Risk Management

Software Procurement
Statement of Work

Revision 1

20 June 2022

RDIMS OTT_LSTL #6191157

TABLE OF CONTENTS

CHANGE RECORD

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

Rev	Section	Change Summary
1	General	Initial Revision

1 SCOPE

1.1 Purpose

1.1.1 The purpose of this Statement of Work (SOW) is to describe the requirements and work effort required from the Contractor by the Department of National Defence (DND) for the supply of items and services to meet the requirements for the provision and implementation of a risk management software.

1.2 Background

1.2.1 DND has developed multiple policies and directives on the management of 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.

1.2.2 The Director General Maritime Equipment Program Management (DGMEPM) and the Director General Air Equipment Program Management (DGAEPM) organizations currently do not have an integrated and robust tool to manage and track various hazard, risk and opportunity item types in line with the applicable policies and directives.

1.2.3 With the increased use of in-service contracts to support the management of projects and programs such as classes and fleets, there is a need to have a central common tool to consolidate and collaborate on the management of hazards, risks and opportunities.

1.2.4 Leveraging a cloud first strategy, this contract aims at procuring and deploying a risk management software meant to address the requirements detailed in the Software Requirements Specifications (SRS) at Appendix 2.

1.3 Intended Use

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

1.3.2 The intention is for the tool to be used by key players involved at all levels in materiel acquisition and support activities. This includes members of the Assistant Deputy Minister (Materiel), members of the Royal Canadian Navy, members of the Royal Canadian Air Force, and In-Service Support Contractors. Additional information on the various types of users has been provided in the SRS in Appendix 2.

1.3.3 It is intended that this tool will be deployed in DND's Microsoft Azure cloud environment within the Joint Defence Cloud Program (JDCP).

1.4 Acronyms and Definitions

1.4.1 Acronyms used in the SOW are contained in Appendix 1.

1.4.2 The following definitions are applicable to the SOW:

1.4.2.1 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 Contract, the cloud hub (also referred as "tenant") is centrally managed by the JDCP team.

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

1.4.2.2 Cloud Spoke: a virtual network that hosts workloads and connects to the central hub through virtual network peering. Within DND, the cloud spoke is managed by DND client organizations. For the context of this Contract, 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.

2 APPLICABLE DOCUMENTS

2.1 References

2.1.1 Government of Canada Specifications, Standards, and Publications:

	Reference	Promulgation	Accessibility of the Specification, Standard, or Publication
[A]	DND/CF Architecture Framework Volume 2 – DND/CF Views and Sub-Views	Version 1.8.1 25 Jan 2013	Intranet link
[B]	IMS 6002-1-1 Network Operating System Naming Conventions	2 Nov 2021	Intranet link
[C]	Information Technology Security Guide 33 (ITSG-33) – IT Security Risk Management: A Lifecycle Approach	1 Nov 2012	Internet Link
[D]	Information Technology Security Guide 22 (ITSG-22) – Baseline Security Requirements for Network Security Zones in the Government of Canada	1 June 2007	Internet Link
[E]	Information Technology Security Guide 38 (ITSG-38) – Network Security Zoning - Design Considerations for Placement of Services within Zones	1 May 2009	Internet Link

2.1.2 Other Specifications, Standards, and Publications:

	Reference	Promulgation	Accessibility of the Specification, Standard, or Publication
	Nil		

2.2 Order of Precedence

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

3 GENERAL REQUIREMENTS

3.1 Scope of Work

3.1.1 The Contractor must supply, deploy, configure and support a risk management software that meets all the requirements identified in this SOW and in the SRS included in Appendix 2.

3.2 Tasks

3.2.1 Provision of Project Management support

3.2.1.1 The Contractor must develop and deliver a Project Schedule in accordance with CDRL RM-PM-001 to elicit the activities and milestones required to complete the work described therein.

3.2.1.2 The Contractor must develop and deliver a Change Request in accordance with CDRL RM-PM-002 as requested by Canada, or if a proposed change affects one of the following baselines:

3.2.1.2.1 Schedule: the change affects the critical path such that the Go-Live milestone is delayed compared to the latest delivered Project Schedule;

3.2.1.2.2 Scope: the change affects the Contractor's ability to meet mandatory requirements of the SOW or the SRS, desirable requirements of the SOW or the SRS that were in scope, or to approve emergent work as defined in section 3.2.10;

3.2.1.2.3 Cost: the change will require additional funding beyond what has been authorized.

3.2.1.3 The Contractor must communicate to Canada any project risks and opportunities, especially as they related to the ability for the project to meet the schedule, scope and cost baselines.

3.2.1.4 The Contractor must coordinate and lead the meetings and design reviews listed in section 3.4, as well as additional meetings deemed necessary for the timely execution of the work.

3.2.1.5 The Contractor must develop and deliver a meeting agenda in accordance with CDRL RM-PM-004 to identify the topics of discussion and prepare stakeholders as to maximize the effectiveness of the meeting.

3.2.1.6 The Contractor must include any relevant documents, including presentation, in the submission of CDRL RM-PM-004.

3.2.1.7 The Contractor must develop and deliver a record of discussion in accordance with CDRL RM-PM-005 to capture the meeting minutes and identify resulting action items.

3.2.1.8 The Contractor must deliver meeting agenda and record of discussions for meetings and design reviews listed in section 3.4 and as requested by Canada.

3.2.2 Provision of the risk management software and licences

3.2.2.1 The Contractor must supply a Software Package in accordance with CDRL RM-SWR-101 that meets the SRS in Appendix 2.

3.2.2.2 The Contractor must develop and deliver the Software Deployment and Configuration Scripts in accordance with CDRL RM-SWR-102 to deploy the risk management software on DND's JDCP Microsoft Azure environment as well as configure the necessary databases.

3.2.2.3 The Contractor must supply any perpetual Software Licences in accordance with CDRL RM-SWR-103 to enable the usage as described in the SRS in Appendix 2.

3.2.2.4 The Contractor must supply any recurring Software Licences in accordance with CDRL RM-SWR-103 to enable the usage as described in the SRS in Appendix 2.

3.2.3 Provision of the risk management software technical data package

3.2.3.1 The Contractor must develop and deliver DND Architecture Views in accordance with CDRL RM-TDP-201.1 to CDRL RM-TDP-201.18.

3.2.3.2 The Contractor must develop and deliver a proposed Cloud Architecture Diagram in accordance with RM-TDP-202 to propose the cloud architecture required to support the application and database, including the naming of each virtual resources.

3.2.3.3 The Contractor must develop and deliver the Cloud Resources List in accordance with RM-TDP-203 to detail the specification of each virtual resource required, their naming, and their estimated cost per year.

3.2.3.4 The Contractor must develop and deliver the Application Programming Interface (API) Specifications in accordance with RM-TDP-204 to detail the protocol used to enable the API functions included in Appendix 2.

3.2.4 Provision of technical support to complete the Security Assessment & Authorization

3.2.4.1 The Contractor must provide support to DND in order to complete the Security Assessment & Authorization (SA&A) process including the successful completion of the interim Authority to Operate (iATO) and the Authority to Operate (ATO) milestones. This may include ad-hoc small reports required to gather the necessary information to support the process, participation in meetings with DND's IT Security team, as well as collecting objective quality evidence from the software.

3.2.4.2 The Contractor must provide support to DND in order to demonstrate how the risk management solution implements the recommended security controls of Ref [C] to achieve the target risk profile identified in the SRS at Appendix 2. A tailored list of minimum security controls is included in the SRS at Appendix 2.

3.2.4.3 The Contractor must develop and deliver the following deliverables to support the iATO submission:

3.2.4.3.1 Preliminary Security Architecture in accordance with CDRL RM-SAA-301;

3.2.4.3.2 Security Concept of Operations in accordance with CDRL RM-SAA-303;

3.2.4.3.3 Security Control Implementation Plan in accordance with CDRL RM-SAA-304 for the identified security controls[2];

3.2.4.3.4 Security Control Questionnaire for Priority Security Controls in accordance with CDRL RM-SAA-305;

3.2.4.3.5 The following DND Architecture Views in accordance with CDRL RM-SAA-201: OV-1, OV-5b, SV-1, SV-2.

3.2.4.4 The Contractor must develop and deliver the following deliverables to support the ATO submission:

3.2.4.4.1 Detailed Security Architecture in accordance with CDRL RM-SAA-302;

3.2.4.4.2 Security Concept of Operations in accordance with CDRL RM-SAA-303;

3.2.4.4.3 Security Test and Evaluation Plan in accordance with CDRL RM-SAA-306 for the identified security controls;

3.2.4.4.4 Security Test and Evaluation Report in accordance with CDRL RM-SAA-307 and associated objective quality evidence in accordance with CDRL RM-SAA-305 for the identified security controls;

3.2.4.4.5 Security Risk Traceability Matrix in accordance with CDRL RM-SAA-308 for the identified security controls;

3.2.4.4.6 Security Treat and Risk Assessment in accordance with CDRL RM-SAA-309 for the identified security controls;

3.2.4.4.7 The following DND Architecture Views in accordance with CDRL RM-SAA-201: OV-1, OV-2, OV-3, OV-4a, OV-4b, OV-5a, OV-5b, OV-7, SV-1, SV-2, SV-3, SV-4, SV-5, SV-6, SV-7, SV-8, SV-9.

