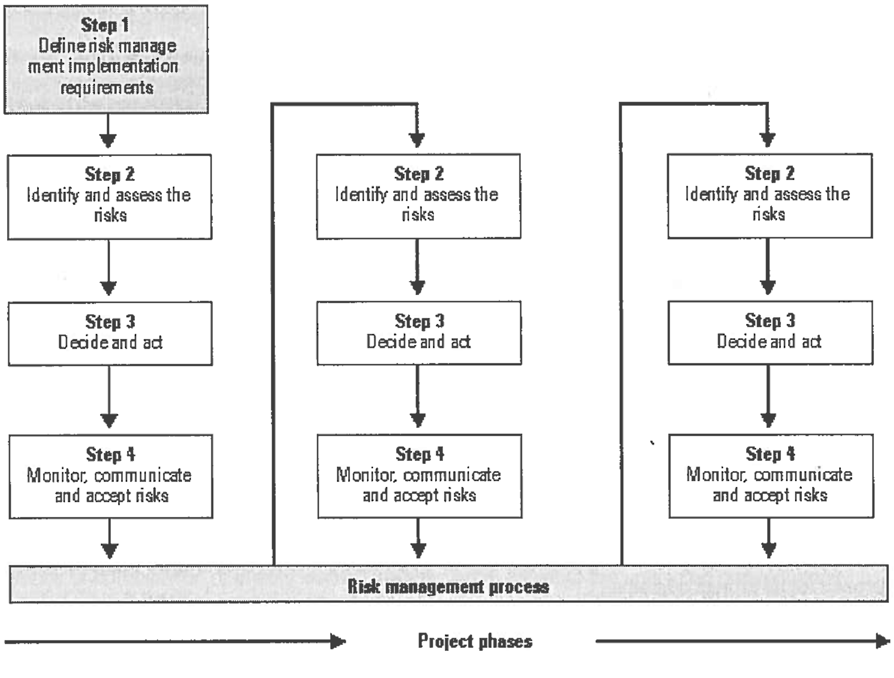
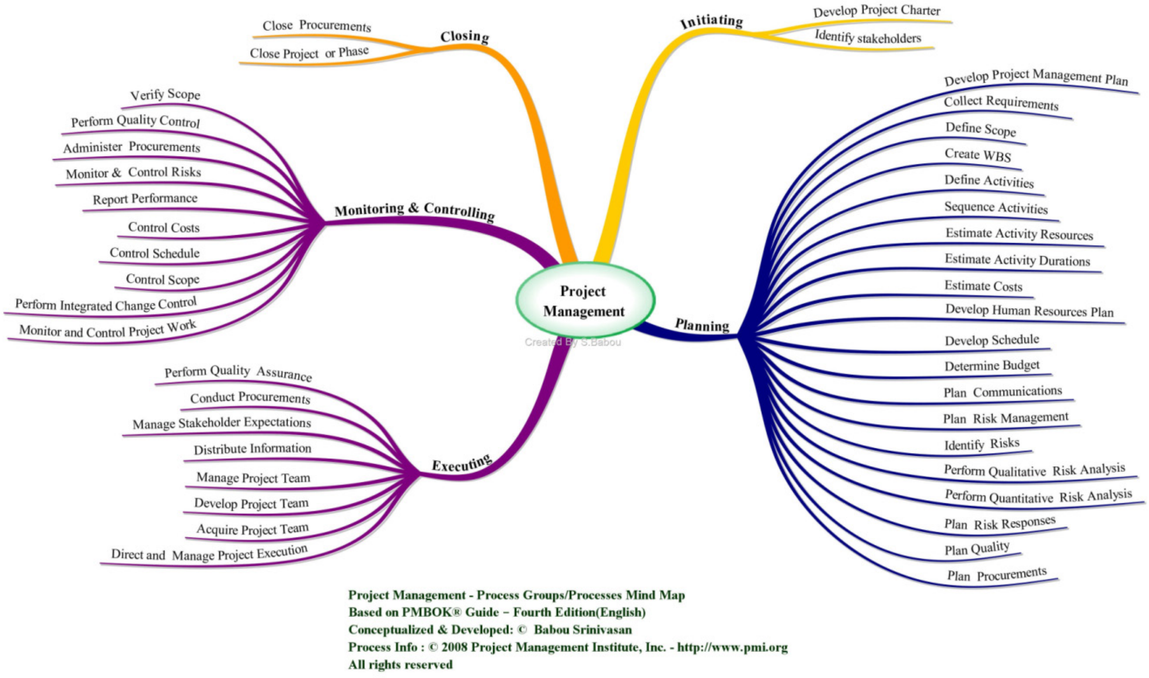

Step 1
Define risk manage ment implementation requirements
Step 2
Identify and assess the risks
Step 3
Decide and act
Step 4
Monitor, communicate and accept risks
Step 2
Identify and assess the risks
Step 3
Decide and act
Step 4
Monitor, communicate and accept risks
Step 2
Identify and assess the risks
Step 3
Decide and act
Step 4
Monitor, communicate and accept risks
Risk management process
Project phases

Figure 5: *Space systems risk management process of ISO 17666 standard.*

ISO 17666 standard suggests exploiting an iterative approach to maintain the accuracy and the relevancy of the RA with time. New findings of the RA may challenge past observations. In this case, a revision of the content of past deliverables might be required. Military platforms are complex and evolve in complex environment. Therefore, an iterative approach seems very relevant to address this kind of issue.

Process 6: Project Management Body of Knowledge (PMBoK) standard

In 2013, the *Project Management Institute* (PMI) published the fifth version of the *PMBoK* guide (PMI Standard, 2013) which presents a set of standard terminology and guidelines for project management. The PMBoK provides guidelines for managing projects through 47 processes distributed into 5 groups (i.e., *Initiating*, *Planning*, *Executing*, *Monitoring & Controlling*, and *Closing*). Various areas, such as project integration, scope, time, cost, quality, human resource, communications, risk, procurement, and stakeholders are addressed. In addition, the standard suggests six specific (6) processes that directly address risk management: (1) plan risk management, (2) identify risks, (3) perform qualitative risk analysis, (4) perform quantitative risk analysis, (5) plan risk response and (6) control risks. Figure 6 shows groups and processes of the PMBOK.



Project Management - Process Groups/Processes Mind Map
Based on PMBOK® Guide – Fourth Edition(English)
Conceptualized & Developed: © Babou Srinivasan
Process Info : © 2008 Project Management Institute, Inc. - http://www.pmi.org
All rights reserved

Figure 6: *Project Management Processes based on the PMBoK guide 4th edition.*

Benefits of the PMBoK standard have already been mentioned by *Requirement 1* in Chapter 2. PRAP should adopt PMBOK processes to standardize RA activities associated to project and risk management aspects.

Process 7: Information security risk management process of the ISO/IEC 27005:2011 standard

In 2011, the ISO and the *International Electrotechnical Commission* (IEC) published the *Information Security Risk Management Standard* (ISO/IEC 27005, 2011) which presents a detailed risk management process. The information risk assessment process consists of *Context Establishment*, *Risk Assessment*, *Risk Treatment*, *Risk Acceptance*, *Risk Communication*, and *Risk Monitoring* (Figure 7).

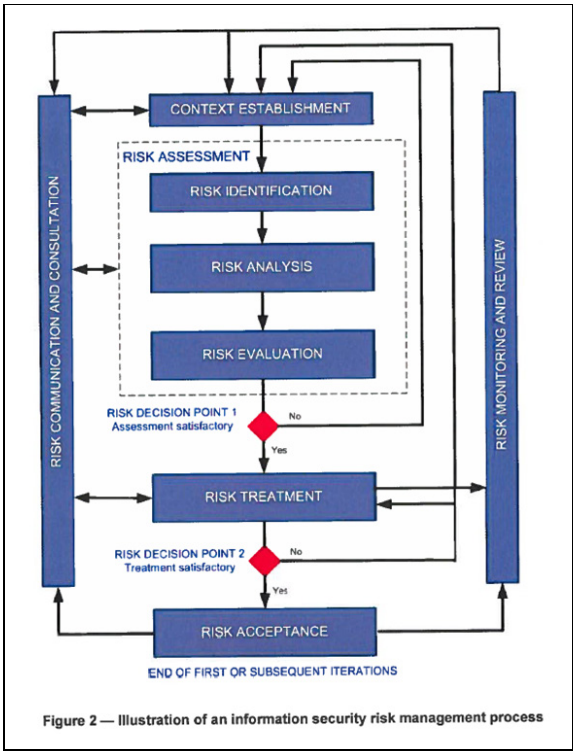


Figure 7: *Risk management process extracted from ISO 27005:2011 standard.*

The ISO 27005:2011 *Risk Management Process* shows many similarities with the *Risk Assessment Process* of NIST SP 800-30 r1 standard. The standard foregrounds concepts of *Risk Treatment*, *Risk Acceptance* and *Residual Risks* (Figure 8). These concepts help stakeholders to understand remaining risks even if risk treatment options are applied. PRAP should integrate the ISO 27005:2011 approach.

