NCIA/ACQ/2023/07184
11 August 2023

To : See Distribution List

Subject : **BOA PLUS INVITATION FOR BID – IFB-CO-115759-DAMS-WCM AMENDMENT 2**

Provision of DIGITAL ASSET AND WEB CONTENT MANAGEMENT SYSTEM (DAMS-WCM)

Responses to Clarification Requests – Release #2

Reference(s) :

A. BC-D(2018)0004-FINAL BC Budget Procurement Guidance dated 16 January 2018
B. NCIA/ACQ/2023/06936 - NOI-IFB-CO-115759-DAMS-WCM dated 02 June 2023
C. NCI Agency Invitation for Bids (IFB), NCIA/ACQ/2023/07137 dated 20 July 2023
D. NOI-IFB-CO-115759-DAMS-WCM Amd 1 – Clarification Request Release 1 dated 27 July 2023

Dear Sir/Madam,

1. The purpose of this Amendment 2 to IFB-CO-115759-DAMS-WCM is to
   a. provide all Prospective Bidders with the responses to the additional questions received from potential bidders.
   b. To modify requirement A.1.19.7 in Book II - Part IV - Statement of Work

2. By virtue of this Amendment 2, above document replaces and supersedes previous version issued in the context of IFB-CO-115759-DAMS-WCM.

3. The reference for this IFB is IFB-CO-115759-DAMS-WCM. All correspondence related to this IFB shall reference this number.

4. The Contracting Officer responsible for this solicitation is Mrs. Lise Vieux-Rochat, all correspondence regarding this IFB should solely be addressed to IFBCO115759DAMSWCM@ncia.nato.int.

5. Except, provided herein, all other terms and conditions of the IFB documents remain unchanged.

FOR THE CHIEF OF ACQUISITION:

Originally signed

Lise Vieux-Rochat
Contracting Officer

Attachment(s):

A. Annex A - Responses to Clarification Requests received for IFB-CO-115759-DAMS-WCM.
B. Revised Book II - Part IV - Statement of Work

ANNEX A

Responses to Clarification Requests release 2 - received for IFB-CO-15759-DAMS-WCM.

	IFB source document	IFB paragraph reference	Type	Question	Answer	IFB Amendment required	Amdt#
CR#13	Book II - Part IV - Statement of Work	1.1.2.1.	Technical	What is the total overview of sites in scope, if any,beyond nato.int? As an example - is https://www.natomultimedia.tv/app/home or any event websites in scope?	The scope of work package 1 is to replace and merge only the current websites www.nato.int and www.natomultimedia.tv into a single solution. The main domain for the future Solution shall be www.nato.int. There might be multiple specific sites for additional events like www.<eventname>.nato.int. As part of work package 3 additional existing websites could be in scope.	No	2
CR#14	Book II - Part IV - Statement of Work	1.1.2.1.	Technical	Is the expectation for the Contractor to replicate the current set of website components? Is there any redesign needed? Are there any enhancements needed to the overall user flow and site hierarchy?	Each of the components currently used will be evaluated for re-use during the “Configuration Gathering and Provisioning phase” in close collaboration between the User (PDD) and the Contractor.	No	2

CR#15	Book II - Part IV - Statement of Work	A.1.2	Technical	Should the static archive of the existing website include anything other than the currently public content of the site, eg non-published pages, previous unpublished pages/content etc?	The Static Archive will only include articles that are published at the time when the new Solution becomes operational – new content will only be published in the new Solution and not in the archive. (Non-published or unpublished content is stored in the current CMS which will be decommissioned after work package 1)	No	2
CR#16	Book II - Part IV - Statement of Work	A.1.2.2	Technical	Can we simply remove pages containing forms and any other interactive elements? Are there any dependencies or considerations you can share?	It is not expected that removing interactive elements will result in breaking changes. As an alternative, making the interactive components in the Static Archive Website “inactive” is also an acceptable solution. Further investigation with the current provider]init[will have to be executed to ensure in the first phase of the project will have to determine what is possible. Bidders are invited to anticipate both scenarios.	No	2
CR#17	Book II - Part IV - Statement of Work	A.1.2.4	Technical	Could the Purchaser provide some examples of the use cases for configuration of 301 and 302 redirect notifications within the SAW?	Based on the page that is trying to be accessed, it should be possible to provide either a generic or a page-specific 301 or 302 message. It is expected that most pages will have a standard 301 and 302 warning message and a few pages will have a “specific” message. FYI The current website contains modified 404-error pages with a message in four languages	No	2
CR#18	Book II - Part IV - Statement of Work	A.1.6.1	Technical	Is there an overview of all in-scope templates and components available?	There is no current overview of all in-scope templates. These will be identified in the “Configuration Gathering and Provisioning phase” in close collaboration between the User (PDD) and the Contractor)	No	2

CR#19	Book II - Part IV - Statement of Work	A.1.6.1	Technical	Could you share any design deliverables, style guides, design system elements which already exist?	The following Figma wireframes provide an example of design elements: Desktop: https://www.figma.com/proto/fhOI5iOAxbA99piLjaYB1s/NT_Public-Website_Wireframes?node-id=1%3A9&viewport=960%2C618%2C0.03157326579093933&scaling=min-zoom Mobile: https://www.figma.com/proto/N4QFsSckM5zRZ1ZMevVOMG/NT_Public-Website_Wireframes-mobile?node-id=52%3A232&viewport=267%2C32%2C0.3342072665691376&scaling=scale-down Desktop: https://www.figma.com/proto/pXluP0Qn7RaN9lGBUJXmqb/NT_Public-Website_UI?node-id=135%3A1&viewport=372%2C105%2C0.03122663125395775&scaling=min-zoom Mobile: https://www.figma.com/proto/pXluP0Qn7RaN9lGBUJXmqb/NT_Public-Website_UI?node-id=135%3A1&viewport=372%2C105%2C0.03122663125395775&scaling=scale-down These are indicative designs and are subject to change	No	2
CR#20	Book II - Part IV - Statement of Work	A.1.6.2	Technical	Could the Purchaser give examples of situations when the history of content templates would be used to provide point in time rollback of content from a User point of view as well as from the Consumer of content point of view? (The public browsing through nato.int)	The expectation is that both the content and the templates will have separate versioning. * If a template is updated, the content version should not change (this would be the case if NATO choses to update the look and feel of the website) If a piece of content requires updating, the template should remain the same even though the change might be in an old template.	No	2
CR#21	Book II - Part IV - Statement of Work	A.1.6.2	Technical	Could the Purchaser provide any additional information around the amount of time or number of changes over which content rollback is expected to be possible?	It is expected that every piece of content can go back in version from the moment it was created.	No	2

CR#22	Book II - Part IV - Statement of Work	4.4.10	Technical	is there an expectation that content editing history will be maintained from the old system into the new system for content which is migrated?	It is not expected that the change history of the content in the old system is maintained.	No	2
CR#23	Book II - Part IV - Statement of Work	A.1.6.3	Technical	Could the Purchaser provide a list of all expected workflows to be accommodated (from those not percieved as 'green field')? Please include the relevant actors / users that are part of these workflows and any other systems that are part of the workflows, as applicable.	There is no current overview of all in-scope workflows. These will be identified in the “Configuration Gathering and Provisioning phase” in close collaboration between the User (PDD) and the Contractor)	No	2
CR#24	Book II - Part IV - Statement of Work	A.1.6.5	Technical	Please provide further detail on scenarios whereby content is assigned to users - who is assigning the content and under which circumstance / trigger? Examples: content assigned for review before publishing, content locked by a user so others can’t make changes.	There is no current overview of all in-scope workflows. These will be identified in the “Configuration Gathering and Provisioning phase” in close collaboration between the User (PDD) and the Contractor)	No	2
CR#25	Book II - Part IV - Statement of Work	A.1.6.5	Technical	Please provide further detail on the action of retiring content - under which circumstance does this happen and what happens to the content after the action is taken?	Content is retired when the user no longer wants to display this to the end-users. At this time the content should recevie a status of "retired" so that it is only visible internal to the Solution. It must also be possible to delete/destroy content completely so that it is no longer retrievable.	No	2
CR#26	Book II - Part IV - Statement of Work	A.1.8.1	Technical	Is the expectation that (some) authors will be editing the CSS and JS? If yes, can you please provide an example scenario.	It is not expected that the authors will directly edit the CSS of JS of the application. It is expected that the Contractor will create the templates and the User will create the content.	No	2
CR#27	Book II - Part IV - Statement of Work	B.1	Technical	What is your definition & expectations of slow accessible storage & fast accessible storage?	Slow accessible shall be available within minutes Fast accessible shall be available within miliseconds	No	2

CR#28	Book II - Part IV - Statement of Work	B.1	Technical	Can you provide details of the criteria used to determine when content is moved from fast to slow storage and how often content is moved back from the slow to fast storage in the system?	The number of times an asset is accessed will be the main driver for slow and fast storage	No	2
CR#29	Book II - Part IV - Statement of Work	5,3	Technical	Can the Purchaser provide a breakdown of how many users will effectively work in the CMS and how many in the DAM?	It is expected that around 100 people will work in the Solution (not counting external contributors like translators).	No	2
CR#30	Book II - Part IV - Statement of Work	A.1.12.4	Technical	Could the Purchaser share any detail of how the existing Theo Player integration works, in particular with regard to how the video playlists etc are stored and exposed via the CDN?	THEOPlayer uses the playlist which is provided and generated by the current CDN, LimeLight: https://cofelylpi-livepush.video.llnw.net/NATO-LIVE-PUSH/playlist.m3u8 The purpose of this IFB is to replace the services provided by the current CDN. Our requirement to the Contractor is to provide a CDN to which our encoder can send a Multilanguage HLS/SRT stream and have the CDN provide a playlist that can be used by THEOplayer	No	2
CR#31	Book II - Part IV - Statement of Work	A.1.8.1	Technical	Could the purchaser provide an example of the data format exposed by Taleo and how the current system imports this data for display?	The current integration with Taleo is being revised. By the time the Solution will be implemented, it is expected that the integration will happen through a REST / GraphQL API or a direct JSON file transfer.	No	2
CR#32	Book II - Part IV - Statement of Work	A.1.8.1	Technical	Could the purchaser provide details of the Emply integration as this is not listed in Annex C?	The current integration with Emply is being revised. By the time the Solution will be implemented, it is expected that the integration will happen through a REST / GraphQL API or a direct JSON file transfer.	No	2
CR#33	Annex C: WCM and DAMS System Integrations	N/A	Technical	Could the Purchaser provide details of their current email service provider integration options as this is not listed in Annex C?	Mass email is currently provided by Campaign Monitor. Notifications and standard email is done by the Internal Email server.	No	2
CR#34	Book II - Part IV - Stateme	A.1.14	Technical	Could the Purchaser confirm whether the list of items under 1.14.2 which should not be provided includes the full	The Bidder is expected to configure their Web Application Firewall to only allow traffic from the Cloudflare entry point to reach the origin server.	No	2

	nt of Work			functionality provided by the Purchaser's SIEM Cloudflare, or whether the solution also needs to integrate with other Cloudflare functionality?			
CR#35	Book II - Part IV - Statement of Work	A.1.1.8	Technical	Annex D use case 1 includes users performing manual translation of content within the solution - is there any requirement for the system to also support or include automated machine translation of content?	Because of political sensitivity and the need for accuracy, machine-based translation is not required.	No	2
CR#36	Book II - Part IV - Statement of Work	A.1.19.9	Technical	Requirement A.1.19.9 includes "focal point" in the list of basic image manipulation options the DAM must support, however Requirement A.1.19.3 states that the solution could provide functionality to indicate focal points when resizing and cropping - could the Purchaser confirm if focal points should be included in the "basic maniplation of images"?	This is an error – the identifying the focal point and maintaining consistency during resizing/cropping is a COULD requirement.	Yes	2
CR#37	Book II - Part IV - Statement of Work	A.1.2	Technical	What is an acceptable size of small portion of content and can you provide any defintiion of what content is classified as "most actual"?	The content that will be in both the SAW and new Solution will be limited to essential content (e.g. background information and key documents) as well as new content issued one month before the transfer from the old systems to the new Solution – this will ensure that the end-user will experience the new website as fully populated with at least a month of history before they have to search in the SAW.	No	2
CR#38	Book II - Part IV - Statement of Work	A.1.2.4	Technical	Could the Purchaser provide any detail of specific expectations around the reporting of internal and external dead links in the SAW? Is this reporting also expected to support the new live website as well?	Both the SAW and the rest of the solution shall be able to detect internal and external dead links and notify specific users in case such a dead link is found. It is expected that dead links in the new Solution will be updated as soon as possible. In the SAW, it is expected that all dead links are identified and removed at the time of creation/transfer followed by only periodic tracking of links.	No	2
CR#39	Book II - Part IV - Stateme	A.1.2.2	Technical	What solution is the Purchaser currently using for the search capability on nato.int website pages?	The current search capabilities visible on the website are considered a minimum for the search capabilities proposed by the Bidder.	No	2

	nt of Work						
CR#40	Book II - Part IV - Statement of Work	A.1.2.2	Technical	Could the Purchaser provide additional details about the current search capabilities of the nato.int website, eg full-text/keyword search, real time results, autofill etc?	All search capabilities can be identified on the current NATO.int website. The current capacity is considered a minimum for the search capabilities proposed by the Contractor	No	2
CR#41	Book II - Part IV - Statement of Work	A.1.2.2	Technical	Does the search needs to return results with references to documents or videos assets as well ?	The solution shall be able to provide search results based on the meta-data of the following assets: • Video • Pictures • Audio The solution shall be able to return results based on the content and metadata of: • Text E.g. it is not required to provide search results based on an analysis of unstructured data like videos, pictures.	No	2
CR#42	Book II - Part IV - Statement of Work	A.1.2.2	Technical	Could the Purchaser confirm whether the search functionality with the SAW should also return results from the new live site, or should the two sites be searched entirely indepedently?	The search in the SAW and the Solution shall be separate.	No	2
CR#43	Book II - Part IV - Statement of Work	4.7.3.1.	Technical	Could the Purchaser provide information on what format and type of system the current DAMS metadata is stored in and how that is associated with the content?	The data of DAMS is stored in a SQL database containing the metadata and the proxy/preview quality thumbnails, and references to the high resolution video and photo files which are stored as separate files.	No	2
CR#44	Book II - Part IV - Statement of Work	4.7.3.1.3.	Technical	Could the Purchaser provide any additional detail on the current security restrictions which are/can be applied to DAMS content which should be migrated to the new solution?	The current security mechanisms are based on physical access and will not be relevant to the new Solution. The privileges and workflows shall be identified and configured in the “Configuration Gathering and Provisioning phase” in close collaboration between the User (PDD) and the Contractor)	No	2

CR#45	Book II - Part IV - Statement of Work	A.1.12.8	Technical	Could the Purchaser provide any additional informaiton on the usage of the Purchaser's Megellan and Interplay networks and which users / functions would be performed from those networks?	The Magellan network is the business network of NATO Headquarters and users need to be able to administer the application from this network. The interplay network is an internal network used for editing content before it is released into the solution.	No	2
CR#46	Book II - Part IV - Statement of Work	A.1.10.1	Technical	In the context of dashboard functionality, could the Purchaser provide additional information on what would constitute a "content block"?	In the “Configuration Gathering and Provisioning phase" the exact definition of the dashboards shall be defined in close collaboration with the user. The context of a content block is the ability to show these dashboards within the Solution.	No	2

IFB-CO-115759-DAMS-WCM

DIGITAL ASSET MANAGEMENT SYSTEM (DAMS)/ WEB CONTENT MANAGEMENT (WCM) REPLACEMENT

BOOK II - PART IV

STATEMENT OF WORK (SOW)

TABLE OF CONTENTS

SECTION 1 : Introduction ... 6
1.1. Background ... 6
1.2. Standards for Interpretation of the SOW ... 7
1.3. Organisation of the SOW ... 7
1.4. Scope of Work ... 7
1.5. Period of Performance (POP) ... 7
1.6. Place of Performance ... 8
1.7. High-level Objectives ... 8
1.8. Critical Periods ... 8
1.9. Low Maintenance Periods ... 9
SECTION 2 : Applicable Documents ... 10
SECTION 3 : Phases and Milestones ... 12
3.1. Introduction ... 12
3.2. Effective Date Contract (EDC) ... 12
3.3. Phases ... 12
3.4. Milestone Overview ... 16
SECTION 4 : Work Package 1: Provisioning of the Solution (CLIN 1) ... 18
4.1. Providing the Solution ... 18
4.2. Organization ... 18
4.3. Project Management ... 19
4.4. Project Documentation ... 20
4.5. Documentation Delivery and Review ... 27
4.6. Design activities ... 27
4.7. Solution Provisioning Activities ... 27
SECTION 5 : Work Package 2: Service Delivery Year until end 2028 ... 30
5.1. Introduction ... 30
5.2. Administering and Operating the Solution ... 30
5.3. Organization ... 30
5.4. Changes ... 31
5.5. Monthly Stress Test ... 32
5.6. Yearly Fall-back Solution Test ... 32
5.7. Yearly Backup Test ... 32
5.8. Monthly Service Delivery Reporting ... 32
5.9. Yearly Service Delivery Report ... 33
5.10. Service Support ... 33

5.11. Incident Response 33

SECTION 6 : Work Package 3 (Option): Additional 3 Years of service delivery 35

6.1. Introduction 35

6.2. Continuation of Service Delivery 35

SECTION 7 : Work Package 4 (Option): Additional Contractor Support 36

7.1. Introduction 36

7.2. Costed Option List (COL) 36

SECTION 8 : Security Accreditation 38

8.1. Information Classification 38

8.2. Security Accreditation Requirements 38

8.3. Security Accreditation Documentation Set (ADS) 39

SECTION 9 : NATO Information Protection 44

SECTION 10 : Safeguarding of NATO RESTRICTED Information 45

SECTION 11 : Test, Verification and Validation 46

11.1. TV&V activities 46

11.2. Deliverables 48

SECTION 12 Quality Assurance 50

12.1. Introduction 50

12.2. Roles and Responsibilities 50

12.3. Quality for Project Documents 51

SECTION 13 System Requirements Specification (SRS) 52

ANNEX B Service Level Agreement (SLA) 64

ANNEX C WCM and DAMS System Integrations 69

ANNEX D User Journeys 70

TABLE OF FIGURES

Figure 1 Timeline Year 1 7
Figure 2 Timeline following years 7
Figure 3 Milestones and Tracks - Phase 1.......... 12
Figure 4 Dependencies ADS Documents and Audits.......... 14
Figure 5 Roles During Solution Provisioning.......... 21
Figure 6 Roles During Service Delivery 33
Figure 7 Test Event Timeline.......... 52
Figure 8 Solution Information Structure 57
Figure 9 Schematic Overview DAM.......... 63

TABLE OF TABLES

Table 1 Short-list of WCM Products.......... 6
Table 2 QA Reference Documents.......... 10
Table 3 NATO Standards Guidance Reference Documents 10
Table 4 NATO Security Reference Documents 10
Table 5 NATO Reference Documents 11
Table 6 Non-NATO Reference Documents.......... 11
Table 7 Hyperlinks.......... 11
Table 8 Milestone Timelines and Dates.......... 16
Table 9: Security Accreditation Documentation and Contractor Responsibility 42
Table 10 Service Level Agreement.......... 72
Table 11 WCM and DAMS System Integrations 75
Table 12 List of Acronyms 81

SECTION 1 : INTRODUCTION

1.1. Background

1.1.1. The North Atlantic Treaty Organization (NATO) Public Diplomacy Division (PDD) efforts serve a vital function within the Alliance by communicating its purpose and priorities to audiences worldwide. In fulfilling this role, the PDD actively strengthens NATO's public image, thereby fostering awareness and understanding of NATO's policies and activities, and ultimately enhances trust in and support for the Alliance.

