Risk Management

Software Procurement
Software Requirements Specifications

Revision 1

20 June 2022

RDIMS OTT_LSTL #6191956

NOTICE

This documentation has been reviewed by the technical authority and does not contain controlled goods. Disclosure notices and handling instructions originally received with the document shall continue to apply.

AVIS

Cette documentation a été révisée par l’autorité technique et ne contient pas de marchandises contrôlées. Les avis de divulgation et les instructions de manutention reçues originalement doivent continuer de s’appliquer.

TABLE OF CONTENTS

CHANGE RECORD

To note: the change record includes all major changes to the document but may omit minor changes such as formatting and grammatical corrections.

Rev	Section	Change Summary
1	General	Initial Revision

Note: this Software Requirements Specifications (SRS) has been developed based on the guidance from ISO/IEC/IEEE 29148-2018 International Standard - Systems and software engineering - Life cycle processes - Requirements engineering

1 INTRODUCTION

1.1 Purpose

1.1.1 The purpose of this Software Requirements Specifications (SRS) is to describe the technical requirements for a risk management software to support the Department of National Defense (DND).

1.2 Scope

1.2.1 The purpose of the risk management software is to enable DND to raise, assess, prioritize, and track risks and opportunities related to materiel acquisition & support.

1.2.2 The risk management software is meant to be a centralized collaboration tool allowing DND and its partners to manage various types of risk and opportunity items such as Project and Program risks and opportunities, Security risks, Cyber Security risks, Ammunition & Explosives risks, In-Service Naval Materiel risks, and Airworthiness risks.

1.3 Acronyms and Definitions

1.3.1 Acronyms used in this Software Requirements Specifications are contained in Appendix 1.

1.3.2 Definitions are as follow:

1.3.2.1 Cloud Hub: a virtual network that acts as a central location for managing external connectivity and hosting services used by multiple workloads[1] or spokes. Within DND, and for the context of this task, the cloud hub (also referred as “tenant”) is centrally managed by the Joint Defence Cloud Program (JDCP) team.

1.3.2.2 Cloud Spoke: a virtual network that host workloads and connect to the central hub through virtual network peering. Within DND, the cloud spoke is managed by the client organization. For the context of this task, the cloud spoke is what the Contractor will be expected to manage and where the Contractor will be responsible to select, deploy and configure cloud resources.

1.3.2.3 Descriptive Statements: any line that is not a Desirable Requirement or Mandatory Requirement, is a descriptive statement or a header and must only be used for context.

1.3.2.4 Desirable Requirement: requirement statement that contains the word “should”.

1.3.2.5 Mandatory Requirement: requirement statement that contains the word “must”.

1.3.2.6 Open Standard: They are standards made available to the general public and are developed (or approved) and maintained via a collaborative and consensus driven process. Open Standards facilitate interoperability and data exchange among different products or services and are intended for widespread adoption.

1.4 References

1.4.1 Government of Canada Specifications, Standards, and Publications:

[1] Software Defined Networking: Hub and spoke, Microsoft Docs (2021-07-09)

	Reference	Promulgation	Accessibility of the Specification, Standard, or Publication
[A]	Standard on Web Accessibility	1 Aug 2011	Internet Link
[B]	Standard on Web Usability	27 Nov 2013	Internet Link
[C]	Defence Enterprise Risk Management Guideline	26 Jun 2018	Link (intranet)
[D]	National Defense Security Orders and Directives – Chapter 3 Security Risk Management	Version 1.2	Link (intranet)
[E]	Information Technology Security Guide 33 (ITSG-33) – IT Security Risk Management: A Lifecycle Approach	1 Nov 2012	Internet Link
[F]	C-09-005-001/TS-000 Ammunition and Explosive Safety Manual – Volume 1 Program Management and Life Cycle Safety	1 Aug 2013	(CFTO)
[G]	C-23-005-000/AG-002 Naval Materiel Risk Management	1 Aug 2013	(CFTO)
[H]	NAVORD 3001-0 In-Service Naval Materiel Risk Management - Policy	13 May 2021	Link (intranet)
[J]	NAVORD 3001-1 In-Service Naval Materiel Risk Management - Process	24 Apr 2014	Link (intranet)
[K]	C-03-005-012/AM-001 Naval Materiel Management System Manual	11 Nov 2013	(CFTO)
[L]	C-05-005-001/AG-001 Technical Airworthiness Manual	1 Apr 2019	(CFTO)
[M]	EMT01.003 Airworthiness Risk Management Process	Version D 14 Aug 2020	(Procedure Document)
[N]	AEPM-009 Risk Alert Notification Email Template	14 Apr 2016	(Template Document)
[O]	AEPM-213 Airworthiness Risk Alert Template	11 July 2017	(Template Document)
[P]	AEPM-215 Record of Airworthiness Risk Management Template	29 May 2017	(Template Document)
[Q]	ITSP.40.111 Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information	1 Aug 2016	Internet Link
[R]	ITSP.40.062 Guidance on Securely Configuring Network Protocols	1 Oct 2020	Internet Link
[S]	Information Technology Security Guide 22 (ITSG-22) - Baseline Security Requirements for Network Security Zones in the Government of Canada	1 Jun 2007	Internet Link
[T]	Information Technology Security Guide 38 (ITSG-38) - Network Security Zoning - Design Considerations for Placement of Services within Zones	1 May 2009	Internet Link

1.4.2 Other Specifications, Standards, and Publications:

	Reference	Promulgation	Accessibility of the Specification, Standard, or Publication
[U]	Open Web Application Security Project (OWASP) Top 10 Web Application Security Risks	2021	https://owasp.org/Top10/

1.4.3 In the event of a conflict between the content of this document and the referenced documents, the content of this document must take precedence.

2 PRODUCT OVERVIEW

2.1 Product Perspective

2.1.1 User Interfaces

2.1.1.1 The risk management software must be accessible by the end-users via a web browser, as further described in section 3.3.

2.1.2 Communications Interfaces

2.1.2.1 The risk management software must provide communication interfaces via an Application Programming Interface (API), as further described in section 3.4.2.

2.1.3 Interfaces with Services

2.1.3.1 The risk management software must be entirely hosted on a Cloud Spoke within the Joint Defence Cloud Program (JDCP) environment, as further described in section 3.4.1.

2.2 Product Functions

2.2.1 The key functions of the risk management software are as follow:

2.2.1.1 Allow users to input, track, and assess aggregate risks and opportunities to projects and programs, including but not limited to:

2.2.1.1.1 Project risk and opportunity items (Ref [C]);

2.2.1.1.2 Security risk items (Ref [D]);

2.2.1.1.3 Cyber security risk items (Ref [E]); and

2.2.1.1.4 Ammunition & Explosive safety risk items (Ref [F]).

2.2.1.2 Allow users to input, track, and assess aggregate risks and opportunities to classes/fleets and specific platforms (ships, submarines, aircrafts, and vehicles), including:

2.2.1.2.1 All of the items listed under 2.2.2.1;

2.2.1.2.2 In-service naval materiel risk items for Navy ships and submarines (Refs [H] and [J]); and

2.2.1.2.3 Technical and Operational Airworthiness risk items for Air Force aeronautical products (Ref [L] and [M]).

2.3 User Characteristics

2.3.1 The following are examples of end-users that will be interacting with the risk management software:

2.3.1.1 First Line Engineering Managers: They manage the first line maintenance for platforms (ships, submarines, aircrafts, and vehicles) and are responsible to communicate risks and opportunities related to systems and equipment to operational authorities (including commanding officers) in order to inform operational decisions. They usually raise risk items in accordance with Ref [F] (for everyone), Refs [H] and [J] (for Navy), and Ref [L] (for Air Force). They are usually involved in the technical endorsement of risks items.

2.3.1.2 Operational Authority and Commanding Officers: They manage the operational usage of platforms (ships, submarines, aircrafts, and vehicles) to achieve a mission. They are involved in the operational acceptance of risk items.

2.3.1.3 Second Line Engineering Managers: They are responsible to communicate risks and opportunities to Fleet Commanders. They are usually involved in reviewing the technical aspect of risk items raised by First Line Engineering Managers and are involved in the technical endorsement of risk items. They usually raise risk items in accordance with Ref [F] (for everyone), Refs [H] and [J] (for Navy), and Ref [L] (for Air Force).

2.3.1.4 Lifecycle Materiel Managers: They are responsible to identify and communicate risks and opportunities related to systems and equipment under their scope of responsibility. They can take the role of Technical Authority and System Authority. They usually raise risk items in accordance with Ref [C] (for everyone), Refs [H] and [J] (for Navy), and Ref [L] and [M] (for Air Force). Lifecycle Materiel Managers are involved in the technical endorsement of risk items.

2.3.1.5 Class Program Managers (Navy): They manage risks and opportunities for a class of ship or submarine. They typically have at least 10 years of experience within the naval technical community and have at a minimum a university degree in science or engineering. They usually raise risk items in accordance with Ref [C], [H], and [J]. Class Program Managers are involved in the technical and operational acceptance of risk items.

2.3.1.6 Weapon System Managers (Air Force): They are the Air Force equivalent to Class Program Managers, managing a fleet of aircraft. They usually raise risk items in accordance with Ref [C], [L] and [M].

2.3.1.7 Technical/Operational Authorities and the Operational Command Risk Acceptance Authority (Air Force): They are the individuals who make up the regulatory bodies of the Technical Airworthiness Authority, Operational Airworthiness Authority, as well as the Operational Command Risk Acceptance Authority. They are usually involved in the technical and operational acceptance of risk items.

2.3.1.8 Project Managers: They are responsible to manage risks and opportunities for programs and projects (such as engineering changes). They usually raise risk and opportunity items in accordance with Ref [C].

2.3.1.9 Information Systems Security Officer: They are responsible to manage risks and opportunities related to security and information systems. They usually raise risk items in accordance with Ref [D] and [E].

2.3.1.10 In-Service Support Contractor: They are contracted by DND to provide services in support of materiel acquisition and support activities. They can be asked to perform any of the roles described above except for Information Systems Security Officer. For security reason, it is important that contractors be restricted to access and edit risk and opportunity items only as they are relevant to the scope of their contract.

2.4 Limitations

2.4.1 (Intentionally left blank)

2.5 Assumptions and dependencies

2.5.1 This Software Requirements Specifications assumes the risk management software (application and associated database) will be deployed in a DND managed cloud environment.

2.5.2 This Software Requirements Specifications will be dependent on DND cloud services, notably:

2.5.2.1 SMTP services;

2.5.2.2 Cryptographic services;

2.5.2.3 User identity and access authorization (through active directory).

2.6 Apportioning of requirements

2.6.1 (Intentionally left blank)

3 REQUIREMENTS

3.1 Functions

3.1.1 Access the risk management software

3.1.1.1 The risk management software must have a home landing page providing users with:

3.1.1.1.1 A description of the web application;

3.1.1.1.2 Information on the steps to gain access;

3.1.1.1.3 Access to support documentation; and

3.1.1.1.4 Access to points of contact to seek additional information or report a problem.

3.1.2 Access and Search the risk and opportunity register

3.1.2.1 The risk management software must only display risk and opportunity items a user is authorized to view and access based on their user role.

3.1.2.2 The risk management software must allow users to search and filter the risk and opportunity register, at a minimum, based on the following:

3.1.2.2.1 Unique Identification number;

3.1.2.2.2 Element;

3.1.2.2.3 Type;

3.1.2.2.4 Project or Program;

3.1.2.2.5 Class/Fleet;

3.1.2.2.6 Platforms;

3.1.2.2.7 System or Equipment;

3.1.2.2.8 Person responsible (owner);

3.1.2.2.9 Overall risk level; and

3.1.2.2.10 Item status.

3.1.2.3 The risk management software must allow users to search and filter the risk and opportunity register based on additional key data fields described in section 3.6.

3.1.2.4 The risk management software should allow users to search the risk and opportunity register based on key words to be crossed referenced with data fields described in section 3.6.

3.1.2.5 The risk management software must allow users to personalize the information presented by the risk and opportunity register (columns).