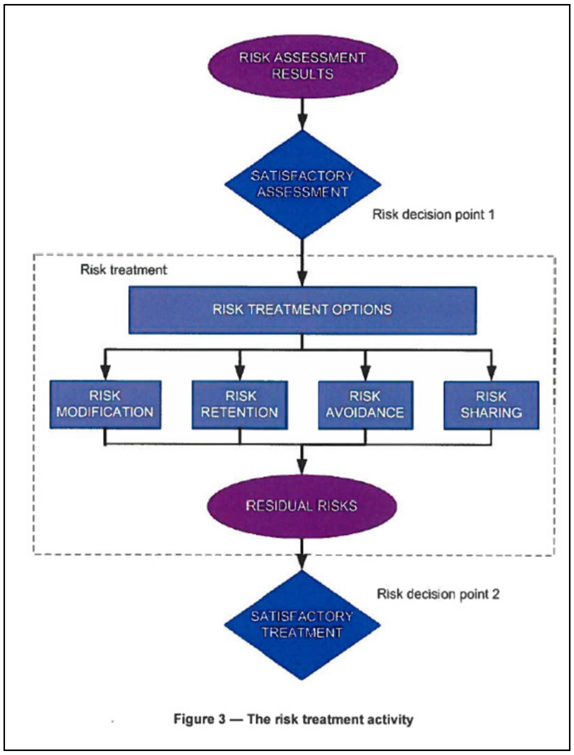


Figure 8: *Risk treatment activity within the ISO 27005:2011 standard.*

Process 8: Threat and Risk Assessment (TRA-1) methodology

In 2007, the *Communications Security Establishment* (CSE) and the *Royal Canadian Mounted Police* (RCMP) published the last version of *Harmonized Threat and Risk Assessment Methodology* (TRA-1) (CSE & RCMP, 2007). TRA-1 applies to both physical security and information security. The document provides a detailed description of the five (5) steps that lead to the production of a plan for assessing threats and risks (Figure 9).

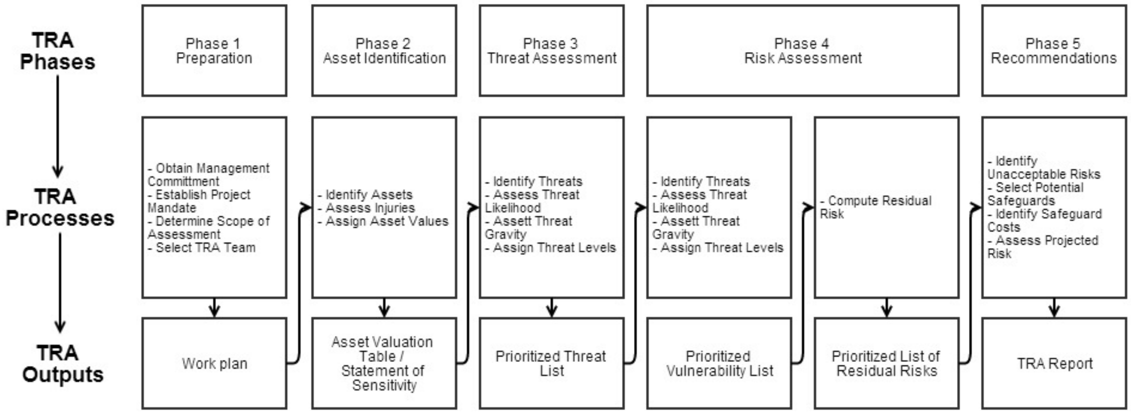

TRA Phases
TRA Processes
TRA Outputs
Phase 1 Preparation
Phase 2 Asset Identification
Phase 3 Threat Assessment
Phase 4 Risk Assessment
Phase 5 Recommendations
- Obtain Management Committment
- Establish Project Mandate
- Determine Scope of Assessment
- Select TRA Team
- Identify Assets
- Assess Injuries
- Assign Asset Values
- Identify Threats
- Assess Threat Likelihood
- Assett Threat Gravity
- Assign Threat Levels
- Identify Threats
- Assess Threat Likelihood
- Assett Threat Gravity
- Assign Threat Levels
- Compute Residual Risk
- Identify Unacceptable Risks
- Select Potential Safeguards
- Identify Safeguard Costs
- Assess Projected Risk
Work plan
Asset Valuation Table / Statement of Sensitivity
Prioritized Threat List
Prioritized Vulnerability List
Prioritized List of Residual Risks
TRA Report

Figure 9: *Harmonized Threat and Risk Assessment (TRA-1) methodology.*

TRA-1 methodology might inspire PRAP on two aspects. First, TRA-1 does not only focus on protecting information. Physical security takes a part of the assessment methodology. External environment should be considered to develop a wide situational awareness capability.

Second, TRA-1 methodology ends with a report formulating recommendations to reduce measured risks. PRAP intents are similar. After conducting an objective assessment, PRAP should be limited to recommend treatment options that reduce risks. Any decision regarding the implementation of control measures for instance should be relied to an external committee driven by the stakeholders' group.

Process 9: Information Operations Vulnerability / Survivability Assessment (IOVSA)

In 2003, the *Army Research Laboratory* (ARL) published the last version of *Information Operations Vulnerability / Survivability Assessment (*IOVSA) (Revilla et al. 2003). IOVSA is a structured assessment method for risks that may affect computer systems used by the DoD. The IOVSA methodology can be applied to both individual systems or to systems-of-systems. IOVSA has had five (5) phases, and each one of them can be divided into what the authors have called *sub-blocks* (Figure 10) Phase 2, called *System Design / Functionality Analysis*, is concerned with determining the functions or aspects of the system that enable it to complete its mission, and describing the information (or data) flow within the system and with external interfaces. This approach may support scoping phase of a RA by focusing on most critical functions of a platform.

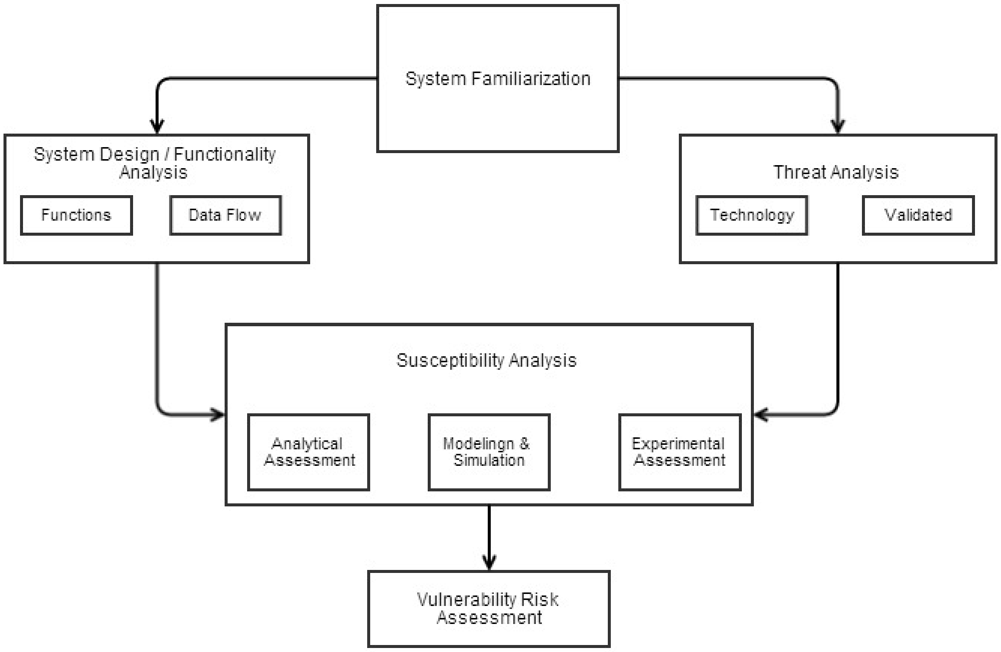


Figure 10: *Information Operations Vulnerability / Survivability Assessment (IOVSA) methodology.*

The IOVSA process is a living process in which the output of one phase may influence the amount of coverage and depth of another. The process allows this interaction to occur, and enables the RA team to customize the IOVSA as necessary (Revilla et al. 2003, p. 5). At a platform level, flexibility is essential to conduct RA. PRAP should include this capability in order to support tailored RA for various military platforms.