1.1.2. Currently, this effort is supported by two main systems:

1.1.2.1. **The Web Content Management (WCM)** system, which is the technical system currently used to support the public NATO website (https://www.nato.int). It includes a hardware component (network infrastructure, servers, databases, IT security devices), a software component (the content management, application), and the content of the NATO website (text, photos, audio, design).

1.1.2.2. **The Digital Asset Management System (DAMS),** which is the media management system that manages, processes and stores public NATO multimedia content. It currently includes 3rd party software that enables the management and storage of content produced by NATO and its partners, as well as the publication of a selection of the assets to be shared through the NATO multimedia portal (https://www.natomultimedia.tv) for viewing by any visitor and for download by professional media.

1.1.3. To continuously improve and adapt to the changing environment, the PDD is undergoing a transformation program to improve the communication infrastructure of the alliance. Part of this transformation includes extending the functionality provided by the current WCM and DAMS systems. This project seeks to re-compete the WCM and DAMS system as a public cloud-based solution while also ensuring a static archive of the current www.nato.int website remains available for historical reference.

1.1.4. In a 2020 design study and market survey, the Purchaser examined possible WCM candidates which resulted in the following short-list:

Product	Website
Liferay Experience platform	https://www.liferay.com
Sitecore	https://www.sitecore.com
Adobe Experience Manager	https://business.adobe.com/
Storyblok	https://www.storyblok.com/
Kentico	https://www.kentico.com/
Contentstack	https://www.contentstack.com/

Table 1 Short-list of WCM Products

1.2. Standards for Interpretation of the Statement of Work (SOW)

1.2.1. The use of shall is defined as follows:

- Shall: This requirement is mandatory and must be implemented.
- Shall not: means that the definition is an absolute prohibition of the specification.
- Could: means that the definition is a Contract option that could be exercised by the Purchaser.

1.3. Scope of Work

1.3.1. The scope of work consists of providing, integrating, configuring, transitioning to, and maintaining a Public Software as a Service (SaaS) solution for the Purchaser that delivers workflow management, content management, and large-scale digital asset management, and content publication according to the styling preferences and way of working of the Purchaser.

1.4. Period of Performance (POP)

1.4.1. The POP is captured in multiple milestones and is detailed in SECTION 3. In summary, the Contract consists of three phases:

1.4.1.1. The first phase constitutes the provisioning and configuration of the Solution, under the Base Contract, shall be no more than 12 months from the Effective Date of Contract (EDC), and is completed via Purchaser confirmed Final System Acceptance (FSA).

1.4.1.2. The second phase constitutes service delivery and will start after the first phase and shall extend until the end of 2028 and is completed by Purchaser confirmation. During this phase, also option 3 of this Contract can be exercised by the Purchaser.

1.4.1.3. The optional third phase constitutes an additional three years of service delivery that could commence after the completion of the second phase and is completed by Purchaser confirmation. During this phase, also option 4 of this Contract can be exercised by the Purchaser.

Figure 1 and Figure 2 display these timelines (both subject to Section 3 of this SOW)

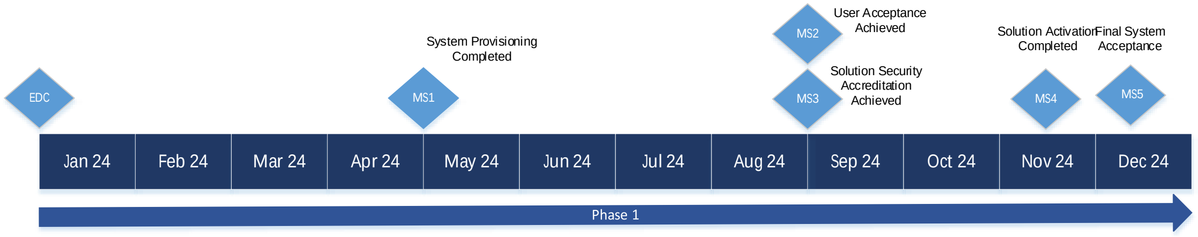


Figure 1 Timeline Year 1

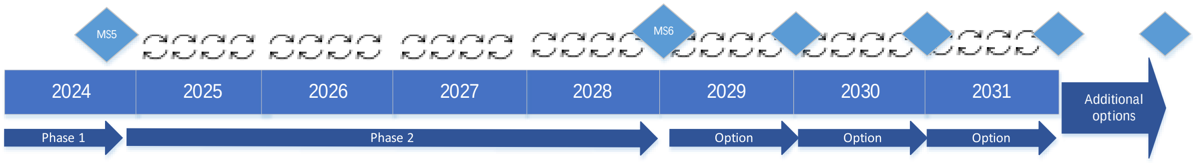


Figure 2 Timeline following years

1.5. Place of Performance

1.5.1. The majority of the work shall be performed offsite, through virtual collaboration and remote working, with the possible exception of workshops and training sessions with the PDD. These workshops and training sessions may be conducted at NATO Headquarters in Brussels, Belgium.

1.6. High-level Objectives

1.6.1. Provide a solution that provides the out-of-the box functionality of one of the Content Management System (CMS) products identified in Table 1 Short-list of WCM Products, the functional requirements identified in this SOW, and the SLA requirements described in ANNEX B.

1.6.2. Ensure that the Solution receives Security Accreditation (SA) by the NATO Security Accreditation Authority (SAA) by adhering to all relevant security directives,, (reference 2.2.3) including the integration of the Solution with the Purchaser's Security Information and Event Management System (SIEM) and the Purchaser's solution for Secure Edge Protection.

1.6.3. Identify all configuration items needed for the PDD to operate the Solution in an effective manner by executing workshops and business analysis of the PDD way-of-working. Then continue to implement these discoveries into the Solution and providing the appropriate training to the PDD.

1.6.4. Migrate the data maintained in the current WCM and DAMS system to the Solution and coordinate the transition into operations of the new solution.

1.6.5. Continue to update and maintain the configuration, functionality, technical, and security aspects of the system once it has received FSA for the ongoing year and for a period of 4 years and additional optional years, according to the Service Level Agreement (SLA) in ANNEX B.

1.7. Critical Periods

Several times per year, the Purchaser will host publically important events like ministerial meetings and summits. These periods are considered critical and the Contractor should consider the following during critical periods:

- During phase 1 of the project, the PDD will be unavailable for configuration solicitation or training, and no technical works can take place on any NATO systems;
- During phase 2 and 3, additional usage of the Solution is expected and additional support from the Contractor will be required.

These critical periods can be planned (approximately 10 times per year) but also unplanned in case of a crisis situation. Planned critical period start and finish dates will be communicated to the Contractor at least 30 calendar days before the start of the period. Unplanned critical periods will be communicated to the Contractor as soon as possible.

1.7.1. (SHALL) The Contractor shall incorporate Critical Periods into all planning aspects of the project.

1.8. Limited Maintenance Periods

Before, during and after critical periods, the Purchaser's organization moves into a Limited Maintenance Period (LMP). During these periods there is limited availability of Purchaser Staff and no significant technical works can take place on any NATO system to reduce risk. Planned LMPs start and finish dates will be communicated to the Contractor at least 30 calendar days before the start of the period. Unplanned LMPs will be communicated to the Contractor as soon as possible.

1.8.1. (SHALL) The Contractor shall incorporate LMPs into all planning aspects of the project.

SECTION 2 : APPLICABLE DOCUMENTS

2.1. Documentation

The documentation related to this Contract consists of NATO documents and non-NATO documents.

2.1.1. The Contractor shall be aware and comply with the documents listed in SECTION 2 throughout the Contract.

2.2. NATO Documents

2.2.1. Reference documents for Quality Assurance (QA) purposes

Abbreviation	Full document Name and Reference
[AQAP-2105, Ed.C, Ver.1]	NATO Requirements for Quality Plans. Ed.C, Ver.1, 2019.
[AQAP-2131, Ed.C, Ver.1]	NATO Quality Assurance Requirements for Final Inspection and Test. Ed.C, Ver.1, 2017.
[AQAP-2210, Ed.A, Ver.2]	NATO Supplementary Software Quality Assurance Requirements to AQAP-2110 or AQAP-2310. Ed.A, Ver.2, 2015.
[AQAP-2310, Ed.B, Ver.1]	NATO Quality Assurance Requirements for Aviation, Space and Defence Suppliers. Ed.B, Ver.1, 2017.

Table 2 QA Reference Documents

2.2.2. NATO Standards Guidance

Abbreviation	Full document Name and Reference
[STANAG 4281, Ed.3]	NATO Standard Marking for Shipment and Storage. Ed.3, 2016.

Table 3 NATO Standards Guidance Reference Documents

2.2.3. NATO Security Documents

Abbreviation	Full document Name and Reference
[NAC AC/35-D/2000-REV8, 2020]	Directive on Personnel Security (AC/35-D/2000-REV8), 2020
[AC/322-D(2019)0038 (INV)]	CIS Security Technical and Implementation Directive for the Security of Web Application, 2019
[AC/322-D(2021)0032]	Technical and Implementation Directive for the Protection of NATO Information within Public Cloud-Based Communication and Information Systems, 2021
[AC/322-D/0048-REV3 (INV)]	Technical and Implementation Directive on CIS Security, Revision 3, 2019
[AC/322-D/0030-REV6]	Technical And Implementation Directive For The Interconnection Of Communications And Information Systems (CIS)

Table 4 NATO Security Reference Documents

2.2.4. Other NATO Documents

Abbreviation	Full document Name and Reference
[NCIA AD 06.03.04, 2015]	Agency Directive AD 06.03.04 Test Verification and Validation - 20 February 2015

Table 5 NATO Reference Documents

2.3. Non-NATO Documents

2.3.1. Reference documents for Quality, Testing, and Integrated Logistic Support (ILS)

Abbreviation	Full document Name and Reference
[ISO/IEC 15288, 2015]	Systems and software engineering -- System life cycle processes
[ISO/IEC 12207, 2008]	Systems and software engineering -- Software life cycle processes
[ISO/IEC 25010, 2011]	Systems and software engineering — Systems and Software Quality Requirements and Evaluation (SQuaRE) — System and software quality models
[ISO 9000/ 9001, 2015]	Quality management systems - Fundamentals and vocabulary & Requirements
[ISO/IEC/IEEE 29119]	Software and systems engineering — Software testing
[ISO/IEC/IEEE-29119-3]	Software and systems engineering — Software testing - Test documentation
[SX000i-B6865-0X000-00, 1.1, 2016.]	International Guide for the use of the S-Series Integrated Logistics Support (ILS) specifications,

Table 6 Non-NATO Reference Documents

2.3.2. Applicable Hyperlinks

Hyperlink	Full document Name and Reference
https://developers.cloudflare.com/	Onboarding criteria for Cloudflare Edge Security Solution

Table 7 Hyperlinks

SECTION 3 : PHASES AND MILESTONES

3.1. Introduction

The delivery timelines for the project are ambitious and the Contractor shall make every effort necessary to avoid delays in execution of the Contract. The phases and delivery milestones of the project are described in this section. The Contract shall take these phases into consideration when creating the Project Management Plan (PMP) and the Project Master Schedule (PMS).

3.1.1. (SHALL) The Contractor shall meet or “exceed” the dates mentioned in Table 8 Milestone (Note: “Exceed” is to be understood as a situation where the Contractor has delivered earlier than the dates mentioned in the schedule, and the Purchaser has accepted the milestone accordingly).

3.1.2. (SHALL) The Contractor shall incorporate the Phases mentioned in this section into the PMP and PMS. Changes to the phases of the project shall only be considered after Purchaser approval.

3.1.3. (SHALL) The Contractor shall ensure that anything that may delay the implementation is brought to the attention of the PPM promptly.

3.2. Effective Date of Contract (EDC)

3.2.1. (SHALL) The EDC will be established at the time of Contract Award.

3.3. Phases

3.3.1. Phase one

Phase one aligns with Work Package 1 and constitutes the provisioning of the system. This phase has three distinct tracks: security, technical, and configuration. These phases and timelines are displayed in Figure 3.

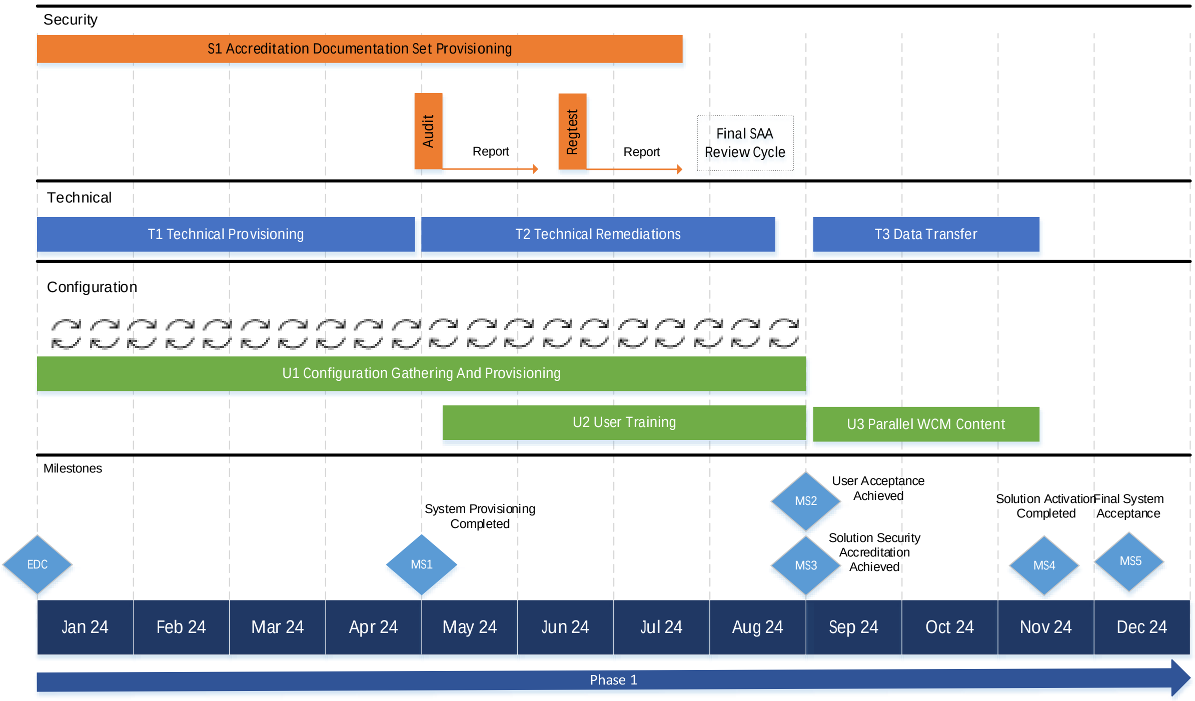


Figure 3 Milestones and Tracks - Phase 1

3.3.1.1. Security Track

The security track relates to all activities that are required to optimize the Security of the Solution and achieve SA. Without forward planning, Security Documentation and Achieving SA will pose a big risk to the success of the project. The Security Track is divided into four elements:

- S1 Security Accreditation Documentation Provisioning.

The Contractor shall deliver all SA documentation and gain written approval of all documents. The Contractor is free to choose the most suitable process for this effort but shall take the different dependencies and review times for documents into consideration. The process, exact planning, and Purchaser and SAA involvement shall be captured in the PMP and PMS

- Audit and Report.

The Security Audit on the system shall be performed by the Purchaser and will require 7 calendar days. On the last day of the audit, an audit debrief will be organized to discuss all findings that the Contractor shall remediate before the Audit Regression Test starts. After the audit debrief, a planning period of 30 calendar days is planned for the delivery of the Audit report by the Purchaser.

- Regression Test and Report

If there are any audit findings that are remediation by the Contractor, the Purchaser will organize an Audit Regression Test on the Solution to verify the changes made by the Contractor. The Audit Regression test will require 7 calendar days. On the last day of the regression test, a debrief will be organized to discuss all findings After the regression test debrief, a planning period of one calendar month should be considered for the delivery of the Audit Regression Test report by the Purchaser.

- Final SAA Review Cycle

In the final review cycle, the SAA will review all documents and the results of the audit reports to conclude on a decision to grant SA of the Solution. This final review cycle takes one month.

3.3.1.1.1. (SHALL) The Contractor shall include one calendar month of SAA review time per review cycle per document in the ADS in the PMP and PMS. These reviews can be executed in parallel.

3.3.1.1.2. (SHALL) The Contractor shall include at least two review cycles per document before gaining SAA approval for that document in the PMP and PMS.

3.3.1.1.3. (SHALL) The Contractor shall include a planned Audit in week 19 of 2024 and a planned Regression Test in in week in 25 of 2024 as critical planning items in the PMP and PMS.

3.3.1.1.4. (SHALL) The Contract shall include the completion of MS1 (System Provisioning Completed) as a dependency for the start of the Audit in the PMP and PMS.

3.3.1.1.5. (SHALL) The Contractor shall include a calendar month of time required for the writing of the audit report and a calendar month of time required for the writing the regression test report in the PMP and PMS.

3.3.1.1.6. (SHALL) The Contractor shall include the ADS Dependencies displayed in Figure 4 in the PMP and PMS. Each document shall be approved before the next dependent document approval process is started.

3.3.1.1.7. (SHALL) The Contractor shall include a calendar month of time required for the SAA to execute a final review cycle in the PMP and PMS.

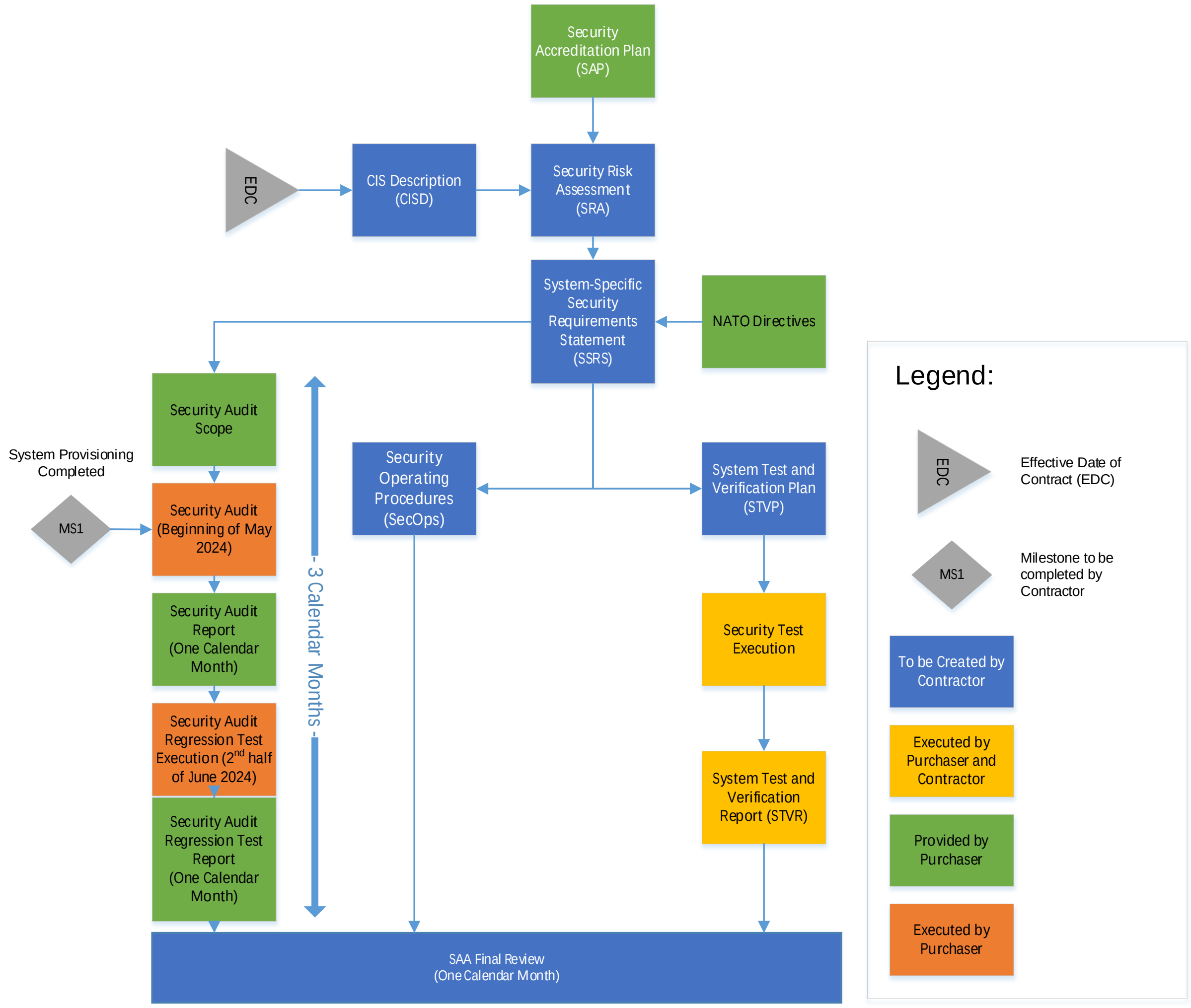

Security Accreditation Plan (SAP)
EDC
CIS Description (CISD)
Security Risk Assessment (SRA)
System-Specific Security Requirements Statement (SSRS)
NATO Directives
System Provisioning Completed
MS1
Security Audit Scope
Security Audit (Beginning of May 2024)
Security Audit Report (One Calendar Month)
Security Audit Regression Test Execution (2nd half of June 2024)
Security Audit Regression Test Report (One Calendar Month)
- 3 Calendar Months -
Security Operating Procedures (SecOps)
System Test and Verification Plan (STVP)
Security Test Execution
System Test and Verification Report (STVR)
SAA Final Review (One Calendar Month)
Legend:
EDC
Effective Date of Contract (EDC)
MS1
Milestone to be completed by Contractor
To be Created by Contractor
Executed by Purchaser and Contractor
Provided by Purchaser
Executed by Purchaser

Figure 4 Dependencies ADS Documents and Audits

Further details on the responsibilities and content of each of the audits and documents in ADS during the SA process can be found in SECTION 8.