3.1.2.6 The risk management software should allow users to easily access a consolidated list of risk and opportunity items for which they are identified as a key stakeholder (such as the owner, technical authority, operational authority).

3.1.2.7 The risk management software must allow users to save specific search criteria or filters to easily access specific portions of the risk and opportunity register.

3.1.2.8 The risk management software must allow users to download the active view of the risk and opportunity register (based on their search criteria), at a minimum in the following format:

3.1.2.8.1 Portable Document Format (PDF); and

3.1.2.8.2 Spreadsheet document compatible with Microsoft Excel.

3.1.3 Reports

3.1.3.1 The risk management software should allow users to extract reports based on pre-determined search criteria and parameters.

3.1.3.2 A generated report should contain, at a minimum, the following information:

3.1.3.2.1 The data and time it was generated;

3.1.3.2.2 The user who generated the report;

3.1.3.2.3 The search criteria used to generate the report; and

3.1.3.2.4 Page numbers.

3.1.3.3 The risk management software must allow users to download reports at a minimum in the following format:

3.1.3.3.1 Portable Document Format (PDF).

3.1.3.4 The risk management software should allow users to personalize the look and feel of a report including the following elements:

3.1.3.4.1 Report title;

3.1.3.4.2 Security designation and classification;

3.1.3.4.3 Disclaimer;

3.1.3.4.4 Logo for the front page;

3.1.3.4.5 The ability display risks and opportunities in a heat map grid, with numbers indicating how many risks or opportunities have their overall risk assessment in each box of the heat map; and

3.1.3.4.6 The columns and fields to be displayed for risks and opportunities included on the report.

3.1.3.5 The risk management software should allow users to generate a bow-tie style report for a selected risk item.

3.1.4 Projects and Programs

3.1.4.1 The risk management software must only allow authorized users to create a new project or program.

3.1.4.2 The risk management software must allow users to easily access a consolidated list of risk and opportunity items associated with a given project or program.

3.1.4.3 The risk management software should allow users to easily access a consolidated list of projects and programs under which the user is a named stakeholder (for example: manager, coordinator, administrator, and collaborator).

3.1.5 Risk and opportunity items

3.1.5.1 The risk management software must allow users to access risk and opportunity items for which they are authorized based on their user role.

3.1.5.2 The risk management software should allow users to share and access risk and opportunity items based on a unique hyperlink address.

3.1.5.3 The risk management software must allow users to create risk and opportunity items if they are authorized based on their user roles.

3.1.5.4 The risk management software must allow for users to create and manage the following types of risk and opportunity items:

3.1.5.4.1 Default risk and opportunity items as described in section 3.6.3;

3.1.5.4.2 Project and program risk and opportunity items as described in section 3.6.4;

3.1.5.4.3 Security risk items as described in section 3.6.5;

3.1.5.4.4 Cyber security risk items as described in section 3.6.6;

3.1.5.4.5 Ammunition & Explosive risk items as described in section 3.6.7;

3.1.5.4.6 In-service naval materiel risk items as described in section 3.6.8; and

3.1.5.4.7 Airworthiness risk items as described in section 3.6.9.

3.1.5.5 The risk management software must allow for users to access a consolidated view for all components that pertain to an individual airworthiness risk assessment. This includes:

3.1.5.5.1 Airworthiness Impact Assessments (AWIA) as described in Section 3.6.10

3.1.5.5.2 Risk Alert Notifications (RAN) as described in Section 3.6.11.

3.1.5.5.3 Airworthiness Risk Alerts (ARA) as described in Section 3.6.12.

3.1.5.5.4 Records of Airworthiness Risk Management (RARM) as described in Section 3.6.13.

3.1.5.6 The risk management software should allow authorized users the ability to configure additional types of risk and opportunity items.

3.1.5.7 The risk management software must allow authorized users to edit risk and opportunity items, including changing their status.

3.1.5.8 The risk management software must allow authorized users to delete risk and opportunity items if they have never been endorsed.

3.1.5.9 The risk management software must allow authorized users to download a risk or opportunity item in the following format:

3.1.5.9.1 Portable Document Format (PDF); and

3.1.5.9.2 Word processing document compatible with Microsoft Word.

3.1.5.10 The risk management software should allow users to register to a risk or opportunity item in order to receive personalized automatic notifications including:

3.1.5.10.1 When the item’s status is changed;

3.1.5.10.2 When the item has been endorsed or approved;

3.1.5.10.3 When a new comment is added;

3.1.5.10.4 When there are any changes to the item.

3.1.5.11 The risk management software should allow users to add comments to risk and opportunity items.

3.1.6 Workflow

3.1.6.1 The risk management software must have the ability to execute workflows for the review and approval of risk and opportunity assessments whereas a pre-set sequence of events is performed that includes automatically notifying users to either perform an action, or to receive information.

3.1.6.2 The risk management software should allow authorized users to configure workflows for risk and opportunity items.

3.1.6.3 The risk management software must allow an authorized user to initiate the review and approval process as described in section 9 of Appendix 6 for an Airworthiness Risk Alert and for a Record of Airworthiness Risk Management.

3.1.7 Electronic Signatures

3.1.7.1 The risk management software must have the ability to capture electronic signatures at a minimum leveraging the user authentication to the software.

3.1.7.2 The risk management software must prompt the user to acknowledge the intent of applying their electronic signature.

3.1.7.3 The risk management software must indicate that a signatory has reviewed or approve the item via electronic signature when a risk or opportunity item is downloaded as a PDF;

3.1.8 Automatic notifications

3.1.8.1 The risk management software must have the ability to send automatic notifications, including via emails, to enable workflows, to notify a user that has registered for personalized notifications for a risk or opportunity item, and for the events listed in Appendix 4 and 5.

3.1.8.2 Email notifications initiated by the risk management software must have the ability to include both English and French text.

3.1.8.3 Email notifications must make use of the SMTP relay service to be provided by DND through the JDCP Hub.

3.1.9 Document Management

3.1.9.1 The risk management software must allow authorized users the ability to manage (upload, download, delete) attachment files to risk and opportunity items.

3.1.9.2 The risk management software must capture the following information, at a minimum, for each file uploaded to the risk management software:

3.1.9.2.1 Information Restriction, including the following choices (multiple choices, multiple selection):

3.1.9.2.1.1 Controlled Goods;

3.1.9.2.1.2 Intellectual Property;

3.1.9.2.1.3 Commercial in Confidence;

3.1.9.2.2 Information Sensitivity, including the following choices (multiple choices, one selection, mandatory field):

3.1.9.2.2.1 Not sensitive;

3.1.9.2.2.2 Protected A;

3.1.9.2.2.3 Protected B.

3.1.9.2.3 File title (default title taken from the file name before the extension);

3.1.9.2.4 File type (default taken from the extension);

3.1.9.2.5 File uploader (username, system generated, taken from the user performing the action);

3.1.9.2.6 Date uploaded (date and time, system generated).

3.1.9.3 The risk management software must strictly prevent any user from uploading, accessing, downloading, or deleting any attachment files that contain restrictions or sensitivity unless the user has been granted access to the level of restriction and sensitivity associated with the file.

3.1.10 Identity and Access

3.1.10.1 The risk management software must leverage the Defense 365 credentials from the JDCP Cloud Hub.

3.1.11 Role Based Access Control

3.1.11.1 The risk management software must have the ability to manage user roles as to restrict read and edit access (separately) to risk and opportunity items, as well as attachments, at a minimum based on the following:

3.1.11.1.1 Element, as described in section 1 of Appendix 4;

3.1.11.1.2 Type, as described in section 1 of Appendix 4;

3.1.11.1.3 Class/Fleet, as described in section 1 of Appendix 4 and as listed in Appendix 2;

3.1.11.1.4 Platform, as described in section 1 of Appendix 4 and as listed in Appendix 2;

3.1.11.1.5 Restriction and Sensitivity of information, as described in section 3.1.9, section 1 of Appendix 4, and section 1 of Appendix 6.

3.1.11.2 The risk management software must allow the ability to restrict read and edit access (separately) based on the roles described in Appendix 7.

3.1.11.3 The risk management software should allow authorized users the ability to assign pre-determined roles to users in order to control read and edit access to risk and opportunity items.

3.1.12 Security Monitoring

3.1.12.1 The risk management software must verify that interactions and events executed via an interface with an external application (including those described in section 3.4) are from pre-authorized applications.

3.1.12.2 The risk management software must capture and send application level log events

3.1.12.3 The risk management software should capture and send the application level log events listed in Appendix 8.

3.1.12.4 The risk management software must forward the application level log events to the Cloud Security Monitoring Team's application (currently Microsoft Azure Sentinel).

3.2 Performance Requirements

3.2.1 Load

3.2.1.1 The risk management software must accommodate a minimum of 500 simultaneous users.

3.2.1.2 The risk management software must accommodate a minimum of 2000 users with access to the application.

3.2.1.3 The risk management software should make use of cloud elasticity in order to maximize the performance while keeping the overall operating cost to a minimum.

3.2.2 Transaction Speed

3.2.2.1 The risk management software must be able to process 95% of the transactions in less than 1 second, with the exception of file uploads and downloads, for a user located in Gatineau QC and accessing the application via the Defence Wide Area Network (DWAN).

3.2.2.2 The risk management software must be able to process 99% of the transactions in less than 10 seconds, with the exception of file uploads and downloads, for a user located in Gatineau QC and accessing the application via the Defence Wide Area Network (DWAN).

3.3 Usability Requirements

3.3.1 Web-based user interface

3.3.1.1 The risk management software must be accessible via Google Chrome.

3.3.1.2 The risk management software must be accessible via Microsoft Edge.

3.3.1.3 The risk management software user interface must comply with the web accessibility standards at Ref [A].

3.3.1.4 The risk management software user interface must comply with the web usability standards at Ref [B].

3.3.2 Official Languages

3.3.2.1 The risk management software user interface must be available in both English and French.

3.4 Interface Requirements

3.4.1 Interface with the Cloud Hub and Spoke

3.4.1.1 The risk management software must interface with the Cloud Hub Microsoft Active Directory in order to manage identity and access.

3.4.2 Application Programming Interface (API)

3.4.2.1 The risk management software must provide an Application Programming Interface (API) in order to allow future applications to be integrated and perform, at a minimum, the following functions:

3.4.2.1.1 Create and edit projects and programs, including all data fields described in section 3.6.1;

3.4.2.1.2 Create and edit risk and opportunity items, including all data fields described for each type in sections 3.6.2 to 3.6.9;

3.4.2.1.3 Extract projects and programs data, including all data fields described in section 3.6.1;

3.4.2.1.4 Extract risk and opportunity items data, including all data fields described for each type in sections 3.6.2 to 3.6.9;

3.4.2.1.5 Extract data from the risk and opportunity register, as described in sections 3.1.1.2 to 3.1.1.5;

3.4.2.1.6 Extract system generated PDF for risk and opportunity items; and

3.4.2.1.7 Extract attachment files to risk and opportunity items.

3.4.2.2 The risk management software should use an Open Standard for the execution of API functions described in section 3.4.3.1.

3.5 Logical Database Requirements

3.5.1 All data at rest generated by the risk management software must remain under complete, and unique, control of Canada.

3.5.2 Pursuant to the above requirement, all data at rest must be stored in a Canada-approved computing facility located within the geographic boundaries of Canada.[2]

3.5.3 Data transiting networks must be adequately protected through the use of appropriate encryption and network safeguards.

3.5.4 Data encryption must be achieved through the use of approved cryptographic mechanisms for protecting information up to Protected B in accordance with Ref [Q].

3.5.5 The exchange of information through network protocols must be compliant with Ref [R].

3.6 Design Constraints

3.6.1 All Projects and Programs

3.6.1.1 All projects and programs must comply with the requirements included in Appendix 5.

3.6.1.2 By default, all projects and programs must assign the user who created the project or program as the project or program manager and as the project or program coordinator.