Process 10: Program Protection Planning (PPP) process

In 2011, the *Assistant Secretary of Defense for Research and Engineering* (ASD(R&E)) of the *United States (US)* DoD published the *Program Protection Planning* (PPP) process (Baldwin, 2011). The PPP process focusses on vulnerabilities associated to supply chain security. For instance, PPP wants to understand:

1. Where and under what conditions the platform was designed;

2. Where and under what conditions critical components were developed;

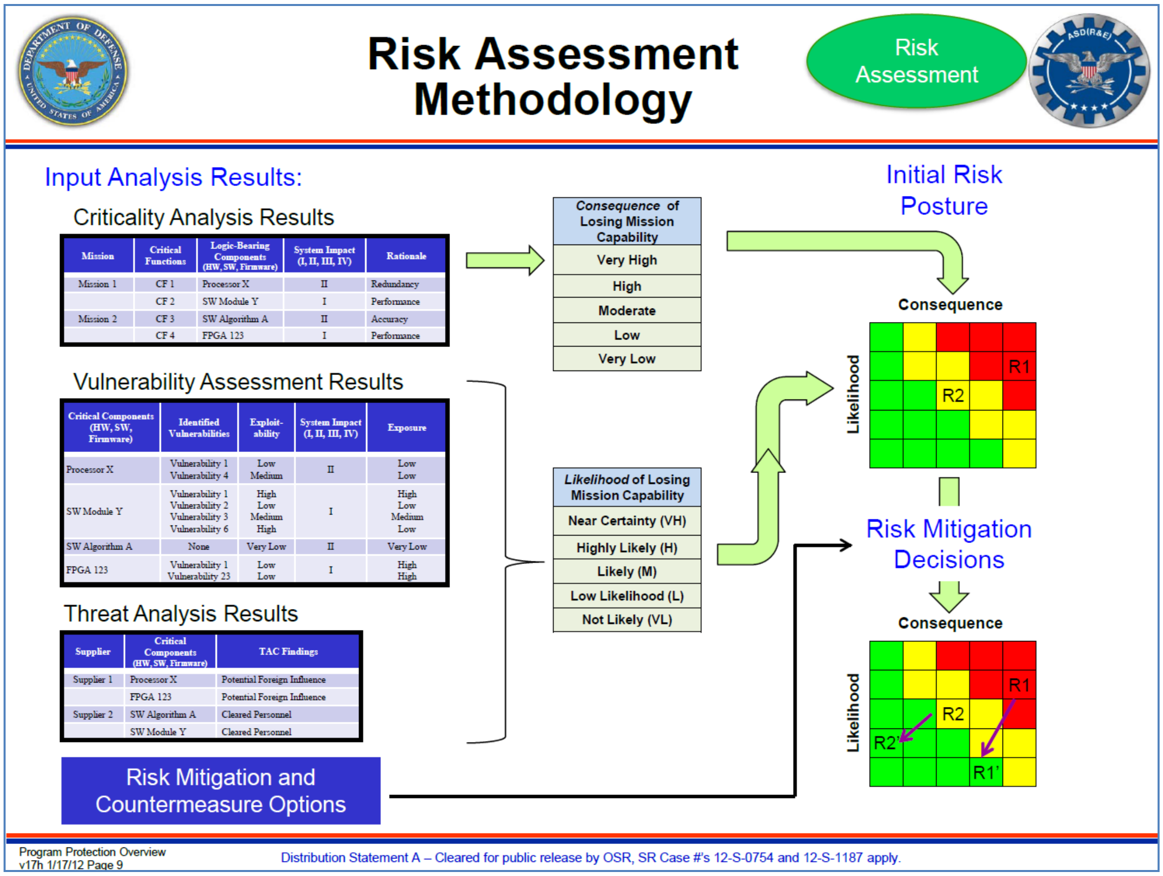
3. How and where components are assembled and integrated into completed systems;

4. Where and under what conditions critical software or firmware was developed;

5. How software updates are distributed and loaded; and

6. How other system maintenance operations are conducted.

Figure 11 shows PPP process steps.



Risk Assessment Methodology

Input Analysis Results:

Criticality Analysis Results

Mission	Critical Functions	Logic-Bearing Components (HW, SW, Firmware)	System Impact (I, II, III, IV)	Rationale
Mission 1	CF 1	Processor X	II	Redundancy
	CF 2	SW Module Y	I	Performance
Mission 2	CF 3	SW Algorithm A	II	Accuracy
	CF 4	FPGA 123	I	Performance

Vulnerability Assessment Results

Critical Components (HW, SW, Firmware)	Identified Vulnerabilities	Exploit-ability	System Impact (I, II, III, IV)	Exposure
Processor X	Vulnerability 1 Vulnerability 4	Low Medium	II	Low Low
SW Module Y	Vulnerability 1 Vulnerability 2 Vulnerability 3 Vulnerability 6	High Low Medium High	I	High Low Medium Low
SW Algorithm A	None	Very Low	II	Very Low
FPGA 123	Vulnerability 1 Vulnerability 23	Low Low	I	High High

Threat Analysis Results

Supplier	Critical Components (HW, SW, Firmware)	TAC Findings
Supplier 1	Processor X	Potential Foreign Influence
	FPGA 123	Potential Foreign Influence
Supplier 2	SW Algorithm A	Cleared Personnel
	SW Module Y	Cleared Personnel

Risk Mitigation and Countermeasure Options

Consequence of Losing Mission Capability
Very High
High
Moderate
Low
Very Low

Likelihood of Losing Mission Capability
Near Certainty (VH)
Highly Likely (H)
Likely (M)
Low Likelihood (L)
Not Likely (VL)

Initial Risk Posture

Risk Mitigation Decisions

Program Protection Overview
v17h 1/17/12 Page 9

Distribution Statement A – Cleared for public release by OSR, SR Case #'s 12-S-0754 and 12-S-1187 apply.

Figure 11: *Program Protection Planning (PPP) process.*

The supplier chain RA is a raising concern inside the US DoD. It is important to note that conducting a rigorous supply chain RA requires a significant amount of resources. Depending on available resources and timeframe, supply chain analysis still an option but should be conducted with precaution.

Summary

Table 1 summarizes retained characteristics to consider for designing PRAP. Each characteristic has been linked with design requirements presented in Chapter 2.

Table 1: *Retained RA processes.*

Processes / Methodologies	Retained characteristics for PRAP	RA requirements
Process 1 *Risk Assessment Methodology* Ref.: NIST SP 800-30, 2002	• Include a cybersecurity risk model; • Could focus on an impact analysis first.	**Requirement 2:** Adopt a risk model; **Requirement 5:** Initiate RA with an adverse impact analysis.

Processes / Methodologies	Retained characteristics for PRAP	RA requirements
Process 2 *Risk Assessment Process* Ref.: NIST SP 800-30 r1, 2012	• Include a cybersecurity risk model; • Dedicate a step to characterisation; • Dedicate a step to continuous communication.	**Requirement 2:** Adopt a risk model; **Requirement 4:** Develop a comprehensive understanding; **Requirement 7:** Keep stakeholder informed.
Process 3 *Risk Management Process* Ref.: NIST SP 800-39, 2011	• Consider various organizational context factors within the RA.	**Requirement 4:** Develop a comprehensive understanding.
Process 4 *Cybersecurity Risk Management* (CSRM) Ref.: Peter Katsumata et al., 2010	• Combine project management concepts to its RA for mastering complexity.	**Requirement 1:** Apply project management concepts.
Process 5 *Space Systems Risk Management Process* Ref.: ISO 17666, 2003	• Foster iterations for refining RA.	**Requirement 3:** Embrace an iterative and flexible approach to conduct RA.
Process 6 *Project Management Body of Knowledge* (PMBoK) Ref.: PMI Standard, 2013	• Provide technics and processes to manage complex projects (such as RA).	**Requirement 1:** Apply project management concepts.
Process 7 *Information Security Risk Management Process* Ref.: ISO/IEC 27005, 2011	• Suggest risk treatment options and residual risk estimation guidance.	**Requirement 6:** Provide comprehensive results.
Process 8 Treat and Risk Assessment (TRA-1) methodology Ref.: CSE & RCMP, 2007	• Consider both information and physical context factors within the RA; • Include a deliverable strategy.	**Requirement 4:** Develop a comprehensive understanding; **Requirement 7:** Keep stakeholder informed.