3.3.1.2. Technical Track

The technical track involves all the technical effort required to deliver a feasible solution that adheres to all the requirements in this SOW, including the transfer of the data from the WCM and DAMS systems to the Solution.

- T1 – Technical Provisioning

This block constitutes all the technical works needed to create the Solution, including the integration with NATO systems and the system of other Contractors. At the end of this phase, the milestone “System Provisioning Complete” is achieved and the system is considered mature enough to receive the security audit and start the configuration of the system.

- T2 – Technical Remediation

The security Audit for the solution is planned for 7 calendar days in the beginning of May 2024 and shall be concluded by an out-brief that details all the remediation actions that will be required to achieve accreditation of the Solution. The Contractor shall effectively use the time between the Audit and the Audit Regression test to ensure all technical remediation items are completed before Audit Regression Test Start (2nd half of June 2024).

- T3 Data Transfer and Activation

After the final SAA review cycle of the ADS has been completed and SA has been achieved for the solution, the Contractor shall execute a data-transfer from the WCM and DAMS systems to the Solution as per the Data Migration Plan (DMP). After the data transfer has successfully concluded, the Contractor shall activate the Solution so that end-users start using the new websites.

3.3.1.2.1. (SHALL) The Contractor shall include the dependency between the provisioning of the technical solution and the Security Audit in the PMP and the PMS.

3.3.1.2.2. (SHALL) The Contractor shall include the dependency between the Technical Remediation and the Security Audit Regression test in the PMP and the PMS.

3.3.1.2.3. (SHALL) The Contractor shall include the dependency between achieving SA for the Solution and the Start of the Data Migration in the PMP and PMS.

3.3.1.2.4. (SHALL) The Contractor shall include the dependency between achieving user acceptance and the start of the Data Migration in the PMP and PMS

3.3.1.2.5. (SHALL) The Contractor shall include the dependency between completing the Data Migration and Solution Activation in the PMP and PMS.

3.3.1.3. Configuration Track

The Configuration track constitutes all the effort required to ensure the User can effectively use the system. This includes the solicitation and implementation of the different configuration items as well as training for the users and ensuring a period in which the current WCM and DAMS systems as well as the Solution operate in parallel.

- U1 - Configuration Gathering and Provisioning

In this block, the Contractor will solicit the configuration items from the User and implement them in the Solution. For this effort, the Contractor is free to propose the most effective process that takes availability of the User organization into consideration. This block will focus on the creation and execution of the Solution Configuration Plan (SCP).

- U2 - User Training

After the Technical System Provisioning has been achieved and a baseline of configuration items have been included in the system. The Contractor can start training of the PDD staff. The most effective way of training and the time commitment required from the PDD staff will be proposed by the Contractor through the Training Plan (TP), which is subject to Purchaser approval.

- U3 – Parallel WCM Content

In the period of time that SA and UA for the Solution have been achieved but the Solution has not been activated yet, there will be a period of overlap during which there may be some duplication of effort across the systems. This period should be kept as short as possible.

3.4. Milestone Overview

Milestone	**Delivery**
MS1 System Provisioning Completed	EDC + 4 months
MS2 User Acceptance Achieved	MS1 + 4 months
MS3 Solution Accreditation Achieved	MS1 + 4 months
MS4 Solution Activation Completed	MS3 + 2.5 months
MS5 Final System Acceptance	MS4 + 1 month
MS6 Service Delivery Completed	End 2028
(Additional Years of Service)	End of each year

Table 8 Milestone Timelines and Dates

3.4.1. MS1 – System Provisioning Completed

This milestone is achieved when the technical provisioning of the system has been achieved according to the functional and non-functional system requirements defined in this SOW. Completion of this milestone is achieved by Purchaser acceptance of the technical implementation.

3.4.2. MS2 – User Acceptance Achieved

This milestone is achieved when the Purchaser considers the Solution configured and fit-for-purpose to be used in an operational capacity, including satisfactory training of the Purchaser staff. Completion of this milestone is achieved by Purchaser approval of the SCP (reference 4.4.12), TP (reference 4.7.7), and written acceptance of the configuration and training deliverables by the Purchaser.

3.4.3. MS3 – Solution Security Accreditation Achieved

This milestone is constitutes the granting of SA of the system according to the applicable security directives described in this SOW. Completion of this milestone is achieved by signature of the SA Statement of the Solution by the SAA.

3.4.4. MS4 – Solution Activation Completed

This milestone constitutes the cutover from the current WCM and DAMS system to the new solution, including transfer of the data. Completion of this milestone is achieved by Purchaser approval of the DMP, and the Solution Activation Plan. The Solution Activation can only be executed if the Purchaser formally approves the Pre-Activation Test (PAT).

3.4.5. MS5 – Final System Acceptance

FSA is the act by which the Purchaser has evaluated and determined that the implemented capability meets the requirements of Work Package 1 and that the Contractor has fully delivered all related requirements. This milestone is achieved by achieving MS1 through MS4.

3.4.6. MS6 – Service Delivery Completed

Service Delivery Completed constitutes the delivery of the service in an operational capacity according to the SLA requirements described in ANNEX B from the point of achieving MS5 (FSA) until the end of 2028. This milestone is achieved by Purchaser signoff.

3.4.7. Additional Years of Service

Additional Service Delivery Completed constitutes the delivery of the service in an operational capacity according to the SLA requirements described in ANNEX B from the point of achieving

MS6 until the end of each extended year. This milestone is achieved by Purchaser signoff at annual review.

An overview of the timelines and milestones is provided in Figure 1 Timeline Year 1and Figure 2 Timeline following years.

SECTION 4 : WORK PACKAGE 1: PROVISIONING OF THE SOLUTION (CLIN 1)

4.1. Providing the Solution

The provisioning of the Solution shall entail all the resources including services, personnel, materials, components, training, equipment, data, documentation, and effort required to deliver a system. This work package shall include all the requirements marked (SHALL) in the System Requirements Statement (SRS) as described in SECTION 13 as well as all the project deliverables marked as (SHALL) in this section.

4.1.1. (SHALL) The Contractor shall procure and configure a public cloud based solution for the Purchaser while ownership of that solution will remain with the Purchaser at all times (see hereafter subsections 4.1.1.1 and 4.1.1.2). The Solution shall be provided as described by the requirements marked (SHALL) in as well as the requirements in this Section.

4.1.1.1 Intellectual Property

The Purchaser shall retain exclusive ownership, title and interest to any development, object/source code, any product, service, tool, application or result (regardless of the stage of finalisation), and derivative works thereof, developed by the Contractor or delivered under the Contract, both directly on the cloud based solution as well as outside a cloud based framework.

The Contractor shall ensure that the Purchaser shall be able to use all necessary or relevant third party technology (including cloud based technology) at its convenience based on a royalty-free, worldwide, irrevocable, sub-licensable, perpetual license to use. Such use shall be included into the overall Contract price.

The Contractor shall remain exclusively liable and responsible towards the Purchaser for any usage of third-party hosting, application or services throughout the Term of the Contract. Any cost or fee related to the licensing of any such third-party hosting, application or services shall be fully included into the final price for the Contract.

The Purchaser shall retain exclusive ownership, title, interest and all applicable intellectual property rights in and to the data (including personal data) and/or content provided (directly or indirectly) to the Contractor throughout the Contract.

4.1.1.2 Data Governance

The Contractor acknowledges that the performance of the Contract will require data (including personal data) to be processed, transmitted and/or stored (including via the Contractor's managed cloud provider).The Contractor shall comply with all applicable Data Protection Laws throughout the Term of the Contract. The Purchaser shall act as the data controller and the Contractor shall act as the data processor.

The Contractor shall provide, as integral part of its offer, a detailed and comprehensive overview of all necessary and/or appropriate **administrative, physical, and technical safeguards** that will be taken (both by the Contractor as well as the managed (cloud) service providers) to ensure the security, confidentiality and integrity of the Purchaser's data processed during the Term of the Contract.

The Contractor shall ensure that the (personal) data processed during the Term of the Contract (including cloud storing) shall be done so in a NATO country.

The Contractor ensures that the Purchaser shall at all times retain full access and control of the data processed by the Contractor (and/or its managed (cloud) service providers).

At the end of the Contract, regardless of the reason for its termination, the Purchaser shall have the right to an easy and rapid (latest 7 calendar days) **data extraction solution** offered by the Contractor at no additional cost. This shall mean that whenever the Contract is terminated or expires, in addition to any rights or remedies the Purchaser might have, the Purchaser shall have the right to obtain the solution and services provided for under the Contract by a third party, and that the Contractor hereby explicitly agrees to cooperate to the fullest extent necessary with the Purchaser and/or any third party (assigned by the Purchaser) so as to accomplish the transaction of the solution/data without an interruption or disruption of the business operations of the Purchaser. The Purchaser shall have one (1) year to request the Contractor to fully cooperate with the Purchaser and/or such assignee, if any, to facilitate the transfer of all deliverables provided by the Contractor up until such termination. This shall include a full transfer of all documentation, licenses for use of third-party (cloud) tools/solutions, and for the Contractor (including any managed (cloud) service provider) to prove that all of the Purchaser’s data provide throughout the Contract have been destroyed (unless other instructions provided by the Purchaser). For reasons of clarity: the present paragraph shall also apply to Section 5 of the present SoW.

The Contractor acknowledges that any data provided by the Purchaser during the Contract is **protected by international treaties** and falls under the **inviolability of archives** as set out in the 1951 Ottawa Agreement on the Status of the North Atlantic Organization, National Representatives and International Staff and the 1952 Paris Protocol on the Status of International Military Headquarters set up pursuant to the North Atlantic Treaty. The Contractor shall ensure to invoke the aforementioned inviolability of NATO data towards any authority, instance or legally competent requestor asking for access to said NATO data. The Contractor shall inform the Purchaser of any such requests immediately and let the Purchaser interact with any authority, instance or legally competent requestor

4.1.2. (SHALL) The Contractor shall provide a solution that utilizes one of the products mentioned in Table 1 for the WCM functionality of the system.

4.1.3. (SHALL) The Contractor shall ensure that any system requirements described in this SOW by the requirements marked (SHALL) that are not covered by the system in 4.1.2 shall be provided by Commercial of the Shelf (COTS) solutions.

The current WCM and DAMS system have integrations with external systems (ANNEX C). The Contractor is free to re-use these integrations to provide the functionality described in this SOW.

4.1.4. (SHALL) If the Contractor decides to re-use one or more of the integrations, the Contractor takes full responsibility of the interconnection and the external system, including adherence to all (security) requirements described in this SOW.

4.1.5. (SHALL) Only if the functionality described in this SOW is not available as a COTS and if the functionality cannot be realized with current integrations shall the Contractor create custom functionality for the Purchaser – subject to Purchaser approval.

4.2. Organization

During the Solution Provisioning, clear definition of roles and responsibilities will be needed to ensure success. The mandatory roles are described in below and in Figure 5.

4.2.1. (SHALL) The Contractor shall appoint a Contractor Project Manager (CPM) as a single Point of Contact (POC) for the project.

4.2.2. (SHALL) The Contractor shall appoint a Contractor Quality Assurance Representative (CQAR) as the single POC for all quality-related aspects of the project (reference SECTION 12).

- NATO Roles

During the Solution Provisioning phase, NATO has specific roles assigned to the project.

- The **User** is one or more representatives of the PDD. They are the Points of Contact (POC) for all items related to configuration and functional requirements of the Solution.
- The Purchaser Project Manager (PPM**)** is an individual from the NATO Communication and Information (NCI) Agency and is the main POC for all items related to technical provisioning and Contracting during this phase of the project.
- The **SAA** is the NATO Office of Security (NOS) and they are the party within NATO that review the risk assessment and grant SA for the Solution
- The **NATO Quality Assurance Representative** (NQAR) is the NCI Agency Independent Verification and Validation (IV&V) Service line and their role is described in SECTION 12).

- 3rd Party Solution POC

The current WCM and DAMS system, as well as some of the integrated systems are (partially) managed by 3rd Party Contractors. In this project, each of these 3rd Party Contractors will have a POC for the integration with the Solution.

- Contractor Roles

During the Solution Provisioning phase, the Contractor shall have the following roles as a minimum to the project. The Contractor is free to propose additional roles as part of the PMP.

- The **CPM** is the main POC for this phase for all items that are not related to the quality of the project or the quality of the deliverables.
- The **CQAR** is the Contractor's POC for quality and their role is described in SECTION 12.

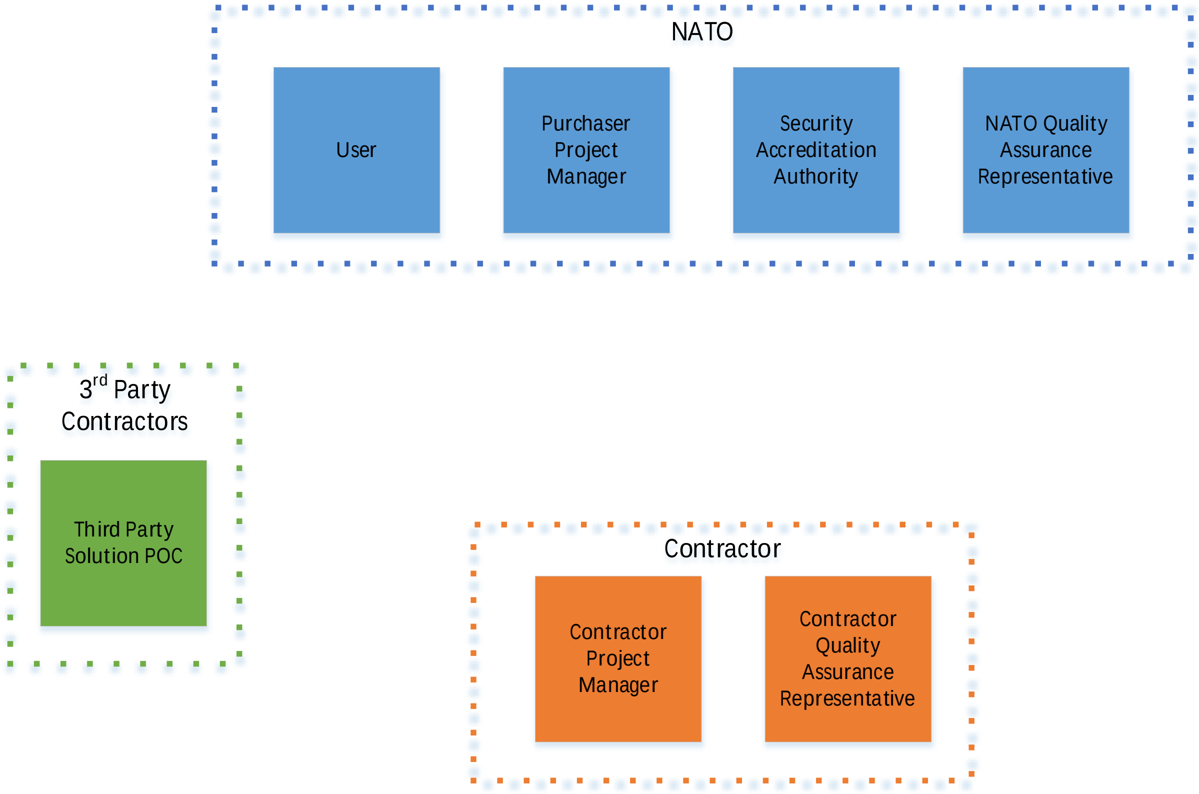

NATO
User
Purchaser Project Manager
Security Accreditation Authority
NATO Quality Assurance Representative
3rd Party Contractors
Third Party Solution POC
Contractor
Contractor Project Manager
Contractor Quality Assurance Representative

Figure 5 Roles During Solution Provisioning

The roles for the Service Delivery phase of the project are described in SECTION 5.

4.3. Project Management

The Purchaser uses the Projects IN Controlled Environments (PRINCE2) Agile Project Management Methodology during the execution of this Contract. The Contractor is free to use any project management methodology deemed efficient for this effort as long as there is a single POC for the project

4.3.1. (SHALL) The Contractor shall at all times ensure that:

- Adequate resources are applied to all activities undertaken under the Contract;
- Milestones are achieved in a timely manner;
- The project status information is comprehensively reported to the Purchaser in a timely manner;
- All risks to project achievement are identified and managed;
- Professional standards of project activities and deliverables through the application of QA techniques are applied;

4.3.2. (SHALL) The Contractor shall proactively coordinate and collaborate with other parties (NATO, Contractors) as required for the implementation of this project, in close coordination with the Purchaser.

4.3.3. (SHALL) The Contractor shall attend, organise and conduct meetings as required by the Purchaser.

4.4. Project Documentation

4.4.1. Project Management Plan (PMP)

4.4.1.1. (SHALL) The Contractor shall establish and maintain a PMP which shall describe how the Contractor will implement the totality of the project as specified in this SOW.

4.4.1.2. (SHALL) The Contractor's PMP shall cover all aspects of the project implementation that are appropriate to provide the capability as required by this Contract.

4.4.1.3. (SHALL) The Contractor's PMP shall be sufficiently detailed to ensure that the Purchaser is able to assess the Contractor plans with insight into the Contractor's plans, capabilities, and ability to satisfactorily implement the entire project in conformance with the requirements as specified in this SOW.

4.4.1.4. (SHALL) The Contractor shall ensure that the PMP comprises of the following sections unless otherwise agreed to by the Purchaser:

- An 'Organisation' section describing the Contractor's organisation for this project according to the requirements. This section shall include an organisational chart showing the members of the Contractor's Project Team (including the members of the Contractor PMO) and showing their respective responsibilities and authority. This section should also include proposed Project Communication Plan.
- A 'Project Planning' section describing the Contractor's processes supporting the development and maintenance of the deliverables according to the requirements.
- A 'NATO Staff Involvement' section describing interactions with NATO staff, including the timeframes and expected involvement from NATO staff with the implementation and configuration activities.
- A 'Risk management' section describing the Contractor's processes supporting Risk Management by the Contractor.