3.2.4.5 The Contractor must liaise and collaborate with Canada in order to obtain the required information beyond the risk management software application itself in support of iATO and ATO documentation. Canada will be responsible to develop the Security Categorization Assessment Report (SCAR) and the necessary service desk related management plans.

3.2.4.6 The Contractor must provide third party audit reports to show compliance with the security standards for Software as a Service components (if applicable), as indicated in section 3.7.3 of the SRS at Appendix 2.

3.2.4.7 The Contractor must provide the application sample logs in accordance with CDRL RM-SAA-310.

3.2.5 Provision of technical support to deploy and configure the risk management software

[2] The minimum list of identified security controls are listed in the SRS at Appendix 2. Canada may add additional security controls to be included in the list of identified security controls.

3.2.5.1 The Contractor must provide technical support to DND in order to successfully deploy the risk management software, including the necessary databases, on the DND's (JDCP Microsoft Azure environment.

3.2.5.2 The Contractor must provide technical support to DND in order to integrate the risk management software with the Cloud Hub Microsoft Active Directory to manage role-based access control.

3.2.5.3 The Contractor must configure the risk management software to enable the requirements described in the SRS in Appendix 2.

3.2.6 Provision of technical support to test and verify the risk management software

3.2.6.1 The Contractor must provide technical support to DND in order to test and verify that the risk management software meets the SRS in Appendix 2.

3.2.6.2 The Contractor must provide a Requirements Verification Report in accordance with RM-QA-501 to ensure a fulsome compliance of all requirements.

3.2.6.3 The Contractor must collaborate with Canada in order to setup penetration testing, to be conducted upon completion of the Pre-Production Environment build. Penetration Testing will be conducted by Canada and require a freeze of the environment when conducted.

3.2.6.4 The Contractor must support Canada in addressing the deficiencies that will result from the penetration testing. Of note, this may result in risk assessing some deficiencies and therefore may not necessarily result in changing the build itself.

3.2.7 Provision of technical support to import data into the risk management software

3.2.7.1 The Contractor must import the data from the current Airworthiness Risk Management Information System (ARMIS) into the risk management software. This includes the development of necessary scripts to import data from the current ARMIS SQL database into the risk management software. Currently, there are under 3,000 risk items in the ARMIS database.

3.2.8 Provision of support to develop and deliver training

3.2.8.1 The Contractor must develop and deliver user manuals and aide memoires in accordance with CDRL RM-TRG-601.

3.2.8.2 The Contractor must develop and deliver training videos in accordance with CDRL RM-TRG-602.

3.2.8.3 The Contractor must develop and deliver training sessions in accordance with CDRL RM-TRG-603.

3.2.9 Provision of maintenance and support

3.2.9.1 The Contractor must provide maintenance and support services for licensed software as specified in the Contract.

3.2.10 Provision of support to execute emergent work

3.2.10.1 On an “as and when requests basis” through the Task Authorization process defined in the Contract, the Contractor must perform emergent work.

3.2.10.2 Emergent work constitutes any work that must be conducted by the Contractor to support the objective of the contract, but is not defined in the SOW or SRS. It can also constitute additional work requested by Canada beyond what has already been defined the SOW or SRS.

3.2.10.3 Emergent work must be accompanied by an approved Change Request, as defined in section 3.2.1. Emergent work may include:

3.2.10.3.1 Support to develop and deliver additional user manuals, aide memoires, training videos, and training sessions beyond those identified in CDRL RM-TRG-601, RM-TRG-602, and RM-TRNG-603; and

3.2.10.3.2 Support to develop and implement new capabilities beyond those identified in the SRS in Appendix 2.

3.3 Document Deliverables Compliance

3.3.1 All deliverables must be sent to the Technical Authority via email, unless otherwise agreed to by Canada.

3.3.2 Unless otherwise specified, all deliverables must comply with the following format:

3.3.2.1 All document deliverables must be provided in the unlocked normal Portable Document Format (PDF) and their native electronic version. In case of any discrepancies, the delivered PDF version will be held as the source of truth;

3.3.2.2 All PDF documents that are a digitized or scanned version of a physical copy must be text searchable using Optical Character Recognition (OCR);

3.3.2.3 Native “Office” documents (e.g. spreadsheet, charts, presentations, word processing documents) must be compatible with the Microsoft Office suite of applications.

3.3.2.4 All document deliverables must include Intellectual Property markings as specified in the Contract;

3.3.2.5 All document deliverables must include a title, a document revision number, a document revision date, and the full name of the person who approved its release;

3.3.2.6 All text-based documents with twenty (20) pages or more must include a table of contents; and

3.3.2.7 All document deliverables must be in English only except for user manuals and training materiel which must be provided in both English and French.

3.4 Meetings and Design Reviews

3.4.1 Program Review Meeting (PRM)

3.4.1.1 The Contractor must organize Program Review Meetings (PRMs) at a regular interval to be determined by the Contractor and Canada.

3.4.1.2 The goal of a PRM is to discuss the current status of the project, and address key issues and risks.

3.4.1.3 At a minimum, the PRM must cover the following items:

3.4.1.3.1 Current status and progression of the work (design, implementation, testing, training);

3.4.1.3.2 Key project issues and concerns requiring resolution or decision;

3.4.1.3.3 Key project risks (scope, schedule, and budget);

3.4.2 Preliminary Design Review (PDR)

3.4.2.1 The Contractor must organize a Preliminary Design Review (PDR).

3.4.2.2 The goal of the PDR is to demonstrate that the preliminary design meets all system requirements with acceptable risk and schedule constraints and establishes the basis for proceeding with detailed design. It will show that the correct design options have been selected, interfaces have been identified, and verification methods have been described.

3.4.2.3 The objectives of the PDR are to provide a high level of assurance that:

3.4.2.3.1 All system requirements have been validated, allocated, and are complete;

3.4.2.3.2 The proposed preliminary design is expected to meet the functional and performance requirements;

3.4.2.3.3 The proposed preliminary design shows sufficient maturity to proceed with the low level design;

3.4.2.3.4 The proposed preliminary design is verifiable and that the risks have been identified, characterized, and mitigated where appropriate; and

3.4.2.3.5 The proposed preliminary design can be developed and implemented within the schedule constraints, with an acceptable level of risk.

3.4.2.4 Concurrence from both the Contractor and Canada must be obtained in order to assess that the above listed PDR objectives have been achieved.

3.4.3 Critical Design Review (CDR)

3.4.3.1 The Contractor must organize a Critical Design Review (CDR).

3.4.3.2 The goal of the CDR is to demonstrate that the maturity of the design is appropriate to support proceeding with full-scale implementation, integration, and testing. CDR determines that the technical effort is on track to complete the system development meeting performance requirements within the identified schedule constraints.

3.4.3.3 The objectives of the CDR are to provide a high level of assurance that:

3.4.3.3.1 The system's baseline contains detailed specifications that can meet functional and performance requirements;

3.4.3.3.2 The detailed design has been satisfactorily reviewed by systems engineering and implementers (both Canada and Contractor), as well as security authorities;

3.4.3.3.3 The detailed design has sufficient details to proceed with the implementation and testing stage;

3.4.3.3.4 Planned Quality Assurance (testing) activities will establish adequate verification;

3.4.3.3.5 The detailed design fulfills the specifications established at PDR; and

3.4.3.3.6 The detailed design can be implemented within the schedule constraints, with an acceptable level of risk.

3.4.3.4 Concurrence from both the Contractor and Canada must be obtained in order to assess that the above listed CDR objectives have been achieved.

4 CONSTRAINTS

4.1 Work Location

4.1.1 All services will be performed at the Contractor's own offices or place of business, unless otherwise specified by the Technical Authority.

4.2 Travel

4.2.1 The authorization for all travel will be done via a DND 626 Task Authorization.

4.2.2 When travel is approved, the Contractor personnel authorized to travel will be reimbursed in accordance with the National Joint Council directives[3] for pre-authorized "travel and living" expenses incurred for travel outside a radius of seventy-five (75) kilometers from the location for the Contractor's facilities to the facilities identified by Canada.