3.6.2 Common and Naval Risk and Opportunity items

3.6.2.1 All common and naval risk and opportunity items defined in sections 3.6.3 to 3.6.8 must comply with the requirements included in Section 1 of Appendix 4.

3.6.2.2 By default, all common and naval risk and opportunity items must assign the user who created the item as the responsible user (owner).

[2] Virtual servers and databases, procured through a cloud service provider contract with Shared Services Canada, deployed in an availability zone within Canada is an acceptable solution.

3.6.2.3 All common and naval active risk and opportunity items should have the ability to have an expiry timeline during which the item has to be reviewed or updated or else it becomes expired. This is aimed at ensuring item owners routinely review their assigned items.

3.6.2.4 Once a common and naval risk or opportunity item has been endorsed or approved, a change that would result in a different overall risk level must void the endorsement or approval. The risk management software must notify the user making the change of this consequence.

3.6.2.5 All common and naval risk and opportunity items must have the ability to track the following historical log events:

3.6.2.5.1 Date and time the item was created (date and time);

3.6.2.5.2 Date and time the item last changed status (date and time);

3.6.2.5.3 Date and time the item was last updated (date and time);

3.6.2.6 All common and naval risk and opportunity items should include Hazard Condition, Hazard Cause(s), and Hazard Effect(s) such that the relationship can be constructed to support the Bow Tie Methodology described in ISO 31000[3].

3.6.3 Default Risk and Opportunity items

3.6.3.1 All default risk and opportunity items must comply with the requirements included in Section 2 of Appendix 4.

3.6.4 Project and Program Risk and Opportunity items

3.6.4.1 All project and program risk and opportunity items must comply with the requirements included in Section 3 of Appendix 4.

3.6.4.2 For all project and program risk and opportunity items, the associated Project or Program field described in Section 1 of Appendix 4 is a mandatory field.

3.6.5 Security Risk items

3.6.5.1 All security risk items must comply with the requirements included in Section 4 of Appendix 4.

3.6.6 Cyber Security Risk items

3.6.6.1 All cyber security risk items must comply with the requirements included in Section 5 of Appendix 4.

3.6.7 Ammunition & Explosive Safety Risk items

3.6.7.1 All ammunition & explosive safety risk items must comply with the requirements included in Section 6 of Appendix 4.

3.6.8 In-Service Naval Materiel Risk items

[3] ISO 31000 Risk Management

3.6.8.1 All in-service naval materiel risk items must comply with the requirements included in Section 7 of Appendix 4.

3.6.8.2 For all in-service naval materiel risk, the associated Classes/Fleet, Platforms field described in Section 1 of Appendix 4 is a mandatory field and must be restricted to Navy classes ships and submarines), and Navy platforms (ships and submarines) as listed in Appendix 2.

3.6.8.3 For all in-service naval materiel risk, the System selection must be restricted to the elements of Ref [K] allowing selection of the NDID Primary Group (Code Field 2) and their associated Supersystem Description as defined Figure 13-2-1 of Ref [K].

3.6.9 Airworthiness Risk Items

3.6.9.1 All airworthiness risk items must have the ability to be comprised of at least one, but can be all, of the following components:

3.6.9.1.1 Airworthiness Impact Assessment (AWIA) described in section 3.6.10;

3.6.9.1.2 Risk Alert Notification (RAN) described in section 3.6.11;

3.6.9.1.3 Airworthiness Risk Alert (ARA) described in section 3.6.12; and

3.6.9.1.4 Record of Airworthiness Risk Management (RARM) described in section 3.6.13.

3.6.9.2 All airworthiness risk items must have the ability to include the following:

3.6.9.2.1 Airworthiness Risk Tracking Log described in section 3.6.14; and

3.6.9.2.2 Airworthiness Risk Audit Review Log described in section 3.6.15.

3.6.9.3 All airworthiness risk items components listed in section 3.6.9.1 must comply with the requirements included in Section 1 of Appendix 6.

3.6.9.4 All airworthiness risk items components listed in section 3.6.9.1 must have the ability to be identified by the same user-inputted serial number as described in section 1 of Appendix 6.

3.6.9.5 All airworthiness risk items components listed in section 3.6.9.1 must have the ability to be version controlled. More specifically:

3.6.9.5.1 Each airworthiness risk items components listed in section 3.6.9.1 must have the ability to have multiple accessible versions; and

3.6.9.5.2 Each airworthiness risk items components listed in section 3.6.9.1 must only allow an authorized user the ability to modify the current (latest) version.

3.6.10 Airworthiness Impact Assessment (AWIA)

3.6.10.1 All airworthiness impact assessment components must comply with the requirements included in Section 2 of Appendix 6.

3.6.10.2 The airworthiness impact assessment must have the ability to automatically generate a Risk Alert Notification from the airworthiness impact assessment and auto-populate the related fields.

3.6.11 Risk Alert Notification (RAN)

3.6.11.1 All risk alert notification (RAN) components must comply with the requirements included in Section 3 of Appendix 6.

3.6.11.2 The risk management software must allow an authorized user to send the Risk Alert Notification via email to the identified recipients which are listed in the Risk Management Team, the Stakeholder list, and the Recipient list.

3.6.11.3 The risk alert notification email must include the following:

3.6.11.3.1 The information captured in the risk alert notification fields described in Section 3 within Appendix 6.

3.6.11.3.2 A hyperlink for the recipient to acknowledge the risk alert notification[4].

3.6.11.4 The risk alert notification email must follow the template at Ref [N].

3.6.11.5 The risk management software should have the ability to track and display the date and time that each recipient of a risk alert notification has acknowledged the notification.

3.6.11.6 The risk alert notification must have the ability to automatically generate an Airworthiness Risk Alert (ARA) and a Record of Airworthiness Risk Management (RARM) [5] from the Risk Alert Notification and auto-populate the related fields.

3.6.12 Airworthiness Risk Alert (ARA)

3.6.12.1 All airworthiness risk alert (ARA) components must comply with the requirements included in Section 4 of Appendix 6.

3.6.12.2 Airworthiness risk alert components must automatically be assigned the status “Draft” upon creation.

3.6.12.3 Airworthiness risk alert components must automatically be assigned the status “Approved” upon receiving all approval signatures.

3.6.12.4 Airworthiness risk alert components must not be editable once they have been subsumed by a RARM, closed, cancelled, archived or assigned any other status meaning they are no longer active.

3.6.12.5 Airworthiness risk alert components must have the ability to be extracted in the PDF format using the template at Ref [O].

[4] It is expected that some recipients might not have an account for the Risk Management Software. They should nonetheless be able to acknowledge a RAN without requiring to access the software.

[5] The user would select one or the other to be generated, but must have the option to generate both.

3.6.12.6 The airworthiness risk alert components must have the ability to automatically generate a Record of Airworthiness Risk Management (RARM) from the airworthiness risk alert and auto-populate the related fields.

3.6.13 Record of Airworthiness Risk Management (RARM)

3.6.13.1 All record of airworthiness risk management (RARM) components must comply with the requirements included in section 5 of Appendix 6.

3.6.13.2 Record of airworthiness risk management components must have the ability to be extracted in the PDF format using the template at Ref [P].

3.6.13.3 The risk management software must prevent a user from closing a record of airworthiness risk management until the following conditions have been met at a minimum:

3.6.13.3.1 The overall risk index is at the Acceptable Level of Safety (ALOS) for Airworthiness and Survivability risks;

3.6.13.3.2 All milestone risk control activities included in the latest version of the RARM have been completed;

3.6.13.3.3 The owner confirms that the Risk Tracking Log is up-to-date and reflect completion of (at a minimum) all milestone risk control activities.

3.6.14 Airworthiness Risk Tracking Log (RTL)

3.6.14.1 All airworthiness risk tracking log components must comply with the requirements included in section 7 of Appendix 6.

3.6.14.2 All airworthiness risk tracking log components must allow users to add risk tracking log events.

3.6.14.3 All airworthiness risk tracking log components must automatically generate risk tracking log events to capture the following at a minimum:

3.6.14.3.1 A new version of an airworthiness component (AWIA, ARA, RARM) is approved, including the overall risk index indicated in the version; and

3.6.14.3.2 An action item from the Risk Index Forecast Table has been completed.

3.6.15 Airworthiness Risk Audit Review

3.6.15.1 All airworthiness risk audit reviews components must comply with the requirements included in section 8 of Appendix 6.

3.6.15.2 All airworthiness risk audit reviews must be associated with a specific revision of an airworthiness impact assessment, an airworthiness risk alert, or a record of airworthiness risk management.

3.6.16 Historical Logs

3.6.16.1 All items described in section 3.6 must have the ability to track the historical log of edit changes including the following:

3.6.16.1.1 The member who made the edit (change) (username);

3.6.16.1.2 The date and time the edit (change) was saved (date and time); and

3.6.16.1.3 The data item that has been changed with its previous and new value (raw text).

3.6.16.2 Historical logs for each item described in section 3.6 must be kept until the item is deleted.

3.7 Software System Attributes

3.7.1 Reliability

3.7.1.1 (Intentionally left blank – see 3.7.3.2 for integrity requirement)

3.7.2 Availability

3.7.2.1 As this software will be managed by Canada, the availability requirements will be determined internally.

3.7.3 Security

3.7.3.1 The risk management software must be able to process and store data up to Protected B.

3.7.3.2 The target risk profile for the risk management solution must be Confidentiality of Protected B / Medium Integrity / Medium Availability, as described in Annex 4A – Profile 1[6] of Ref [E].

3.7.3.3 The risk management software, and its supporting architecture, must be deployed in security zones in accordance with Ref [S].

3.7.3.4 The risk management software, and its supporting architecture, should be deployed in security zones following the guidance provided in Ref [T].

3.7.3.5 Software as a Service components (if any) to the solution:

3.7.3.5.1 Must be compliant with ISO 27001 Information Security Management[7];

3.7.3.5.2 Must be compliant with ISO 27017 Information Technology – Security Techniques – Codes of practice for information security controls based on ISO/IEC 27002 for cloud services[8];

3.7.3.5.3 Must be compliant with SOC 2 Type II, as detailed by the Association of International Certified Professional Accountants (AICPA)[9].

3.7.3.6 The risk management software solution must comply with the security controls listed in Appendix 9.

[6] Annex 4A – Profile 1 – Protected B / Medium Integrity / Medium Availability https://cyber.gc.ca/en/guidance/annex-4a-profile-1-protected-b-medium-integrity-medium-availability-itsg-33

[7] ISO 27001 Information Security Management

[8] ISO 27017 IT – Security Techniques – Cloud Services

[9] AICPA SOC 2 Type II

3.7.3.7 The risk management software should have preventive measures to counter the top 10 application security risks, as detailed in Ref [U].

3.7.4 Maintainability

3.7.4.1 In order to reduce the Canada's maintenance requirement, the solution must use Platform as a Service components wherever possible, unless unavailable or otherwise specified.

3.7.4.2 In order to reduce JCDP's involvement in the project and in-service phases, the number of network security groups must be kept to a minimum necessary.

3.7.4.3 The risk management software and all of its component must be deployed on virtual servers using CIS server benchmark images.

3.7.4.4 The risk management software and all of its component should be deployed on virtual servers using CIS server benchmark 2 images, or higher level if available.

3.7.5 Portability

3.7.5.1 The risk management software must allow for data portability. More specifically:

3.7.5.1.1 The data generated by the risk management software must not be dependent on the use of a specific commercial proprietary application.

3.7.5.1.2 The data generated by the risk management software must be the sole property of the Government of Canada.

3.7.5.2 The risk management software must allow for application portability. More specifically:

3.7.5.2.1 The risk management software must be a platform agnostic solution meaning that it is portable and interoperable with other cloud service providers.

3.7.5.2.2 The risk management software should have the ability to integrate with JDCP DevOps and CI/CD pipelines using open source tools.

