National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

THE RECORD OF AIRWORTHINESS RISK MANAGEMENT AND OPERATIONAL RISK ASSESSMENT TOOL FOR RCAF CYBER MISSION ASSURANCE

Major Robyn B. Scholes

JCSP 47

Service Paper

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 47

Étude militaire

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 47 - PCEMI 47
2020 - 2021

SERVICE PAPER – ÉTUDE MILITAIRE

THE RARM AND ORAT FOR RCAF CYBER MISSION ASSURANCE

By Major Robyn G. Scholes

Word Count: 2,356

Nombre de mots : 2.356

THE RARM AND ORAT FOR RCAF CYBER MISSION ASSURANCE

AIM

1. The aim of this service paper is to assess existing risk management framework suitability for Cyber Mission Assurance (CMA) of Royal Canadian Air Force (RCAF) weapons systems and Command, Control, Communication, Computer and Intelligence, Surveillance and Reconnaissance (C4ISR) systems. The paper will analyze the two risk management frameworks used at the operational level of the RCAF: the Record of Airworthiness Risk Management (RARM) and the Operational Risk Assessment Tool (ORAT).[1] The resulting recommendation identifies that both the ORAT and the RARM are necessary to cover the full scope of risk management, but that adjustments are required to effectively conduct CMA.

INTRODUCTION

2. The commander's intent of the draft Fragmentary Order for the RCAF Cyber Mission Assurance Program is "to keep cyber related risks to an acceptable level in the RCAF."[2] The constraints and restraints of this order identify a need to comply with existing Operational and Technical Airworthiness regulations and integrate with their existing processes. Further, the order identifies that risk management should be carried out in accordance with the DND/CAF CMA Risk Management Process pictured in Annex. This process is limited to generic tasks and Level 1 organizational responsibilities. As such, L1 users are required to develop sub-processes for in-service risk management.[3]

3. The paper will begin with a description of the problem space to describe why risk management is necessary to achieve resiliency of RCAF air and ground-based aviation systems in today's cyber-contested environment. It will then introduce and assess the RARM and ORAT risk management processes in order to identify the suitability of each for CMA. Advantages, disadvantages and gaps in each process will be described in order to provide recommendations for each risk management framework.

DISCUSSION

4. Information Technology (IT) is well understood to be susceptible to cyber threats, and deliberate processes and security measures have developed and internalized in this field. For DND/CAF, this is reflected in the numerous directives, policies and procedures that minimize threat vectors, conduct detection activities and provide a robust response and recovery framework for computers, networks and other traditional IT systems. However, while it is widely recognized that these same cyber threats apply to any device with a processor or circuit board, process maturity has not been achieved for non-traditional IT such as Platform Technology (PT).

---

[1] Mission Acceptance and Launch Authority (MA/LA) and Fatigue Risk Management System (FRMS) are risk management tools at the tactical level that serve to implement risk mitigation measures initiated at the operational level and approved by Comd 1 CAD. As such, these will not be assessed in this paper.

[2] Director of Air Domain Development, *DRAFT: Fragmentary Order (FragO) 2021-Xx to Campaign Plan 3.0 - RCAF Cyber Mission Assurance Program* (Ottawa: DND Canada,[2020])., 2.

[3] Canada. Department of National Defence., *Cyber Mission Assurance Program Charter* (Ottawa: Vice Chief of Defence Staff, 2020)., 7.

For the RCAF, this means that PT such as aircraft, radars, navigation aids, and C4ISR systems are susceptible to cyber threats. While cyber security has been incorporated as a mandatory requirement in new acquisitions, upgrades and design changes to RCAF PT,[4] incorporation of these same considerations for life-cycle management of legacy systems has yet to be accomplished.

5. Threats and hazards posed to PT that are not addressed by system design or standard operating procedures are handled on a case-by-case basis through risk management. The acceptance of a risk, or applied mitigation measures, ensure that an acceptable level of safety and effectiveness is maintained in operations. In this context, airworthiness risks such as an unforeseen degradation of a hydraulic component in an aircraft's flight control system, or an unexplained loss of precision in a ground-based navigational aid, are addressed in the same way as an operational risk such as the threat of surface-to-air-missiles in an operating environment. CMA is another variant to risk management; in lieu of physical threats and hazards, it addresses threats arising in cyberspace that manifest in the physical world.