Processes / Methodologies	Retained characteristics for PRAP	RA requirements
Process 9 Information Operations Vulnerability / Survivability Assessment *(*IOVSA) methodology Ref.: Revilla et al. 2003	• Provide a customizable process. • Include a system familiarization step;	**Requirement 3:** Embrace an iterative and flexible approach to conduct RA. **Requirement 4:** Develop a comprehensive understanding;
Process 10 Program Protection Planning (PPP) process Ref.: (Baldwin, 2011)	• [Optional] Focus on Supplier chain security RA.	**Requirement 4:** Develop a comprehensive understanding.

Now, RA requirements (Chapter 2) and wished process characteristics (Chapter 3) have been identified. The following section presents foundations of PRAP which will be used for assessing cyber risks of three (3) CAF military platforms selected by the PASS project.

4 Platform Risk Analysis Process (PRAP)

PRAP stands for *Platform Risk Analysis Process*. It was designed by DRDC in order to support cybersecurity RA on military platforms. PRAP includes five (5) steps: *Plan*, *Characterize*, *Assess*, *Mitigate* and *Monitor* (Figure 12).

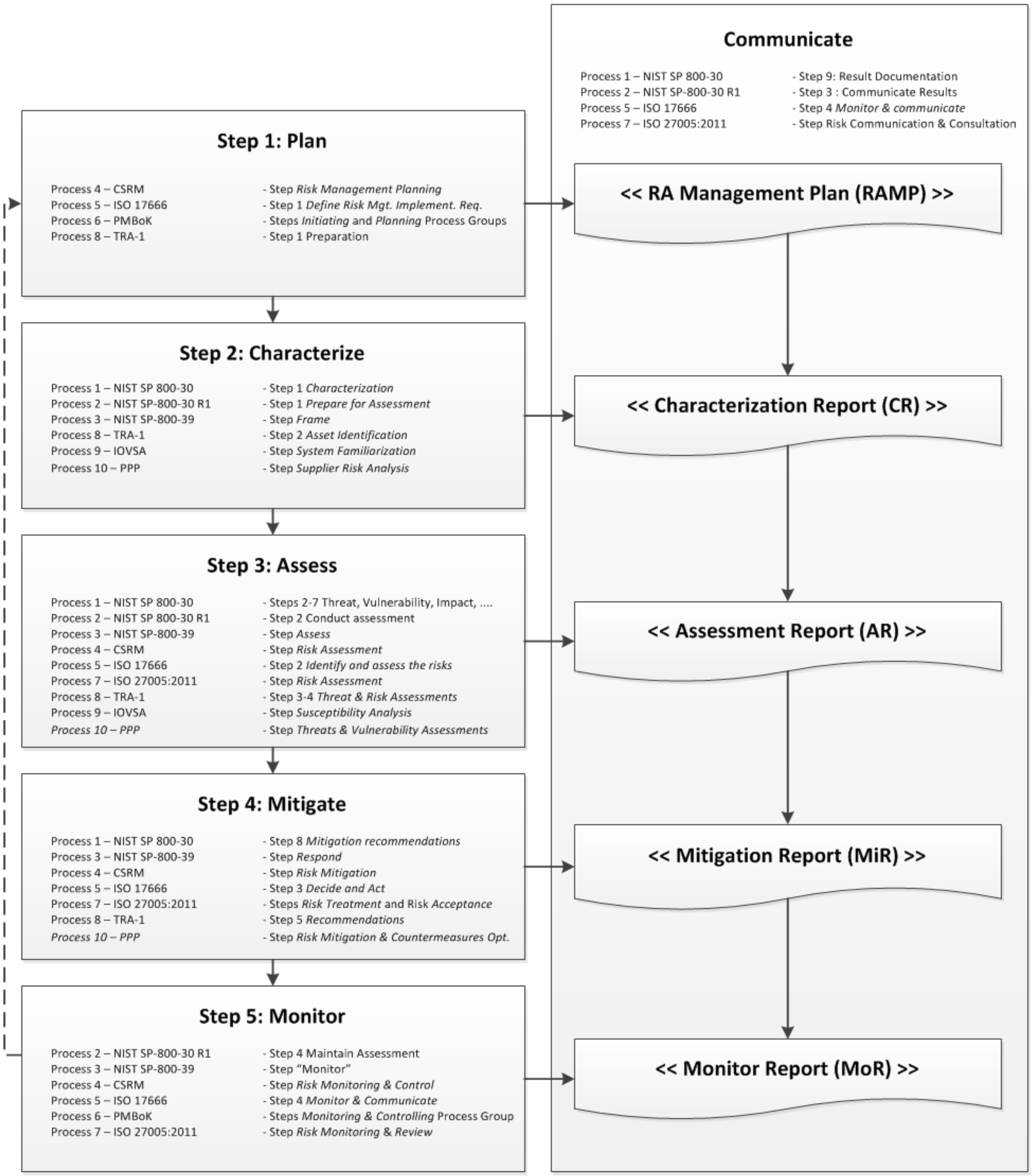

Communicate
Process 1 – NIST SP 800-30 - Step 9: Result Documentation
Process 2 – NIST SP-800-30 R1 - Step 3 : Communicate Results
Process 5 – ISO 17666 - Step 4 Monitor & communicate
Process 7 – ISO 27005:2011 - Step Risk Communication & Consultation
Step 1: Plan
Process 4 – CSRM - Step Risk Management Planning
Process 5 – ISO 17666 - Step 1 Define Risk Mgt. Implement. Req.
Process 6 – PMBoK - Steps Initiating and Planning Process Groups
Process 8 – TRA-1 - Step 1 Preparation
<< RA Management Plan (RAMP) >>
Step 2: Characterize
Process 1 – NIST SP 800-30 - Step 1 Characterization
Process 2 – NIST SP-800-30 R1 - Step 1 Prepare for Assessment
Process 3 – NIST SP-800-39 - Step Frame
Process 8 – TRA-1 - Step 2 Asset Identification
Process 9 – IOVSA - Step System Familiarization
Process 10 – PPP - Step Supplier Risk Analysis
<< Characterization Report (CR) >>
Step 3: Assess
Process 1 – NIST SP 800-30 - Steps 2-7 Threat, Vulnerability, Impact, ...
Process 2 – NIST SP 800-30 R1 - Step 2 Conduct assessment
Process 3 – NIST SP-800-39 - Step Assess
Process 4 – CSRM - Step Risk Assessment
Process 5 – ISO 17666 - Step 2 Identify and assess the risks
Process 7 – ISO 27005:2011 - Step Risk Assessment
Process 8 – TRA-1 - Step 3-4 Threat & Risk Assessments
Process 9 – IOVSA - Step Susceptibility Analysis
Process 10 – PPP - Step Threats & Vulnerability Assessments
<< Assessment Report (AR) >>
Step 4: Mitigate
Process 1 – NIST SP 800-30 - Step 8 Mitigation recommendations
Process 3 – NIST SP-800-39 - Step Respond
Process 4 – CSRM - Step Risk Mitigation
Process 5 – ISO 17666 - Step 3 Decide and Act
Process 7 – ISO 27005:2011 - Steps Risk Treatment and Risk Acceptance
Process 8 – TRA-1 - Step 5 Recommendations
Process 10 – PPP - Step Risk Mitigation & Countermeasures Opt.
<< Mitigation Report (MiR) >>
Step 5: Monitor
Process 2 – NIST SP-800-30 R1 - Step 4 Maintain Assessment
Process 3 – NIST SP-800-39 - Step "Monitor"
Process 4 – CSRM - Step Risk Monitoring & Control
Process 5 – ISO 17666 - Step 4 Monitor & Communicate
Process 6 – PMBoK - Steps Monitoring & Controlling Process Group
Process 7 – ISO 27005:2011 - Step Risk Monitoring & Review
<< Monitor Report (MoR) >>

Figure 12: *Platform Risk Analysis Process (PRAP).*

Steps of PRAP are self-descriptive and should be conducted successively. They are composed of a mix of steps and sub-steps of various RA processes presented in Chapter 3. Steps that inspired PRAP were regrouped and added to Figure 12 to express similarities.

PRAP embraces requirements stated in Chapter 2. A special emphasis was paid on the communication aspect with stakeholders. A continuous deliverable strategy was integrated to the process, illustrated by *Communicate* in Figure 12, in order to keep stakeholders informed along the RA.

PRAP adopts an iterative and flexible approach for each of its steps. When required, parts could be added or adapted, and content of deliverables could be updated to reflect latest stakeholders' concerns. Following sections describe briefly PRAP steps.

Step 1: Plan

The main objective of ***Step 1: Plan*** is the establishment of the scope and boundaries of the RA. The deliverable of this step is the *Risk Analysis Management Plan* (RAMP) which should include, but not limited to, three (3) parts: ***Context***, ***Mandate*** and ***Work plan*** (Figure 13).