3.7.5.2.3 The risk management software should be compatible to the use of containers/immutable servers.

3.8 Supporting Information

3.8.1 The following is provided to support this Software Requirements Specifications:

3.8.1.1 Appendix 1 – Acronyms

3.8.1.2 Appendix 2 – List of platforms, classes and fleets

3.8.1.3 Appendix 3 – Not used

3.8.1.4 Appendix 4 – List of Common and Naval Risk and Opportunity Items

3.8.1.5 Appendix 5 – Projects and Programs

3.8.1.6 Appendix 6 – List of Airworthiness Items

3.8.1.7 Appendix 7 – Role Based Access Control

3.8.1.8 Appendix 8 – List of Application Level Logs

3.8.1.9 Appendix 9 – List of Security Controls

APPENDIX 1 – ACRONYMS

ADM(IM)	Assistant Deputy Minister (Information Management)
API	Application Programming Interface
CA	Canadian Army
DGAEPM	Director General Air Equipment and Program Management
DGMEPM	Director General Maritime Equipment and Program Management
DND	Department of National Defense
DRMIS	Defense Resources Management Information System
DWAN	Defense Wide Area Network
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
JDCP	Joint Defence Cloud Programme
LCMM	Lifecycle Materiel Manager
NIDE	Naval Integrated Data Environment
RCAF	Royal Canadian Air Force
RCN	Royal Canadian Navy
SOW	Statement of Work
SRS	Software Requirements Specifications
ITSG	Information Technology Security Guide

APPENDIX 2 – LIST OF PLATFORMS, CLASSES AND FLEETS

NAVY	RCAF
Class Program Manager: Major Surface Combatant (MSC) **Class/Fleet**: HALIFAX CLASS **Platforms/Aircrafts/Vehicles**: 330 – HMCS HALIFAX (HAL) 331 – HMCS VANCOUVER (VAN) 332 – HMCS VILLE-DE-QUÉBEC (VDQ) 333 – HMCS TORONTO (TOR) 334 – HMCS REGINA (REG) 335 – HMCS CALGARY (CAL) 336 – HMCS MONTRÉAL (MON) 337 – HMCS FREDERICTON (FRE) 338 – HMCS WINNIPEG (WIN) 339 – HMCS CHARLOTTETOWN (CHA) 340 – HMCS ST-JOHN'S (STJ) 341 – HMCS OTTAWA (OTT) **Class Program Manager**: Major Surface Combatant (MSC) **Class/Fleet**: CANADIAN SURFACE COMBATANT CLASS **Platforms/Aircrafts/Vehicles**: (To be determined) **Class Program Manager**: Non-Combatant (NC) **Class/Fleet**: HARRY DEWOLF CLASS **Platforms/Aircrafts/Vehicles**: 430 – HMCS HARRY DEWOLF (HDW) 431 – HMCS MARGARET BROOKE 432 – HMCS MAX BERNAYS 433 – HMCS WILLIAM HALL 434 – HMCS FRÉDÉRICK ROLETTE 435 – HMCS ROBERT HAMPTON GRAY **Class Program Manager**: Non-Combatant (NC) **Class/Fleet**: PROTECTEUR CLASS **Platforms/Aircrafts/Vehicles**: 520 – HMCS PROTECTEUR 521 – HMCS PRESERVER **Class Program Manager**: Non-Combatant (NC) **Class/Fleet**: KINGSTON CLASS **Platforms/Aircrafts/Vehicles**: 700 – HMCS KINGSTON 701 – HMCS GLACE BAY 702 – HMCS NANAIMO 703 – HMCS EDMONTON 704 – HMCS SHAWINIGAN 705 – HMCS WHITEHORSE 706 – HMCS YELLOWKNIFE 707 – HMCS GOOSE BAY 708 – HMCS MONCTON 709 – HMCS SASKATOON 710 – HMCS BRANDON 711 – HMCS SUMMERSIDE **Class Program Manager**: Non-Combatant (NC) **Class/Fleet**: ORCA CLASS	Fighters • CF-188 Hornet Maritime Aircraft • CP-140 Aurora • CH-148 Cyclone Search and Rescue Aircraft • CC-115 Buffalo • CC-130H Hercules • CH-149 Cormorant • CC-295 Kingfisher (Fixed Wing SAR) Tactical Helicopters • CH-146 Griffon • CH-147F Chinook Trainers • CT-114 Tutor • CT-155 Hawk • CT-156 Harvard • CT-142 Dash 8 • Gliders and Tow planes (ACGP) Transport Aircraft • CC-130J Hercules • CC-138 Twin Otter • CC-144 Challenger • CC-150 Polaris • CC-177 Globemaster III Unoccupied Aircraft • CU171 Super Hauler • CU172 Blackjack • CU173 Raven • CU174 Sky Ranger • CU175 Puma • CU176 Skeldar Miscellaneous Systems • Aviation Life Support Equipment (ALSE) • Other

Platforms/Aircrafts/Vehicles: PCT 55 – ORCA PCT 56 – RAVEN PCT 57 – CARIBOU PCT 58 – RENARD PCT 59 – WOLF PCT 60 – GRIZZLY PCT 61 – COUGAR PCT 62 - MOOSE **Class Program Manager**: Submarines (SM) **Class/Fleet**: VICTORIA CLASS **Platforms/Aircrafts/Vehicles**: 876 – HMCS VICTORIA (VIC) 877 – HMCS WINDSOR (WSR) 878 – HMCS CORNER BROOK (COR) 879 – HMCS CHICOUTIMI (CHI)	

APPENDIX 3 – (NOT USED)

APPENDIX 4 – LIST OF COMMON AND NAVAL RISK AND OPPORTUNITY ITEMS

1.1. This appendix describes the requirements associated with each type of risk and opportunity.

1.2. "Mandatory Field" means that if the field does not contain a valid input, the risk management software must warn and prompt the user to provide an input.

Section 1 - All Common and Naval Risk and Opportunity

Part 1 – Fields

At a minimum, all common and naval risk and opportunity items must have the following fields:

ID	Title	Field Type	Requirement
1.	Risk or Opportunity	multiple choices, one answer, mandatory field	All risk and opportunity items must have the ability to be identified as either a risk or an opportunity.
2.	Title	raw text, mandatory field	All risk and opportunity items must have a title
3.	Identification Code	software generated, mandatory field	All risk and opportunity items must have a unique identification code, automatically generated by the software
4.	DND Identification Number	raw text	All risk and opportunity items must have the ability to be linked to an identification number generated by another system and used within the Department of National Defence as a reference (for example: "ND 8406924")

5.	Information Restriction	multiple choices, multiple selection	All risk and opportunity items must have the ability to identify restrictions based on the confidentiality of the information they contain as follow:
			a. Contains Controlled Goods information;
			b. Contains Intellectual Property information;
			c. Contains Commercial in Confidence information;

6.	Information Sensitivity	multiple choices, one selection, mandatory field	All risk and opportunity items must have the ability to identify information sensitivity as follow: a. Not sensitive. b. Contains Protected A information; and c. Contains Protected B information.

7.	Element	multiple choices, multiple selection, mandatory field	All risk and opportunity items must have the ability to be associated with an applicable element from the following list:
			a. Royal Canadian Navy (RCN);
			b. Royal Canadian Air Force (RCAF);

			c. Canadian Army (CA); and d. Purple (DND);

8.	Item Type	multiple choices, one answer, mandatory field	All risk and opportunity items must have the ability to be identified based on their type from the following list:
			a. Default Risk or Opportunity;
			b. Project and Program Risk or Opportunity (as per Ref [C]);
			c. Security Risk (as per Ref [D]);
			d. Cyber Security Risk (Ref [IT Security]);
			e. Ammunition & Explosive Safety Risk (Ref [F]);
			f. In-Service Naval Materiel Risk (as per Refs [H], [J]);
			g. Airworthiness Risk (as per Ref [L]);

9.	Item Owner	Username, mandatory field	All risk and opportunity items must have a responsible user (owner)
10.	Associated Projects or Programs	multiple choices, multiple selection	All risk and opportunity items must have the ability to be associated to projects or programs
11.	Classes / Fleets and Platforms	multiple choices, multiple selection	All risk and opportunity items must have the ability to be linked to classes/fleets (classes of ships or submarines, fleet of aircraft, fleet of vehicles) as listed in Appendix 2, and to platforms (ships, submarines, aircrafts, vehicles) as listed in Appendix 2.
12.	System	raw text (unless further restricted)	All risk and opportunity items must have the ability to be linked to a system.
13.	System Stock Code	Raw text	All risk and opportunity items must have the ability to be linked to a system stock code.
14.	System Serial Number	Raw text	All risk and opportunity items must have the ability to be linked to a system serial number.
15.	Status	multiple choices, one answer, mandatory field	All risk and opportunity items must have the ability to identify their current status to differentiate between active and inactive (or archived) items. All risk and opportunity items must have the ability to identify their current status to identify various stages in the lifecycle of the item including draft, under review, endorsed, and archived.
16.	Risk Statement	raw text	All risk and opportunity items must have a risk or opportunity statement
17.	Background Statement	raw text	All risk and opportunity items must have the ability to include background information

18.	Likelihood Justification	Raw text	All risk and opportunity items must have the ability to include justification statement for the likelihood evaluation.
19.	Impact Justification	Raw text	All risk and opportunity items must have the ability to include justification statement for the impact evaluation.
20.	Mitigation Measures	Multiple entries, Raw Text	All risk and opportunity items must have the ability to include mitigation measures.
21.	Overall Risk Level	software generated based on the likelihood and impact of the risk	All risk and opportunity items must have an overall risk level.
22.	Additional Information	Raw Text	All risk and opportunity items must have the ability to include additional information.
23.	Attachments	Multiple files	All risk items must have the ability to attach multiple files, such as emails, PDF documents and images, in order to provide additional information and to capture endorsements and approvals.
24.	Action Items	Multiple Action Items	All risk and opportunity items must have the ability to include related action items as described in Appendix 4 Section 1 Part 3.

Part 2 – Automatic Notifications for all risk and opportunity items

At a minimum, the following automatic notification must be sent as it relates to all risk and opportunity items:

ID	Title	Notification Recipient	Trigger
1.	New Risk or Opportunity Owner	Risk or Opportunity item owner	A user has been assigned as the owner of a risk or opportunity item
2.	Risk or Opportunity requires imminent review before expiry	Risk or Opportunity item owner	A risk or opportunity item will expire within the next week
3.	Risk or Opportunity requires review due to expiry	Risk or Opportunity item owner	A risk or opportunity item has expired
4.	Risk or Opportunity has changed status	Risk or Opportunity item owner	A risk or opportunity item has changed status (including being archived and deleted)

5.	Modification of a risk or opportunity of interest	User subscribed to the risk or opportunity	A risk or opportunity item of interest[10] has been modified

Part 3 – Action Items

At a minimum, all action items must have the following fields:

ID	Title	Field Type	Requirement
1.	Identification Code	software generated, mandatory field	All action items must have a unique identification code, automatically generated by the software.
2.	Title	Raw text, mandatory field	All action items must have the ability to include a title.
3.	Description	Raw text	All action items must have the ability to include a description.
4.	Assigned Member	Username, mandatory field	All action items must have the ability to be assigned to a user.
5.	Due Date	Date, mandatory field	All action items must have the ability to include a due date.
6.	Status	Multiple Choices, mandatory field	All action items must have the ability to have a status from the following choices: a. Active; b. Completed; and c. Cancelled.

Part 4 – Automatic Notifications for action items

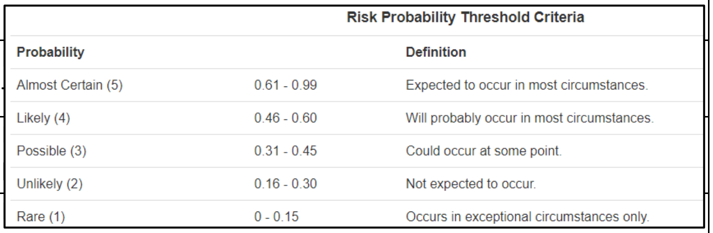
At a minimum, the following automatic notification must be sent as it relates to action items:

ID	Title	Notification Recipient	Trigger
1.	New Action Item Owner	Action item owner	A user has been assigned as the owner of an action item
2.	Action Item imminent due date	Action item owner	An action item will reach its due date within the next week
3.	Action Item pass due date	Action item owner	An action item has passed its due date
4.	Action Item Cancelled	Action item owner	An action item has been cancelled

[10] Of interest means that a user has subscribed to receive notifications for a particular risk or opportunity item.