6. While risk management is philosophically the same, the RCAF differentiates between airworthiness and operational risks. Airworthiness risk are described as a "danger or threat to safety of flight caused by a failure related to operational or technical standards related to the design, manufacture, operation or maintenance of an aeronautical product."[5] In contrast, operational risks relate to threats "due to the specific conditions that exist that may impact the successful conduct of any operation, mission or task."[6] Each program possesses its own risk management process, the RARM and ORAT respectively. Both processes are fundamentally the same: identify the threat, assess its probability and severity, assign a risk index, identify possible mitigation measures, and command acceptance of the risk and/or mitigation plan. Three core differences between the two programs can be used to describe their suitability for CMA risk management: scope, stakeholder involvement and oversight, and approval authorities.

Scope

7. Airworthiness Risk. The airworthiness program scope is limited to safety aspects of military aviation, and therefore clear bounds exist for what can be treated by a RARM. Cyber threats may pose a risk to safety, but this is not always the case. For example, if a cyber threat affects the hardware or software of a precision guided munition, or jammer, on an aircraft, it poses a risk to the ability to effectively conduct the mission, but safety of flight is not in question. In contrast, a cyber threat on a flight control computer could directly impact the ability of that same aircraft to fly. Further, while ground-based systems such as Aircraft Maintenance Support Equipment (AMSE) and air navigation/control are included in the scope of the airworthiness program, other RCAF ground-based PT such as NORAD's Battle Control System – Fixed (BCS-F), are excluded.

8. The existing scope of the RARM process covers cyber threats that have an impact on safety of flight. While the work instruction on RARMs does not explicitly describe how to treat

[4] DTAES Canada, *Technical Airworthiness Authority Advisory 2019-03* (Ottawa: DND Canada, [2019]).

[5] Canada. Department of National Defence, *Operational Airworthiness Manual (OAM). B-GA-104-000/FP-001* (Winnipeg: DND Canada, [2017])., 5-1.

[6] Ibid.

cyber threats, the process is generic enough to be suitable for this purpose.[7] However, if the RARM were to be used for the full scope of CMA, the inclusion of mission systems and all forms of ground systems needs to be addressed. This could be accomplished as either a new category of RARM, or as additional scope to the airworthiness program. The option for a variation of the RARM previously existed, a Record of Operational Risk Management (RORM), but was rescinded in 2014 because it was determined that mission equipment and operational risks should not be incorporated into the airworthiness program.[8] Therefore, both proposals which effectively expand the airworthiness program's scope to include non-safety related risks are expected to be highly opposed and are not a feasible option.

9. Operational Risk. The operational risk program covers anything outside the domain of the airworthiness program. Therefore a wide variety of threats, including cyber, may be treated by the ORAT. Like the RARM, the order covering the implementation of the ORAT does not specifically address cyber threats, but is sufficiently generic to be suited to their assessment.[9] Of note, given that there is potential for overlap with airworthiness risks, the ORAT requires review by the Operational Airworthiness staff (SSO OA) at 1 Canadian Air Division (1 CAD).[10] In the event that an airworthiness risk is inadvertently identified as an ORAT, it is immediately referred to the appropriate Technical and Operational Airworthiness authorities to initiate a RARM. This demonstrates a hierarchy between the two risk management processes, and a clear delineation between the programs.

10. Assessment. From the perspective of scope, it is necessary to include the ORAT and the RARM as risk management tools for CMA given the exclusive nature of the RARM for safety of flight risks. No changes are required to the scope of threats treated by each risk management tool, as each are sufficiently broadly defined to include cyber threats.

Stakeholder Involvement & Oversight

11. Airworthiness Risk. While a RARM can be initiated by either technical or operational staff, typically an Aerospace Engineering Officer (AERE), or civilian equivalent, working for the Director General of Aerospace Equipment Program Management (DGAEPM) is responsible for the development of the contents of the RARM. Given this role and associated airworthiness responsibilities of the AERE occupation, professional expertise, through formal training and authorization processes, is very high. Further, an entire sub-section of DGAEPM, residing in the Directorate of Technical Airworthiness and Engineering Support (DTAES), has delegated responsibility from the Technical Airworthiness Authority (TAA) to oversee that the RARM is rigorously applied, risk levels are correctly identified, and regulatory timelines are met. While training and familiarity for fleet readiness staff at 1 CAD involved in the RARM process is lower, the process is sufficiently well understood, and training is in development to further

[7] Directorate of Technical Airworthiness and Engineering Support, *EMT 01.003: Airworthiness Risk Management Process* (Gatineau: DND Canada, [2020]).