4.4.2. Project Master Schedule (PMS)

The PMS will form the basis of aligning the planning between the Contractor and the Purchaser and will remain relevant throughout the lifecycle of the project.

4.4.2.1. (SHALL) The Contractor shall establish, maintain and deliver as required a PMS containing all tasks and milestones.

4.4.2.2. (SHALL) The PMS shall contain the following items unless otherwise stated by the Purchaser:

- Contain all events and milestones
- Delivery times of all documentation to be provided to the Purchaser

- Identify the critical path for the overall project
- Identify the start and finish dates, duration, predecessors, constraints (as necessary) and the total slack of each task
- Identify the main project milestones
- Identify the progress for each task
- Identify the applicable baseline, and shall show progress against the baseline
- Minimise the use of constraints and absolute dates
- Identify the main deliverables.

4.4.3. Service Delivery Plan (SDP)

The SDP shall describe the approach to Service Delivery after FSA has been reached and the Solution is in operations.

4.4.3.1. (SHALL) The Contractor shall create and maintain a SDP that describes the following items:

- Organization
  - The Contractor and Purchaser roles during the Service Delivery Phase
  - The Contractor’s Points of Contract for each of the Contractor roles
- Communication
  - Communication mechanisms for service delivery and incident response
  - Hours of availability for both incident response and service support
  - Approach to reporting, including meeting formats and report formats
- SLA
  - Metrics used for each of the items in the SLA (reference ANNEX B)
  - Traceability between system components (COTS products) and the functional requirements in this SOW
  - Patching, Security, and License management
- Changes
  - Change management process for Purchaser-initiated changes (normally perfective changes (as per ISO 9126 (reference 2.3))
  - Change management process for Contractor-initiated changes (normally corrective, adaptive, and preventive changes (as per ISO 9126 (reference 2.3)).
- Testing
  - Approach, timing, and cadence to each test related to service delivery (reference SECTION 5):
    - Monthly Stress Test
    - Yearly Fall-back Solution Test
    - Yearly Backup Test
    - Security Tests and Audits

- Contractor, Purchaser, and third-party responsibilities per test
- Risks and mitigations involved in each of the tests

4.4.3.2. Project Status Report (PSR)

The PSR is one of the mechanisms used by PMs to increase understanding and keep track of the progress of the project

4.4.3.3. (SHALL). The Contractor shall provide a weekly PSR to the Purchaser.

4.4.3.4. (SHALL) The Contractor's PSR shall at minimum summarise completed, ongoing, and upcoming activities, as well as attached updated PMS.

4.4.3.5. (SHALL) The Contractor shall ensure that the PSR summarises activities, including (but not limited to):

- Changes in key Contractor personnel;
- Summary of Contract activities during the preceding month, including the status of current and pending activities;
- Progress of work and schedule status, highlighting any changes since the preceding report;
- Change Requests status;
- Off-Specifications status;
- Test(s) conducted and results;
- Plans for activities during the following reporting period;

4.4.4. Security Accreditation Documentation Set (ADS)

The ADS contains all of the documentation required for the accreditation of the Solution.

4.4.4.1. (SHALL) The Contractor shall ensure that ADS comprises all documentation described in SECTION 8.

4.4.5. Contractor Cyber Incident Management Plan (CIMP)

4.4.5.1. (SHALL) The Contractor shall be required to deliver a CIMP that is aligned to cyber security controls in line with NATO Security Policy and its supporting directives.

4.4.5.2. (SHALL) The Contractor shall create, maintain and operate a formal incident response and forensic capability for protection of NATO Information residing on non-NATO Information Systems. The Contractor shall include the subcontractors and suppliers that perform support work that involves NATO Information.

4.4.5.3. (SHALL) The Contractor shall establish an incident-handling capability plan that consists of:

- Incident response policy and plan
- Procedures for performing incident handling and reporting
- Guidelines for communicating with outside parties regarding incidents

- Incident team structure and staffing model relationships and lines of communication between the incident response team and other groups,
- Both internal and external services the incident response team should provide, and
- Staffing and training the incident response team

4.4.5.4. (SHALL) The final Program CIMP shall be in Adobe Acrobat format with a digital signature from the Contractor cognizant authority

4.4.5.5. (SHALL) If no approved Program CIMP currently exists between the Contractor and NATO, then one must be created and submitted. If an approved Program CIMP already exists and sufficiently satisfies the CIMP requirements for the Contract, then no new CIMP delivery is required. In such cases, the Contractor in consultation with the Purchaser shall only submit a Contract Letter to the Contracting Officer stating that all CIMP requirements are satisfied by the existing Program CIMP.

4.4.5.6. (SHALL) The Contractor shall report cyber incidents that result in an actual or potentially adverse effect on the Contractor Communication and Information Systems (CIS) and/or NATO Information residing therein, or on a Contractor's ability to deliver on the requirement.

4.4.5.7. (SHALL) The Contractor shall report status of the incident-handling capability including plan-of actions for capabilities not at full operational status, and periodic operational status.

4.4.5.8. (SHALL) The Contractor shall provide status of a cyber-incident from first identification to closure as described in the CIMP.

4.4.5.9. (SHALL) The Contractor shall report cyber incidents for all section of the SOW to the Purchaser as described in the NCI Agency Special Provisions Clause, Cyber Incident Reporting.

4.4.5.10. (SHALL) The Contractor shall establish and document a digital forensics readiness plan, and upon an incident execute the plan on the Contractor CIS to include the collection, examination, analysis, and reporting.

4.4.5.11. (SHALL) The Contractor shall use a community-developed, standardized specification language for representing and exchanging information in the broadest possible range for cyber-investigation domains, including forensic science, incident response, and counter terrorism.

4.4.5.12. (SHALL) The Contractor forensic team assessment as required shall initiate corrective actions to include securing identified vulnerabilities, improve existing security controls, and provide recommendations for improvement to policies, procedures, tools, and other aspects of the forensic process.

4.4.5.13. (SHALL) Subject to the Purchaser’s consultation with the Contractor’s national cyber defense authority and/or as prescribed in the Contractor’s nation’s Memorandum of Understanding (MoU) on Cyber Defence with NATO, the Purchaser reserves the right to examine and audit all records and other evidence sufficient to reflect proper program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of NATO Information. If the Purchaser identifies any security deficiencies during the audit, the Contractor shall implement corrective actions to address the shortfalls identified during these assessments at its own expense within a timeframe agreed with the Purchaser. The Purchaser reserves the right to re-examine and audit evidence of the implemented corrective actions.

4.4.6. Requirements Traceability Matrix (RTM)

4.4.6.1. (SHALL) The Contractor shall develop and maintain a RTM that establishes a complete cross-reference between on the one hand the requirements stated in the SRS, System Security Requirements Statement (SSRS), and on the other hand the detailed contents of the SDS in terms of SDS statements and lowest-level CIs.

4.4.6.2. (SHALL) The Contractor shall maintain the RTM updated during the project lifecycle.

4.4.6.3. (SHALL) The Contractor shall provide the Purchaser with updates (via the tools) to the RTM daily during the execution of each formal test event, and following the conclusion of each acceptance test event. Content, Verification Methods to be used and the workflow for updating the RTM shall be proposed and documented in the PMTP by the Contractor and approved by the Purchaser.

4.4.6.4. (SHALL) The Contractor shall ensure that the RTM includes the following information (but is not limited to):

- List of all functional and non-functional requirements
- List of all numbered requirements in the SRA and the SSRS.
- For each requirement, two-way traceability between the requirement and the design feature that implements the requirement.
- For each requirement, identification of any Off-specifications associated with the requirement.
- For each requirement already successfully tested: identification of the test(s) or test waiver(s) on the basis of which the requirement was demonstrated.
- For each requirement not yet successfully tested: identification of the test(s) or test waiver(s) that are intended to demonstrate the requirement; identification of the associated problem report.

4.4.7. Technical System Design Specification (SDS)

4.4.7.1. (SHALL) The Contractor SDS shall describe the Solution to a level of detail that is sufficient for the Purchaser to be able to ensure that the requirements in this SOW are implemented.

4.4.8. Log Ingestion and Processing Survey (LIPS)

4.4.8.1. (SHALL) The Contractor shall support the Purchaser in the creation of a LIPS that details the logs to be provided from the solution to the Purchaser's SIEM. These logs will be a subset of the following:

- All event logs of cloud components that will process data related to the Solution
- All application of logs of the Solution
- All Security logs of cloud components that will process data related to the Solution

What logs are needed will be based on the SRA of the solution. Therefore it is important the planning takes the dependency between the SRA and the LIPS into consideration.

4.4.8.2. (SHALL) The Contractor shall include the dependency between the SRA and the LIPS in the PMP and PMS.

4.4.9. Training Plan (TP)

4.4.9.1. (SHALL) The Contractor shall provide a TP that describes the training approach, modality, planning, content, and Purchaser Involvement for the initial training activities required to make all users and application admins proficient operators of the Solution;

4.4.9.2. (SHALL) The TP shall include all the training required for the Users to execute works and responsibilities as described in 5.3.

4.4.10. Data Migration Plan (DMP)

The migration of data from the WCM and DAMS system to the solution is critical to the continuous character of the NATO websites. The Contractor shall prepare and execute a DMP that ensures safe transition of data between the systems without affecting availability.

4.4.10.1. (SHALL) The Contractor shall provide a DMP that describes the approach, activities, timing, responsibilities, risks, and rollback approach for data migration between the WCM and DAMS system and the Solution.

4.4.10.2. (SHALL) The DMP shall describe the full migration of data and metadata from the DAMS system to the Solution.

4.4.10.3. (SHALL) The DMP shall describe the migration of the initial WCM content that shall be migrated to the Solution as described by the Purchaser

4.4.10.4. (SHALL) The DMP shall describe the migration of WCM data that shall be migrated to the static archive website.

4.4.10.5. (SHALL) The Contractor shall ensure the structure, format and context of the migrated data will fit the new configuration as per the SCP (reference 4.4.12)

4.4.11. Solution Activation Plan (SOAP)

4.4.11.1. (SHALL) The Contractor shall provide a SOAP that describes the approach, activities, timing, responsibilities, risks, and rollback approach for switching end-user-traffic from the current WCM and DAMS systems to the Solution, including the activation of the fall-back solution.

4.4.12. Solution Configuration Plan (SCP)

The detailed requirements for configuring the system will have to be distilled from the User organization in the first stage of the project (reference 1.4.1.1). The Contractor shall create a collaboration process the User to ensure all the detailed configuration requirements are identified, captured, and implemented. The Contractor is free to select the most effective process but an iterative process that is based on close collaboration is advised. This requirements gathering process, together with the result will be described in the SCP.

The Contractor shall be aware that the configuration requirements will not be based on the current WCM and DAMS systems and processes. Instead, the configuration requirements shall be created “green field” with the User.

4.4.12.1. (SHALL) The Contractor shall provide a SCP that describes:

- **The Requirements Gathering Approach (RGA):** The process, planning, and Purchaser involvement to capture the solution implementation requirements from the User.
- **The Solution Configuration Approach (SCA)**: The process, planning, and Purchaser involvement to configure the Solution so these workflows, privileges, and templates are available for use by the Purchaser.

4.4.12.2. (SHALL) The Contractor shall describe the following elements in the RGA and SCA of the SCP :

- Site Templates
- Component Schemas
- Content Statuses
- Workflows
- User-groups
- Users
- Privileges
- Dashboards
- Information Exchanges
- API Configurations

4.4.13. System Test Documentation Package (STDP)

4.4.13.1. (SHALL) The Contractor shall provide a STDP as per SECTION 11.

4.5. Documentation Delivery and Review

4.5.1.1. (SHALL) The Contractor shall deliver all documents to the Purchaser in electronic format (MS Office unless otherwise stated in this SOW) for review and approval. The Purchaser shall provide reasonable effort to review and approve these documents in a timely manner.

4.5.1.2. (SHALL) The Contractor shall ensure that any documentation delivered to the Purchaser has been properly reviewed according to Contractor quality management process.

4.5.1.3. (SHALL) All documentation provided by the Contractor shall be subject to Purchaser approval. The Contract should expect additional review rounds of the documentation before acceptance by the Purchaser is achieved.

4.5.1.4. (SHALL) The Contractor shall take into account Purchaser comments and shall issue up other documentation versions as required.

The acceptance of documents by the Purchaser signifies only that the Purchaser agrees to the Contractor's approach in meeting the requirements. This acceptance in no way relieves the Contractor from its responsibilities to meet the requirements stated in this Contract.

4.5.1.5. (SHALL) The Contractor shall remain responsible for updating the documents in the course of the Contract (to correct errors, inconsistencies, omissions, etc. and to reflect changes in the system design, system implementation, support arrangements).

4.6. Design activities

4.6.1.1. (SHALL) The Contractor shall conduct the necessary activities and develop a design of the Solution at the Preliminary and Critical levels, including all interfaces to other systems to meet the SOW requirements.

4.6.1.2. (SHALL) The Contractor shall keep the SDS up to date throughout project execution, in particular in order to obtain and maintain the SA.

4.7. Solution Provisioning Activities

4.7.1. The Purchaser reserves the right to suspend the Contractor's installation and/or activation work for up to 14 calendar days to avoid interfering with or disrupting other activities.

4.7.2. Technical System Provisioning

4.7.2.1. (SHALL) The Contractor shall provision a solution that provides the functionality described in SECTION 12 and adheres to the SLA requirements in ANNEX B.

4.7.3. System Migration

(SHALL) The current WCM and DAMS systems contain data that is used daily by various users and end-users. The content, assets, metadata, user-data, workflow data, and privileges shall be migrated to the Solution.

4.7.3.1. DAMS Data

The current DAMS system contains approximately 450. TB of data consisting of videos, audios, images, texts, and metadata. This data will need to be included in the new solution to ensure its operational use in the new solution and to ensure the current on-premises DAMS solution can be decommissioned.

4.7.3.1.1. (SHALL) The Contractor shall migrate all DAMS data to the Solution according to the DMP (reference 4.4.10)

4.7.3.1.2. (SHALL) The Contractor shall preserve the logical structure in the migration of the DAMS data: hierarchies and dependencies and web content linkages.

4.7.3.1.3. (SHALL) The Contractor shall preserve the security restrictions of the content in alignment with the DAMS system and compatibility with the new solution.

4.7.3.2. WCM Data

The WCM data in the content-related data that is used on the nato.int website. A small portion of this data shall be transferred to the new solution as part of the new nato.int website while most of the data will be transferred to a Static Archive Website (SAW) that is accessible for historic reference.

4.7.3.2.1. (SHALL) The Contractor shall migrate the data of the WCM system to the Solution according to the DMP (reference 4.4.10)

4.7.3.2.2. (SHALL) The Contractor shall assist the User with the manual migration of selected content from the WCM system to the Solution to be used as active content, taking into consideration the new configuration.

4.7.3.2.3. (SHALL) The Contractor shall export the remaining data of the WCM system to the new solution as part of the SAW as per the DMP (reference 4.4.10)

4.7.4. Solution Activation

After the technical solution has been provisioned, testing has successfully concluded, and SA has been achieved, all the user-facing elements of the old WCM and DAMS system will have to be re-directed to the new solution.

4.7.4.1. (SHALL) The Contractor shall create a SOAP as per 4.4.11.

4.7.4.2. (SHALL) After Purchaser approval of the SOAP, the Contractor shall activate the Solution in close coordination with the Purchaser.

4.7.5. Solution Testing

4.7.5.1. (SHALL) The Contractor shall create a System Test Documentation Package as per 4.4.13 and in accordance with SECTION 11

4.7.5.2. (SHALL) The Contractor shall execute a series of tests to confirm that the Solution meets its requirements, in accordance with SECTION 11.

4.7.6. System Configuration

The new solution will have to be configured in a way that is aligned with the way-of-working of the PDD staff. This requires all configurable elements to be identified, captured, and implemented during the first phase of the project (reference 1.4). ANNEX D gives an indication on the complexity of the configuration.

4.7.6.1. (SHALL) The Contractor shall create a SCP as per 4.4.12.

4.7.6.2. (SHALL) After Purchaser approval of the SCP, the Contractor shall execute the SCP.

4.7.7. Training

Training of the PDD as users and application administrators of the system will be a critical part of the adoption of the solution.

4.7.7.1. (SHALL) The Contractor shall provide a TP as described in 4.4.9.

4.7.7.2. (SHALL) After Purchaser approval, the Contractor shall provide the training as described in the TP.

4.7.8. Security Accreditation

All NATO systems require SA before NATO information can be processed. Therefor the Contractor will have to work with the SAA and the Purchaser to get SA of the system before it can become operational.

4.7.8.1. (SHALL) The Contractor shall achieve SA for the Solution as per SECTION 8.

SECTION 5 : WORK PACKAGE 2: SERVICE DELIVERY YEAR UNTIL END 2028

5.1. Introduction

After the Contractor has completed the first phase and the FSA milestone has been achieved, the Contractor will continue to coordinate and operate the service on behalf of the Purchaser as per the SLA (reference ANNEX B) and the below annual requirements.

5.2. Administering and Operating the Solution

5.2.1. (SHALL) The Contractor shall continue to administer and operate the Purchaser-owned public cloud based solution in section 4.1 and the SDP (reference 4.4.3)

5.2.2. (SHALL) The Contractor shall ensure that all licenses are registered with the NCI Agency as end-User. The Contractor shall ensure that any and all User Licenses and User Agreements presented to the Purchaser for signature shall be coherent with and make cross-reference to the terms of this Contract.

5.3. Organization

During the Service Delivery phase, the roles involved with the Solution shall be different from the Solution Provisioning phase. The roles for each of the parties involved is describe below and displayed in Figure 6.

- NATO Roles

During the Solution Provisioning phase, NATO has specific roles assigned.

  - The **User** is one or more representatives of the PDD. They are the POC for all items related to service delivery and functional requirements of the Solution. The user has elevated privileges in the Solution and can connect to the Solution from a NATO network using a NATO-managed device or through Internet using a non-NATO managed device. It is planned to have 100 Users for the Solution. During this phase, the User will have the following responsibilities:
    - Application admin – able to configure the application (e.g. privileges, templates, workflows) with elevated privileges.
    - Content and asset management (e.g. creating and publishing content, creating and enriching assets).
  - The **Service Delivery Manager (SDM)** is an individual from the NCI Agency and is the main POC for all items related to technical provisioning and Contracting during this phase of the project.
  - The **SAA** is the NOS and they are the party within NATO that review the risk assessment and grant SA for the Solution
  - The **NQAR** is the NCI Agency Independent Verification and Validation (IV&V) Service line and their role is described in SECTION 12).

- 3rd Party Contractor Roles
  - The **Third Party Solution POCs** are the 3rd Party Contractors responsible for different solution that have interaction or an interaction with the Solution. These will be the primary POCs for each solution.
  - The **Third Party Users** are individuals that operate the Solution and provide content to the NATO Users. They hold privileged access to the system and do not operate from within a NATO network, but instead shall use unmanaged devices to

access the Solution. Examples of these are translators and external content contributors. It is planned to have up to 100 Third Party Users for the Solution.

- Contractor Roles

During the Solution Provisioning phase, the Contractor shall have the following roles as a minimum to the project. The Contractor is free to propose additional roles as part of the PMP.

- The **SDM** is the main POC for this phase for all items that are not related to the quality of the service or the QA of the service.
- The **CQAR** is the Contractor's POC for quality and their role is described in SECTION 12.

Next to the formal roles, there are also roles that could be utilized on an optional basis as described in SECTION 7

- End-users

The end-users are the ones that will be consuming the content and assets of the Solution. These users are the audience of the system and are categorized into three sets:

- **Regular End-users** are individuals that browse each of the sites and consume the information. They have no elevated privileges on the system and cannot downloads assets. The number of regular end-users is described in B.1.
- **Authenticated End-users** are individuals that can also browse each of the websites but they have the extended ability to download assets from the DAM portion of the Solution. This privilege is granted through single-factor authentication. There are around 10.000 Authenticated End-users.
- **Authenticated CIS** are digital systems that are allowed to connect to the Solution's API and execute download and search actions in an automated manner. These systems require authentication by the User before they are granted these privileges.