Section 2 – Default Risk and Opportunity Items

At a minimum, default risk and opportunity items must have the following fields:

ID	Title	Field Type	Requirement
1.	Likelihood (probability)	multiple choices, one answer	For all default risk and opportunity items, the likelihood (probability) must be assessed based on the following table[11] 
2.	Risk Impact	multiple choices, one answer	
3.	Opportunity Impact	multiple choices, one answer	
4.	Overall Risk Level	software generated	(evaluation) must be assessed based on Figure 2 of Ref [C]
5.	Risk Acceptance Authority	Username	All default risk and opportunity items must have the ability to identify the risk acceptance authority
6.	Risk Acceptance Authority Position	Raw text	All default risk and opportunity items must have the ability to identify the risk acceptance authority's position.
7.	Risk Endorsement	Date and time	All default risk and opportunity items must have the ability to track the date and time the risk item has been endorsed by the risk acceptance authority.

Risk Probability Threshold Criteria

Probability		Definition
Almost Certain (5)	0.61 - 0.99	Expected to occur in most circumstances.
Likely (4)	0.46 - 0.60	Will probably occur in most circumstances.
Possible (3)	0.31 - 0.45	Could occur at some point.
Unlikely (2)	0.16 - 0.30	Not expected to occur.
Rare (1)	0 - 0.15	Occurs in exceptional circumstances only.

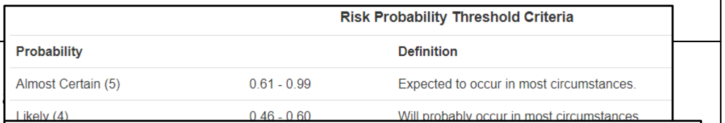
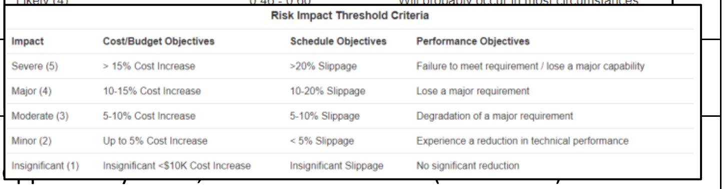
[11] Extracted from the Project Risk Management webpage of the Assistant Deputy Minister (Materiel) intranet website.

Section 3 – Project and Program Risk and Opportunity Items

At a minimum, project and program risk and opportunity items must have the following fields:

ID	Title	Field Type	Requirement

1.	Project or Program Phase	multiple choices, multiple answers	All project and program risk and opportunity items must have the ability to be associated with a project or program phase as follow:
			a. Identification;
			b. Options Analysis;
			c. Definition;
			d. Implementation;
			e. Closure;
			f. In-Service; and
			g. Disposal.

2.	Likelihood (probability)	multiple choices, one answer	For all project and program risk and opportunity items, the likelihood (probability) must be assessed based on the following table[12]  
3.	Impact - Risk	multiple choices, one answer	
4.	Impact - Opportunity	multiple choices, one answer	
5.	Overall Risk Level	Software generated	assessed based on Figure 2 of Ref [C]
6.	Pre-Mitigation Risk Assessment Scope	(risk assessment)	All project and program risk and opportunity items must have the ability to be assessed for both likelihood and impact, pre mitigation, for the following category: Scope.
7.	Pre-Mitigation Risk Assessment Schedule	(risk assessment)	All project and program risk and opportunity items must have the ability to be assessed for both likelihood and impact, pre mitigation, for the following category: Schedule.
8.	Pre-Mitigation Risk Assessment Cost	(risk assessment)	All project and program risk and opportunity items must have the ability to be assessed for both likelihood and impact, pre mitigation, for the following category: Cost.
9.	Pre-Mitigation Justifications	Raw text	All project and program risk and opportunity items must have the ability to include justification statements for each pre-mitigation assessment and for each category (Scope, Schedule, and Cost).

Risk Probability Threshold Criteria

Probability		Definition
Almost Certain (5)	0.61 - 0.99	Expected to occur in most circumstances.
Likely (4)	0.46 - 0.60	Will probably occur in most circumstances

Risk Impact Threshold Criteria

Impact	Cost/Budget Objectives	Schedule Objectives	Performance Objectives
Severe (5)	> 15% Cost Increase	>20% Slippage	Failure to meet requirement / lose a major capability
Major (4)	10-15% Cost Increase	10-20% Slippage	Lose a major requirement
Moderate (3)	5-10% Cost Increase	5-10% Slippage	Degradation of a major requirement
Minor (2)	Up to 5% Cost Increase	< 5% Slippage	Experience a reduction in technical performance
Insignificant (1)	Insignificant <$10K Cost Increase	Insignificant Slippage	No significant reduction

[12] Extracted from the Project Risk Management webpage of the Assistant Deputy Minister (Materiel) intranet website.

[13] Extracted from the Project Risk Management webpage of the Assistant Deputy Minister (Materiel) intranet website.

10.	Pre Mitigation Overall Risk Level	software generated	All project and program risk and opportunity items must have an overall pre-mitigation risk assessment level based on the highest assessment (level) from the three pre-mitigation assessment category (Scope, Schedule, and Cost).
11.	Post-Mitigation Risk Assessment Scope	(risk assessment)	All project and program risk and opportunity items must have the ability to be assessed for both likelihood and impact, post mitigation, for the following category: Scope.
12.	Post-Mitigation Risk Assessment Schedule	(risk assessment)	All project and program risk and opportunity items must have the ability to be assessed for both likelihood and impact, post mitigation, for the following category: Schedule.
13.	Post-Mitigation Risk Assessment Cost	(risk assessment)	All project and program risk and opportunity items must have the ability to be assessed for both likelihood and impact, post mitigation, for the following category: Cost.
14.	Post-Mitigation Justifications	Raw text	All project and program risk and opportunity items must have the ability to include justification statements for each post-mitigation assessment and for each category (Scope, Schedule, and Cost).
15.	Overall Risk Level	software generated	All project and program risk and opportunity items must have an overall post-mitigation risk assessment level based on the highest assessment (level) from the three post-mitigation assessment category (Scope, Schedule, and Cost).
16.	Risk Acceptance Authority	Username	All project and program risk and opportunity items must have the ability to identify the risk acceptance authority
17.	Risk Acceptance Authority Position	Raw text	All project and program risk and opportunity items must have the ability to identify the risk acceptance authority’s position.
18.	Risk Endorsement	Date and time	All project and program risk and opportunity items must have the ability to track the date and time the risk item has been endorsed by the risk acceptance authority.

Section 4 – Security Risk Items

At a minimum, security risk items must have the following fields:

ID	Title	Field Type	Requirement
1.	Likelihood	Multiple choices, one answer	For all security risk items, the likelihood must be assessed based on the levels in para 3.26-a of Ref [D]
2.	Impact	Multiple choices, one answer	For all security risk items, the impact must be assessed based on the levels in para 3.26-b of Ref [D]
3.	Overall Risk Level	software generated	For all security risk items, the overall risk assessment (evaluation) must be calculated based on the risk heat map at para 3.27 of Ref [D]
4.	Pre-Mitigation Risk Assessment	(risk assessment)	All security risk items must have the ability to be assessed for both likelihood and impact and both pre mitigations.
5.	Pre-Mitigation Justifications	Raw text	All security risk items must have the ability to include a justification statement for the pre-mitigation assessment.
6.	Post-Mitigation Risk Assessment	(risk assessment)	All security risk items must have the ability to be assessed for both likelihood and impact post mitigations.
7.	Pre-Mitigation Justifications	Raw text	All security risk items must have the ability to include a justification statement for the post-mitigation assessment.
8.	Risk Acceptance Authority	Username	All security risk items must have the ability to identify the risk acceptance authority
9.	Risk Acceptance Authority Position	Raw text	All security risk items must have the ability to identify the risk acceptance authority's position.
10.	Risk Endorsement	Date and time	All security risk items must have the ability to track the date and time the risk item has been endorsed by the risk acceptance authority.

Section 5 – Cyber Security Risk Items

At a minimum, cyber security risk items must have the following fields:

ID	Title	Field Type	Requirement
1.	Information System	Raw text	All cyber security risk items must have the ability to identify an associated information system that would impacted.
2.	Likelihood	multiple choices, one answer	For all cyber security risk items, the likelihood must be assessed based on the levels in para 3.26-a of Ref [D].
3.	Impact	multiple choices, one answer	For all cyber security risk items, the impact must be assessed based on the levels in para 3.26-b of Ref [D].
4.	Overall Risk Level	Software generated	For each category assessment of cyber security risk items, the overall risk level (evaluation) must be assessed based on the risk heat map at para 3.27 of Ref [D].
5.	Pre-Mitigation Risk Assessment Confidentiality	(risk assessment)	All cyber security risk items must have the ability to be assessed for both likelihood and impact, pre mitigation, for the following category: Confidentiality, as defined in Annex 5 of Ref [E].
6.	Pre-Mitigation Risk Assessment Integrity	(risk assessment)	All cyber security risk items must have the ability to be assessed for both likelihood and impact, pre mitigation, for the following category: Integrity, as defined in Annex 5 of Ref [E].
7.	Pre-Mitigation Risk Assessment Availability	(risk assessment)	All cyber security risk items must have the ability to be assessed for both likelihood and impact, pre mitigation, for the following category: Availability, as defined in Annex 5 of Ref [E].
8.	Pre-Mitigation Justifications	Raw text	All cyber security risk items must have the ability to include justification statements for each pre-mitigation assessment and for each category (Confidentiality, Integrity, and Availability).
9.	Pre Mitigation Overall Risk Level	software generated	All cyber security risk items must have an overall pre-mitigation risk assessment level based on the highest assessment (level) from the three pre-mitigation assessment category (Confidentiality, Integrity, and Availability).
10.	Post-Mitigation Risk Assessment Confidentiality	(risk assessment)	All cyber security risk items must have the ability to be assessed for both likelihood and impact, post mitigation, for the following category: Confidentiality.
11.	Post-Mitigation Risk Assessment Integrity	(risk assessment)	All cyber security risk items must have the ability to be assessed for both likelihood and impact, post mitigation, for the following category: Integrity.
12.	Post-Mitigation Risk Assessment Availability	(risk assessment)	All cyber security risk items must have the ability to be assessed for both likelihood and impact, post mitigation, for the following category: Availability.
13.	Post-Mitigation Justifications	Raw text	All cyber security risk items must have the ability to include justification statements for each post-mitigation assessment and for each category (Confidentiality, Integrity, and Availability).
14.	Overall Risk Level	software generated	All cyber security risk items must have an overall post-mitigation risk assessment level based on the highest assessment (level) from the three post-mitigation assessment category (Scope, Schedule, and Cost).

15.	Risk Acceptance Authority	Username	All cyber security risk items must have the ability to identify the risk acceptance authority
16.	Risk Acceptance Authority Position	Raw text	All cyber security risk items must have the ability to identify the risk acceptance authority’s position.
17.	Risk Endorsement	Date and time	All cyber security risk items must have the ability to track the date and time the risk item has been endorsed by the risk acceptance authority.