4.3 Other limitations and constraints

4.3.1 The Contractor personnel providing the services must be independent of direct control by servants of Canada and are not in any respect employees or servants of Canada.

4.3.2 The Contractor must ensure that their personnel do not use either Government of Canada or DND designations, logos, or insignia on any business cards, cubicle/office signs, or written/electronic correspondence that in any manner lead others to perceive Contractor personnel as being an employee of Canada.

4.3.3 During the performance of the Contract, the Contractor and his personnel must not direct any departmental organizations, or any personnel of any third parties with whom Canada has or intends to contract, to perform any action.

4.3.4 At all times during the provision of the required services, the Contractor personnel are not to have access to any proprietary information including but not limited to financial information (including unit prices or rates) or technical information concerning any third parties with whom Canada has contracted or intends to contract, other than information that is in the public domain, (e.g. total value of contract(s) awarded). Proprietary technical information may be provided to Contractor personnel in the performance of the services.

4.3.5 All drawings, software codes, reports, data, documents, or materials, provided to the Contractor by Canada or produced by the Contractor personnel in providing services under the Contract remains the property of Canada.

4.3.6 All drawings, software codes, reports, data, documents, or materials, provided to the Contractor by Canada or produced by the Contractor personnel in providing services under the Contract must be used solely in support of this requirement.

4.3.7 The Contractor must safeguard the preceding information and materials from unauthorized use and must not release them to any third party, person, or agency external to DND without the express written permission of the Technical Authority.

[3] https://www.njc-cnm.gc.ca/en

4.3.8 Such information and material must be returned to the Technical Authority upon completion of the services or when requested by the Technical Authority.

5 SUPPORT PROVIDED BY CANADA

5.1 Government Furnished Information

5.1.1 Canada will provide access to the Specifications, Standards, and Publications listed in section 2.1.1.

5.2 Additional support provided by Canada

5.2.1 Canada will arrange for the necessary subject matter experts to meet with the Contractor, at the Contractor's request and as deemed necessary by Canada, to facilitate the timely execution of tasks described within this SOW, and answer any questions that may arise from the Contractor.

5.2.2 Canada will review every deliverable and provide comments, if any, within 10 working days of official receipt from the Contractor. Canada will advise the contractor if this review timeline must be extended.

APPENDIX 1 – ACRONYMS

ADM(IM)	Assistant Deputy Minister (Information Management)
API	Application Programming Interface
ATO	Authority To Operate
CDRL	Contract Data Requirement List
CONOPS	Concept of Operations
DGAEPM	Director General Air Equipment and Program Management
DGMEPM	Director General Maritime Equipment and Program Management
DID	Data Item Description
DIM Secur	Director Information Management Security
DND	Department of National Defense
DRMIS	Defense Resources Management Information System
DWAN	Defense Wide Area Network
iATO	Interim Authority To Operate
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
JDCP	Joint Defence Cloud Program
RCAF	Royal Canadian Air Force
RCN	Royal Canadian Navy
SA&A	Security Assessment & Authorization
SCAR	Security Categorization Assessment Report
SOW	Statement of Work
SRS	Software Requirements Specifications
ITSG	Information Technology Security Guide

APPENDIX 2 – SOFTWARE REQUIREMENTS SPECIFICATIONS (SRS)

(Separate document)

APPENDIX 3 – CONTRACT DATA REQUIREMENT LIST (CDRL)

CDRL No	DID No	Title	Submission Timing	Remarks
RM-PM-001	PM-001	Project Schedule	Initial submission no later than 14 working days after Contract award	Subsequent submissions if an update is required
RM-PM-002	PM-002	Change Request	As required	
RM-PM-004	PM-004	Meeting Agenda	No later than 1 working day before the meeting	
RM-PM-005	PM-005	Record of Discussion	No later than 3 working days after the meeting	
RM-SWR-101	SWR-101	Software Package	No later than 1 week prior to configuring the sandbox environment	Additional submissions as required.
RM-SWR-102	SWR-102	Software Deployment and Configuration Scripts	No later than 1 week prior to configuring the sandbox environment	Additional submissions as required.
RM-SWR-103	SWR-103	Software Licenses	As defined in the project schedule (to be delivered concurrently, with the software licenses)	
RM-TDP-201.1	TDP-201	OV-1 High-Level Operational Concept Graphic	No later than 3 weeks prior to PDR	Additional submissions if updated Required for iATO
RM-TDP-201.2	TDP-201	OV-2 Operational Node Connectivity Description	No later than 3 weeks prior to CDR	Additional submissions if updated Required for ATO
RM-TDP-201.3	TDP-201	OV-3 Operational Information Exchange Matrix	No later than 3 weeks prior to CDR	Additional submissions if updated Required for ATO
RM-TDP-201.4	TDP-201	OV-4a Organizational Relationship Chart	No later than 3 weeks prior to CDR	Additional submissions if updated Required for ATO
RM-TDP-201.5	TDP-201	OV-4b Organization to Role/Skill Model	No later than 3 weeks prior to CDR	Additional submissions if updated Required for ATO
RM-TDP-201.6	TDP-201	OV-5a Functional Model	No later than 3 weeks prior to CDR	Additional submissions if updated Required for ATO
RM-TDP-201.7	TDP-201	OV-5b Operational Process Model	No later than 3 weeks prior to PDR	Additional submissions if updated Required for iATO

RM-TDP-201.8	TDP-201	OV-7 Logical Data Model	No later than 3 weeks prior to CDR	Additional submissions if updated Required for ATO
RM-TDP-201.9	TDP-SV1	SV-1 Systems Interface Description	No later than 3 weeks prior to PDR	Additional submissions if updated Required for iATO
RM-TDP-201.10	TDP-201	SV-2 Systems Communications Description	No later than 3 weeks prior to PDR	Additional submissions if updated Required for iATO
RM-TDP-201.11	TDP-201	SV-3 Systems-Systems Matrix	No later than 3 weeks prior to CDR	Additional submissions if updated Required for ATO
RM-TDP-201.12	TDP-201	SV-4 Systems Functionality Description	No later than 3 weeks prior to CDR	Additional submissions if updated Required for ATO
RM-TDP-201.13	TDP-201	SV-5 Operational Activity to Systems Function Traceability Matrix	No later than 3 weeks prior to CDR	Additional submissions if updated Required for ATO
RM-TDP-201.14	TDP-201	SV-6 Systems Data Exchange Matrix	No later than 3 weeks prior to CDR	Additional submissions if updated Required for ATO
RM-TDP-201.15	TDP-201	SV-7 Systems Performance Parameters Matrix	No later than 3 weeks prior to CDR	Additional submissions if updated Required for ATO
RM-TDP-201.16	TDP-201	SV-8 Systems Evolution Description	No later than 3 weeks prior to CDR	Additional submissions if updated Required for ATO
RM-TDP-201.17	TDP-201	SV-9 Systems Technology Forecast	No later than 3 weeks prior to CDR	Additional submissions if updated Required for ATO
RM-TDP-201.18	TDP-201	SV-11 Physical Schema	No later than 3 weeks prior to CDR	Additional submissions if updated Required for ATO
RM-TDP-202	TDP-202	Cloud Architecture Diagram	No later than 3 weeks prior to PDR and CDR	Additional updates as required prior to configuring each environment (Dev, pre-production,

				production) and at the Go-Live milestone to reflect any changes.
RM-TDP-203	TDP-203	Cloud Resources List	No later than 3 weeks prior to CDR	Additional updates as required prior to configuring each environment (Dev, pre-production, production) and at the Go-Live milestone to reflect any changes.
RM-TDP-204	TDP-204	API Specifications	No later than 2 weeks prior to Penetration Testing	
RM-SAA-301	SAA-301	Preliminary Security Architecture	No later than 3 weeks prior to PDR	Required for iATO
RM-SAA-302	SAA-302	Detailed Security Architecture	No later than 3 weeks prior to CDR	Required for ATO
RM-SAA-303	SAA-303	Security Concept of Operations	Draft version no later than 3 weeks prior to PDR Final version no later than 3 weeks prior to CDR, updated prior to iATO and ATO submission as required	Required for iATO and ATO
RM-SAA-304	SAA-304	Security Control Implementation Plan	No later than 3 weeks prior to CDR, updated prior to iATO submission as required	Required for iATO
RM-SAA-305	SAA-305	Security Control Questionnaire for Priority Security Controls	No later than 3 weeks prior to CDR, updated prior to iATO submission as required	Required for iATO
RM-SAA-306	SAA-306	Security Test and Evaluation Plan	No later than 3 weeks prior to CDR, updated prior to ATO submission as required	Required for ATO
RM-SAA-307	SAA-307	Security Test and Evaluation Report	No later than 3 weeks prior to ATO submission	Required for ATO
RM-SAA-308	SAA-308	Security Risk Traceability Matrix	No later than 3 weeks prior to ATO submission	Required for ATO
RM-SAA-309	SAA-309	Security Treat and Risk Assessment	No later than 3 weeks prior to ATO submission	Required for ATO
RM-SAA-310	SAA-310	Security Monitoring Sample Logs	No later than the start of the Sandbox build	
RM-QA-501	QA-501	Requirements Verification Report	Completed report for final acceptance no later than 1 day prior to the Go-Live milestone.	