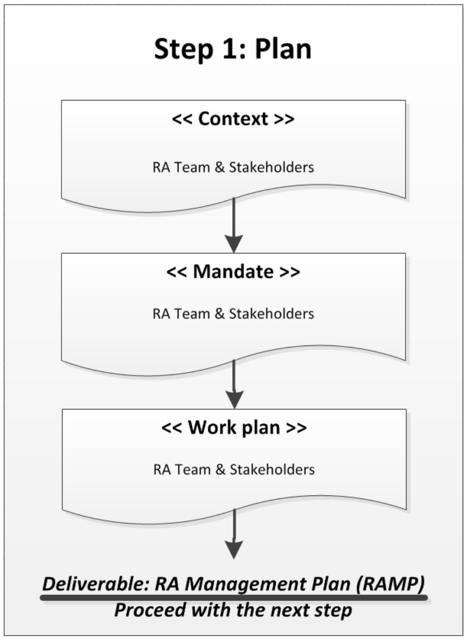


Figure 13: *Platform Risk Analysis Process – Step 1: Plan.*

The involvement of stakeholders is crucial for each part. The *Context* part identifies the platform to assess and stakeholders. The *Mandate* part establishes the scope and boundaries of the RA based on various factors, such as the principal platform asset to protect, the operational context, and cyber security domains to address. If required, this part could also include lists of constraints, limitations, assumptions, risk factors and criteria of success which frame the execution of the RA. Finally, the *Work plan* part provides an estimate on how and how much resource is required to achieve the RA. According to the communication plan presented in Figure 18, Step 1 will be described in depth in an upcoming publication.

Step 1 is strongly inspired by the *Initiating* and *Planning* phases of the PMBoK (PMI Standard, 2013) theory. At last, additional PMBoK processes are likely to be integrated to others steps of PRAP in order to support the RA team to master the complexity of the RA.

Step 2: Characterize

The main objective of ***Step 2: Characterize*** is to understand how the platform works regarding the principal platform asset identified in Step 1. During this step, no opinion is formulated about the security of the platform, and no change is applied to the platform. This step just wants to understand the platform has is. The deliverable of this step is the *Characterization Report* (CR) which should include, but not limited to, three (3) parts: ***Platform familiarisation***, ***Asset inventory*** and ***Assessment preparation*** (Figure 14).

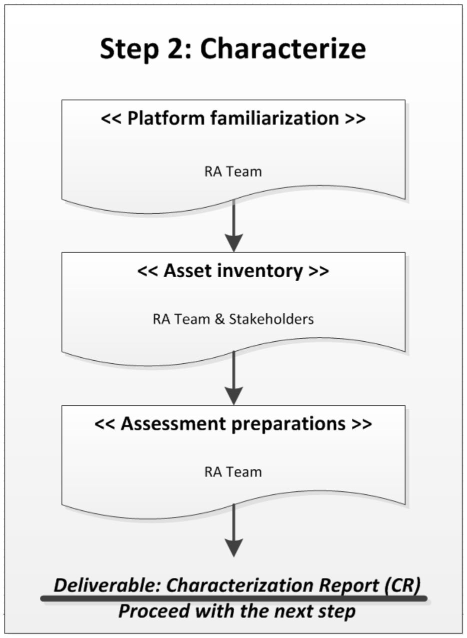

Step 2: Characterize
<< Platform familiarization >>
RA Team
<< Asset inventory >>
RA Team & Stakeholders
<< Assessment preparations >>
RA Team
Deliverable: Characterization Report (CR)
Proceed with the next step

Figure 14: *Platform Risk Analysis Process – Step 2: Characterize.*

The *Platform familiarization* part describes, but not limited to, the architecture, behaviors and interactions of the platform according with the *Mandate part* included in Step 1. This part could require access to various information sources, such as guidelines, operators, subject matter experts and/or platform systems (i.e., real or virtual). A lack of information may extend the time allocated to this part and constrain the scope of the RA. The *Asset inventory* part lists critical systems and/or components of the platform that should be considered in the RA. Finally, the *Assessment preparation* part prepares the field for the assessment step. Depending on which assessment technics are privileged (i.e., *Historical review, Policy analysis, Theoretical analysis, Quantitative analysis, Operational analysis, Log based analysis, Best practices analysis, Red teaming analysis)* information, people, resources should be mobilized. According to the communication plan presented in Figure 18, Step 2 will be described in depth in an upcoming publication.

Step 2 is strongly inspired by the IOVSA process for its *System familiarization* part. The step has also been inspired by process 8 (ref. TRA-1) for its *Asset identification* and Process 2 (Ref. NIST SP 800-30 r1) for its *Preparation for assessment*.

Step 3: Assess

The main objective of ***Step 3: Assess*** is to determine what risks threat the integrity of identified assets of the military platform. The deliverable of this step is the *Assessment Report* (AR) which should include, but not limited to, three (3) parts: ***Threats-Vulnerabilities (T-V) determination***, ***Risk identification*** and ***Risk prioritization*** (Figure 15).

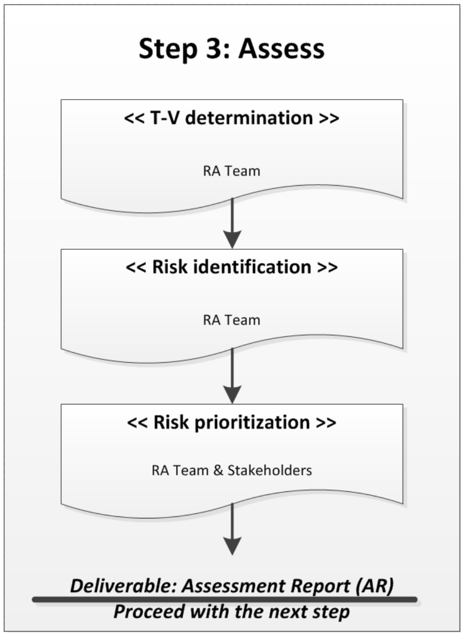

Step 3: Assess
<< T-V determination >>
RA Team
<< Risk identification >>
RA Team
<< Risk prioritization >>
RA Team & Stakeholders
Deliverable: Assessment Report (AR)
Proceed with the next step

Figure 15: *Platform Risk Analysis Process – Step 3: Assess.*

The *T-V determination* part identifies threats and vulnerabilities regarding the platform. Depending on which assessment technics are privileged, required time to perform this part could vary. During the *Risk identification* part, risks are identified, qualified and quantified when possible. The objective of this part is to provide to the stakeholder a clear understanding of what is at risk. Finally, the *Risk prioritization* part points risks out which should be addressed in priority. The involvement of the stakeholders at this last part is essential. Sometimes, external factors could influence which risks should be tackling first. According to the communication plan presented in Figure 18, Step 3 will be described in depth in an upcoming publication.

Step 3 is strongly inspired by the *Risk Assessment Process* described by NIST SP 800-30 standard.

Step 4: Mitigate

The main objective of the ***Step 4: Mitigation*** is to suggest mitigation actions for reducing measured risks in Step 3. The deliverable of this step is the *Mitigation Report* (MiR) which should include, but not limited to, three (3) parts: ***Treatment options***, ***Performance impacts*** and ***Residual risks*** (Figure 16).

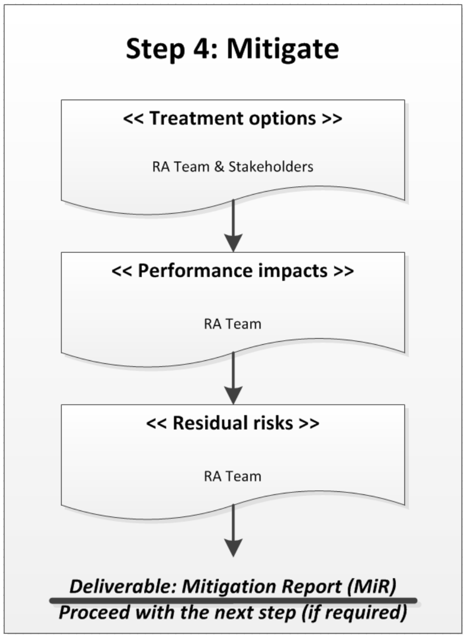

Step 4: Mitigate
<< Treatment options >>
RA Team & Stakeholders
<< Performance impacts >>
RA Team
<< Residual risks >>
RA Team
Deliverable: Mitigation Report (MiR)
Proceed with the next step (if required)

Figure 16: *Platform Risk Analysis Process – Step 4: Mitigate.*

The *Treatment options* part lists mitigation actions to perform to lower risk levels of prioritized risks. A cost/benefit analysis may be required if a mitigation action implies a significant change on the platform. The next part, *Performance impacts*, identifies any potential side effects to consider that may impact platform performances. Sometimes, mitigation actions may result in a lost a performance for a critical aspect of the platform. At last, the *Residual risks* part informs stakeholders of remaining risks (if it is the case). According to the communication plan presented in Figure 18, Step 4 will be described in depth in an upcoming publication.