[8] Michael Krak (1 CAD Operational Airworthiness cell), telephone and email with author, 27 Jan 2021

[9] Canada. 1 Canadian Air Division, *1 CAD Orders, Volume 3, 3-310. Operational Risk Management for Air Operations* (Winnipeg: DND Canada, [2014]).

[10] Ibid, 3.

improve this pan-RCAF.[11] Further, a center of excellence exists in the 1 CAD SSO OA section to provide oversight, support and expertise.

12. The RARM describes the Risk Management Team (RMT) as those stakeholders involved in identifying, assessing and determining possible mitigation measures. There is a clear understanding, and documented requirement, for collaboration between technical and operational staff as part of the RMT. Further it clearly specifies that DTAES and SSO OA are mandatory stakeholders, with both sections playing a key role in monitoring the RARM process.[12] In addition to the aforementioned deadlines in the RARM Process, there is an annual audit cycle that occurs as part of the Airworthiness Review Boards which validates that overall fleet operations remain within accepted risk levels by the operational commander.[13]

13. Operational Risk. Like the RARM, the ORAT incorporates the use of a RMT. However, there is no requirement for technical/operational staff collaboration or obligatory stakeholders.[14] There is also no training established, no timelines for ORAT completion, no direction regarding compounded risks, and no responsibilities for oversight beyond the commander accepting the risk. The SSO OA cell provides assistance with ORATs, but this is because no other section is formally assigned this role or responsibility.[15]

14. Assessment. Overall, the RARM is a far more formalized, understood and managed process than the ORAT as a result of the airworthiness regulatory environment. However, there is presently no link to cyber subject matter experts. Given the nascence of the CMA Program, it could be valuable to incorporate a note in the RARM work instruction for cyber support in the RMT. Further, if it is determined valuable and within the capacity of the cyber experts residing in DTAES, they could be incorporated as a mandatory stakeholder in the RARM RMT.

15. The ORAT could benefit from incorporating detailed instructions from the RARM in the 1 CAD Order on ORAT development. In particular, formalized timelines for completion and discrete direction on who should be included in the RMT should be described. As recommended for the RARM, this should mention cyber expertise in 1 CAD and/or DTAES. Recent inclusion of ORATs in the Airworthiness Review Board is assessed as a very positive step to increasing oversight of the ORATs.

Approval Authority

16. Airworthiness Risk. The RARM provides strict parameters for recommending and approval authorities. Recommending authorities are required to be authorized by the TAA[16] with

[11] Michael Krak (1 CAD Operational Airworthiness cell), telephone and email with author, 27 Jan 2021.

[12] Directorate of Technical Airworthiness and Engineering Support, *EMT 01.003: Airworthiness Risk Management Process*.

[13] The Airworthiness Review Board covers all aspects of safety of flight and is jointly presided by the Operational Airworthiness Authority, TAA and Airworthiness Investigative Authority (AIA). Recent additions by the SSO OA include a requirement to report on ORATs, coupled risks. In the near future it will be expanded to report on outstanding Flight Safety preventive measures that may increase overall risk to a fleet's operation.

[14] Review for airworthiness implications in an ORAT by SSO OA staff are unrelated to the RMT.

[15] Michael Krak (1 CAD Operational Airworthiness cell), telephone and email with author, 27 Jan 2021.

[16] Ibid.

corresponding recommending and approval authorities assigned by the OAA.[17] Alternatively, RARMs can arrive at an "acceptable level of risk" where no OAA approval is required. As Technical and Operational Airworthiness are residual authorities for Force Employment (FE), the RARM is used in Force Generation (FG) and FE.[18] Finally, the approval authority is directly tied to the risk acceptance level, and not the threat type.