RM-TRG-601	TRG-601	User Manuals and Aide Memoires	No later than 2 weeks prior to the Go-Live milestone	
RM-TRG-602	TRG-602	Training Videos	No later than 2 weeks prior to the Go-Live milestone	
RM-TRG-603	TRG-603	Training Sessions	As agreed to for each training session	

APPENDIX 4 – DATA ITEM DESCRIPTIONS (DID)

A DID is only applicable within a SOW if it is called upon in the main SOW document and has an associated delivery schedule in the Appendix 3 – *Contract Data Requirement List* (CDRL).

Data Item Description

The following section defines the various blocks of information found on the Data Item Description (DID) forms:

BLOCK 1 – TITLE

The title of the data item for the DID.

BLOCK 2 – IDENTIFICATION NUMBER

The DID number, consisting of a sequential three-digit number and prefixed with an abbreviation code, to uniquely identify the DID.

BLOCK 3 – DESCRIPTION

Provides a general description of the data content requirements.

BLOCK 4 – CDRL IDENTIFICATION

Indicates the identification number for the Contract Data Requirement List.

BLOCK 5 – OFFICE OF PRIMARY INTEREST (OPI)

The office of primary interest for review, acceptance and/or approval of the data item.

BLOCK 6 – GIDEP APPLICABLE

An "X" indicates that the data is to be submitted by a Government organization or the Contractor to the Government/Industry Data Exchange Program (GIDEP). Otherwise the block is left blank.

BLOCK 7 – APPLICATION / INTERRELATIONSHIP

Provides the application details and interrelationship of the data item to other DIDs or documents.

BLOCK 8 – SOURCE

Indicates the Contract reference for the DID.

BLOCK 9 – APPLICABLE FORMS

Indicates any form associated with the DID.

BLOCK 10 – PREPARATION INSTRUCTIONS

Provides the preparation instructions, including format and content requirements for the data.

PM-001 Project Schedule

1. TITLE	2. IDENTIFICATION NUMBER
Project Schedule	**PM-001**

3. DESCRIPTION/PURPOSE

3.1 The Project Schedule (PS) must reflect the time-phased sequence of activities and milestones necessary for the successful completion of the project. The Project Schedule will be used to coordinate joint Contractor / DND activities and can be used to track the work status, as well as monitor project performance.

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL PM-001	Project Manager	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

No reference.

10.2 FORMAT

10.2.1. This deliverable must be prepared in the Contractor's format and must be compliant with the requirements cited in the "Document Deliverables Compliance" section of the SOW.

10.2.2. The Project Schedule must include a time scaled bar (Gantt) chart showing the work activities as they relate to time.

10.3 CONTENT

10.3.1. **Project Schedule Elements**

a. The Project Schedule must include elements (activities and milestones) necessary for the completion of the work described in the SOW including, but not limited to:
    i. Activities and milestones related to the work described in the SOW;
    ii. Deliverables identified in the SOW;
    iii. Elements and assumptions listed in this DID under para 10.3.3;
    iv. Any approved emergent work.
b. The Project Schedule must include elements based on discrete work activities;
c. Each activities of the Project Schedule must include the following:
    i. Identification number;
    ii. Title;
    iii. Responsible Organization (at a minimum: "Contractor" or "Canada");

iv. Baseline Duration;

v. Baseline Start Date;

vi. Baseline End Date;

vii. Actual Duration;

viii. Actual Start Date; and

ix. Actual End Date.

d. Each milestones of the Project Schedule must include the following:

i. Identification number;

ii. Title;

iii. Responsible Organization (at a minimum: "Contractor" or "Canada");

iv. Baseline Date; and

v. Actual Date.

10.3.2. **Project Schedule Reporting Requirements**

a. The Project Schedule must include appropriate titles and legends that define all symbols used on the schedule;

b. The Project Schedule must clearly indicate the date when the data was taken for the update. This "as of date" can be indicated either by a line extending from the appropriate point of the time scale and/or labelled in the legend;

c. The Project Schedule must clearly indicate relevant schedule assumptions. This includes the list of incorporated Change Requests, major design decisions, list and version of applicable SOW;

d. The Project Schedule must indicate dependencies between elements (predecessor and successor);

e. The Project Schedule must clearly identify elements (activities and milestones) on the critical path[4], including links between predecessor and successor for elements on the critical path;

f. Progress indications and planned or actual schedule slippage/accelerations of the current schedule should be clearly shown in relation to the baseline schedule; and

g. The Project Schedule can be submitted in multiple files to clearly show the above sections, however a consolidated Project Schedule, depicting the entire remaining scope of work to deploy and configure the risk management software, as an integrated activity, and presented in a single file must also be provided.

10.3.3. **Key Activities, Milestones, and Assumptions**

a. The following activities, milestones, and assumptions (listed in no particular order) must be included in the Project Schedule:

	Title	**Type**	**Responsible**	**Comment**
1	Deliverable RM-TDP-OV01	Activity	Contractor	Required prior to iATO and RFC submission, with sufficient time for Canada to review

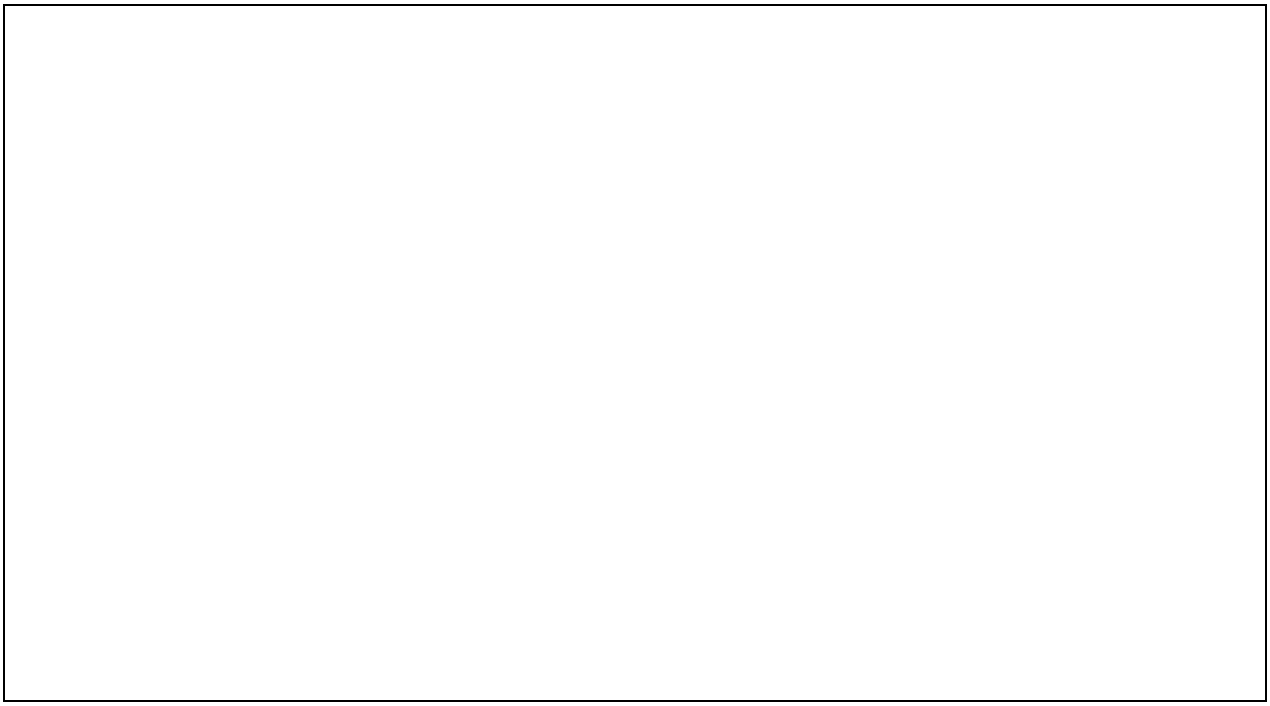
[4] The critical path is the longest sequence of activities in the task which must be completed on time for the task to complete on due date. An activity on the critical path cannot be started until its predecessor activity is complete; if it is delayed for a day, the entire project will be delayed for a day unless the activity following the delayed activity is completed a day earlier.