Often, the MiR deliverable concludes the RA when *Monitor* step is not planned. Therefore, the RA team should pay a special attention to provide a comprehensive mitigation plan to stakeholders.

Step 4 is strongly inspired by the *Risk Management Process* described by the ISO 27005:2011 standard.

Step 5: Monitor

The ***Step 5: Monitor*** is optional. The main objective is to implement a long term analysis strategy. The deliverable of this step is the *Monitoring Report* (MoR) which should include, but not limited to, three (3) parts: ***Context changes***, ***Performance changes*** and ***Compliance*** (Figure 17).

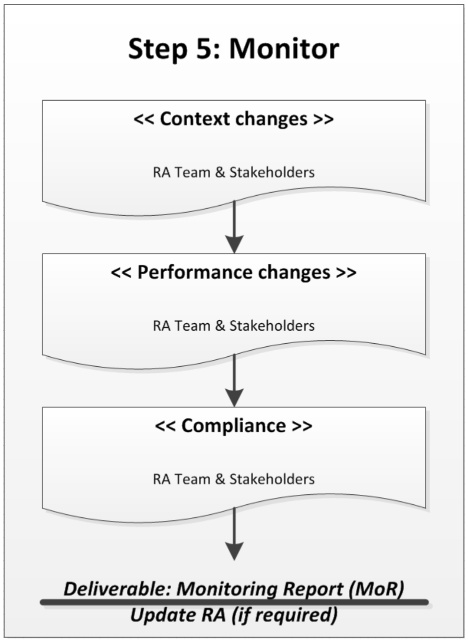


Figure 17: *Platform Risk Analysis Process – Step 5: Monitor.*

The *Context changes* part lists environmental changes affecting the platform. New threats and new mission-context are examples. The *Performance changes* part tries to determine if platform responses still adequate against evolving threats. Technological improvements or control enhancements may be suggested to meet stakeholders' performance baseline. The last part, *Compliance*, ensures that applied regulations, standards and/or standards operating procedures remains in force and up-to-date. According to the communication plan presented in Figure 18, Step 5 will be described in depth in an upcoming publication.

The MoR deliverable concludes the cycle of the RA. Once again, RA team should pay special attention to provide comprehensive recommendations to stakeholders.

Step 5 is strongly inspired by the Risk Management Methodology described by the NIST SP 800-30 r1 standard.

Communicate

The main objective of ***Communicate*** is to foster a continuous information exchange by imposing to the RA team a deliverable strategy (Figure 18). PRAP suggests providing a least, but not limited to, a deliverable for each step of the RA process (see Platform RA Deliverable side in Figure 18). The content of each deliverables are detailed into corresponding reports (See Platform RA Process side in Figure 18).

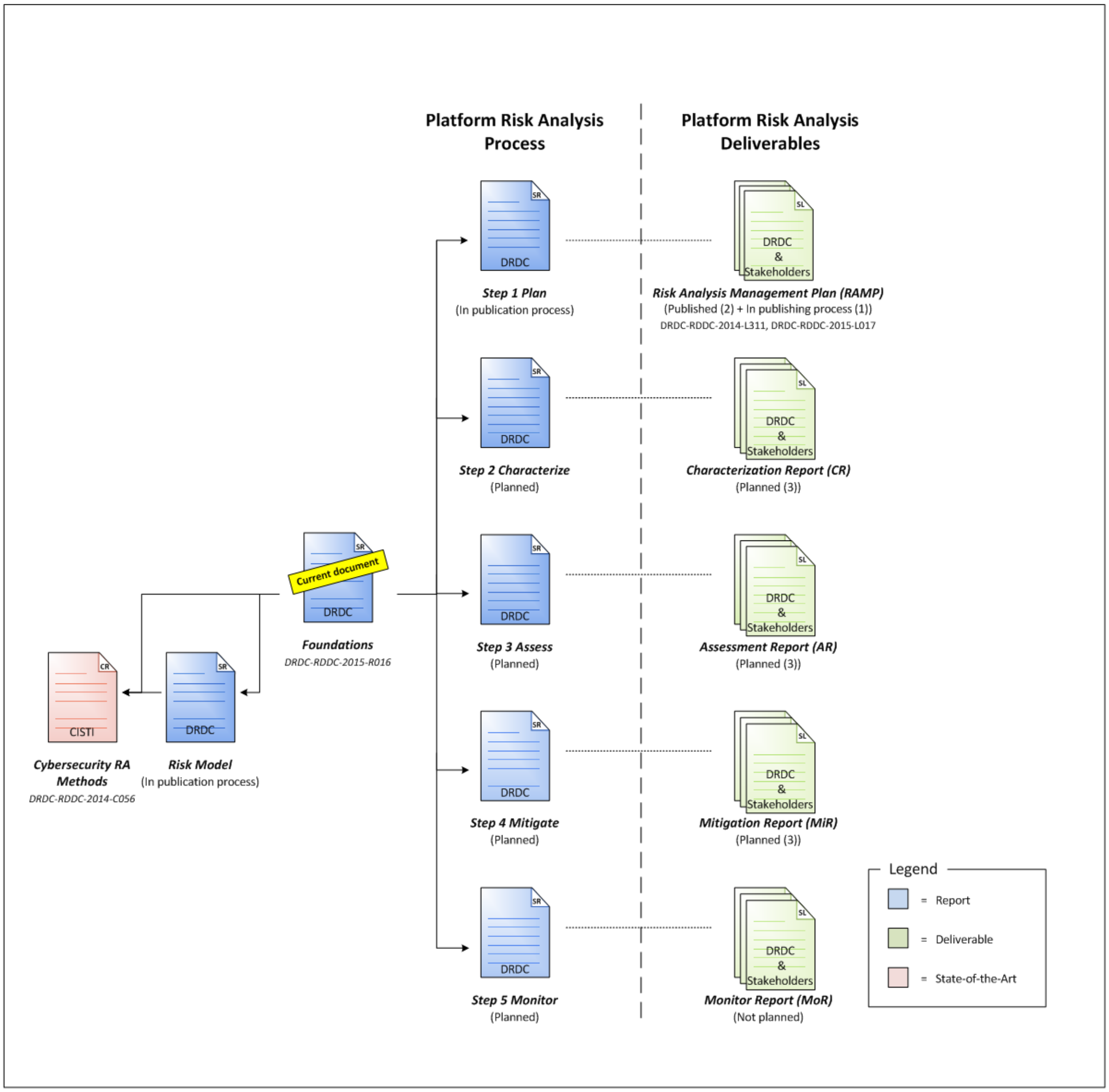


Figure 18: *Platform Risk Analysis Process – Communication plan.*

Summary

Table 2 summarizes how PRAP steps response to cited RA requirements in Chapter 2.

Table 2: *PRAP steps vs RA requirements.*

PRAP steps	RA Requirements
All steps	
• Various management processes of PMBoK have been integrate to PRAP for mastering RA complexity.	**Requirement 1:** Apply project management concepts.
• When required, any steps of PRAP could be adapted and content of deliverables could be updated to reflect latest stakeholders' concerns;	**Requirement 3:** Embrace an iterative approach to conduct RA.
• A special attention is given to provide a comprehensive follow-up plan for stakeholders.	**Requirement 6:** Provide comprehensive results.
Step 1: Plan	
• See ***All steps***;	
•	N / A
Step 2: Characterize	
• See ***All steps***;	**Requirement 2:** Adopt a risk model;
• A cybersecurity *Risk model* has been included in the *Mandate* to develop a mutual understanding;	**Requirement 4:** Develop a comprehensive understanding;
• PRAP dedicates Step 2 to understanding how works the platform and how it is designed;	
Step 3: Assess	
• See ***All steps***;	
• PRAP favors an adverse impact analysis first to limit boundaries of the RA;	**Requirement 5:** Initiate RA with an adverse impact analysis.
Step 4: Mitigate	
• See ***All steps***;	N / A
Step 5: Monitor	
• See ***All steps***;	N / A
Communicate	
• See ***All steps***;	
• PRAP puts forward a communication strategy based on a frequent delivery of reports.	**Requirement 7:** Keep stakeholder informed.