17. Operational Risk. "Command Risk Acceptance of an ORAT shall be by the appropriate Commander responsible for implementing the operation at risk…. The onus will be on each Commander in the chain of command to determine if they have the authority to proceed."[19] Although the order specifies that risk acceptance levels may be designated on a theatre-by-theatre basis, there is no established standard. To further compound this ambiguity, the ORAT is governed by a 1 CAD order which means that it is only applicable for operations under the authority of Comd 1 CAD, or via residual authorities. Therefore, the ORAT applies for FG activities, and could be considered applicable for NORAD as 1 CAD Comd is designated NORAD FE Comd. However, as operational risk is not a residual authority, when assets are assigned Operational Command (OPCOM) to a FE Comd the operational risk authority also transfers. As the lowest level of risk possible in an ORAT is low, there is always a requirement for operational command acceptance.

18. While the ORAT generally follows the joint doctrine for operational risk management, it provides a more tailored process for RCAF assets and leverages air force subject matter expertise for completion. It is feasible that a large Air Task Force (ATF) could provide a similar capability on behalf of a FE Comd, but this is dependent on the scale of the ATF and is not consistent in all deployments.

19. Assessment. In respect to approval authorities, the RARM is suitable for cyber related risks. While not specific only to CMA, improvements are noted for the ORAT. First, it should have the command risk acceptance authority delineated by position and/or minimum rank. Secondly, while suitable for FG purposes, the ORAT needs to be adjusted to reflect that it is a risk management tool used by the Joint Forces Air Component Commander (JFACC) on behalf of a FE. This could be achieved by retaining the ORAT under a 1 CAD order, but expanding residual authorities for operational risk management of air assets. Alternatively, it could be transferred to the joint doctrine as a specialized annex which identifies obligatory RCAF development. Finally, it is recommended that the approval authority remains with the operational level FE commander, once assessed and co-signed by technical and operational staff.

CONCLUSION

20. To ensure mission success in today's cyber contested environment, the RCAF needs to leverage the existing operational risk management frameworks for CMA. The analysis provided of the RARM and ORAT indicate that these tools are already broadly suitable for assessing

[17] Canada. Department of National Defence, *Operational Airworthiness Manual (OAM). B-GA-104-000/FP-001*, 2-4 - 2-9.

[18] Canada. Department of National Defence, *RCAF Doctrine: Command and Control. B-GA-402-001/FP-001* (Trenton: Canadian Forces Aerospace Warfare Centre, 2018), 9.

[19] Canada. 1 Canadian Air Division, *1 CAD Orders, Volume 3, 3-310. Operational Risk Management for Air Operations*, 8.

cyber threats, although minor adjustments would better task tailor them for this purpose. It also underscores that professional risk management through operational and technical expert collaboration is key to describing, identifying, accepting and/or mitigating cyber, and other threats.

RECOMMENDATION

21. In summary, the ORAT and the RARM are both required to achieve the scope of the CMA program for RCAF assets. In order to accomplish this, the RARM and ORAT should incorporate cyber subject matter expertise in the RMT. More substantial changes are also proposed to improve formality and rigor of the ORAT, but these are not directly related to CMA.