				and for the contractor to make adjustments if required.
2	Deliverable RM-TDP-OV05B	Activity	Contractor	Required prior to iATO and RFC submission, with sufficient time for Canada to review and for the contractor to make adjustments if required.
3	Deliverable RM-TDP-SV01	Activity	Contractor	Required prior to iATO and RFC submission, with sufficient time for Canada to review and for the contractor to make adjustments if required.
4	Deliverable RM-TDP-SV02	Activity	Contractor	Required prior to iATO and RFC submission, with sufficient time for Canada to review and for the contractor to make adjustments if required.
5	Concept of Operations (CONOPS)	Activity	Canada and Contractor	Required prior to iATO and RFC submission. Expected duration to produce is 1 month.
6	Security Categorization Assessment Report (SCAR)	Activity	Canada	Required prior to iATO and RFC submission. Expected duration to produce and obtain approval is 1 month, which should be done 1 month prior to the iATO submission milestone.
7	Security Categorization Assessment Report (SCAR) approval by the Director General	Milestone	Canada	Required prior to iATO and RFC submission. Expected timeline is 1 month after the completion of the SCAR (activity).
8	Security Control Questionnaire for Priority Security Controls	Activity	Canada and Contractor	Required prior to iATO and RFC submission. Expected duration to produce is 1.5 month.
9	RFC submission	Milestone	Canada	Submission of documents in support of the “Request for Change” process.
10	RFC assessment	Activity	Canada	Expected duration is 2 months
11	RFC approval	Milestone	Canada	
12	iATO submission	Milestone	Canada	Submission of documents and necessary Objective Quality Evidence to DND IT Security Team for assessment. This milestone should not occur until the sandbox environment is ready and the project is ready to move to the development and test environment.
13	iATO assessment	Activity	Canada (DIM Secur)	Expected duration is 1 month.
14	iATO	Milestone	Canada	
15	Security Controls Full Assessment	Activity	Canada and Contractor	Required prior to ATO submission. Expected duration to produce is 3 months
16	ATO submission	Milestone	Canada	Submission of documents and necessary Objective Quality Evidence to DND IT Security Team for assessment.
17	ATO assessment	Activity	Canada (DIM Secur)	Expected duration is 1 month.
18	ATO	Milestone	Canada	Requires approved RFC prior to.
19	Deliverable RM-TDP-201	Activity	Contractor	Required prior to any configuration of the cloud environment

20	Deliverable RM-TDP-202	Activity	Contractor	Required prior to any configuration of the cloud environment
21	Configuration (zoning) of the sandbox environment	Activity	Canada (JDCP)	Expected duration is 2 weeks.
22	Configuration of the sandbox environment	Activity	Canada and Contractor	Expected duration depends on the complexity of the cloud architecture proposed by the contractor (RM-TDP-201, RM-TDP-202).
23	Configuration (zoning) of the development and test environment	Activity	Canada (JDCP)	Expected duration is 2 weeks.
24	Configuration of the development and test environment	Activity	Canada and Contractor	Expected duration depends on the complexity of the cloud architecture proposed by the contractor (RM-TDP-201, RM-TDP-202)
25	Configuration (zoning) of the pre-production environment	Activity	Canada (JDCP)	Expected duration is 2 weeks. Requires a completed iATO prior to.
26	Configuration of the pre-production environment	Activity	Canada and Contractor	Expected duration depends on the complexity of the cloud architecture proposed by the contractor (RM-TDP-201, RM-TDP-202).
27	Configuration (zoning) of the production environment	Activity	Canada (JDCP)	Expected duration is 2 weeks.
28	Configuration of the production environment	Activity	Canada and Contractor	Expected duration depends on the complexity of the cloud architecture proposed by the contractor (RM-TDP-201, RM-TDP-202).
29	Utilization of production data in the Pre-Production Environment and Production Environment	Milestone	Canada	Requires the iATO approval prior to.
30	Testing and Validation	Activity	Contractor	
31	Acceptance by Canada of the completed Requirements Verification Report (RM-QA-501)	Milestone	Contractor	
32	Go-Live	Milestone	Contractor	
33	Initial Training Delivery	Activity	Contractor	

Activities required for Contractors to gain extended privilege access to the cloud environment (access to the back-end). Note: D365, DWAN accounts, and a DWAN workstations are required to access the front-end.

	Title	**Type**	**Responsible**	**Comment**
34	Obtain Security Clearance	Activity	Contractor	Required Level: SECRET.
35	Obtain approved Visit Clearance Request (VCR)	Activity	Contractor	Expected duration is 1 month. Requires approved Security Clearance.
36	Obtain DWAN and Defense 365 (D365) accounts	Activity	Canada	Expected duration is 2 weeks. Requires approved VCR
37	Obtain Azure Extended Privilege account	Activity	Canada	Expected duration is 1 months. Requires DWAN and D365 accounts.



PM-002 Change Request

1. TITLE	2. IDENTIFICATION NUMBER
Change Request	**PM-002**

3. DESCRIPTION/PURPOSE

3.1 The Change Request must detail the impact to project baselines to implement a proposed change. The Change Request will be used to make a formal decision, track the decision, and amend baselines as required.

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL PM-002	Project Manager	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

No reference.

10.2 FORMAT

10.2.1. This deliverable must be prepared in the contractor's format and must be compliant with the requirements cited in the "Document Deliverables Compliance" section of the SOW.

10.3 CONTENT

10.3.1. The Change Request **identification section** must include, at a minimum, the following:

a. A Change Request identification number;

b. A Change Request title; and

c. A problem statement describing what the change is meant to address.

10.3.2. The Change Request **options analysis section** must include, at a minimum, the following:

a. The list of possible options that were investigated including a short description for each option; and

b. The recommended best option with justification for its selection.

10.3.3. The Change Request **impact section** must include, at a minimum, the following:

a. Impact to the project's schedule baseline, as it relates to the latest approved Project Schedule specifically if the change impacts the critical path and the "Go-Live" milestone;

b. Impact to the project's scope baseline, as it relates to mandatory requirements and desirable requirements that were previously agreed to be part of the scope;

c. Impact to the project's cost baseline, as it relates to the estimate provided in the proposal, and the current amount authorized via the Task Authorization; and

d. Additional project risks or opportunities, or changes to existing project risks and opportunities, resulting from the change.

10.3.4. The Change Request **approval section** must include, at a minimum, the following**:**

a. Recommendation from the Contractor to proceed or not proceed with the change;

b. Name, designation, and signature of the member who developed the change request;

c. Name, designation, and signature of the Contractor's Project Manager; and

d. Name, designation, and signature of Canada's Project Manager.

Note: the approval of a change request that would include a change to the cost baseline does not mean the Contractor is automatically authorized to spend additional funds beyond the amount stated in the Task Authorization. Any Change Request that would necessitate changes to the Contract or Task Authorization must be done formally via the Contracting Authority. An approved Change Request would serve as the basis to request the necessary changes to the Contract or Task Authorization.

PM-004 Meeting Agenda

1. TITLE	2. IDENTIFICATION NUMBER
Meeting Agenda	**PM-004**

3. DESCRIPTION/PURPOSE

3.1 The meeting agenda serves to inform stakeholders on topics to be discussed at a future meeting as to be prepared and consequently increase the meeting efficiency.

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL PM-004	Project Manager	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

No reference.

10.2 FORMAT

10.2.1. This deliverable must be prepared in the contractor's format and must be compliant with the requirements cited in the "Document Deliverables Compliance" section of the SOW.

10.3 CONTENT

10.3.1. The meeting agenda must contain, at a minimum, the following:

a. Meeting title;

b. Data and time of the meeting;

c. Location of the meeting;

d. Expected participants names and roles (both required and optional);

e. Meeting topics.

10.3.2. The meeting agenda must be accompanied with any relevant documentation (such as presentation materiel) when applicable.

PM-005 Record of Discussion

1. TITLE	2. IDENTIFICATION NUMBER
Record of Discussion	**PM-005**

3. DESCRIPTION/PURPOSE

3.1 The record of discussion serves to capture the meeting minutes and identify resulting action items.

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL PM-005	Project Manager	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

No reference.

10.2 FORMAT

10.2.1. This deliverable must be prepared in the contractor's format and must be compliant with the requirements cited in the "Document Deliverables Compliance" section of the SOW.