Section 6 – Ammunition and Explosive Safety Risk Items

At a minimum, ammunition and explosive safety risk items must have the following fields:

ID	Title	Field Type	Requirement
1.	Likelihood	Multiple choices, one answer	For all ammunition & explosive safety risk items, the likelihood (probability) must be assessed based on the levels figure 3-2-2 “Hazard Probability Table” of Ref [F]
2.	Impact	Multiple choices, one answer	For all ammunition & explosive safety risk items, the impact (consequence) must be assessed based on the levels figure 3-2-6 “Hazard Consequence Table” of Ref [F]
3.	Overall Risk Level	software generated	For all ammunition & explosive safety risk items, the overall risk assessment (index) must be calculated based on the risk index table at figure 3-2-7 of Ref [F]
4.	Pre-Mitigation Risk Assessment	(risk assessment)	All ammunition & explosive safety risk items must have the ability to be assessed for both likelihood and impact and both pre mitigations.
5.	Pre-Mitigation Justifications	Raw text	All ammunition & explosive safety risk items must have the ability to include a justification statement for the pre-mitigation assessment.
6.	Post-Mitigation Risk Assessment	(risk assessment)	All ammunition & explosive safety risk items must have the ability to be assessed for both likelihood and impact post mitigations.
7.	Pre-Mitigation Justifications	Raw text	All ammunition & explosive safety risk items must have the ability to include a justification statement for the post-mitigation assessment.
8.	Technical Review Authority User	Username	All ammunition & explosive safety risk items must have the ability to identify the technical review authority
9.	Technical Review Authority User Position	Raw text	All ammunition & explosive safety risk items must have the ability to identify the technical review authority’s position.
10.	Technical Review Authority Risk Endorsement	Date and time	All ammunition & explosive safety risk items must have the ability to track the date and time the risk item has been endorsed by the technical review authority.
11.	Operational Approval Authority User	Username	All ammunition & explosive safety risk items must have the ability to identify the operational approval authority
12.	Operational Approval Authority User Position	Raw text	All ammunition & explosive safety risk items must have the ability to identify the operational approval authority’s position.
13.	Operational Approval Authority Risk Endorsement	Date and time	All ammunition & explosive safety risk items must have the ability to track the date and time the risk item has been endorsed by the operational approval authority.

Section 7 – In-Service Naval Materiel Risk Items

At a minimum, in-service naval materiel risk items must have the following fields:

ID	Title	Field Type	Requirement
1.	Risk Scenario	multiple choices, one answer, mandatory field	All in-service naval materiel risk items must have the ability to include the applicable in-service naval materiel risk scenario from the following choices as described in Ref [H] a. Scenario 1 – Basis of Design and Design Intent; b. Scenario 2 – Certification Baseline and Certification Plan; c. Scenario 3 – Operational Departures from Certification Baseline; and d. Scenario 4 – Mission Readiness and Performance.
2.	Safety Areas	Multiple choices, multiple answers	All in-service naval materiel risk items must have the ability to be associated with safety areas listed in Table 3-1 of Ref [G].
3.	Hazards	Multiple entries, raw text	All in-service naval materiel risk items must have the ability to list hazards that would arise from the implementation of the materiel issue.
4.	Likelihood	multiple choices, one answer	For all in-service naval materiel risk items, the likelihood (probability) for each of the category listed above must be assessed based on the probability table in Appendix 1 of Ref [J].
5.	Impact	multiple choices, one answer	For all in-service naval materiel risk items, the impact (severity) for each of the category listed above must be assessed based on their respective severity tables in Appendix 1 of Ref [J].
6.	Overall Risk Level	Software generated	For each category assessment of in-service naval materiel risk items, the overall risk level must be assessed based on the risk matrix in Appendix 1 of Ref [J].
7.	Pre-Mitigation Risk Assessment Personnel	(risk assessment)	All in-service naval materiel risk items must have the ability to be assessed for both likelihood and impact, pre mitigation, for the following category: Personnel.
8.	Pre-Mitigation Risk Assessment Materiel	(risk assessment)	All in-service naval materiel risk items must have the ability to be assessed for both likelihood and impact, pre mitigation, for the following category: Materiel.
9.	Pre-Mitigation Risk Assessment Mission	(risk assessment)	All in-service naval materiel risk items must have the ability to be assessed for both likelihood and impact, pre mitigation, for the following category: Mission.
10.	Pre-Mitigation Risk Assessment Environment	(risk assessment)	All in-service naval materiel risk items must have the ability to be assessed for both likelihood and impact, pre mitigation, for the following category: Environment.
11.	Pre-Mitigation Justifications	Raw text	All in-service naval materiel risk items must have the ability to include justification statements for each pre-mitigation assessment and for each category (Personnel, Materiel, Mission, and Environment).

12.	Pre Mitigation Overall Risk Level	software generated	All in-service naval materiel risk items must have an overall pre-mitigation risk assessment level based on the highest assessment (level) from the pre-mitigation assessment categories (Personnel, Materiel, Mission, and Environment).
13.	Post-Mitigation Risk Assessment Personnel	(risk assessment)	All in-service naval materiel risk items must have the ability to be assessed for both likelihood and impact, post mitigation, for the following category: Personnel.
14.	Post-Mitigation Risk Assessment Materiel	(risk assessment)	All in-service naval materiel risk items must have the ability to be assessed for both likelihood and impact, post mitigation, for the following category: Materiel.
15.	Post-Mitigation Risk Assessment Mission	(risk assessment)	All in-service naval materiel risk items must have the ability to be assessed for both likelihood and impact, post mitigation, for the following category: Mission.
16.	Post-Mitigation Risk Assessment Environment	(risk assessment)	All in-service naval materiel risk items must have the ability to be assessed for both likelihood and impact, post mitigation, for the following category: Environment.
17.	Post-Mitigation Justifications	Raw text	All in-service naval materiel risk items must have the ability to include justification statements for each post-mitigation assessment and for each category (Personnel, Materiel, Mission, and Environment).
18.	Overall Risk Level	software generated	All in-service naval materiel risk items must have an overall post-mitigation risk assessment level based on the highest assessment (level) from the post-mitigation assessment categories (Personnel, Materiel, Mission, and Environment).
19.	Technical Authority User	Username	All in-service naval materiel risk items must have the ability to identify the technical authority
20.	Technical Authority User Position	Raw text	All in-service naval materiel risk items must have the ability to identify the technical authority’s position.
21.	Technical Authority Risk Endorsement	Date and time	All in-service naval materiel risk items must have the ability to track the date and time the risk item has been endorsed by the technical authority.
22.	Operational Authority User	Username	All in-service naval materiel risk items must have the ability to identify the operational authority
23.	Operational Authority User Position	Raw text	All in-service naval materiel risk items must have the ability to identify the operational authority’s position.
24.	Operational Authority Risk Endorsement	Date and time	All in-service naval materiel risk items must have the ability to track the date and time the risk item has been endorsed by the operational authority.

APPENDIX 5 – PROJECTS AND PROGRAMS

Part 1 - Fields

At a minimum, projects and programs must have the following fields:

ID	Title	Field Type	Requirement
1.	Project or Program	multiple choices, one answer, mandatory field	All projects and programs must have the ability to be identified as either a project or a program.
2.	Title	raw text, mandatory field	All projects and programs must have a title
3.	Identification Code	software generated, mandatory field	All projects and programs must have a unique identification code
4.	DND Identification Number	Raw text	All projects and programs must have the ability to be associated with an identification number generated by another system and used within the Department of National Defence as a reference (for example: “N.002885”)

5.	Element	multiple choices, multiple selection, mandatory field	All projects and programs must have the ability to be associated with an applicable element from the following list:
			a. Royal Canadian Navy (RCN);
			b. Royal Canadian Air Force (RCAF);
			c. Canadian Army (CA); and
			d. Purple (DND);

6.	Parent Project or Program	multiple choices, one answer	All projects and programs must have the ability to be associated to a parent project or program
7.	Project or Program Description	Raw text	All projects and programs must have the ability to include a description.
8.	Project or Program Manager	Username, mandatory field	All projects and programs must have the ability to identify the project or program manager
9.	Project or Program Manager Position	Raw text	All projects and programs must have the ability to identify the project or program manager position
10.	Project or Program Coordinator	Username, mandatory field	All projects and programs must have the ability to identify the project or program coordinator
11.	Project or Program Coordinator Position	Raw text	All projects and programs must have the ability to identify the project or program coordinator position

12.	Project or Program Administrators	Username (multiple entries)	All projects and programs must have the ability to identify project or program administrators
13.	Project or Program Administrators Position	Raw text	All projects and programs must have the ability to identify project or program administrators position (for each administrator)
14.	Project or Program Collaborators	Username (multiple entries)	All projects and programs must have the ability to identify project or program collaborators
15.	Project or Program Collaborators Position	Raw text	All projects and programs must have the ability to identify project or program collaborators position (for each collaborator)

Part 2 – Automatic Notifications for Projects and Programs

At a minimum, the following automatic notification must be sent as it relates to action items:

ID	Title	Notification Recipient	Trigger
1.	New Project or Program Stakeholder	New Project or Program Stakeholder	A user has been assigned as a project or program stakeholder (manager, coordinator, administrator, collaborator)
2.	Project or Program is being archived or deleted	Project or Program Manager, Coordinator, and Administrators	A project or program is being archived or deleted

APPENDIX 6 – LIST OF AIRWORTHINESS RISK ITEMS

Airworthiness Process Overview

The Airworthiness Risk Management Process is a decision making product that begins with the identification of a Hazard (Risk) which could be identified by any user authorized to use the system. The current process as defined in EMT01.003 Airworthiness Risk Management Procedure will be modified but still applies to the new system. This procedure describes the Airworthiness Process to use within DND, Canadian Forces Airworthiness Program and the Aerospace Program Management Division (AEPM).

For guidelines on the standards to be followed, please refer to the Technical Airworthiness Manual (TAM) and Operational Airworthiness Manual (OAM).

Policy and Procedural Requirements

The primary objective of the TAM is to provide an Acceptable Level of Safety (ALOS) by regulating the technical aspects of aviation related activities to ensure the safe flight and landing of aircraft in all situations.

The Airworthiness requirements are also translated into a detailed instruction within the AF9000 business process EMT01.003. This includes the policies enabling the airworthiness requirements that are detailed in Part 12 of C-05-005-P12/AM-001 AEPM Division Engineering Process Manual (EPM), Part 5 of C-05-005-001/AG-001Technical Airworthiness Manual (TAM) and Chapter 5 of B-GA-104-000/FP-001 Operations Airworthiness Manual (OAM). This policy is satisfied by the AF9000 process numbered EMT01.003.

Section 1 – Airworthiness Risk Items

At a minimum, all airworthiness risk items must have the following fields:

ID	Title	Field Type	Requirement
1.	Categorization	multiple choices, one answer, mandatory field	All airworthiness risk items must have the ability to be categorized as either Technical Airworthiness or Operational Airworthiness.

2.	Information Restriction	multiple choices, multiple selection	All airworthiness risk items must have the ability to identify restrictions based on the confidentiality of the information they contain as follow:
			a. Contains Controlled Goods information;
			b. Contains Intellectual Property information;
			a. Contains Commercial in Confidence information.

3.	Information Sensitivity	multiple choices, one selection, mandatory field	All airworthiness risk items must have the ability to identify information sensitivity as follow: a. Not sensitive. b. Contains Protected A information; and c. Contains Protected B information.
4.	Title	raw text, mandatory field	All airworthiness risk items must have a title
5.	Unique Identification Code	software generated, mandatory field	All airworthiness risk items must have a unique identification code.
6.	Record Serial Number	Raw text	All airworthiness risk items must have the ability to include a Record Serial Number following the format prescribed in para 5.4.1 (b) of Ref [M].
7.	Version Number	Raw text	All airworthiness risk items must have the ability to track the version number.
8.	Owner	Username, mandatory field	All airworthiness risk items must have an owner responsible for the item.
9.	Aircraft Type	Multiple choices, multiple selection, mandatory field	All airworthiness risk items must list which aircraft type is affected, based on the list from Appendix 2.
10.	Product(s) Identification	Multiple Entries, Raw text	All airworthiness risk items must have the ability to include the product identification
11.	Summary of Situation	Rich Text	All airworthiness risk items must have the ability to include a summary of situation.
12.	Date Opened	Date and Time, software generated	All airworthiness risk items must have an associated opened date.
13.	Date Closed	Date and Time, software generated	All airworthiness risk items must have an associated closed date.
14.	Risk Management Team	Multiple entries, username, organization, and role.	All airworthiness risk items must have the ability to list members part of the risk management team.