Annex: A. DND/ CAF Cyber Mission Assurance Risk Management Process

ANNEX A: DND/ CAF Cyber Mission Assurance Risk Management Process

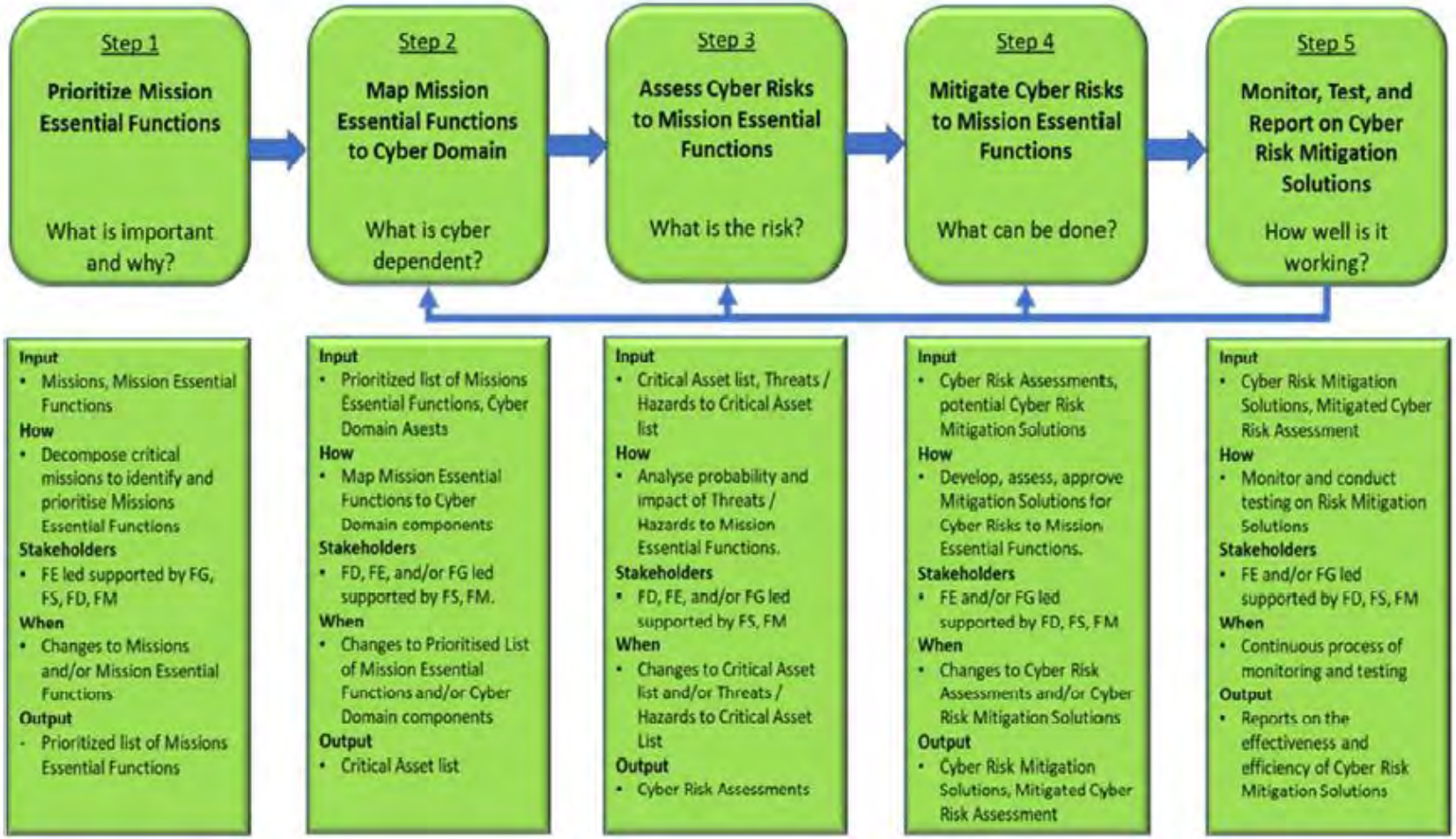

Figure A-1 - Cyber Mission Assurance Risk Management Process
Source: Canada, *Cyber Mission Assurance Program Charter*, 8.

BIBLIOGRAPHY

Canada. 1 Canadian Air Division. *1 CAD Orders, Volume 3, 3-310. Operational Risk Management for Air Operations*. Winnipeg: DND Canada, 2014.

Canada. Department of National Defence. *Operational Airworthiness Manual (OAM). B-GA-104-000/FP-001*. Winnipeg: DND Canada, 2017.

———. *RCAF Doctrine: Command and Control. B-GA-402-001/FP-001*. Trenton: Canadian Forces Aerospace Warfare Centre, 2018.

Canada. Department of National Defence. *Cyber Mission Assurance Program Charter*. Ottawa: Vice Chief of Defence Staff, 2020.

Canada., DTAES. *Technical Airworthiness Authority Advisory 2019-03*. Ottawa: DND Canada, 2019.

Director of Air Domain Development. *DRAFT: Fragmentary Order (FragO) 2021-xx to Campaign Plan 3.0 - RCAF Cyber Mission Assurance Program*. Ottawa: DND Canada, 2020.

Directorate of Technical Airworthiness and Engineering Support. *EMT 01.003: Airworthiness Risk Management Process*. Gatineau: DND Canada, 2020.