10.3 CONTENT

10.3.1. The meeting agenda must contain, at a minimum, the following:

a. Meeting title;

b. Data and time of the meeting;

c. Location of the meeting;

d. Participants names and roles;

e. Meeting topics.

f. Relevant record of discussion for each topic.

g. Action items for each topic with an assigned action item owner and due date.

10.3.2. The record of discussion must be accompanied with any relevant documentation (such as presentation materiel used during the meeting) when applicable.

SWR-101 Software Package

1. TITLE	2. IDENTIFICATION NUMBER
Software Package	**SWR-101**

3. DESCRIPTION/PURPOSE

3.1 This software package forms the core component of the software solution. These are the files that will be uploaded on the Cloud Spoke environment to execute the software solution. This package will form an integral part of the technical data package and will be under configuration control.

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL SWR-101	Lifecycle Application Manager	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

No reference.

10.2 FORMAT

10.2.1. The software package must be delivered electronically such that Canada can load the software in the Cloud Spoke environment.

10.2.2. All documentation associated with this deliverable must be prepared in the Contractor's format and must be compliant with the requirements cited in the "Document Deliverables Compliance" section of the SOW.

10.3 CONTENT

10.3.1. The software package must contain all of the required files that can be deployed in a cloud environment to execute the risk management software.

SWR-102 Software Deployment and Configuration Scripts

1. TITLE	2. IDENTIFICATION NUMBER
Software Deployment and Configuration Scripts	**SWR-102**

3. DESCRIPTION/PURPOSE

3.1 This deployment and configuration scripts package must contain the necessary files that will be executed on the Cloud Spoke to load, deploy and configure the software solution including associated databases. This package will form an integral part of the technical data package and will be under configuration control.

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL SWR-102	Lifecycle Application Manager	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

No reference.

10.2 FORMAT

10.2.1. The software package must be delivered electronically such that Canada can load the software in the Cloud Spoke environment.

10.2.2. All documentation associated with this deliverable must be prepared in the contractor's format and must be compliant with the requirements cited in the "Document Deliverables Compliance" section of the SOW.

10.3 CONTENT

10.3.1. The software package must contain all of the scripts necessary to fully load, deploy, and configure the risk management software solution and associated databases in the Cloud Spoke.

10.3.2. The software package must contain the necessary scripts to deploy the solution using infrastructure as code.

10.3.3. The software package must be accompanied by instructions on how to run the various scripts.

SWR-103 Software Licence

1. TITLE	2. IDENTIFICATION NUMBER
Software Licence	**SWR-103**

3. DESCRIPTION/PURPOSE

3.1 The purpose of this deliverable is to capture the necessary information related to the acquisition of software licenses related to the acquisition, operation, and ongoing maintenance of the risk management software.

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL SWR-103	Lifecycle Application Manager	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

No reference.

10.2 FORMAT

This deliverable must be prepared in the contractor's format and must be compliant with the requirements cited in the "Document Deliverables Compliance" section of the SOW.

10.3 CONTENT

10.3.1. The licence description section must include, at a minimum, the following:

a. Licence title;

b. The software, product, or services associated with the licence;

c. The company responsible for the issuance and renewal (as applicable) of the licence;

d. Description of the licence including its applicability and benefits;

e. Any restrictions associated with the licence (such as number of users);

f. Validity period for the licence;

g. Total cost to Canada for the licence for the validity period;

10.3.2. The licence instructions section must include, at a minimum, the following:

a. Detailed instructions on how to apply the licence to the software;

b. Detailed instructions on how to exchange the licence between users, if applicable (if the licence is per user).

10.3.3. This deliverable must include any additional information or instructions relevant to the use of the licence by Canada.

TDP-201 DND Architecture View

1. TITLE	2. IDENTIFICATION NUMBER
DND Architecture View	**TDP-201**

3. DESCRIPTION/PURPOSE

3.1 All DND Architecture Views must be developed in line with the specifications of Ref [A]. These documents will be part of the configuration baseline.

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL TDP-201	Lifecycle Application Manager	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

Ref [A] DND/CF Architecture Framework Volume 2 – DND/CF Views and Sub-Views

10.2 FORMAT

This deliverable must be prepared in the contractor's format and must be compliant with the requirements cited in the "Document Deliverables Compliance" section of the SOW.

10.3 CONTENT

10.3.1. The content of this deliverable, along with examples, is detailed in Ref [A].

TDP-202 Cloud Architecture Diagram

1. TITLE	2. IDENTIFICATION NUMBER
Cloud Architecture Diagram	**TDP-202**

3. DESCRIPTION/PURPOSE

3.1 This document must detail the cloud architecture required to host and support the software solution, including the naming of each virtual resources. This diagram will be used by the cloud system administrator to build and configure the cloud environment to support the software solution. This diagram will also form an integral part of the technical data package that will be under configuration control.

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL TDP-202	Cloud System Administrator	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

Ref [B] IMS 6002-1-1 Network Operating System Naming Convention

10.2 FORMAT

This deliverable must be prepared in the contractor's format and must be compliant with the requirements cited in the "Document Deliverables Compliance" section of the SOW.

10.3 CONTENT

10.3.1. The cloud architecture diagram must depict the complete cloud architecture required to host and support the risk management software solution, including databases and interface to other systems and components.

10.3.2. At a minimum, each component listed in TDP-202 must be included in the cloud architecture diagram.

10.3.3. This deliverable must show the various network zones.

10.3.4. The selection of network zones, and the placement of components within, must be compliant with Refs [D] and [E].

10.3.5. This deliverable must be based on Microsoft Azure cloud components, and as such utilise Microsoft Azure icons to represent those components.

10.3.6. The naming of each cloud component must be compliant with Ref [B].

TDP-203 List of Cloud Resources

1. TITLE	2. IDENTIFICATION NUMBER
List of Cloud Resources	**TDP-203**

3. DESCRIPTION/PURPOSE

3.1 This document must detail each cloud resources identified in TDP-201 that is required to host and support the software solution, including the naming of each virtual resources. This list will be used by the cloud system administrator to build and configure the cloud environment to support the software solution. This diagram will also form an integral part of the technical data package that will be under configuration control.

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL TDP-203	Cloud System Administrator	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

Ref [B] IMS 6002-1-1 Network Operating System Naming Convention

10.2 FORMAT

This deliverable must be prepared in the contractor's format and must be compliant with the requirements cited in the "Document Deliverables Compliance" section of the SOW.

10.3 CONTENT

10.3.1. The list of cloud resource must include the comprehensive list of virtual resources required to host and support the risk management software solution, including databases.

10.3.2. This deliverable must be based on Microsoft Azure cloud components, and as such utilise Microsoft Azure resource names.

10.3.3. The naming of each cloud component must be compliant with Ref [B].

10.3.4. For each virtual resources, the following must be provided at a minimum:

a. Naming of the component, in accordance with Ref [B];

b. Name and Type of Microsoft Azure virtual resource;

c. Minimum specifications required for the virtual resource (for example: amount of core and RAM);

d. Short description of its purpose in support of the risk management software;

e. Assumption on its monthly and yearly usage; and

f. Estimated monthly and yearly cost based on the assumed usage.

10.3.5. Where it would be of best value for money to Canada to make usage of reserved instances to lower the operating cost, this must be identified as such and the total price to purchase the reserve instance must be indicated in addition to the monthly and yearly cost estimate.

10.3.6. The deliverable must include a total summary estimated monthly and yearly cost for the resources listed.

TDP-204 Application Programming Interface Specifications

1. TITLE	2. IDENTIFICATION NUMBER
Application Programming Interface Specifications	**TDP-204**

3. DESCRIPTION/PURPOSE

3.1 This document must detail the protocol such that DND can use the Application Programming Interface (API) to interconnect the software solution with other solutions.

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL TDP-204	Lifecycle Application Manager	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

Nil

10.2 FORMAT

This deliverable must be prepared in the contractor's format and must be compliant with the requirements cited in the "Document Deliverables Compliance" section of the SOW.

10.3 CONTENT

10.3.1. The deliverable must describe the API protocol used to interface with the risk management software.

10.3.2. The deliverable must include details about connectivity requirement in order for an external software to connect with the risk management software and execute functions available through the API.

10.3.3. The deliverable must detail security protocols in place to restrict access to the API only to approved external applications.

10.3.4. The deliverable must include, for each function available through the API:

a. The name of the function;

b. The specifications on how to use the API to perform the function; and

c. An example of code where the function is being used.

SAA-301 Preliminary Security Architecture

1. TITLE	2. IDENTIFICATION NUMBER
High Level Security Architecture	**SAA-301**

3. DESCRIPTION/PURPOSE

3.1 This document must document the preliminary (high level) security architecture of the solution. This document is required for the iATO within the SA&A process.