5 Conclusion

This report presents the foundations of the *Platform Risk Analysis Process* (PRAP) developed by *DRDC – Valcartier Research Centre*. PRAP integrates seven (7) RA requirements fostering structured and standardized communication exchanges between stakeholders and the RA team. PRA is inspired from ten (10) RA process / methodologies / standards. It integrates project management processes and best cyber risk management practices. Each step of PRAP has been described summarily. According to the communication plan, a detailed description of each step will be published in subsequent reports to it.

Steps of PRAP have the advantage of relying on well-known and recognized standards. However, efforts should be investing in order to adapt best practices of the cyber security industry to military platform context dealing with legacy, generic, and brand new IT hardware and software components.

At this stage, PRAP remains a theoretical process and it has not been validated yet. PASS project envisages applying PRAP on three (3) military platforms of CAF, such as the *Block IV systems* of the *Aurora CP-140* of *Royal Canadian Air Force* (RCAF), the *Combat Management System* (CMS-330) of the *Post-Frigate Life Extension* (FELEX) *of Halifax-class Frigate* of the *Royal Canadian Navy* (RCN), and the *Land Combat and Support System* (LCSS) of the *Light Amour Vehicle Upgrade* (LAV UP) of the *Canadian Army* (CA). A detailed description and the result of the application of PRAP to selected platforms will be published in subsequent reports to it.

This page intentionally left blank.

References

Baldwin, M. K. (2011). *Comprehensive Program Protection Planning*. Defense Acquisition University.

CSE & RCMP. (2007). *Harmonized Threat and Risk Assessment (TRA) Methodology* (No. TRA-1). Communications Security Establishment (CSE), Royal Canadian Mounted Police (RCMP). Retrieved from http://www.cse-cst.gc.ca/documents/publications/tra-emr/tra-emr-1-e.pdf.

DEA 4. (2013a). Department of National Defence and the Canadian Forces Architecture Framework (DNDAF) Volume 1: Overview and Definitions. DND/CF.

DEA 4. (2013b). Department of National Defence and the Canadian Forces Architecture Framework (DNDAF) Volume 2: DND/CF Views and Sub-views. DND/CF.

DEA 4. (2013c). Department of National Defence and the Canadian Forces Architecture Framework (DNDAF) Volume 3: DND/CF Architecture Data Model (DADM). DND/CF.

DoD. (2006). Risk management guide for DoD acquisition, 6th edition. Retrieved from https://acc.dau.mil/adl/en-US/108201/file/24105/2006%20RM%20Guide_%204%20Aug%2006%20version.doc.

ISO 17666. (2003). Space systems – Risk management.

ISO/IEC 27005. (2011). Information technology – Security techniques – Information security risk management.

Nécaille, C. (2014). *Cybersecurity Risk Models for Military Platform of Canadian Armed Forces (CAF)* (No. DRDC-RDDC Rxxxx). DRDC Valcartier (in process).

NIST SP 800-30. (2002). Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

NIST SP 800-30 r1. (2012). Guide for Conducting Risk Assessments. National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

NIST SP 800-39. (2011). Managing Information Security Risk – Organization, Mission, and Information System View. National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

Peter Katsumata, Judy Hemenway, & Wes Gavins. (2010). Cybersecurity Risk Management. Presented at the The 2010 Military Communications Conference. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5680181&tag=1.

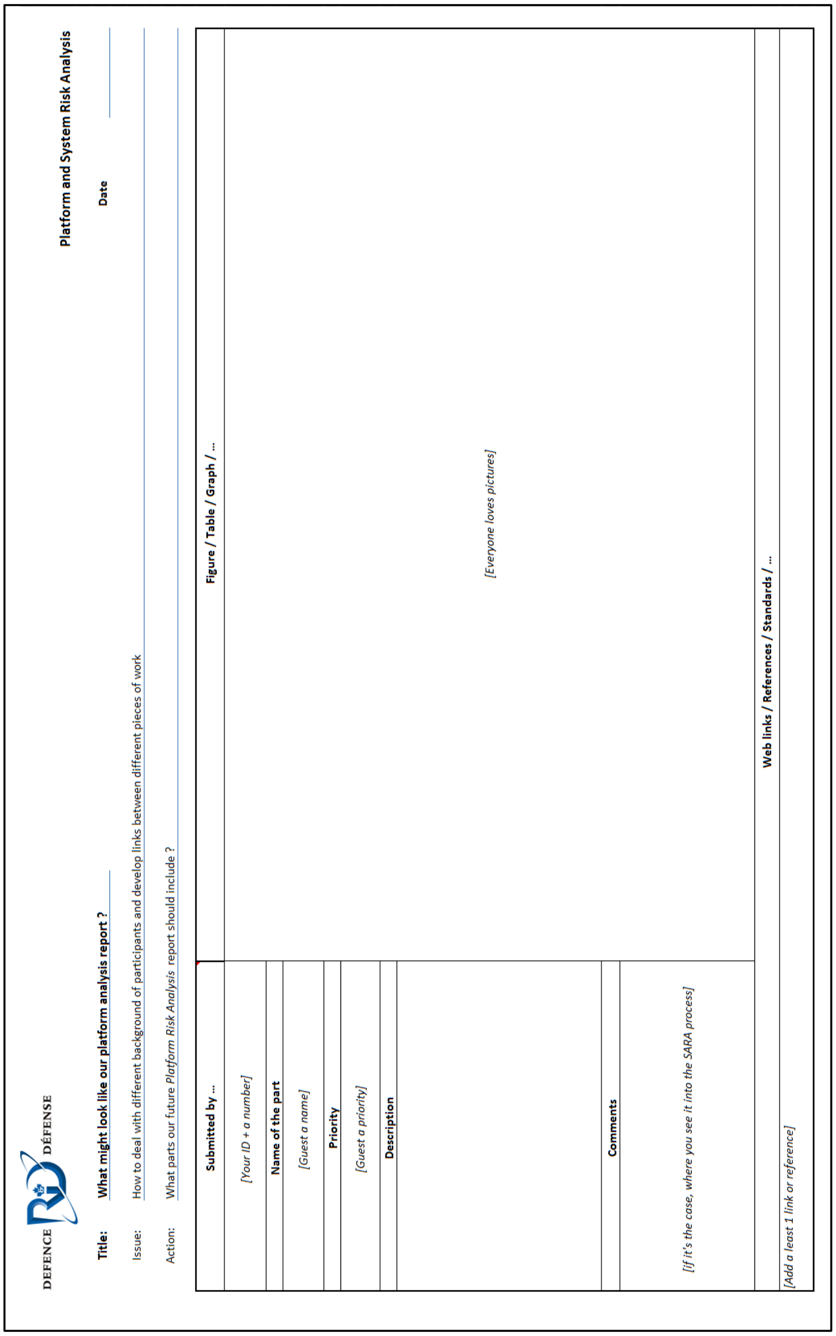
PMI Standard. (2013). *A Guide to the Project Management Body of Knowledge: PMBOK Guide* (5th ed.). Project Management Institute. Retrieved from http://books.google.ca/books/about/A_Guide_to_the_Project_Management_Body_o.html?id=FpatMQEACAAJ&redir_esc=y.

Revilla, A., Ochoa, C., Gunderson, E., Christianson, N., & Brunnen, R. zum. (2003). *Information Operations Vulnerability/Survivability Assessment (IOVSA): Process Structure (Revision A)*.

Senay, M. (2014). *Cybersecurity Risk Assessment Methods* (Contrat Report No. DRDC-RDDC 2014-C056) (p. 58). National Research Council Canada.

Annex A Questionnaire for identifying PRAP requirements

This form was used for gathering and identifying PRAP requirements. Results of the survey are presented in Chapter 2.



DEFENCE DÉFENSE

Platform and System Risk Analysis

Title: **What might look like our platform analysis report ?**

Date

Issue: How to deal with different background of participants and develop links between different pieces of work

Action: What parts our future *Platform Risk Analysis* report should include ?

Submitted by ...

[Your ID + a number]

Name of the part

[Guest a name]

Priority

[Guest a priority]

Description

Comments

[If it's the case, where you see it into the SARA process]

Figure / Table / Graph / ...

[Everyone loves pictures]

Web links / References / Standards / ...

[Add a least 1 link or reference]

Figure A.1: *Questionnaire used for identifying PRAP requirements.*

This page intentionally left blank.

Annex B Risk model adopted by PRAP

In order to develop a mutual understanding of the cybersecurity RA domain between stakeholders and the RA team, PRAP has adopted the following risk model (Figure B.1). Full description of the risk model could be retrieved under the reference. (Nécaille, 2014) [1].