			Each member listed must have the ability to include the username (email), the organization (raw text), and their role (raw text).
15.	Stakeholder list	Multiple entries, username, organization, and role.	All airworthiness risk items must have the ability to list members part of the stakeholder list. Each member listed must have the ability to include the username (email), the organization (raw text), and their role (raw text).

Section 2 – Airworthiness Impact Assessment (AWIA)

At a minimum, airworthiness impact assessment components must have the following fields:

ID	Title	Field Type	Requirement

1.	Status	Multiple Choices, one selection, mandatory field	All airworthiness impact assessment components must have an associated status amongst the following choices:
			a. Draft;
			b. Under Review;
			c. Approved;
			d. Subsumed by a RARM;
			e. Closed.

2.	Hazard Condition	Raw text	All airworthiness impact assessment items must have the ability to include hazard condition.
3.	Hazard Causes	Multiple entries	All airworthiness impact assessment items must have the ability to include hazard causes.

4.	Hazard Effects - Airworthiness	Multiple entries, risk assessment	All airworthiness impact assessment items must have the ability to list airworthiness hazard effects.
			Each Hazard Effect Airworthiness included in an airworthiness risk alert item must have the ability to include the following:
			a. Title;
			b. Hazard Severity, multiple choices (one selection) based on Table A-1 of Ref [M];
			c. Hazard Severity Substantiation (raw text);
			d. Hazard Probability, multiple choices (one selection) based on Table A-3 of Ref [M];
			e. Hazard Probability Substantiation (raw text);
			Airworthiness Risk Index, software generated based on Table A-6 of Ref [M].

5.	Hazard Effects – Survivability	Multiple entries, risk assessment	All airworthiness impact assessment items must have the ability to list survivability hazard effects.
			Each Hazard Effect Survivability included in an airworthiness risk alert item must have the ability to include the following:
			a. Title;
			b. Hazard Severity, multiple choices (one selection) based on Table A-4 of Ref [M];
			c. Hazard Severity Substantiation (raw text);
			d. Hazard Probability, multiple choices (one selection) based on Table A-5 of Ref [M];
			e. Hazard Probability Substantiation (raw text);
			Survivability Risk Index, software generated based on Table A-6 of Ref [M].

6.	Overall Airworthiness Risk Index	Software Generated	All airworthiness impact assessment items must include the overall airworthiness risk index, based on the highest risk index identified by the Airworthiness Hazard Effects.

7.	Overall Survivability Risk Index	Software Generated	All airworthiness impact assessment items must include the overall survivability risk index, based on the highest risk index identified by the Survivability Hazard Effects.
8.	Attachments	Multiple files	All airworthiness hazard items must have the ability to attach multiple files, such as emails, PDF documents and images, in order to provide additional information and to capture endorsements and approvals.

Section 3 – Risk Alert Notification (RAN)

Context and Purpose: As per para 5.2 of Ref [M]: "*When a hazard condition that reduces the level of safety of an aircraft or fleet is discovered, it is imperative that a RARM be initiated and communicated to the Operational Command Risk Acceptance Authority as quickly as possible. This shall be done by producing a Risk Alert Notification and a subsequent ARA (which is a simplified form of RARM) for any risk issue that is not at an ALOS and currently affects aircraft or the fleet.*"

At a minimum, risk alert notice (RAN) items must have the following fields:

ID	Title	Field Type	Requirement
1.	Additional Recipients	Multiple entries, username	All risk alert notifications items must have the ability to identify additional recipients (beyond those listed in the risk management team, and the stakeholder list)
2.	Nature of Hazard Condition	Raw text, mandatory field	All risk alert notification items must have the ability to identify
3.	Hazard Causes	Multiple entries	All risk alert notification items must have the ability to identify hazard causes.
4.	Hazard Effects	Multiple entries	All risk alert notification items must have the ability to identify hazard effects.
5.	Hazard Type	Multiple Choices, one answer	Each risk alert notification hazard must have the ability to be attributed a type between Airworthiness and Survivability
6.	Hazard Effect Probability	Multiple Choices, one answer	Each risk alert notification hazard effect must have the ability to be assessed on its probability based on table A-3 of Ref [M] (for airworthiness type) and table A-5 of Ref [M] (for survivability type)
7.	Hazard Effect Severity	Multiple Choices, one answer	Each risk alert notification hazard effect must have the ability to be assessed on its severity based on table A-1 of Ref [M] (for airworthiness type) and table A-4 of Ref [M] (for survivability type)
8.	Informal Operational Impact Assessment	Raw text, mandatory field	All risk alert notification items must have the ability to identify the operational impact assessment.
9.	Immediate Mitigation Actions	Raw text	All risk alert notification must have the ability to must include any immediate mitigating actions being suggested for implementation.
10.	ARA/RARM Issuance	Date and Time	All risk alert notification must identify when the ARA/RARM are expected to be distributed
11.	Disclaimer	Raw text	All risk alert notification must have the ability to include a disclaimer. The default disclaimer must be as follow: "*The information in this Risk Alert Notification is preliminary and may be inaccurate; the content may be revised in the ARA/RARM*."
12.	Distribution date	Date and Time (system generated)	All risk alert notification must have the ability to track the date and time the risk alert notification has been distributed (sent) to the recipients

13.	Recipients Acknowledgement	Date and Time (system generated)	All risk alert notification must have the ability to track the acknowledgment of each recipient.

Section 4 – Airworthiness Risk Alert (ARA)

Context and Purpose: As per para 5.3 of Ref [M], the purpose of an ARA is to "*advise all stakeholders of (a) the situation and the estimated risk level; (b) the steps being taken to fully determine the actual risk level; and (c) any Risk Control Activities planned or in place as interim measures*". Additionally, as per Ref [O], the aim is to "*advise the Operational Command Acceptance Authority of a new issue (or a substantial change in an existing issue) affecting the airworthiness of a fleet or part of a fleet, and to seek acceptance of the risk.*"

At a minimum, airworthiness risk alert (ARA) items must have the following fields:

ID	Title	Field Type	Requirement
	GENERAL RISK COMPONENT IDENTIFICATION SUB-SECTION		

1.	Status	Multiple Choices, one selection, mandatory field	All airworthiness risk alert items must have an associated status amongst the following choices:
			a. Draft;
			b. Under Review;
			c. Approved;
			d. Subsumed by a RARM;
			e. Closed;
			f. Cancelled.

	HAZARD IDENTIFICATION SUB-SECTION		
2.	Hazard Condition	Raw text	All airworthiness risk alert items must have the ability to include hazard condition.
3.	Hazard Causes	Multiple entries	All airworthiness risk alert items must have the ability to include hazard causes.
	RISK ASSESSMENT SUB-SECTION		

4.	Hazard Effects - Airworthiness	Multiple entries, risk assessment	All airworthiness risk alert items must have the ability to list airworthiness hazard effects.
			Each Hazard Effect Airworthiness included in an airworthiness risk alert item must have the ability to include the following:
			a. Title;
			b. Hazard Severity, multiple choices (one selection) based on Table A-1 of Ref [M];
			c. Hazard Severity Substantiation (raw text);
			d. Hazard Probability, multiple choices (one selection) based on Table A-3 of Ref [M];
			e. Hazard Probability Substantiation (raw text);
			f. Airworthiness Risk Index, software generated based on Table A-6 of Ref [M].

5.	Hazard Effects – Survivability	Multiple entries, risk assessment	All airworthiness risk alert items must have the ability to list survivability hazard effects.
			
			Each Hazard Effect Survivability included in an airworthiness risk alert item must have the ability to include the following:
			a. Title;
			b. Hazard Severity, multiple choices (one selection) based on Table A-4 of Ref [M];
			c. Hazard Severity Substantiation (raw text);
			d. Hazard Probability, multiple choices (one selection) based on Table A-5 of Ref [M];

			e. Hazard Probability Substantiation (raw text); f. Survivability Risk Index, software generated based on Table A-6 of Ref [M].
6.	Airworthiness Risk Index	Software Generated	All airworthiness risk alert items must include the overall airworthiness risk index, based on the highest risk index identified by the Airworthiness Hazard Effects.
7.	Survivability Risk Index	Software Generated	All airworthiness risk alert items must include the overall survivability risk index, based on the highest risk index identified by the Survivability Hazard Effects.
8.	Level of Confidence	Raw Text	All airworthiness risk alert items must have the ability to include the level of confidence.
	IMMEDIATE RISK MITIGATION PLAN SUB-SECTION		
9.	Next Revisions	Raw Text	All airworthiness risk alert items must have the ability to include a plan for the next revisions.
10.	Immediate Mitigation Plan	Raw text	All airworthiness risk alert items must have the ability to include any immediate mitigating activities actions being suggested for implementation.
11.	Immediate Risk Control Activities	Multiple entries, Raw Text	All airworthiness risk alert items must have the ability to include immediate risk control activities, as described in para 5.3.1 of Ref [M].
12.	Flight Restrictions or Limitations Conditional to Operational Command Risk Acceptance	Multiple entries, Raw Text	All airworthiness risk alert items must have the ability to include any flight restrictions or limitations conditional to operational command risk acceptance.
	ATTACHMENT SUB-SECTION		
13.	Attachments	Multiple files	All airworthiness risk alert items must have the ability to attach multiple files, such as emails, PDF documents and images, in order to provide additional information and to capture endorsements and approvals.
	APPROVAL AND RISK ACCEPTANCE SUB-SECTION		

14.	Technical Airworthiness Authority Approval	Approval Signature	All airworthiness risk alert items must have the ability to track the approval from the Technical Airworthiness Authority.
			The approval signature must include:
			a. Username (email);
			b. Full name (raw text);
			c. Rank (raw text);
			d. Position (raw text);
			e. Phone number (raw text);
			f. Decision (multiple choice, one answer: “Approved” or “Not Approved”);
			g. Decision justification (raw text); and
			h. Decision timestamp (date and time).

15.	Independent Technical	Approval Signature	All airworthiness risk alert items must have the ability to track the approval from the Independent Technical Airworthiness

	Airworthiness Authority Staff Review Approval		Authority Staff Review for High and Extremely High Overall Risk Index.
			The approval signature must include:
			a. Username (email);
			b. Full name (raw text);
			c. Rank (raw text);
			d. Position (raw text);
			e. Phone number (raw text);
			f. Decision (multiple choice, one answer: “Approved” or “Not Approved”);
			g. Decision justification (raw text); and
			h. Decision timestamp (date and time).

16.	Operational Airworthiness Authority Approval	Approval Signature	All airworthiness risk alert items must have the ability to track the approval from the Operational Airworthiness Authority.
			The approval signature must include:
			a. Username (email);
			b. Full name (raw text);
			c. Rank (raw text);
			d. Position (raw text);
			e. Phone number (raw text);
			f. Decision (multiple choice, one answer: “Approved” or “Not Approved”);
			g. Decision justification (raw text); and
			h. Decision timestamp (date and time).

17.	Operational Command Risk Acceptance	Approval Signature	All airworthiness risk alert items must have the ability to track the approval from the Operational Command.
			The approval signature must include:
			a. Username (email);
			b. Full name (raw text);
			c. Rank (raw text);
			d. Position (raw text);
			e. Phone number (raw text);
			f. Decision (multiple choice, one answer: “Approved” or “Not Approved”);
			g. Decision justification (raw text); and
			h. Decision timestamp (date and time).

	COMMENTS SUB-SECTION		
18.	Comments and Feedback	Multiple entries, Raw Text	All airworthiness risk alert items must have the ability to collect comments and feedback from users. Each comment or feedback added to an airworthiness risk alert item must have the following: a. Username (email) of the author; b. Comment (raw text); c. Timestamp the comment was posted (date and time).

Section 5 - Record of Airworthiness Risk Management (RARM)

At a minimum, records of airworthiness risk management (RARM) items must have the following fields:

ID	Title	Field Type	Requirement
	GENERAL RISK COMPONENT IDENTIFICATION SUB-SECTION		

1.	Status	Multiple Choices, one selection, mandatory field	All record of airworthiness risk management items must have an associated status amongst the following choices (Ref [M] para 5.10):
			a. Draft;
			b. Open-Active;
			c. Open-Inactive;
			d. Open-Revising;
			e. Closed;
			f. Cancelled.