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL SAA-301	Information Systems Security Officer	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

Refs [C] ITSG-33, [D] ITSG-22, [E] ITSG-38

10.2 FORMAT

This deliverable must be prepared in the contractor's format and must be compliant with the requirements cited in the "Document Deliverables Compliance" section of the SOW.

10.3 CONTENT

10.3.1. The deliverable must include a description of the operational and systems views required for iATO.

10.3.2. The deliverable must include details on how the IT zoning will comply with Ref [D] and [E].

10.3.3. The deliverables must include details on the intended boundary protection devices/services.

10.3.4. The deliverable must include details on how the application intends on controlling the user and data flows of information within the system and between interconnected systems. This includes, but not limited to:

a. Keeping Controlled Goods from being transmitted in the clear to the Internet;

b. Blocking outside traffic that claims to be from within the organization;

c. Restricting web requests to the Internet that are not from the internal web proxy server; and

d. Limiting information transfers between organizations based on data structures and content.

SAA-302 Detailed Security Architecture

1. TITLE	2. IDENTIFICATION NUMBER
Detailed Security Architecture	**SAA-302**

3. DESCRIPTION/PURPOSE

3.1 This document must document the detailed security architecture of the solution. This document is required for the ATO within the SA&A process.

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL SAA-302	Information Systems Security Officer	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

Refs [C] ITSG-33, [D] ITSG-22, [E] ITSG-38

10.2 FORMAT

This deliverable must be prepared in the contractor's format and must be compliant with the requirements cited in the "Document Deliverables Compliance" section of the SOW.

10.3 CONTENT

10.3.5. The deliverable must include a description of the operational and systems views required for ATO.

10.3.6. The deliverable must include details on how the IT zoning will comply with Ref [D] and [E].

10.3.7. The deliverables must include details on the intended boundary protection devices/services.

10.3.8. The deliverable must include details on how the application intends on controlling the user and data flows of information within the system and between interconnected systems. This includes, but not limited to:

a. Keeping Controlled Goods from being transmitted in the clear to the Internet;

b. Blocking outside traffic that claims to be from within the organization;

c. Restricting web requests to the Internet that are not from the internal web proxy server;

d. Limiting information transfers between organizations based on data structures and content;

e. Detecting and preventing unauthorized exfiltration of information; and

f. Use of Role-Based Access Control / Authorization-Based Access Control (to achieve a least privilege access based on a need to know).

10.3.9. The deliverable must include details related to vulnerability management.

10.3.10. The deliverable must include details related to identity and access management (including multi-factor authentication where applicable).

10.3.11. The deliverable must include details related to logging (types of logs, log collection and monitoring).

10.3.12. The deliverable must include details related to incident detection and response.

10.3.13. The deliverable must include details related to data loss prevention.

10.3.14. The deliverable must include details on data and application integrity will be assured within the solution.

10.3.15. The deliverable must include details on how encryption will be applied to data at rest, in transit, and in process.

SAA-303 Security Concept of Operations

1. TITLE	2. IDENTIFICATION NUMBER
Concept of Operations	**SAA-303**

3. DESCRIPTION/PURPOSE

3.1 This document must provide a summary on the application is intended to be operated from the perspective of information security. This document is required for iATO and ATO within the SA&A process

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL SAA-303	Information Systems Security Officer	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

Ref [C] ITSG-33

10.2 FORMAT

The template for this deliverable will be provided by Canada.

10.3 CONTENT

10.3.1. The deliverable must include, at a minimum, the following sections:

a. Introduction;
b. Security Categorization Report Summary (to be provided by Canada);
c. Roles and Responsibilities (to be provided by Canada);
d. System Description, which includes:
    i. Operation Views;
    ii. System Views; and
    iii. Server Description.
e. Priority Baseline Security Description, which includes:
    i. Vulnerability Management;
    ii. Identity and Access Management;
    iii. Logging;
    iv. Incident Detection and Response;
    v. Data Loss Prevention; and
    vi. Zoning Requirements.

SAA-304 Security Control Implementation Plan

1. TITLE	2. IDENTIFICATION NUMBER
Security Control Implementation Plan	**SAA-304**

3. DESCRIPTION/PURPOSE

3.1 This document must detail the plan to implement the identified security controls. This document is required for the SA&A process.

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL SAA-304	Information Systems Security Officer	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

Ref [C] ITSG-33

10.2 FORMAT

This deliverable must be prepared in the contractor's format and must be compliant with the requirements cited in the "Document Deliverables Compliance" section of the SOW.

10.3 CONTENT

10.3.1. The deliverable must list the identified security controls and include a description on how and when they would be implemented in the resulting solution.

SAA-305 Security Control Questionnaire for Priority Security Control

1. TITLE	2. IDENTIFICATION NUMBER
Security Control Questionnaire for Priority Security Control	**SAA-305**

3. DESCRIPTION/PURPOSE

3.1 This document must detail the intended implementation for a select set of priority security controls in support of the iATO within the SA&A process.

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL SAA-305	Information Systems Security Officer	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

Ref [C] ITSG-33

10.2 FORMAT

The template for this deliverable will be provided by Canada (available on DND intranet).

10.3 CONTENT

10.3.1. The deliverable must include the relevant evidence to be provided, as indicated in the template document.

SAA-306 Security Test and Evaluation Plan

1. TITLE	2. IDENTIFICATION NUMBER
Security Test and Evaluation Plan	**SAA-306**

3. DESCRIPTION/PURPOSE

3.1 This document must detail the test and evaluation plan for the identified security controls. This document is required as part of the SA&A process.

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL SAA-306	Information Systems Security Officer	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

Nil

10.2 FORMAT

This deliverable must be prepared in the contractor's format and must be compliant with the requirements cited in the "Document Deliverables Compliance" section of the SOW.

10.3 CONTENT

10.3.1. The deliverable must describe how compliance to each identified security control is expected to be tested and what are the expected results.

SAA-307 Security Test and Evaluation Report

1. TITLE	2. IDENTIFICATION NUMBER
Security Test and Evaluation Report	**SAA-307**

3. DESCRIPTION/PURPOSE

3.1 This document must detail the result, based on the security test and evaluation plan, for the identified security controls. This document is required for ATO as part of the SA&A process.

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL SAA-307	Information Systems Security Officer	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

Nil

10.2 FORMAT

This deliverable must be prepared in the contractor's format and must be compliant with the requirements cited in the "Document Deliverables Compliance" section of the SOW.

10.3 CONTENT

10.3.1. The deliverable must document the results from the compliance tests and evaluations, as defined in the Security Test and Evaluation Plan.

10.3.2. When required, objective quality evidence of the test results must be attached to the deliverable.

SAA-308 Security Risk Traceability Matrix

1. TITLE	2. IDENTIFICATION NUMBER
Security Risk Traceability Matrix	**SAA-308**

3. DESCRIPTION/PURPOSE

3.1 This document must detail the final implementation of the security controls. This document is required for ATO as part of the SA&A process.

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL SAA-308	Information Systems Security Officer	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

Nil

10.2 FORMAT

This deliverable must be prepared in the contractor's format and must be compliant with the requirements cited in the "Document Deliverables Compliance" section of the SOW.

10.3 CONTENT

10.3.1. The deliverable must list the security controls that have been implemented with the following information:

a. The security control identification code and title; and

b. Objective Quality Evidence.

10.3.2. The deliverable must list the security controls that have not been implemented with the following information:

a. The security control identification code and title;

b. The justification as to why it has been tailored out, or the planned implementation phase or target date.

SAA-309 Security Treat and Risk Assessment

1. TITLE	2. IDENTIFICATION NUMBER
Security Treat and Risk Assessment	**SAA-309**

3. DESCRIPTION/PURPOSE

3.1 This document must assess the residual security risk based on the security architecture and security control implementation. This document will serve to inform the DND IT Security Authority on the residual risk, which will ultimately be presented to the Operational Authority for acceptance. This document is required for ATO as part of the SA&A process.

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL SAA-309	Information Systems Security Officer	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

National Defence Security Orders and Directives (NDSODs)

10.2 FORMAT

This deliverable must be prepared in the contractor's format and must be compliant with the requirements cited in the "Document Deliverables Compliance" section of the SOW.

10.3 CONTENT

10.3.1. The deliverable must include a summary report of the results of the injury assessment.

10.3.2. The deliverable must include, for each risk item:

a. A short description;

b. The level of expected injury as they relate to confidentiality, integrity, and availability (likelihood, impact and resulting risk index for each);

c. The rationale for attributing the levels of injury.

10.3.3. The security risk assessment must be conducted in accordance with NDSODs Chapter 3 (Security Risk Management) and 7 (IT Security).