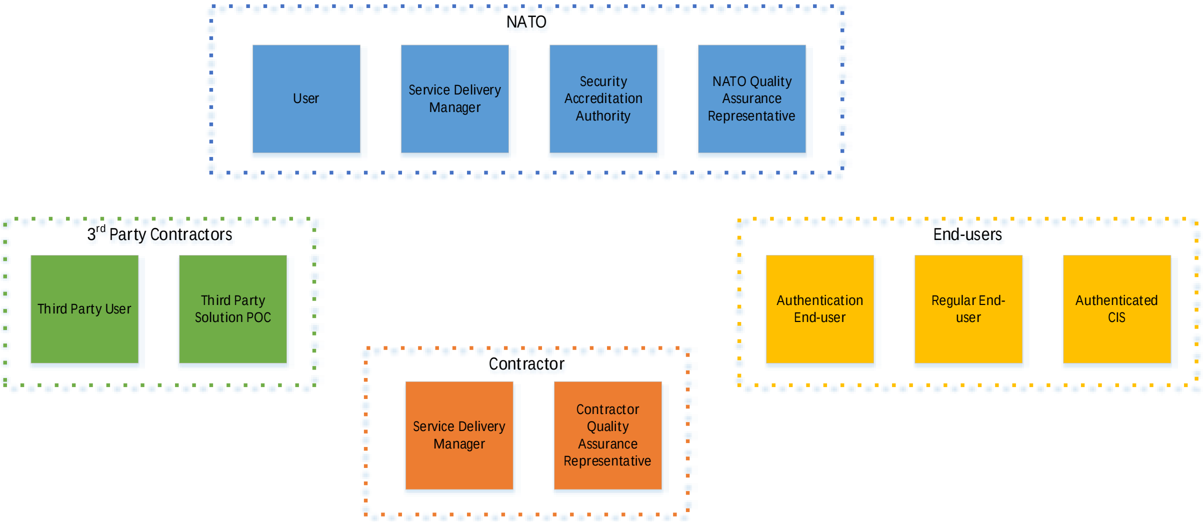


Figure 6 Roles During Service Delivery

5.4. Changes

Technology will continue to evolve over the course of this Contract. It is important that the Solution stays secure and relevant in the POP.

5.4.1. (SHALL) The Contractor shall inform the Purchaser of any significant changes in technology, software, dependencies, or best practices arising in the content management industry.

5.4.2. (SHALL) All changes considered corrective, adaptive, and preventive as per ISO 9126 (reference 2.3) shall be considered regular maintenance of the Solution and shall be executed by the Contractor without additional cost to the Purchaser.

5.4.3. (SHALL) At the request of the Purchaser, the Contractor shall incorporate any changes to the Solution that fall outside of corrective, adaptive, or preventive changes as per ISO 9126 (reference 2.3), based on the Costed Options List (COL – reference 7.2).

5.5. Monthly Stress Test

Part of the Purchaser's business continuity approach is a monthly stress test of the Solution.

5.5.1. (SHALL) On a monthly basis, the Contractor shall organize a Stress Test that is executed by the Contractor. A report of this test shall be provided to the Purchaser.

5.5.2. (SHALL) The Stress Test shall be executed by the independent third-party in close coordination with the Purchaser and the Contractor.

5.5.3. (SHALL) The Stress Test shall be based on the peak metrics for the system, as described in B.1.

5.6. Yearly Fall-back Solution Test

As the Fall-back Solutions remains critical to the business continuity approach of the Purchaser, the Fall-back Solution shall be tested on an annual basis.

5.6.1. (SHALL) The Contractor shall organize a yearly test of the Fall-back Solution together with the Purchaser.

5.7. Yearly Backup Test

Because of the historic value of the data maintained in the Solution, yearly tests of the backups shall be executed.

5.7.1. (SHALL) The Contractor shall organize a Yearly Restore Test of the backups. This includes the data backups and backups of the logs.

5.7.2. (SHALL) The Contractor shall provide the Purchaser with a report of the Yearly Restore Test.

5.8. Monthly Service Delivery Reporting

5.8.1. (SHALL) The Contractor shall provide a Monthly Service Delivery Report to the Purchaser with the following information:

- Patching
- Monthly Stress Test results
- Upcoming and ongoing changes (including status)
- Service Requests and their Status
- Overview of (security) incidents and findings

- Changes in Contractor personnel and/or points of contact
- Any downtime/service degradation in reporting period
- If applicable: results of the Fall-back test results and backup-test results
- Site usage in terms of
    - Monthly usage (# of Requests)
    - Data Transferred
    - Storage used

5.8.2. (SHALL) The Contractor shall organize a Monthly Service Delivery Retrospective meeting with the Purchaser in which the contents of the Monthly Service Delivery Report are presented.

5.9. Yearly Service Delivery Report

Next to the monthly reporting, the Contractor shall provide an annual reporting of the Service delivery of that year.

5.9.1. (SHALL) The Contractor shall provide an annual service report with an aggregate of the monthly Service Delivery Report with specific focus on outlying metrics and visible trends in the service delivery metrics.

5.10. Service Support

During the POP of the Contract, the Purchaser shall receive service support for the Solution. Service support is considered first-line helpdesk that deals with service requests, information sharing, and non-critical issues of the users.

(SHALL) The Contractor shall provide service support in the POP of the Contract from 08:00 until 18:00 on business days (excluding Belgium holidays) in the GMT+1 time zone.

(SHALL) The Contractor shall allow the Purchaser to make service request via phone and a ticketing system.

(SHALL) The Service Support shall include:

- Providing information on known issues and workarounds
- Answers to Frequently Asked Questions
- Registering of Non-critical Issues
- Logging of Feature Request
- Service Requests for changes to the following items:
    - Site Templates
    - Component Schemas
    - Content Statuses
    - Workflows
    - User-groups
    - Users
    - Privileges
    - Dashboards

5.11. Incident Response

An incident can either be discovered by the Contractor or the Purchaser and consists of two types:

- Critical – an incident (include cyber incident) that causes the end-user functionality of the Solution to be interrupted or degraded.
- Normal – an incident (including cyber incident) that causes other functionality (back-end) functionality of the Solution to be interrupted or degraded

5.11.1. (SHALL) The Contractor shall respond to Incidents from 08:00 until 18:00 on business days (excluding NATO holidays) in the GMT+1 time zone.

5.11.2. (SHALL) The Contractor shall respond to Incidents 24 hours per day during the entire duration of Critical Events (reference 1.7) and LMPs (reference 1.8).

5.11.3. (COULD) The Contractor could respond to Incidents 24 hours per day, 365 days per year.

SECTION 6 : WORK PACKAGE 3 (OPTION): ADDITIONAL 3 YEARS OF SERVICE DELIVERY

6.1. Introduction

After the Contractor has completed the first five years of Service Delivery by completing Milestone MS5 (reference 3.4.5), the Contract can optionally be extended to include another three years of service delivery.

6.2. Continuation of Service Delivery

6.2.1. (SHALL) The Contractor shall continue to deliver the service as described under Work Package 2 as described in SECTION 4.

SECTION 7 : WORK PACKAGE 4 (OPTION): ADDITIONAL CONTRACTOR SUPPORT

7.1. Introduction

During the execution of Work Package 2 and optionally Work Package 3, additional (technical) support from the Contractor might be required to further configure the system and to make perfective changes to the system (as per ISO 9126 (reference 2.3)). The Purchaser can decide to execute multiple instances of the options mentioned in this Work Package.

7.1.1. (SHALL) In the case that multiple options are needed to accomplish a perfective change to the Solution, the Contractor shall create a non-binding quote to the Purchaser that describes all options required. The process for providing and approving a quote will be established at EDC.

7.2. Costed Option List (COL)

7.2.1. (COULD) **Project Management Support** - The Contractor could provide one hour of Project Management Support where an individual is assigned to oversee all the Contractor efforts required for a significant perfective change.

7.2.2. (COULD) **Junior Technical Support** – The Contractor could provide one hour of Senior Technical Support where an individual shall plan, execute, test, and document complex perfective technical changes to the Solution.

7.2.3. (COULD) **Senior Technical Support** - The Contractor could provide one hour of Senior Technical Support where an individual shall plan, execute, test, and document complex perfective technical changes to the Solution.

7.2.4. (COULD) **Data Expert Support** - The Contractor could provide one hour of Data Expert Support where an individual execute any complex data-related effort, including but not limited to data-mining, data-analysis, data-structuring, data-migration, and data quality checks

7.2.5. (COULD) **Workflow Support** - The Contractor could provide one hour of Workflow Support where the Purchaser is assisted by an individual to make changes to the workflow of the Solution.

7.2.6. (COULD) **Content Support** - The Contractor could provide one hour of Content Support where the Purchaser is assisted by an individual to make changes to content (e.g. templates and component schemas).

7.2.7. (COULD) **Privilege Management and IAM Support** - The Contractor could provide one hour of Privilege Management and IAM Support where the Purchaser is assisted by an individual to make changes to the IAM aspect and privileges in the system (e.g. Identity Access Management and user-group management).

7.2.8. (COULD) **Solution Training** - The Contractor could provide one hour of Solution Training on the Solution as provisioned for this environment (e.g. on-the-job training). The per diem is not included in this option and will be contracted separately.

7.2.9. (COULD) **Product Training** - The Contractor could provide one hour of Product Training on one of the six products that will be provisioned as part of the Solution (reference Table 1 Short-list of WCM Products. The per diem is not included in this option and will be contracted separately.

7.2.10. (COULD) **Per Diem** – The Contractor could provide one day of travel, per diem, and any cost associated with providing any support on-premises at NATO Headquarters in Brussels, Belgium.

SECTION 8 : SECURITY ACCREDITATION

8.1. Information Classification

The Solution as well as the WCM and DAMS system have various levels of sensitive information that need to be viewed and processed by the Contractor.

- The maximum classification and ownership level of the information that is processed by the Solution is NATO UNCLASSIFIED.
- Notwithstanding the NATO UNCLASSIFIED confidentiality level of the information contained in the Solution, it is of utmost importance that the integrity and availability of the information is ensured at all times.
- While integrating with the Purchaser's CIS or CIS provided by 3rd party contractors, the Contractor might need to process NATO RESTRICTED information.

8.1.1. (SHALL) The data in the current WCM and DAMS systems as well as in the future Solution shall protected as NATO UNCLASSIFIED because the public information originated from NATO.

8.1.2. (SHALL) The Contractor shall be aware of sensitivity and ownership of the data being processed and shall adhere to the applicable Security Requirements of the data according to the policies in 2.2.3.

8.2. Security Accreditation Requirements

The SAA for the Solution is the NOS. Coordination with the SAA will be conducted by the Purchaser.

8.2.1. (SHALL) The Solution shall achieve SA, in order to demonstrate compliance with the NATO relevant Security Policy, supporting directives and system-specific documentation (e.g., System Security Requirement Statements (SSRS) and to be granted authority to go live.

8.2.2. (SHALL) To receive a SA statement from the SAA, the Contractor shall develop an ADS (reference 8.3) and obtain SAA approval for the individual documents. The Contractor should expect a number of review rounds per document before it will be approved by the SAA.

8.2.3. (SHALL) The Contractor shall produce a Security Test and Verification Plan (STVP), execute security testing witnessed by the Purchaser and formally documented in a Security Test and Verification Report (STVR) as part of the ADS.

8.2.4. (SHALL) The Contractor shall support security audits from both independent third-party auditors (selected by the Contractor) and Audits executed by the Purchaser, including but not limited to:

- Security Testing and Verification
- Type 3 Security Audits (i.e. validation tests)
- Type 4 Security Audits (i.e. pen-testing)

8.2.5. (SHALL) Type 3 and Type 4 Security Audits are conducted by the NATO Cyber Security Center (NCSC) in line with [AC/35-D/2005-REV3]. A Type 3 Security Audit audit comprises amongst others vulnerability detection, software inventory, system patching & update services, insecure port & service detection, anti-malware measures, data loss prevention and security configuration. The Audit results will be communicated in a report. The Contractor shall address any findings and recommendations from the Audit and report on remediation status.

8.2.6. (SHALL) Where the remediation of audit findings results in the modification of the design (without introducing additional components), other documentation requirements, and changes to configuration of components, the Contractor shall consider these changes to be within the technical and financial scope of this Contract; no Engineering Change Proposal (ECP) shall be generated. Where the implementation of security measures results in a requirement for additional components to be procured for implementation that could not be reasonably foreseen beforehand, an ECP shall be raised by the Contractor.

8.2.7. (SHALL) The Contractor shall take action to follow, carry out the necessary work, and to implement the advice, instructions and changes required to remediate findings resulting from security testing and security audit(s).

8.2.8. (SHALL) The Contractor shall take action to follow, carry out the necessary work, and to implement the advice, instructions and changes required by the SAA.

8.2.9. (SHALL) The Contractor shall designate Security Subject Matter Experts (SME) as points of contact for SA and security-related issues.

8.2.10. The Contractor may need to request Approval for Pilot (AfP) before the interim Security Accreditation (iSA) can be requested to the SAA. The AfP will have to be agreed by the Purchaser with the SAA, in order to define to what extent the Solution may be operated during a period of time ad until iSA is requested and granted.

8.3. Security Accreditation Documentation Set (ADS)

The achievement of the Solution SA will require a prescribed set of security documentation to be produced based on SA documentation templates. The templates will be made available to the Contractor after the EDC.

8.3.1. (SHALL) The Contractor shall produce SA documentation and provide inputs to documents in support of the Solution SA.

8.3.2. (SHALL) The Contractor shall identify and document any COTS products included in the system in the security documentation.

The documentation to be developed to support the Solution SA process is listed in the table; which also summarizes responsibilities related to the development of each document Column “Baseline/Guidance” lists available templates, relevant NATO Security Directives and Guidance, and similar documentation existing NATO CIS which can be used as an example or initial input. All Security Accreditation documents will be subject to Purchaser and SAA approval.

Document	**Baseline/Guidance**	**Contractor Responsibility (The Contractor shall)**	**Purchaser Responsibility**
Security Accreditation Plan (SAP)	Latest approved SAP template	· None	· Create the SAP

Document	Baseline/Guidance	Contractor Responsibility (The Contractor shall)	Purchaser Responsibility
CIS description (CISD)	CISD template NU Reference baselines	· Create the CISD document based on the CISD template provided by the Purchaser.	· Provide template and guidance to the Contractor · Review · Coordination with the SAA
Security Risk Assessment (SRA)	SRA template	· Provide support to Purchaser for SRA development · Address any additional technical security requirements from the SRA	· Provide SRA template · Identify scope, assets, threats and vulnerabilities · Review · Coordination with the SAA
Site Security Requirement Statement (SSRS)	SSRS template	· Develop SSRS · Provide technical input to SSRS	· Provide template · Provide guidance and support to Purchaser · Review · Coordination with the SAA
Security Test & Verification Plan (STVP)	STVP template	· Develop STVP	· Provide template · Provide guidance and support to the Contractor · Review · Coordination with the SAA
Security Test Report (STR)	STVR template	· Execute testing · Record results	· Provide test report template · Supervise and witness security testing
Security Operating Procedures (SecOPs)	SecOPs	· Production and delivery of SecOPs	· Provide generic SecOPs template · Provide guidance and support to the Contractor · Review · Coordination with the SAA

Table 9: Security Accreditation Documentation and Contractor Responsibility

Security Accreditation Plan (SAP)

8.3.3. (SHALL) A Security Accreditation Plan for the Solution shall be developed by the Purchaser.

8.3.4. (SHALL) The SAP shall describe the steps to be taken to achieve SA of the Solution.

8.3.5. (SHALL) The Contractor shall strictly adhere to the SA activities described in the SAP as approved by the SAA. All activities related with the SA process shall be identified in the PMP and correlated with the overall system design and implementation.

CIS Description (CISD)

8.3.6. (SHALL) A CISD for the Solution shall be developed by the Contractor. A template will be provided by the Purchaser.

8.3.7. (SHALL) The CISD shall be formulated by the Contractor at the earliest stage of the project. The Contractor shall maintain the CISD during the project, including all relevant information taken from the SDS as required to understand the content of the CISD document. CISD shall be standalone document and shall not refer to any document from SDS.

8.3.8. (SHALL) The Contractor shall take into account any comments from the Purchaser and SAA and shall update the CISD document as many times as necessary in order to obtain SAA approval.

Security Risk Assessments (SRA)

8.3.9. (SHALL) The Contractor shall support the development of the SRA, including risks related to modern CIS technologies and the Solution specific risks. The SRA shall be conducted in accordance with AC/35-D/1017.

8.3.10. (SHALL) The Contractor shall consider any change to be within the technical and financial scope of this Contract whenever the implementation of security measures results in the modification of the design, other documentation requirements, and changes to the Solution; no changes to the Contract shall be generated.

8.3.11. (SHALL) The Contractor shall take into account any comments from the Purchaser and SAA and shall update the SRA as many times as necessary in order to obtain SAA approval.

System-specific Security Requirements Statement (SSRS)

A SSRS will be developed, as directed by the SAA, defining the security requirements for the Solution.

8.3.12. (SHALL) The Contractor shall support the development of the SSRS to include the minimum levels of security deemed necessary.

8.3.13. (SHALL) The SSRS shall be formulated at the earliest stage of the project and shall be further developed and enhanced and updated as the project develops.

8.3.14. (SHALL) The Contractor shall take into account any comments from the Purchaser and SAA and SHALL update the SSRS as many times as necessary in order to obtain SAA approval.

Security Test and Verification Plan (STVP)

The STVP provides a plan of all security tests. The STVP shall be generated by the Purchaser with support provided by Contractor.

8.3.15. (SHALL) The Contractor shall support the development of STVP, using the STVP template provided by the Purchaser.

8.3.16. (SHALL) The Contractor shall ensure all security mechanisms are planned for testing.

8.3.17. (SHALL) The Contractor shall take into account any comments from the Purchaser and SAA and shall update the STVP as many times as necessary in order to obtain SAA approval.

Security Test and Verification Report (STVR)

The STVR provides results of all security tests specified in the STVP.

8.3.18. (SHALL) The Contractor shall execute the SAA approved STVP under the supervision of the Purchaser.

8.3.19. (SHALL) The Contractor shall produce and deliver a STVR, containing results of all security tests specified in the STVP, using the template provided by the Purchaser.

8.3.20. (SHALL) The Contractor shall ensure security test identifiers are preserved in the Report as defined in the STVP.

Security Operating Procedures (SecOPs)

SecOPs will be developed for the Solution. The SecOPs are a description of the implementation of the security measures to be adopted, the operating procedures to be followed and the responsibilities of the personnel.

8.3.21. (SHALL) The Contractor shall deliver the Solution SecOPs using the template provided by the Purchaser.

8.3.22. (SHALL) SecOPs shall also cover all security requirements identified in the SRA and SSRS which are not fully fulfilled by technical countermeasures. For example, following security procedures should be addressed (not exhaustive list):

- System configuration and maintenance;
- System backup;
- System recovery, etc.

8.3.23. (SHALL) The Contractor shall take into account any comments from the Purchaser and SAA and shall update the SecOPs as many times as necessary in order to obtain SAA approval.

8.3.24. Security Documentation Review

All documents for SA shall be subject to Purchaser and SAA review and approval. The Contractor should expect a number of review rounds per document before it will be approved by the SAA.

8.3.25. (SHALL) The Contractor shall produce Security Documentation under the close supervision and guidance of Purchaser’s specialists.

8.3.26. (SHALL) The Contractor shall submit Security Documentation to the Purchaser for review before submission to SAA for approval.

8.3.27. (SHALL) The Contractor SHALL take into account any comments from the Purchaser and SAA and shall update the ADS as many times as necessary in order to obtain SAA approval.