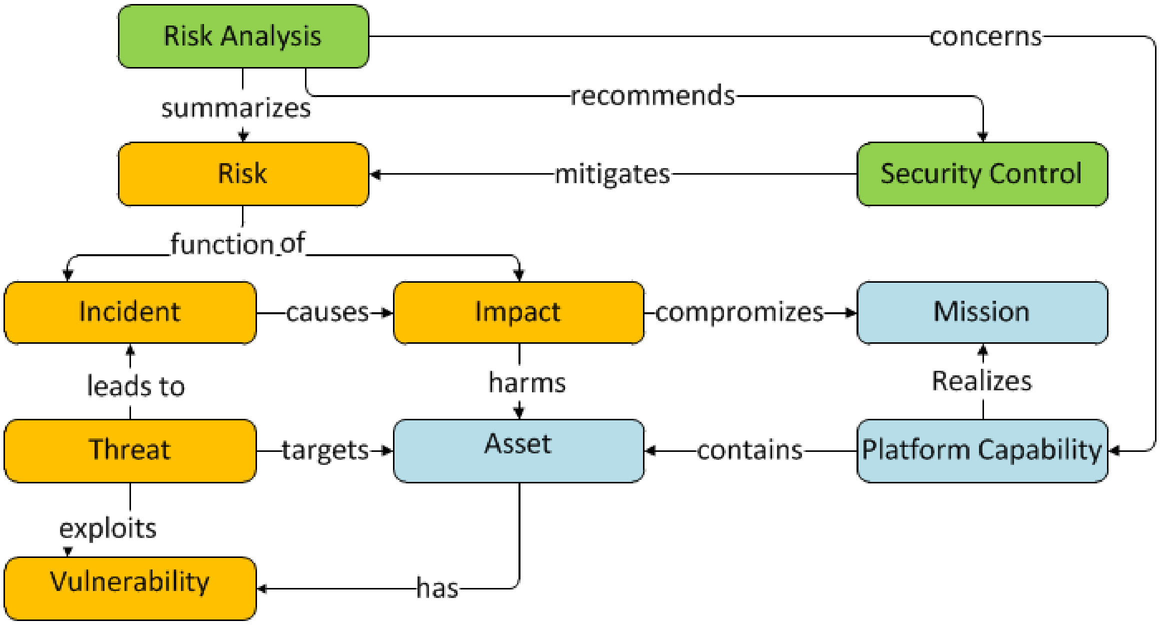


Figure B.1: *Cybersecurity risk model adopted by PRAP.*

This risk model defines keys terms, risk factors and relationships among factors that could support the RA for a military platform. Definitions of concepts used by the risk model are available in Table B.1.

Table B.1: *Concepts of the risk model used by PRAP.*

Concepts	Definitions
Asset	Anything that has value to the owner. Note: assets include platform, hardware, software, network, systems, crew, weapons, information…
Impact	The consequence (direct or indirect) of an incident on an asset.
Incident	The result of a security event.
Mission	An activity assigned to an individual, unit or force by an authority who has full command, operational command or operational control.
Platform	A coherent set of people, process and technology resources enabling a unit to carry out military

[6] This is an upcoming publication. Year of publication is given as an indication.

Concepts	Definitions
Capability	operations or mission activities based on a platform e.g., a Light Armoured Vehicle capability.
Risk	A measure of the extent to which an entity is threatened by an incident, and typically a function of: (1) the adverse impacts that would arise if the circumstance or event occurs; and (2) the likelihood of an incident.
Risk Analysis	Study of risks and their mitigations through security controls.
Security Control	Mechanism to prevent the occurrence of incidents or to reduce their impacts on assets.
Threat	A person, software or hardware that has the capability and/or intent to exploit a vulnerability in an asset.
Vulnerability	A weakness in an asset that might be subject to exploitation or misuse.

List of symbols/abbreviations/acronyms/initialisms

AC	*Armée canadienne*
AR	Assessment report
ARC	*Aviation royale canadienne*
ARL	Army Research Laboratory
ASD(R&E)	Assistant Secretary of Defense for Research and Engineering
CA	Canadian Army
CAF	Canadian Armed Forces
CISTI	Canada Institute for Scientific and Technical Information
CR	Characterization report
CSE	Communications Security Establishment
CSRM	Cybersecurity Risk Management
DoD	Department of Defence
DRDC	Defence Research and Development Canada
FAC	*Forces armées canadiennes*
FELEX	Frigate Life Extension
IEC	International Electrotechnical Commission
IOVSA	Information Operations Vulnerability / Survivability Assessment
ISO	International Organization for Standardization
IT	Information Technology
LAV	Light Amour Vehicle
LCSS	Land Combat and Support System
MiR	Mitigation report
MoR	Monitor report
MRC	*Marine royale canadienne*
NIST	National Institute of Standards and Technology
NRC	National Research Council Canada
PASS	Platform-to-Assembly Secured System
PMBoK	Project Management Body of Knowledge
PMI	Project Management Institute
PPP	Program Protection Planning

PRAP	Platform Risk Analysis Process
R&D	Research & Development
RA	Risk Analysis
RAMP	Risk Analysis Management Plan
RCAF	Royal Canadian Air Force
RCMP	Royal Canadian Mounted Police
RDDC	*Recherche et développement pour la défense Canada*
S&T	Science and Technology
SP	Special Publication
TRA-1	Treat and Risk Assessment methodology
T-V	Threats-Vulnerabilities
US	United States

DOCUMENT CONTROL DATA

(Security markings for the title, abstract and indexing annotation must be entered when the document is Classified or Designated)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g., Centre sponsoring a contractor's report, or tasking agency, are entered in Section 8.)

DRDC – Valcartier Research Centre
Defence Research and Development Canada
2459 route de la Bravoure
Québec (Québec) G3J 1X5
Canada

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

UNCLASSIFIED

2b. CONTROLLED GOODS

(NON-CONTROLLED GOODS)
DMC A
REVIEW: GCEC DECEMBER 2012

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Foundations of the Platform Risk Analysis Process (PRAP) : Cyber Security Risk Analysis Process for Military Platforms of Canadian Armed Forces (CAF)

4. AUTHORS (last name, followed by initials – ranks, titles, etc., not to be used)

Boivin E.

5. DATE OF PUBLICATION (Month and year of publication of document.)

February 2015

6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)

46

6b. NO. OF REFS (Total cited in document.)

17

7. DESCRIPTIVE NOTES (The category of the document, e.g., technical report, technical note or memorandum. If appropriate, enter the type of report, e.g., interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Scientific Report

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

DRDC – Valcartier Research Centre
Defence Research and Development Canada
2459 route de la Bravoure
Québec (Québec) G3J 1X5
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)

05aa

9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)

DRDC-RDDC-2015-R016

10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

The *Platform Risk Analysis Process* (PRAP) provides a generic methodology to conduct cybersecurity *risk analysis* (RA) for military platforms. This report describes foundations of PRAP designed by *Defence Research and Development Canada* (DRDC) – *Valcartier Research Centre* under the *Platform-to-Assembly Secured System* (PASS) project (2013-2018) (05aa). PASS project envisages to apply PRAP on three (3) military platforms of the *Canadian Armed Forces* (CAF), such as the *Aurora CP-140* of *Royal Canadian Air Force* (RCAF), the *Halifax-class Frigate* of the *Royal Canadian Navy* (RCN), and the *Land Combat Support System* (LCSS) of the *Light Amour Vehicle 6* (LAV) of the *Canadian Army* (CA). These platform assessments will contribute to validate concepts carried by PRAP.

Le *processus d'analyse des risques de plateformes* PRAP (en anglais, *Platform Risk Analysis Process*) présente une méthodologie générique pour mener l’évaluation des risques cybernétiques de plateformes militaires. Ce rapport décrit les fondements du processus PRAP conçu par *Recherche et développement pour la défense Canada* (RDDC) – Centre de recherche *Valcartier* dans le cadre du projet *Platform-to-Assembly Secured System* (PASS) (2013-2018) (de 05aa). Le projet PASS envisage d'appliquer PRAP à trois plateformes militaires des *Forces armées canadiennes* (FAC) dont, le *CP-140 Aurora* de l’*Aviation royale canadienne* (ARC), la *Frégate Halifax* de la *Marine royale canadienne* (MRC), ainsi que le système de soutien au combat terrestre LCSS (en anglais, *Land Combat Support System*) de la nouvelle version du véhicule blindé léger LAV 6 (en anglais *Light Amour Vehicle*) de l’*Armée canadienne* (AC). L’analyse de ces plateformes contribuera à valider les concepts véhiculés par PRAP.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g., Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Cybersecurity; Risk Analysis; Risk Assessment; Process; Military platform;