10.3.4. The security risk assessment should make use of the Harmonized Threat Risk Assessment Methodology[5] (TRA-1) as developed by the Canadian Centre for Cyber Security.

[5] https://cyber.gc.ca/en/guidance/harmonized-tra-methodology-tra-1

SAA-310 Security Monitoring Sample Logs

1. TITLE	2. IDENTIFICATION NUMBER
Security Monitoring Sample Logs	**SAA-310**

3. DESCRIPTION/PURPOSE

3.1 This deliverable must provide concrete examples of application logs that will be generated, with explanation on what would or wouldn't be normal, such that the security monitoring team can establish a proper set of rules.

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL SAA-310	Information Systems Security Officer	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

Nil

10.2 FORMAT

This deliverable must be prepared in the contractor's format and must be compliant with the requirements cited in the "Document Deliverables Compliance" section of the SOW.

10.3 CONTENT

10.3.1. The deliverable must include example logs for each selected application log item.

10.3.2. For each item, examples and explanations must be provided to define what is considered a normal event, and what would constitute a security incident.

QA-501 Requirements Verification Report

1. TITLE	2. IDENTIFICATION NUMBER
Requirements Verification Report	**QA-501**

3. DESCRIPTION/PURPOSE

3.1 This document must detail the cloud architecture required to host and support the software solution, including the naming of each virtual resources. This diagram will be used by the cloud system administrator to build and configure the cloud environment to support the software solution. This diagram will also form an integral part of the technical data package that will be under configuration control.

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL QA-501	Project Manager	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

Appendix 2 - SRS

10.2 FORMAT

This deliverable must be prepared in the contractor's format and must be compliant with the requirements cited in the "Document Deliverables Compliance" section of the SOW.

10.3 CONTENT

10.3.1. For each requirement listed in the SRS at Appendix 2, the following must be provided at a minimum:

a. Requirement number;
b. Requirement statement;
c. Requirement type as follow:
    i. Mandatory;
    ii. Desirable included in the scope;
    iii. Desirable not included in the scope; or
    iv. Statement or Header (not a requirement).
d. Plan to verify the requirement;
e. Requirement verification Status as follow:
    i. Not verified;
    ii. Verified Incorrect;
    iii. Verified Correct; or

iv. Waived.

f. Date Canada verified the requirement;

g. Name of the member (within Canada) who verified the requirement; and

h. Additional comments (such as reason why the requirement was verified incorrect, or was waived).

10.3.2. The deliverable must include a final approval section with the following:

a. Name, designation, and signature of the Contractor's Project Manager confirming that all requirements have been verified correct or waived; and

b. Name, designation, and signature of Canada's Project Manager confirming that all requirements have been verified correct or waived, thus accepting the deliverable.

TRG-601 User Manuals and Aide Memoires

1. TITLE	2. IDENTIFICATION NUMBER
User Manuals and Aide Memoires	**TRG-601**

3. DESCRIPTION/PURPOSE

3.1 These deliverables will from the core references for training and software usage, both for administrators and end-users.

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL TRG-601	Lifecycle Application Manager	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

Appendix 2 - SRS

10.2 FORMAT

10.2.1. This deliverable must be prepared in the contractor's format and must be compliant with the requirements cited in the "Document Deliverables Compliance" section of the SOW.

10.2.2. All user manuals and aide memoires must be bilingual. This can be achieved by providing one copy that contains the same content in both French and English, or two copies (one in French and one in English).

10.2.3. The PDF version of all user manuals and aide memoires must be WCAG 2.0[6] compliant. The compliance verification can be done using a free PDF accessibility checker[7].

10.3 CONTENT

10.3.3. At a minimum, the following must be provided:

Item	Target Audience	Content description
Technical Manual	Lifecycle Application Manager, Cloud System Administrator	It must describe the various modules and components of the risk management software solution, as well as components required to host and support the software solution (such as databases and other interfaces). This manual can be supported, and reference, diagrams and other documents produced and delivered under the project. The purpose of the technical manual is to allow the digital support team to investigate issues, allow them to re-deploy the software as required, allow them to install updates, and allow them to integrate the software solution with other applications.

[6] Web Content Accessibility Guidelines (WCAG) 2.0 https://www.w3.org/TR/WCAG20/
[7] Free PDF Accessibility Checker (PAC) https://www.access-for-all.ch/en/pdf-accessibility-checker.html

Administrative Manual	Administrative users	It must include key administrative functions such the management of role based access control and other elevated privilege functions within the risk management software. The purpose of the administrative manual is to allow administrative users to perform their elevated privilege functions.
Risk and Opportunity Aide Memoires	End-users	One aide memoire for each type of risk, opportunity, notification, and notice. Each aide memoire must include the main DND reference standards and directives associated with the type of risk and opportunity; describes each field and associated choices, and describes the lifecycle (status) of the risk and opportunity. The purpose of those aide memoires is to be of quick reference for end-users when filling out a new, or editing an existing, risk or opportunity item.

TRG-602 Training Videos

1. TITLE	2. IDENTIFICATION NUMBER
Training Videos	**TRG-602**

3. DESCRIPTION/PURPOSE

3.1 These deliverables will from the core references for training and software usage, both for administrators and end-users.

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL TRG-602	Lifecycle Application Manager	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

Appendix 2 - SRS

10.2 FORMAT

10.2.1. This deliverable must be prepared in the contractor's format and must be compliant with the requirements cited in the "Document Deliverables Compliance" section of the SOW.

10.2.2. All training videos must be bilingual. This must be achieved by providing two copies of the training video (one in French and one in English).

10.2.3. All training videos must be WCAG 2.0[8] Level AA compliant. More specifically, this means that close captioning must be available.

10.3 CONTENT

10.3.4. At a minimum, the following must be provided:

Item	Target Audience	Content description
Introduction to the Risk Management Software	All end-users	It must provide the following: a. Overview of the key capabilities and features of the risk management software; **Identity & Access** b. Demonstration on how to access the risk management application; c. Overview of the key user roles and their associated restrictions; **Risk Registry**

[8] Web Content Accessibility Guidelines (WCAG) 2.0 https://www.w3.org/TR/WCAG20/

		d. Demonstration on how to access and search the registry; e. Demonstration on how to extract data from the registry; f. Demonstration on how to save registry search parameters; **Projects and Programs** g. Demonstration on how to create a project or program; **Risks and Opportunities** h. Overview of the different types of risks and opportunities, and their purpose; i. Demonstration on how to create a risk and opportunity item; j. Demonstration on how to create and manage action items associated with risk and opportunity item; k. Overview of the lifecycle of a risk and opportunity item (including different status); **Security** l. Overview on the security beyond the risk management software, specifically on how it ensures the confidentiality, integrity, and availability of the data generated and stored by the risk management software; **Other** m. Demonstration of other capabilities that would benefit the end-user adopting and using the risk management software.
Managing Airworthiness Risk Items	Air Force end-users	It must provide the following: a. Overview of the different types of airworthiness risk and notifications, and their purpose; b. Demonstration on how to create hazard, risk and notification items as it relates to airworthiness.

TRG-603 Training Sessions

1. TITLE	2. IDENTIFICATION NUMBER
Training Sessions	**TRG-603**

3. DESCRIPTION/PURPOSE

3.1 These deliverables will form the core references for training and software usage, both for administrators and end-users.

4. CDRL IDENTIFICATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE	6. GIDEP APPLICATION
CDRL TRG-603	Lifecycle Application Manager	N/A

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format, content and preparation instructions.

8. SOURCE	9. APPLICABLE FORMS
CDRL	N/A

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS

Appendix 2 - SRS

10.2 FORMAT

10.2.1. This deliverable must be prepared in the Contractor's format and must be compliant with the requirements cited in the "Document Deliverables Compliance" section of the SOW.

10.2.2. The delivery location of training sessions will be determined by Canada and the Contractor. It can be a mix of in-class sessions and online delivery using Microsoft Teams.

10.2.3. The Contractor may propose the number (frequency) of training sessions based on a maximum number of participants per session.

10.2.4. The scheduling of training sessions must be agreed to by the Contractor and Canada.

10.3 CONTENT

10.3.1. At a minimum, the following training sessions must be provided:

Session	Target Audience	Content description
Administrative Training Session	Administrative Users	The administrative training session must complement the Administrative Manual, and provide initial training for administrative users on how to conduct the functions requiring elevated privileges. Estimated total number of participants: 20
Navy End-User Training Session	Navy End-Users	The end-user training session must complement the introduction video and provide initial training for various Navy end-users. Estimated total number of participants: 100

Air Force End-User Training Session	Air Force End-Users	The end-user training session must complement the introduction video and provide initial training for various Air Force end-users. Estimated total number of participants: 200