8.3.28. Security Mechanisms to be implemented by the Solution

The Security Mechanisms to be implemented by the Solution will be based on:

a. The outcome of the SRA, and

b. CIS Security Technical and Implementation Directive for the Security of Web Applications (Reference 2.2.3) and

c. Technical and Implementation Directive for the Protection of NATO Information within Public Cloud-Based Communication and Information Systems (Reference 2.2.3), and

d. Technical and Implementation Directive on CIS Security (Reference 2.2.3), and

e. Technical And Implementation Directive For The Interconnection Of Communications And Information Systems (Reference 2.2.3).

8.3.29. (SHALL) The Contractor shall address SRA-recommended changes in security mechanisms in the design.

8.3.30. (SHALL) The Contractor, in the Solution design, shall include implementation of the Security Mechanisms and provide full traceability of high level security measures requirements down to the implementation level.

8.3.31. (SHALL) The Contractor shall maintain an end-to-end traceability of the required security measures throughout the project.

8.3.32. (SHALL) The Contractor shall include any additional security measures resulting from the follow-on risk assessments as part of the end-to-end traceability.

8.3.33. (SHALL) The Contractor shall design the security mechanisms for the Solution to be complementary to not overlap with the NATO wide IA Services capability already provided by other NATO systems.

8.3.34. (SHALL) The Contractor shall design the Solution security mechanisms to integrate with the existing NATO wide IA Services capability.

8.3.35. (SHALL) The Contractor shall implement the security mechanisms, approved by the Purchaser after coordination with the SAA, as a part of the Solution design and SA work and shall produce the associated documentation.

SECTION 9 : NATO INFORMATION PROTECTION

9.1. (SHALL) The Contractor shall identify all NATO Information associated with the execution and performance of this Contract. At the post-award conference, the Contractor and Purchaser PM shall identify and affirm marking requirements for all NATO Information to be provided to the Contractor, and/or to be developed by the Contractor, associated with the execution and performance of this Contract.

9.2. (SHALL) The Contractor shall track all NATO Information associated with the execution and performance of this Contract. The Contractor shall document, maintain, and upon request, provide to the Purchaser, a record of subcontractors, vendors, and/or suppliers who will receive or develop NATO Information and associated with the execution and performance of this Contract.

9.3. (SHALL) The Contractor shall restrict unnecessary sharing and/or flow down of NATO Information associated with the execution and performance of this Contract – in accordance with NATO marking and dissemination requirements and based on a 'need-to-know' to execute and perform the requirements of this Contract.

9.4. (SHALL) The Contractor shall develop and store all NATO technical data (e.g., source code) in a secure facility. The Contractor shall prevent computer software, in the possession or control of non-NATO entities on non-NATO information systems, from having connections to the network through segregation control (e.g., firewall, isolated network, etc.).

9.5. (SHALL) The Contractor shall flow down the requirements of this clause to their subcontractors, vendors, and/or suppliers.

SECTION 10 : SAFEGUARDING OF NATO RESTRICTED INFORMATION

10.1. (SHALL) The Contractor shall identify all NATO Information associated with the execution and performance of this Contract. At the post-award conference, the Contractor and Purchaser PM shall identify and affirm marking requirements for all NATO Information to be provided to the Contractor, and/or to be developed by the Contractor, associated with the execution and performance of this Contract.

10.2. (SHALL) The Contractor shall track all NATO Information associated with the execution and performance of this Contract. The Contractor shall document, maintain, and upon request, provide to the Purchaser, a record of subcontractors, vendors, and/or suppliers who will receive or develop NATO Information and associated with the execution and performance of this Contract.

10.3. (SHALL) The Contractor shall restrict unnecessary sharing and/or flow down of NATO Information associated with the execution and performance of this Contract – in accordance with NATO marking and dissemination requirements and based on a 'need-to-know' to execute and perform the requirements of this Contract.

10.4. (SHALL) The Contractor shall develop and store all NATO technical data (e.g., source code) in a secure facility. The Contractor shall prevent computer software, in the possession or control of non-NATO entities on non-NATO information systems, from having connections to the network through segregation control (e.g., firewall, isolated network, etc.).

10.5. (SHALL) The Contractor shall flow down the requirements of this clause to their subcontractors, vendors, and/or suppliers.

SECTION 11 : TEST, VERIFICATION AND VALIDATION

11.1. TV&V activities

11.1.1. (SHALL) All information items used during the verification and validation activities shall be handled according to their security classification, in accordance with the applicable Security Directives (reference 2.2.3).

11.1.2. (SHALL) The Contractor shall have the overall responsibility for meeting the TV&V requirements and conducting all related activities. This includes the development of all TV&V documentation required under the Contract, the conduct of all-independent verification and validation as well as the evaluation and documentation of the results.

11.1.3. (SHALL) All Contract-related deliverables supplied by the Contractor shall be verified and validated to meet the requirements of this Contract.

11.1.4. (SHALL) All document-based deliverables shall be produced in a manner compliant with the templates provided by the Purchaser.

11.1.5. (SHALL) Each (Acceptance) Test Event shall start with the Test Readiness Review (TRR) and finishes with the Event Review Meeting (ERM).

11.1.6. (SHALL) During each (Acceptance) Test, a daily progress debrief shall be scheduled. Participation to the daily progress debrief will be agreed between Purchaser and Contractor. The aim of the debrief is to get a common understanding on what tests were run, which passed, which failed, and whatever defects were reported during the day.

11.1.7. (SHALL) For each TV&V activity, the Contractor shall provide log/record of the event, including but not limited to individual test results, defects found, requirement coverage, test execution durations, deviations during execution and sign-off for each result by both the Contractor and Purchaser.

11.1.8. (SHALL) The Contractor shall support Purchaser led Validation activities to confirm that the Solution is fit for purpose.

11.1.9. (SHALL) The Contractor shall be responsible for the planning, execution and follow-up of all TV&V activities. The Purchaser will assist in preparations by reviewing and providing feedback on all Contractor produced Configuration Items. The Purchaser will also provide testing and Functional Expertise during all TV&V activities to witness and assist with these activities.

11.1.10. (SHALL) The Contractor shall demonstrate to the Purchaser that there is a Test Process in place for the project, supported by Contractor QA.

11.1.11. (SHALL) Where requested by the Purchaser, the Contractor shall provide test data to support all TV&V activities. Test data shall be prepared by Contractor with support from the Purchaser and made available before each test activity. The Contractor shall provide, if necessary, a Data Sheet with all Master data needed to execute the test scenarios.

11.1.12. (SHALL) The Contractor shall follow the Purchaser defined TV&V processes.

11.1.13. (SHALL) If the Contractor wishes to propose a modification to the process, the proposal shall be approved by the Purchaser and documented accordingly.

11.1.14. (SHALL) The Contractor shall ensure that rigorous testing, including regression testing when required, is performed at every step in order to identify and correct defects as early as possible and minimise impact on cost and schedule.

11.1.15. (SHALL) All test, verification and validation material developed and used under the Contract shall be delivered to the Purchaser.

11.1.16. (SHALL) The Contractor shall appoint a Test Manager (See Section 2.3.4.11) for the activities defined in Table 6. Who will work closely with the Purchaser's assigned NQAR. The Purchaser will appoint Functional Experts for each test activity.

11.1.17. (SHALL) The Contractor shall have the overall responsibility for meeting the TV&V requirements and conducting all related activities during each Test Step or Event defined in Table 6 below:

Phase	TV&V Activity	Purchaser Involvement
Phase 1 (Solution Provisioning)	**System Integration Test (SIT)** – Requirements based testing, focused on verifying integration of the different components together and with any external interface as defined by the SOW. Including but not limited to the Purchaser SIEM, the Purchaser Edge Security Solution, and APIs with external systems **User Acceptance Test (UAT)** – Scenario based testing, focused on validating the system as per User needs. Testing by users to determine whether or not a system complies with its functional requirements and satisfies user needs. **Initial Stress Test (IST)** – Initial peak-test of the non-functional requirements of the Solution. The Initial Stress Test shall test all elements described in the SLA (reference ANNEX B) under the peak circumstances described in B.1. **Fall-back Solution Test (FBST)** - Operational test of the Fall-back Solution described in 5.5. This test shall validate the readiness of the fallback Solution to be activated by the Purchaser at any time. **Pre-activation-test (PAT) –** A regression test of the SIT, UAT, IST, and FBST after the WCM and DAMS data have been transferred to the Solution. This test shall assess the readiness for the Solution to be activated.	**Review**: Test Plans, Test Data, Test Planning, and Test Reports of all tests in phase 1. **Participate:** Test Preparation of the Purchaser owned Systems and test execution/witness.

Phase	TV&V Activity	Purchaser Involvement
Phase 2 and optionally phase 3 (Service Delivery)	**Monthly Stress Test (MST)** – Peak-test of the non-functional requirements of the Solution. The Monthly Stress Test shall test all elements described in the SLA (reference ANNEX B) under the peak circumstances described in B.1. **Yearly Fall-back Solution Test (YFBST)** - Annual test of the Fall-back Solution described in section A.1.5. This test shall validate the readiness of the fallback Solution to be activated by the Purchaser at any time. **Yearly Backup Test** – Annual restoration test of both the data-backups and the log backups. This test is to verify both types of backup adhere to the restoration-time and retention time described in the SLA (reference ANNEX B)	**Review**: Test Plans, Test Data, Test Planning, and Test Reports of all tests in phase 2 and optionally phase 3. **Participate:** Test Preparation of the Purchaser owned Systems and test execution/witness.

Table 6 - List of TV&V Activities

11.1.18. The Purchaser reserves the right to monitor and inspect the Contractor's TV&V activities to verify their compliance with the requirements set forth in this Contract.

11.1.19. (SHALL) The Contractor shall only proceed to the next formal TV&V activity, after the successful achievement of the previous TV&V activity and after the agreement/approval by the Purchaser.

11.1.20. (SHALL) The Contractor shall generate and deliver automated test procedures/cases compatible with Purchaser test management and automation tools.

11.1.21. (SHALL) The Contractor shall make use of automated testing and supporting testing tools (Test management, requirement coverage, defect management, etc.) to the maximum applicable extent, for all system development, implementation, internal and formal tests. The process and proposed supportive tools shall be described in the Project Master Test Plan (PMTP).

11.1.22. (SHALL) The Contractor shall identify and describe in the Project Master Test Plan (PMTP) which best practices and international standards will be applied and how.

11.1.23. (SHALL) The Contractor shall describe how the Quality Based Testing is addressed and implemented in the PMTP. ISO 25010 should be used as product quality criteria model.

11.1.24. (SHALL) The Contractor shall describe all formal TVVA activities in the PMTP with testing methodology and strategy that fit the development methodology chosen by the Project.

11.1.25. (SHALL) At the start of each Test Steps or Event, the Contractor shall follow TV&V process defined in PMTP to perform the following activities:

- Planning and management of the test activity;

- The design and development of all tests cases and associated documentation required under this Contract;
- Running a TRR to go through the TRR checklist;
- The conducting of all testing;
- Reporting the results in a Test Review Meeting (TRM) ; and,
- Closure of the test Event (including the final version of all test artefacts created during the test event, providing an updated status of requirements verified and an updated status of all defects).

11.1.26. (SHALL) The Contractor shall describe in the PMTP the proposed testing methodology to complete and achieving the success in all the test phases and shall describe how the following objectives will be met:

- Compliance with the requirements of the Contract;
- Verification that the design produce the capability required;
- Compatibility among internal system components;
- Compliance with the SRS requirements;
- Compliance with external system interfaces and/or systems;
- Confidence that system defects are detected early, classified and tracked through to correction, including re-test and regression approach;
- Compliance with Purchaser policy and guidance (i.e. security regulations, etc.)
- Operational readiness and suitability; and
- Product Quality Criteria.

11.1.27. (SHALL) The Contractor shall describe the Contractor’s Test Organization and its relationship with the Contractor’s Project Management Office and Quality Assurance (QA) functions in the PMTP.

11.1.28. (SHALL) The Contractor shall describe in the PMTP the “Entry” and “Exit” criteria for each of the formal TVVA events. The Contractor shall seek approval of all criteria related to an event not later that the TRR of the event.

11.1.29. (SHALL) The Contractor shall provide in the PMTP the schedule, location and scope for all the events to be run, specifying to which phase they belong. When the Contractor identifies that multiple events are required for a phase, this shall also be specified in the PMTP.

11.1.30. (SHALL) The Contractor shall provide together with the PMTP a Defect Reporting and Management Plan (DRMP) to explain the Defect Reporting and Management process to be applied during all TVVA activities. Additionally, Contractor shall describe how defects/non-conformances encountered during TVVA events will be reported, managed and remedied.

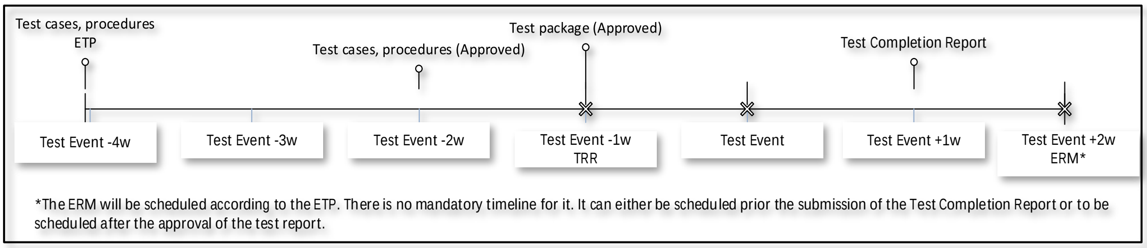
11.2. Deliverables

11.2.1. (SHALL) The Contractor shall provide a STDP, that is comprised of the following documents:

Deliverable	Sent to Review/Approve
The Project Master Test Plan (PMTP)	With the PMP
Event Test Plans for individual test events (ETP)	30 calendar days before start of TV&V event (i.e. Test Step)
Any submitted test Waivers together with supporting material	30 calendar days start of TV&V event
The Test Cases/Scripts/Steps	30 calendar days before start of TV&V event
Status Reports	Periodically (to be defined in the PMTP)
Test Completion Report	7 calendar days after end of TV&V event

Table 7 - Test Deliverables

The following timeline indicates by when the deliverables need to be provided to the Purchaser (and approved by the Purchaser) for each Test iteration (dates follow the timelines of the previous table):



*The ERM will be scheduled according to the ETP. There is no mandatory timeline for it. It can either be scheduled prior the submission of the Test Completion Report or to be scheduled after the approval of the test report.

Figure 7 Test Event Timeline

11.2.2. (SHALL) Modification of inaccurate or inadequate TV&V deliverables and any subsequent work arising as a result shall be carried out at the Contractor's expense.

11.2.3. (SHALL) Templates provided by the Purchaser are to be utilized by the Contractor as structure guides and for the content, the Purchaser expects to be detailed. If the Contractor would like to propose a modification of the templates, it shall be approved by the Purchaser.

11.2.4. (SHALL) All deliverables shall undergo as many review cycles as are required, and shall be approved once all deficiencies have been corrected.

SECTION 12 QUALITY ASSURANCE

12.1. Introduction

12.1.1. (SHALL) The Contractor shall establish, execute, document and maintain an effective QA programme throughout the Contract.

12.1.2. (SHALL) The QA programme shall apply both the Contractual requirements and the NATO requirements for ISO 9000/ 9001:2015 (reference 2.3.1) to provide confidence in the Contractor’s ability to deliver products that conform to the Contractual requirements.

12.1.3. (SHALL) If any inconsistency exists between the SOW requirements and the references, the SOW requirements shall prevail.

12.1.4. (SHALL) The Contractor‘s QA effort shall apply to all services and products (both management and specialist) to be provided under the Contract. This includes all software and documentation being developed, designed, acquired, installed, integrated, maintained, or used under the Contract.

12.1.5. (SHALL) The Contractor‘s QA efforts shall ensure that procedures are developed, implemented and maintained to adequately control the design, development, production, purchasing, installation, inspection, testing, configuration management and customer support of all services and all products, in accordance with the requirements of this Contract.

12.2. Roles and Responsibilities

12.2.1. (SHALL) During the entire Contract implementation, the NQAR(s) assures the Contractor's compliance with all Quality related Contractual requirements. The Purchaser, through its NQAR(s), is the authority concerning all Quality related matters.

12.2.2. (SHALL) The Contractor shall be responsible for assurance and control of quality for all deliverables and associated Contractual products, processes and services through the Contract.

12.2.3. (SHALL) The CQAR shall be accountable for the compliance to the defined QA process.

12.2.4. (SHALL) The CQAR(s) shall be responsible for assessing that the Contractual requirements have been complied with, prior proposing the Contractual services and products.

12.2.5. (SHALL) The CQAR shall report to a distinct manager within the Contractor's organisation.

12.2.6. (SHALL) The CQAR shall be the POC for interface with and resolution of quality matters raised by the NCI Agency or its delegated NQAR.

12.2.7. (SHALL) The Contractor shall support any Purchaser or its delegated NQAR activity focused on monitoring Contractor activities at Contractor’s facilities or other sites related to the development, testing and implementation. In particular, the Contractor shall:

- Make themselves available to answer questions and provide information related to the project,
- Allow the Purchaser representatives to inspect and monitor testing activities, and management, technical and quality processes applicable to the project.

- Transfer to the Purchaser representatives all information deemed necessary to perform the QA activities, on his/her own initiative or on request by the Purchaser representative.

12.2.8. (SHALL) The Contractor shall ensure that CQAR(s) have the required qualifications, knowledge, skills, ability, practical experience and training for performing their tasks.

12.2.9. (SHALL) The CQAR(s) shall have sufficient responsibility, resources, authority and independence to review and evaluate activities, identify problems and initiate or recommend appropriate corrective actions.

12.2.10. (SHALL) The CQAR(s) shall participate in the early stages of the project to ensure that all quality related requirements are specified in plans, standards, specifications and documentation.

12.2.11. (SHALL) The Contractor, through its CQAR(s), shall be responsible for product quality control and for submitting to Purchaser acceptance products, supplies and services that conform to Contractual requirements only.

12.2.12. (SHALL) The Contractor shall maintain and, when required, deliver objective evidence of this conformance.

12.2.13. (SHALL) The Contractor shall prepare the testing process according to the Contractual requirements and ISO/IEC/IEEE 29119 and ISO/IEC/IEEE-29119-3 (reference 2.3.1)

12.2.14. (SHALL) The Contractor shall perform verification and validation of the Contractual deliverables before proposing them for the Purchaser review and approval.

12.3. Quality for Project Documents

12.3.1. (SHALL) A formal change management process shall be applied to all project documents, including documents naming conventions as defined by the Purchaser and coordinated with the Contractor.

12.3.2. (SHALL) Project documents shall be configuration controlled. Each version of a project document is subject to Purchaser approval (unless otherwise specified).

12.3.3. (SHALL) The Contractor shall ensure that any change related to the project documents are controlled, with the identity, approval status, version and date of issue are clearly identified.

12.3.4. (SHALL) Project documents file names shall not contain any variable part, like version number, reviewer initials or maturity status. Version numbers and maturity status shall be designated in the document content and/or attributes.

SECTION 13 SYSTEM REQUIREMENTS SPECIFICATION (SRS)

A.1. Functional Requirements

This section describes the functional requirements of the Solution.

A.1.1. General Functional Requirements

A.1.1.1. (SHALL) The Solution shall provide any and all out-of-the-box functionality provided by one the six products in Table 1 Short-list of WCM Products.

A.1.1.2. (SHALL) The Solution shall be configured according to the System Configuration Plan (reference 4.4.12)

A.1.1.3. (SHALL) The Solution shall contain the sanitized data from both the WCM and DAMS system, according to the DMP (reference 4.4.10)

A.1.1.4. (SHALL) The Solution shall comply with the CIS Security Technical and Implementation Directive for the Security of Web Applications (reference 2.2.3)

A.1.1.5. (SHALL) The Solution shall comply with the Technical and Implementation Directive for the Protection of NATO Information within Public Cloud-Based Communication and Information Systems (reference 2.2.3)

A.1.1.6. (SHALL) The Solution shall receive SA as described in SECTION 8.