	HAZARD IDENTIFICATION SUB-SECTION		
2.	(same as ARA)	(same as ARA)	(same as ARA)
	RISK ASSESSMENT SUB-SECTION		
3.	(same as ARA)	(same as ARA)	(same as ARA)
	RISK CONTROL PLAN SUB-SECTION		
4.	Risk Control Options	Multiple entries, raw text	All record of airworthiness risk management items must have the ability to identify risk control options
5.	Options Analysis	Rich Text	All record of airworthiness risk management items must have the ability to include an options analysis
6.	Preferred Option	Raw Text	All record of airworthiness risk management items must have the ability to identify a preferred option
7.	Plan Implementation	Rich Text	All record of airworthiness risk management items must have the ability to include a description of plan implementation
8.	Risk Index Forecast Table	(Risk Index Forecast Table)	All record of airworthiness risk management items must have the ability to include a Risk Index Forecast Table as described in Section 6 of Appendix 6, in order to track action items.
	ATTACHMENT SUB-SECTION		
9.	(same as ARA)	(same as ARA)	(same as ARA)
	APPROVAL AND RISK ACCEPTANCE SUB-SECTION		
10.	(same as ARA)	(same as ARA)	(same as ARA)
	COMMENTS SUB-SECTION		
11.	(same as ARA)	(same as ARA)	(same as ARA)

Section 6 – Risk Index Forecast Table (RIFT)

At a minimum, the Risk Index Forecast Table (RIFT) must have the following field:

ID	Title	Field Type	Requirement
1.	Unique Identification Code	software generated, mandatory field	All risk control action items must have a unique identification code.
2.	Risk Control Action Title	Raw text, mandatory field	All risk control action items must have a title.
3.	Risk Control Action Description	Rich Text	All risk control action items must have the ability to include a description.
4.	Importance	Multiple Choices, one selection	All risk control action items must have the ability to include an importance level: a. Milestone; b. Non-Milestone.
5.	Milestone	Multiple Choices, one selection	All risk control action items must have the ability to be identified as a milestone or not (yes or no choice).
6.	Expected Completion	Date	All risk control action items must have the ability to include a date when the item is expected to be completed.
7.	Assigned Organization	Raw text	All risk control action items must have the ability to be assigned to an organization.
8.	Assigned User	Username	All risk control action items must have the ability to be assigned to a user.
9.	Residual Risk Index	Multiple choices, one selection	All risk control action items must have the ability to identify a residual risk index, based on the risk index choices from Ref [M]
10.	Substantiation for Residual Risk Index	Raw text	All risk control action items must have the ability to include a substantiation for the residual risk index.
11.	Status	software generated, Mandatory field.	All risk control action items must have the ability to be assigned the following status: a. Active; b. Completed (assigned once a completion date has been inputted); c. Overdue (assigned if the item isn't completed and the due date has passed); d. Revised due date (status only available and assigned for non-milestone items)
12.	Actual Completion Date	Date	All risk control action items must have the ability to include a completion date.
13.	Additional Information	Rich text	All risk control action items must have the ability to include additional information.

Section 7 – Risk Tracking Log (RTL)

At a minimum, Airworthiness Risk Tracking Log (RTL) must have the following field:

ID	Title	Field Type	Requirement
1.	Unique Identification Code	software generated, mandatory field	All airworthiness risk tracking log items must have a unique identification code.
2.	Associated Airworthiness risk Identification	Raw Text, software generated	All airworthiness risk tracking log items must be associated with an airworthiness risk.
3.	Associated Risk Index Forecast Table Item	(Risk Index Forecast Table Item)	All airworthiness risk tracking log items must have the ability to be linked with an existing Risk Index Forecast Table Item. Correlated RIFT item status will be modified as per Section 6 item 11.
4.	Risk Tracking Log Table	Multiple Entries, Audit Risk Tracking Log Event Items	All airworthiness risk tracking log items must have the ability to include risk tracking log event items, as described in Part 2 of Section 7 of Appendix 6.

Part 2 – Risk Tracking Log Event Item

ID	Title	Field Type	Requirement
1.	Unique Identification Code	software generated, mandatory field	All risk control log event items must have a unique identification code.
2.	Title	Raw text, mandatory field	All risk control log event items must have a title.
3.	Description	Raw text	All risk control log event items must have the ability to include a description.
4.	Date	Date, mandatory field	All risk control log event items must have a date when the event was recorded.
5.	Username	Username	All risk control log event items must have a user associated with the event.

Section 8 – Airworthiness Risk Audit Review

At a minimum, Airworthiness Risk Audit Reviews must have the following field:

ID	Title	Field Type	Requirement
1.	Unique Identification Code	software generated, mandatory field	All airworthiness risk audit review items must have a unique identification code.
2.	Associated Airworthiness risk component	Raw Text, software generated	All airworthiness risk audit review items must be associated with a specific version of an AWIA, ARA, or RARM
3.	Date	Date, software generated	All airworthiness risk audit review items must indicate the date the audit review was generated.
4.	Audit Review Deficiency Table	Multiple Entries, Audit Review Deficiency Items	All airworthiness risk audit review items must have the ability to include a list of deficiency items, as described in Part 2 of Section 8 of Appendix 6.
5.	Additional Information	Rich text	All airworthiness risk audit review items must have the ability to include additional information.

Part 2 – Audit Review Deficiency Item

ID	Title	Field Type	Requirement
1.	Unique Identification Code	software generated, mandatory field	All audit deficiency items must have a unique identification code.
2.	Title	Raw text, mandatory field	All audit deficiency items must have a title.
3.	Description	Rich Text	All audit deficiency items must have the ability to include a description.

4.	Importance	Multiple Choices, one selection	All audit deficiency items must have the ability to include an importance level:
			a. Normal;
			b. Significant;
			c. Critical.

Section 9 – Airworthiness Review and Approval Workflow

1. The review and approval workflow for airworthiness items (ARA and RARM) is as follow:

Step	Type	Action
1.	User Input	An authorized user initiates the review and approval workflow.
2.	Software	The Technical Airworthiness Authority is notified that their action is required.
3.	User Input	The Technical Airworthiness Authority inputs their decision and electronic signature.
4.	Software	If the overall risk index is high or extremely high, the Independent Technical Airworthiness Authority Staff Review is notified that their action is required.
5.	User Input	If the overall risk index is high or extremely high, the Independent Technical Airworthiness Authority inputs their decision and electronic signature.
6.	Software	The Operational Airworthiness Authority is notified that their action is required.
7.	User Input	The Operational Airworthiness Authority inputs their decision and electronic signature.
8.	Software	The Operational Command is notified that their action is required.
9.	User Input	The Operational Command input their decision and electronic signature
10.	Software	All stakeholders (comprised of the risk management team, and stakeholder lists) are notified of the workflow completion.
11.	Software	If fully approved, the current version is locked. The risk owner can create a new version if necessary.

2. If any of the reviewing or approving authorities along the workflow select “not approved”, the owner is notified and the workflow does not continue.

APPENDIX 7 – ROLE BASED ACCESS CONTROL

This appendix contains proposed default roles to be enabled in the risk management software as to separate the level of access based on user need. As per section 3.1.11, every user must have the ability to be restricted based on specific aspects such as Class/Fleet for example.

Section 1 – Administrator Roles

ROLE	READ	EDIT
System Administrator	All	All
Navy Administrator	All, restricted to Navy and Purple	All, restricted to Navy and Purple
Air Force Administrator	All, restricted to Air Force and Purple	All, restricted to Air Force and Purple
Purple Administrator	All, restricted to Purple	All, restricted to Purple

Section 2 – Purple Roles

ROLE	READ	EDIT
Purple User	Can read all items (purple only)	Can create new items (purple only) Can create new project / program (purple only) Can edit items for which they are the owner or an approver (purple only)
Purple Restricted	Can read all items that have no information restrictions (purple only), except for items they are assigned as the owner	Can create new items (purple only) Can edit items for which they are the owner or an approver (purple only)

Section 3 – Navy Roles

ROLE	READ	EDIT
Navy User	Can read all items (Navy and purple only)	Can create new items (Navy and purple only) Can create new project / program (Navy and purple only) Can edit items for which they are the owner or an approver (purple only)
Navy Restricted	Can read all items that have no information restrictions (Navy and purple only), except for items they are assigned as the owner	Can create new items (Navy and purple only) Can edit items for which they are the owner or an approver (Navy and purple only)

Section 4 – Air Force Roles

ROLE	READ	EDIT
Air Force User	Can read all items (Air Force and purple only)	Can create new items (Air Force and purple only) Can create new project / program (Air Force and purple only) Can edit items for which they are the owner or an approver (purple only)
Air Force Restricted	Can read all items that have no information restrictions (Air Force and purple only), except for items they are assigned as the owner	Can create new items (Air Force and purple only) Can edit items for which they are the owner or an approver (Air Force and purple only)

Section 5 – Projects and Programs Roles

	System Role	Project or Program stakeholder role			
	Administrator	Manager	Coordinator	Administrators	Collaborators
Read items under the project or program	X	X	X	X	X
Create new items under the project or program	X	X	X	X	X
Edit any items associated with the project or program	X	X	X	X	
Add and remove “Collaborators” users	X	X	X	X	
Add and remove “Administrators” users	X	X	X	X	
Modify the “Coordinator” user	X	X	X		
Modify the “Manager” user	X	X			

APPENDIX 8 – LIST OF APPLICATION LEVEL LOGS

The following is a list of recommended application level logs:

Authentication [AUTHN]
authn_login_success[:userid]
authn_login_successafterfail[:userid,retries]
authn_login_fail[:userid]
authn_login_fail_max[:userid,maxlimit(int)]
authn_login_lock[:userid,reason]
authn_token_delete[:appid]
authn_password_change[:userid]
authn_impossible_travel[:userid,region1,region2]
authn_token_created[:userid, entitlement(s)]
authn_token_revoked[:userid,tokenid]
authn_token_reuse[:userid,tokenid]

Authorization [AUTHZ]
authz_fail[:userid,resource]
authz_change[:userid,from,to]
authz_admin[:userid,event]

Excessive Use [EXCESS]
excess_rate_limit_exceeded[userid,max]

File Upload [UPLOAD]
upload_complete[userid,filename,type]
upload_stored[filename,from,to]
upload_validation[filename,(virusscan|imagemagick|...):(FAILED|incomplete|passed)]
upload_delete[userid,fileid]

Input Validation [INPUT]
input_validation_fail[:field,userid]

Malicious Behavior [MALICIOUS]
malicious_excess_404:[userid|IP,useragent]
malicious_extraneous:[userid|IP,inputname,useragent]
malicious_attack_tool:[userid|IP,toolname,useragent]
malicious_cors:[userid|IP,useragent,referer]
malicious_direct_reference:[userid|IP, useragent]

Privilege Changes [PRIVILEGE]
privilege_permissions_changed:[userid,file|object,fromlevel,tolevel]

Sensitive Data Changes [DATA]
sensitive_create:[userid,file|object]
sensitive_read:[userid,file|object]

sensitive_update:[userid,file|object]
sensitive_delete:[userid,file|object]

Sequence Errors [SEQUENCE]
sequence_fail:[userid]

Session Management [SESSION]
session_created:[userid]
session_renewed:[userid]
session_expired:[userid,reason]
session_use_after_expire:[userid]

System Events [SYS]
sys_startup:[userid]
sys_shutdown:[userid]
sys_restart:[userid]
sys_crash[:reason]
sys_monitor_disabled:[userid,monitor]
sys_monitor_enabled:[userid,monitor]

User Management [USER]
user_created:[userid,newuserid,attributes[one,two,three]]
user_updated:[userid,onuserid,attributes[one,two,three]]
user_archived:[userid,onuserid]
user_deleted:[userid,onuserid]

APPENDIX 9 – LIST OF SECURITY CONTROLS

(Separate document)