A.1.1.7. (SHALL) The Solution shall support different domain names (top URL) per site (e.g.: www.nato.int, www.nato-example-event.nato.int)

A.1.1.8. (SHALL) The Solution shall support multisite functionality allowing the creation and management of multiple sites, as well as the management of and access to content on different sites through a centralized system.

A.1.1.9. (SHALL) The end-user facing aspect as well as the user-facing backend of the system shall be accessible in all common modalities (for example phone, browser, and tablet).

A.1.2. Static Archive Website (SAW)

The Solution shall contain small portion of the (most actual) content data residing in the WCM system. For historic purposes, it is critical that the remaining WCM content stays available to the end-users in a static and searchable format.

A.1.2.1. (SHALL) The Solution shall provide a SAW of all the content on the nato.int website at the time of the Solution Activation Completed milestone (reference 3.4.4) for the duration of the Contract.

A.1.2.2. (SHALL) The Solution shall have no elements in the SAW that allow the user to interact with the website other than navigation and search (e.g. no subscription subscriptions forms, etc.)

A.1.2.3. (SHALL) The Solution shall provide end-users that access the SAW with a notification that they are visiting the archived version of the nato.int website.

A.1.2.4. (SHALL) The Solution shall report dead links in the SAW, both within the SAW or for external links. The Solution shall have a redirect configurable interface where customer notifications can be created for 301 (moved permanently) and 302 (moved temporary) HTTP response codes.

A.1.3. **Backup**

The backup strategy is split-up between the backup of content and assets, and the backup of logs that are required by the NATO Security Directives. Each type of backup has different requirements in terms of retention time and time to restore (reference ANNEX B).

A.1.3.1. (SHALL) The Solution shall create a backup strategy for the Solution logs in accordance with the Security Requirements as defined in SECTION 8 and 2.2.3.

A.1.3.2. (SHALL) The Solution shall ensure backups of the Solution's content and assets are retained for the full POP of the Contract.

A.1.4. **Purchaser Backup**

A Purchaser-maintained copy of the Solution data is part of the Purchaser's backup and archiving strategy.

A.1.4.1. (COULD) The Contractor could provide a monthly full backup of all asset-data of the Solution to a location specified by the Purchaser. The Contractor could provide a weekly incremental backup of all new and/or changed asset-data of the Solution to a location specified by the Purchaser

A.1.5. **Fall-back Solution**

Given the nature of the information that will be processed by the Solution, compromised data on the website and possible defacement is considered one of the major risks. Part of the disaster planning by the Purchaser is the ability to activate a Fall-back Solution that reverts the website to an older state before it was compromised.

A.1.5.1. (SHALL) The Solution shall have a Fall-back Solution that can be activated if the origin server(s) of the Solution have been compromised or there is loss of service

A.1.5.2. (SHALL) The Solution shall allow for a mechanism that only NATO can activate the Fall-back Solution

A.1.5.3. (SHALL) The Solution shall ensure that the Fall-back Solution can be activated at all times (even then when the data and origin of the Solution have been compromised and are not reachable)

A.1.5.4. (SHALL) The Solution shall ensure that there are three points-in-time to which the Fall-back Solution can revert:

- 2 Hours from activation
- 24 Hours from activation
- 72 Hours from activation

The Fall-back Solution shall remain updated according to the service level described in the SLA (reference ANNEX B) even if the Fall-back Solution is activated. It is acceptable that the information displayed by the Fall-back Solution is static and can only be manually updated by the Purchaser.

A.1.6. **Workflows and Templates**

To maximize usability and to maintain a consistent look and feel towards the end-user of the Solution, re-use of information in the system is encouraged. Therefore, the system shall consist of re-usable site templates and content component schemas that can be shared amongst the users of the system. The correlation between these items is displayed in Figure 8 Solution Information Structure. An example of a typical User Journey is described in ANNEX D.

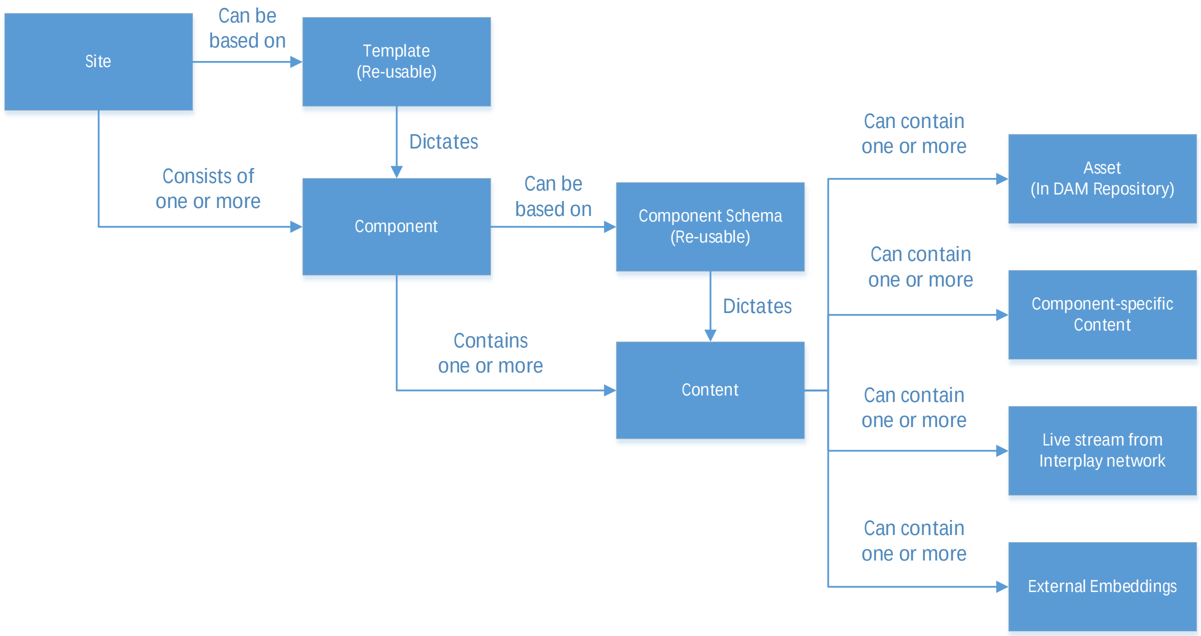


Figure 8 Solution Information Structure

A.1.6.1. (SHALL) The Solution shall provide re-usable templates and content components and shall provide an easy way to build new templates and custom content components.

A.1.6.2. (SHALL) The Solution shall keep the history of content templates so point-in-time rollbacks of content are possible.

A.1.6.3. (SHALL) The Solution shall ensure content is managed in workflows

A.1.6.4. (SHALL) The workflows shall be configurable based on business rules and based on the following criteria:

- Stage of the workflow
- Type of content
- Status of the content
- User assigned to the content

A.1.6.5. (SHALL) The Solution shall ensure content can be assigned to users and that user privileges can be limited based on the following actions on the content:

- Create
- Read
- Update
- Delete

- Publish
- Move
- De-publish
- Retire

A.1.7. **Usability**

A.1.7.1. (SHALL) All end-user facing elements of the Solution shall comply with the latest version of the Web Content Accessibility Guidelines (WCAG) on the AA level.

A.1.8. **Content**

A.1.8.1. (SHALL) The Solution shall use content components. These components can consist of the following items:

- A What You See Is What You Get (WYSIWYG) content editor with the following options:
    - Header: H1, H2, H3, H4, H5, H6
    - Paragraph
    - Text format: bold, underline, strikethrough, italic
    - Unordered list
    - Ordered list
    - Nested list
    - Link (both internal reference links as external links)
    - Table
    - Paste without formatting
    - Code / Source view & editor
    - CSS styles
    - Inline images
    - JavaScript
- Assets from the DAM functionality of the system (photo, audio, video).
- Metadata from the assets in the DAM functionality of the system
- The EXIF metadata of images
- IPTC metadata of images
- Embedded references (e.g. embedded Tweets and YouTube videos).
- HTML Forms (potentially through FormStack)
- Live Video streaming (in H264/AAC or HLS/MP4)
- Information from external system received through API, including:
    - TALEO
    - Campaign Monitor
    - Emply

- Twitter
- Youtube
- FormStack (or any other external forms provider)
- Theo Player (or any other external video player)
- Any other APIs that receive data and are included in the SCP (reference 4.4.12)

A.1.8.2. (SHALL) The Solution shall allow users to create component schemas that pre-define the elements that should be contained within a content component.

A.1.8.3. (SHALL) The Solution shall allow for sharing and re-use of the component schemas among users.

A.1.8.4. (SHALL) The Solution shall have the ability to bulk manage content statuses, at least:

- Content publication and de-publication
- Content deletion
- Content workflow status updates
- Content duplication
- Content moving
- Assign content to a user
- Viewport/device configurable

A.1.8.5. (COULD) The Solution could have the possibility to choose if a component block should be visible according to the select device / viewport. For example: Component X can be hidden on mobile but shown on desktop. Component Y can be hidden on desktop but shown on mobile only.

A.1.8.6. (SHALL) The Solution shall store the history of content changes with version control. Each content change should be stored as a new version both for drafts as well as published content.

A.1.8.7. (COULD) The Solution could provide a comparison interface to view and compare change between content versions. For multimedia assets (video and audio) only versioning for metadata is required.

A.1.8.8. (SHALL) The Solution must have advanced scheduling for content publishing with and de-publishing, based on a date and time.

A.1.9. **Content Editing**

A.1.9.1. (SHALL) The Solution shall have a WYSIWYG page builder to generate stand-alone pages (for example: event pages). These stand-alone pages shall not be constraint by a content schema and can use component-blocks.

A.1.9.2. (SHALL) The Solution shall contain provide easy way for the user to preview content in the final look & feel before publishing where the preview is a 100% match with the final publication.

A.1.9.3. (SHALL) The Solution shall allow users to select and/or upload multiple assets when creating content.

A.1.9.4. (COULD) The Solution could have an integrated A/B testing suite. The editor could configure a test based on:

- defined pages
- test duration
- extra known visitor criteria such as region, visit count, general known interest of previous visits

A.1.9.5. (COULD) The Solution could have a Social media preview to show Users how the page will show up in social media platforms like:

- Google Search
- Bing Search
- Facebook share
- Twitter share
- LinkedIn share

A.1.10. Dashboard and Notifications

A.1.10.1. (SHALL) The Solution shall provide dashboard functionality that shall be configured according to the SCP (reference 4.4.12) and shall at least display the following real-time information:

- Overview of all individual content blocks and the state of that content
- Overview of all changed content, including the status change and date/time of change
- End-user engagement metrics of the individual content blocks, including views, clicks, shares, audio clicks and video views
- End-user engagement metrics of individual sites and the aggregate of content blocks used in that website.

A.1.10.2. (COULD) The Solution could send notifications of content status updates. For example as an e-mail or SMS.

A.1.11. Content Publishing

Publishing content refers to the act of displaying information to the end-user optimally adapted to standard devices (e.g. smartphone, tablet, desktop) through one of the sites provided by the Solution.

A.1.11.1. (COULD) The Solution could have a customisation features to personalize content/target audience/authenticated visitors on the level of content block.

A.1.11.2. (SHALL) By default the Solution shall provide an auto-generated, unique, and human readable URL (slug) for the generated content. This will be based on the page title.

A.1.11.3. (SHALL) The Solution shall allow the editor to overwrite the auto-generated URL with a custom input. The Solution will validate the input on submissions to see if the exact URL is not yet in use. An URL must be unique.

A.1.11.4. (COULD) The Solution could allow the user to enable a generated short URL for the current content. The Solution must preserve this URL. Even if the linked content is removed, the URL may not be reused. The shorted URL returns response code 301.

A.1.11.5. (COULD) The Solution could implement Canonical tag to indicate the canonical URL if multiple URL's exist for the same page.

A.1.11.6. (SHALL) The Solution shall report dead links, both within the Solution or for external links.

A.1.11.7. (COULD) The Solution could have a redirect configurable interface. The editor can configure URLs to redirect to a new URL with HTTP response code 301 (301 Moved permanently) or 302 (302 Moved temporarily).

A.1.11.8. (SHALL) The Solution shall provide system generated SEO metadata constructed from the content. Users shall be able to overwrite this metadata when required. This metadata includes, but is not limited to:

- <title> tags
- og:title
- og:url
- og:type
- og:description
- og:image
- og:site_name
- twitter:title
- twitter:description
- twitter:url
- twitter:image
- twitter:site

A.1.11.9. (COULD) The Solution could allow the management of email responses: view, re-send, tag and archive.

A.1.12. Integrations and connections

A.1.12.1. (SHALL) The Solution shall provide an API for content delivery so content can be shared without the visual layer and in pure data form.

A.1.12.2. (SHALL) The API shall have a REST architecture.

A.1.12.3. (SHALL) The API shall have a GraphQL architecture.

A.1.12.4. (SHALL) The Solution shall allow live streaming in H264/AAC format to be embedded content blocks on the sites.

A.1.12.5. (SHALL) The Solution shall integrate with Google Analytics using Google Tag Manager or a similar web analysis service.

A.1.12.6. (SHALL) The Solution shall integrate with the Purchaser SIEM Solution

A.1.12.7. (SHALL) The Contractor shall configure the Cloud Service such that it integrates with the Purchaser's services including Security Monitoring and Incident Management, and write procedural descriptions for NCSC to include the Cloud Service into the NATO Enterprise scope. The Solution shall provide security and event logs of all services, components, and devices that are utilised by the Solution.

A.1.12.8. (SHALL) The Solution shall be accessible from the Purchaser's Magellan network and Interplay network, while maintaining compliance with the applicable NATO security directives (reference 2.2.3)

A.1.12.9. (SHALL) The Solution shall provide Email functionality for mass emailing, with configurable addressees list, content templates and scheduling.

A.1.12.10. (SHALL) The Solution shall provide Web Forms functionality based on HTML 5 standards for user input.

A.1.12.11. (SHALL) The Solution shall be able to publish video and audio to a dedicated player that supports multiple tracks for audio for different languages.

A.1.12.12. (SHALL) The Solution shall integrate with systems like Taleo and Emply, or similar to sync career information that is published to the end-users through content blocks.

Next to the functional integrations the Contractor shall also ensure integration with the Purchaser's SIEM and Edge Security Solution are present to maintain the security posture and response for the Solution

A.1.13. Security Information and Event Management System (SIEM) Integration

The Purchaser's' SIEM solution ingests a subset of event logs, security-logs, and application logs of different systems within the Solution. The exact logging ingestion and processing requirements are based on the Solution's SRA and can only be detailed after a LIPS.

A.1.13.1. (SHALL) The Solution shall integrate with the Purchaser SIEM Solution

A.1.13.2. (SHALL) The Solution shall provide logs to the Purchaser According to the LIPS (reference 4.4.8) until the end of the POP.

A.1.13.3. (SHALL) The Solution shall provide the logs near real-time. Meaning that the logs have to be ingested by the Purchaser SIEM Solution < 1 minute.

A.1.13.4. (SHALL) The Solution shall provide the logs in in one of the following ways:

- Through a SPLUNK universal forwarder – configured by the Purchaser
- Through delivery of logs in JSON format

A.1.14. Integration Edge Security Solution

The Purchaser uses an enterprise-wide Solution for the edge security protection of Internet-facing websites.

A.1.14.1. (SHALL) The Solution shall integrate with the Purchaser's Secure Edge Protection Solution as per the Solution documentation and guidance from the Purchaser (reference 2.3.2).

To avoid conflicts in functionality, certain Security Elements shall not be included in the Solution.

A.1.14.2. (SHALL NOT) The Contractor shall not provide Boundary Web Application Firewall, API protection, Distributed Denial of Service Protection, Rate Limiting, Content Delivery Network Services, and Bot Management.

A.1.15. Digital Asset Management

Digital assets are all the “NATO Generated” assets that are used in the Solution. These assets are used for historic purposes but also serve as input to the different content components of the system. Figure 9 gives a schematic overview of the DAM within the Solution.

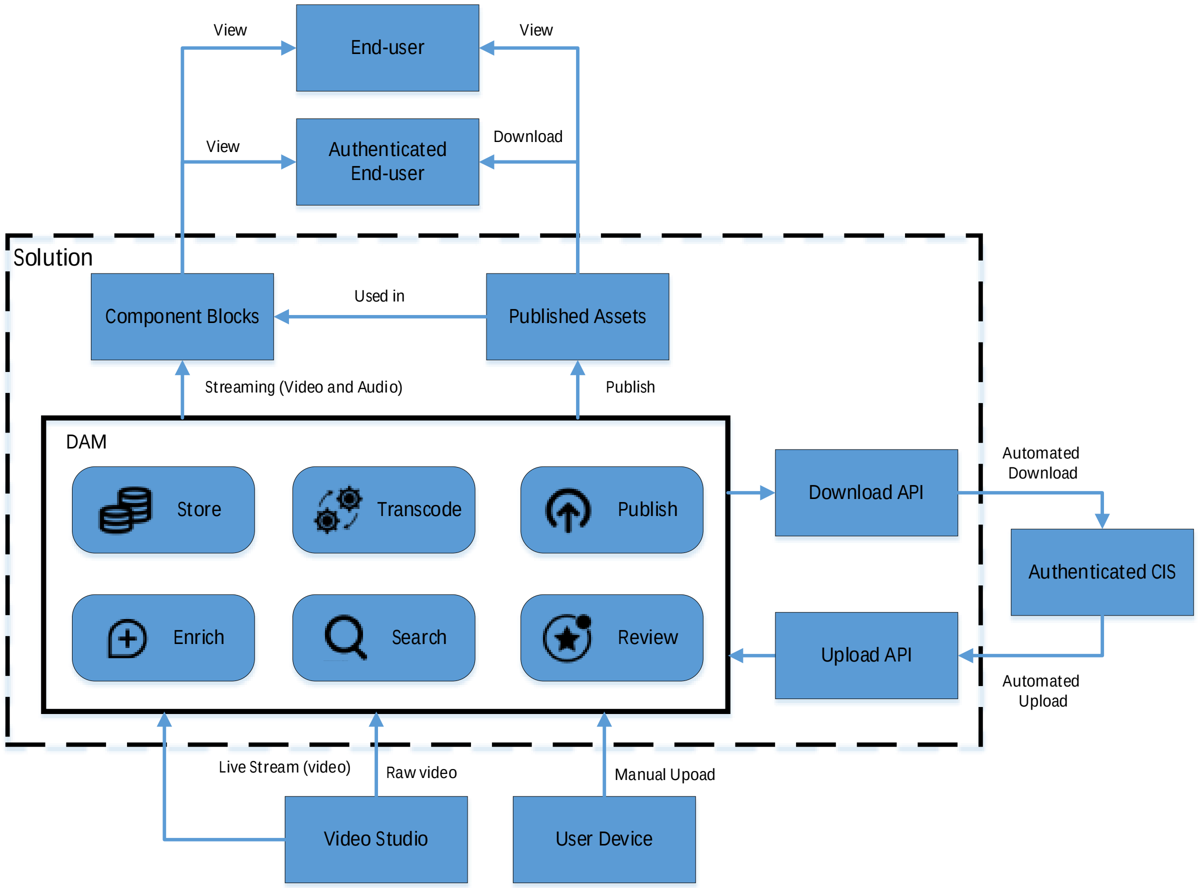


Figure 9 Schematic Overview DAM

A.1.16. Uploading to DAM

A.1.16.1. (SHALL) The Solution shall allow for manual uploading of assets by users

A.1.16.2. (SHALL) The Solution shall including bulk upload of assets by users.

A.1.16.3. (SHALL) The Solution shall allow for automated uploads of assets to the Solution by means of an API by Authenticated CIS.

A.1.16.1. (SHALL) The Solution shall allow for automated extraction of metadata embedded inside the media assets during uploads (e.g. XMP metadata embedded in JPG)

A.1.16.2. (SHALL) The Solution shall allow (bulk) uploading of raw assets from the NATO Interplay network to the Solution (.mxf format)

A.1.16.3. (SHALL) The Solution shall support uploading average file size of 1 MB and up to 100 GB maximum file size.

A.1.16.4. (SHALL The Solution shall enable the multiplication of video feed through the Purchaser provided CDN. This feel shall reach audiences worldwide with one or more live video feed coming from media encoders located within the NATO TV Studio in HSL/SRT or technically similar video format with multiple audio channels embedded.

A.1.16.5. (COULD) The Solution could support the raw format Adobe Digital Negative (DNG).

A.1.16.6. (SHALL)The following MIME types shall be supported out of the box including, but not limited to:

·	.pdf	application/pdf
·	.svg	image/svg+xml
·	.png	image/png
·	.jpeg	image/jpeg
·	.jpeg	image/pjpeg
·	.jpg	image/jpeg
·	.jpg	image/pjpeg
·	.gif	image/gif
·	.webp	image/webp
·	.mp3	audio/mpeg3
·	.mp3	audio/x-mpeg-3
·	.wav	audio/wav
·	.mp3	video/mpeg
·	.mp3	video/x-mpeg
·	.mp4	video/mp4
·	.mxf	video/mxf

A.1.17. Encoding and Transcoding in DAM

A.1.17.1. (SHALL) The Solution shall allow transcoding (conversion) of high quality (1080i/p and/or 4K HD) video.

A.1.17.2. (SHALL) The Solution shall transcode H.264 for video.

A.1.17.3. (SHALL) The Solution shall transcode AAC for audio.

A.1.17.4. (SHALL) The Solution shall allow for transcoding of commonly-used video formats.

A.1.18. Storing and Searching in DAM

A.1.18.1. (SHALL) The Solution shall store all assets (published and unpublished) until completion of the Contract.

A.1.18.2. (SHALL) The Solution shall provide a Search functionality for searching assets based on keywords, tags, asset types, and facetted search.

A.1.18.3. (SHALL) The Solution shall have the functionality to create, automatically manage, and publish a collection of assets based on their properties like format, size and tags.

A.1.19. **Enriching DAM Assets**

A.1.19.1. (SHALL) The Solution shall have an integrated image resize and optimization service. Image are auto scaled to a defined list of dimensions.

A.1.19.2. (SHALL) The Solution must allow assets to be tagged with free and or auto-completed tags. Auto-completed tags will show up for selection when a match is found to a previous tag.

A.1.19.1. (COULD) The Solution could provide a functionality to indicate focal points for responsive images when resizing and cropping.

A.1.19.2. (COULD) The Solution could provide a mechanisms to automatically tag the uploaded assets based on the content. For instance using Artificial Intelligence or content inspector.

A.1.19.3. (COULD) The Solution could allow facial and object recognition to aid with the recognition and subsequent tagging of images. This could happen through integration with a 3rd party image analysis and tagging tool via an API.

A.1.19.4. (SHALL) The Solution must have a mechanism to manage multiple assets for bulk management of tags, and CRUD operations on the asset.

A.1.19.5. (SHALL) The Solution shall including the option to manually enrich the missing metadata when bulk-uploading media (reference A.1.16.2).

A.1.19.6. (SHALL) The Solution shall allow the editor to append ALT tags to images

A.1.19.7. The DAM must allow basic manipulation of images, including, but not limited to:

- rotation
- modifying brightness
- modifying contrast
- cropping

A.1.19.8. (SHALL) The Solution shall have an integrated image resize and optimization service. Image are auto scaled to a defined list of dimensions.

A.1.19.9. (COULD) The Solution could provide multiple media file (video and image) renditions aside from original asset format:

- Images: to Preview, Thumbnail, Banner and PDF
- Video: to Preview, Thumbnail, Banner

A.1.20. **Reviewing and Publishing in DAM**

A.1.20.1. (SHALL) The Solution shall provide a Graphical User Interface (GUI) for publishing content.

A.1.20.2. (SHALL) The Solution shall be able to support multi-channel distribution through an API, including all renditions of the original asset.

A.1.20.3. (SHALL) The Solution shall provide a workflow functionality to manage assets approval, via stages so that authorized users approve/reject assets changes.

A.1.20.4. (SHALL) The Solution shall allow for the streaming of audio and video assets directly in content blocks in HLS and MP4 format.

A.2. Non-functional Requirements

The non-functional requirements of the system are captured in the SLA (reference ANNEX B) and SECTION 5.

ANNEX B Service Level Agreement (SLA)

Table 10 describes the SLA for work package 2 and 3 (reference SECTION 5 and SECTION 6)

SLA #	Category	Item	Description	Goal	Measurement	Service Credit
1	Availability	Uptime	The percentage of time in a given period that the Solution is accessible and usable.	99.999% Uptime – this excludes any downtime introduced by the Purchaser's Edge Security Solution	Tracked continuously from the Edge Security Solution. Monthly Stress Test	**Monthly:** If more than 26.30 seconds of total downtime are measured for that month, the credit will be 20% of the monthly payment in CLIN 2. **Yearly:** If more than 315.60 seconds of total downtime are measured for that year, the credit will be 5% of the yearly payment of CLIN 2. **Monthly Stress-test:** If the Solution experiences more than 5.00 seconds of total downtime during the monthly stress-test, the credit will be 10% of the monthly payment in CLIN 2.

SLA #	Category	Item	Description	Goal	Measurement	Service Credit
2	Performance	First View	The time for the Solution to send an initial response to the Purchaser's Edge Security Solution after receiving a request.	< 300 Milliseconds	Measured at 80th percentile in from all requests from the Edge Security Solution Monthly Stress Test	**Monthly:** If more than 80% of the request that month do not receive a response faster than 300 milliseconds, the credit will be 20% of the monthly payment in CLIN 2. **Monthly Stress-test:** If more than 80% of the requests during the test do not receive a response time faster than 300 milliseconds, the credit will be 10% of the monthly payment in CLIN 2.
3	Resilience	Maximum Service failure notification time	The maximum time it takes take the Contractor to notify the Purchaser of any (partial) service outage	< 1 Minute	Monthly report of all interruptions	N/A
4	Resilience	Maximum Service restore notification time	The maximum time it takes the Contractor to notify the Purchaser of any (partial) service restoration.	< 1 Minute	Monthly report of all interruptions	N/A

SLA #	Category	Item	Description	Goal	Measurement	Service Credit
5	Resilience	Data Backup – Retention Time	The retention time for the backup of all the assets and content of the Solution	The total POP of the Contract	Yearly backup-test	N/A
6	Resilience	Data Backup – Time to Restore (TTR)	The time needed to restore the assets and content data of the Solution	24 Hours	Yearly backup-test	**Yearly backup-test:** If during the Yearly Backup-test, the recovery time for the assets of the Solution is more than 48 hours, the credit is 1% of the yearly payment of CLIN 2.
7	Security	Logs Backup – Retention Time	The retention time for the backup of the required Solution logs (reference 2.2.3)	3 Years	Yearly backup-test	N/A
8	Security	Logs Backup – Time to Restore (TTR)	The time needed to restore the backup of the required Solution logs (reference 2.2.3)	48 Hours	Yearly backup-test	Yearly backup-test: If during the Yearly Backup-test, the recovery time for the logs of the Solution is more than 48 hours, the penalty is 2%

SLA #	Category	Item	Description	Goal	Measurement	Service Credit
9	Security	Information Security	The Level of Security of the Solution Provided by the Contractor	Continuous compliance with the applicable NATO security directives described in 2.2.3. Including security documentation, audits, and any security testing.	Yearly re-accreditation by the SAA.	For every month that the Solution does not have a SA by the SAA, the total credit will be 0.5% of the yearly payment of CLIN 2.
10	Security	Incident Response Time	Time needed to provide an initial response to an incident notification from the Purchaser.	Critical Incidents:10 minutes Normal Incidents: 2 hours	Ticket logs (monthly reporting)	N/A
11	Security	Incident Resolution Time	Time needed to resolve an incident after the incident notification from the Purchaser.	Critical Incidents:1 Hour Note: Any downtime due to critical incidents will also count negative toward the Uptime SLA Metric (#1). Normal Incidents: 48 Hours	Ticket logs (monthly reporting)	N/A
12	Security	Fall-back Solution Availability	The percentage of time in a given period that the Fall-back Solution is accessible and usable.	99.999% Uptime – this excludes any downtime introduced by the Purchaser’s Edge Security Solution	Tracked continuously from the Edge Security Solution.	**Yearly:** If more than 315.60 seconds of total downtime are measured for that year, the credit will be 2% of the yearly payment of CLIN 2.

SLA #	Category	Item	Description	Goal	Measurement	Service Credit
13	Security	Fall-back Solution Activation Time	The time between activation of the Fall-back Solution and the time it is available to the end-users	< 5 Minutes	Yearly Fall-back Solution Test	**Yearly Fall-back Solution Test:** If the activation time is longer than 5 minutes during the yearly Fall-back Solution test, the credit will be 1% of the yearly payment of CLIN 2.
14	Service Support	Service Support Request Response Time	Time needed to provide an initial response to a service request from the Purchaser.	1 Working Hour	Ticket logs (monthly reporting)	**Monthly:** If more than 25% of the tickets raised that month did not receive an initial response within one hour, the penalty will be 5% of the monthly payment of CLIN 2.

SLA #	Category	Item	Description	Goal	Measurement	Service Credit
15	Service Support	Service Support Resolution Time	Time needed to provide the requested service support to the Purchaser.	2 Working Hours after initial response for the following information requests: · Known issues and workarounds · Frequently Asked Questions · Registering of Non-critical Issues · Logging of Feature Request 8 Working Hours after initial response for the following service requests: · User-groups · Users · Privileges 5 Working Days for the following service requests o Site Templates o Component Schemas o Content Statuses o Workflows o Dashboards	Ticket logs (monthly reporti ng)	**Monthly:** If more than 25% of the requests raised that month did not receive support within the specified goal, the penalty will be 5% of the monthly payment of CLIN 2.

Table 10 Service Level Agreement

B.1. Current System Metrics:

Order to meet the SLA Requirements, the Contractor should take the following current system(s) metrics into account:

- Average data-transfer is 13 TB per month
- Peak data-transfer is 61 TB per month
- Average throughput (monthly): 3,250 Mbps
- Peak throughput (monthly): 16,900 Mbps
- Current storage of DAMS data is 400 TB slow accessible storage and 50 TB fast accessible storage
- Average hourly users on the nato.int website is 2,000
- Peak hourly of users on the nato.int website is 400,000
- Average monthly page views on the nato.int website is 2.7 MLN
- Peak monthly page views on the nato.int website is 20 MLN.

These metrics are anticipated to grow 10% annually.

B.1.1. (SHALL) The Contractor shall take 10% annual growth in into account for both average and peak utilization for the following aspects of the Solution: throughput, storage, hourly users, data transfer, and number of hits on the site.

ANNEX C WCM and DAMS System Integrations

Displays the integration of the WCM and DAMS that will remain relevant for the scope of this Contract. The Contractor could choose to take ownership of these integrations and use them as part of the Solution to provide the functionality described in this SOW.

Integration	Function	Technical Description
FormStack	Integration of interactive forms and surveys.	On https://www.nato.int/cps/en/natohq/198183.htm the code for a form including reCAPTCHA functionality generated by Formstack is embedded via an iFrame. Formstack forwards the incoming forms to preselected NATO email addresses
Theo Player	Advanced (Live) media player functionality	The code for the THEO media player is inserted on the page at https://www.nato.int/cps/en/natohq/events_67375.htm to play the web stream from a CDN, to offer a more user-friendly UI to choose between the different audio/languages of the webstream and to allow monitoring and assessment of the usage of the webstream (duration of viewing; selection of languages)
Campaign Monitor	Mass email, email scheduling, email address-list management, email response tracking.	Via the page at https://www.nato.int/cps/en/natohq/e-mail_distribution.htm visitors can subscribe to receive multiple newsletters via e-mail. Via the page at: https://www.natomultimedia.tv/app/home visitors can register and automatically be added to the distribution list to receive notifications when new videos are published. Content is manually copied and pasted by users into Campaign Monitor for distribution via e-mail.
Taleo/ HR Clearing House	Job vacancies to be displayed on the website.	On the page at: https://www.nato.int/cps/en/natohq/recruit-wide.htm a list of all vacancies in all NATO bodies worldwide is published and update on an hourly basis. The list is exported from an internal server, synchronized to the NATO webserver and embedded in this page.
Google Analytics	Site and engagement analytics	Using the Google Tag Manager, usage of both www.nato.int and www.natomultimedia.tv is being monitored using Google Analytics 4.
YouTube	Embedding of video player on webpages to play NATO videos hosted on YouTube	A wide selection of public NATO videos are hosted on YouTube. Many of these videos are embedded on pages at www.nato.int using the YT video player.

Table 11 WCM and DAMS System Integrations

ANNEX D Use Case

The following Use Cases describe the different actors and flow of content for a typical publication on the nato.int website. This is a fictional example that can be used to size the Solution and level of configuration required for the Solution.

1. Official visit

   The NATO Secretary General visits a capital of a NATO nation to meet with the national representatives. Next to bilateral meetings, the NATO Secretary General also hosts a press conference with the prime minister.

   A photographer accompanies the Secretary General and on average makes a selection of 50 photos that he/she uploads to the Solution using a non-managed laptop. At NATO HQ, a Photo Editor using the Solution on a NATO-managed device immediately sees the 50 photos, adds generic metadata for all photos (what, when, where) and specific metadata for each photo (who). The Photo Editor prepares a selection of photos to be published as a photo gallery on the website and/or to be shared via social media.

   A cameraperson and an audio engineer film the press conference and transmit the live video feed in high definition and in real time to NATO HQ. A Video Editor at NATO HQ retransmits the live HD video via web streaming (using the Solution) and via social media. The Video Editor also records and edits the HD video. The Video Editor uploads the finished HD Video Product to the Solution and adds metadata to be published.

   A Press Officer sits at NATO Headquarters and uses a NATO Managed Laptop to write a draft News Story which is one part of a predetermined template for News Stories that usually follows the following format:

   - Title
   - First paragraph
   - Story Text
   - Start Date
   - End Date (optional)
   - Keywords
   - Header Picture (selected from the related photos in the Solution)
   - Supporting Picture (optional)
   - Links to related content (optional)
   - External Links (optional)
   - Supporting Video (optional)

   This News Story is intended to be published on a site for a specific NATO event with a distinct URL (e.g. www.nato.int/news/year_month_day_title-of-websttory)

   After writing the News Story, the Press Officer illustrates the News Story by selecting an existing Header Picture from the DAM repository of the Solution. Finally, the Press

Officer submits the draft story and Header Picture for review and approval. The Solution notifies the relevant Senior Press Officer based on the workflow.

The Senior Press Officer uses a non-NATO device to review the draft News Story and decides to automatically publish the News Story at 20:00 that evening. Next to publication on the event URL, the Senior Press Officer also selects the option to have the News Story distributed at 20:00 using the mass e-mail functionality to an email-correspondence group called “external-test-event – Relevant press”, who will receive a notification that the News Story is ready on the event URL and a copy of the article is included.. Finally, the Senior Press Officer notifies the Social Media Expert that the News Story will be published at 20:00 that evening.

The Social Media expert uses the Solution’s Social Media Preview functionality to ensure that the link to the event-URL is displayed correctly on Twitter, Facebook, and Instagram and continues to pre-plan the notification releases to these Social Media Platforms from the official NATO accounts by adding additional text relevant to each social media platform.

After publication, a Content Manager monitors the engagement of the News Story by using the Solution’s dashboard to examine e.g.:

- How often was the News Story viewed? How much time did viewers spend on the page?
- On which geographical location where viewers located?
- How did viewers come to the News Story (e.g. via Social Media, via E-mail, via Referrer websites, via search engines?
- Is there additional traffic to the related content, links or other NATO websites after the release of the Web Story

As part of the approval process, the Senior Press Officer selects in which languages the webstory needs to be translated and published. Upon approval, the Solution sends a notification to the relevant translators according to the workflow. The translator is notified that a translation is requested, translates the text and submits the translation of the Web Story by logging-in the Solution using an external non-NATO device.

2. Storytelling videos

NATO Video Journalists are sent outside of NATO HQ to produce videos illustrating NATO in action during exercises, missions and other events. These videos are posted by NATO on social media channels to engage with our audiences and/or are shared in high resolution with professional media and broadcasters. Video products are produced in multiple formats for standard broadcasting (16:9), but also tailored for social media (9:16; 1:1)

The Video Journalist films and edits recorded HD video footage into multiple video products: B-roll (i.e. an extensive selection of recorded HD video footage), master file (edited finished video product with a voice-over and lower-thirds) and international version (edited video product without voice-over or lower-thirds).

The Video Journalist uploads the different format and files into the Solution.

The Media Producer is notified when a new video has been uploaded and approves the video. The Media Producer adds relevant metadata to the video prior to publication and links the video to a relevant web story or transcript.

As part of the publication, the Media Producer sends an e-mail message to the list of Professional Broadcasters to notify them that a new video is available to be viewed and downloaded.

After publication, the Media Producer monitors the engagement of each video product by using the Solution’s dashboard to examine e.g.:

- How often was the Video Product viewed/downloaded? How much time did viewers spend watching the video?
- On which geographical location where viewers located?
- How did viewers come to the Video Product (e.g. via Social Media, via E-mail, via Referrer websites, via search engines?
- Is there additional traffic to the related content, links or other NATO websites after the release of the Video Product

Next.

ANNEX E List of Acronyms

Acronym	Text
ADS	Accreditation Documentation Set
AfP	Approval for Pilot
API	Application Programming Interface
AWS	Amazon Web Services
CIMP	Cyber Incident Management Plan
CIS	Communication and Information System
CISD	CIS Description
CMS	Content Management System
COL	Costed Option List
COTS	Commercial of the Shelf
CPM	Contractor Project Manager
CQAR	Contractor Quality Assurance Representative
DAMS	Digital Asset Management System
DMP	Data Migration Plan
ECP	Engineering Change Proposal
EDC	Effective Date of Contract
ERM	Event Review Meeting
GUI	Graphical User Interface
iSA	Interim Security Accreditation
IV&V	Independent Verification and Validation
IV&V	Independent Verification and Validation
LIPS	Log Ingestion and Processing Survey
LMP	Low Maintenance Period
MoU	Memorandum of Understanding
NATO	North Atlantic Treaty Organization
NCI Agency	NATO Communication and Information Agency
NCSC	NATO Cyber Security Center
NOS	NATO Office of Security
NQAR	NATO Quality Assurance Representative
PAT	Pre-Activation Test
PDD	Public Diplomacy Division
PFE	Purchaser Furbished Equipment

Acronym	Text
PMP	Project Management Plan
PMS	Project Master Schedule
PMTP	Project Master Test Plan
POC	Point of Contact
POP	Period of Performance
PPM	Purchaser Project Manager
PRINCE2	Projects IN Controlled Environments
PSR	Project Status Report
QA	Quality Assurance
RFP	Request for Proposal
RGA	Requirements Gathering Approach
RSR	System Requirements Statement
RTM	Requirements Traceability Matrix
SA	Security Accreditation
SAA	Security Accreditation Authority
SaaS	Software as a Service
SAP	Security Accreditation Plan
SAW	Static Archive Website
SCA	Solution Configuration Approach
SCP	Solution Configuration Plan
SDP	Service Delivery Plan
SDS	System Design Specification
SecOPs	Security Operating Procedures
SIEM	Security Information and Event Management System
SLA	Service Level Agreement
SME	Subject Matter Expert
SOAP	Solution Activation Plan
SOW	Statement of Work
SRA	Security Risk Assessment
SSRS	System Security Requirements Statement
STDP	System Test Documentation Package
STVP	Security Test and Verification Plan

Acronym	Text
STVR	Security Test and Verification Report
TP	Training Plan
TRM	Test Review Meeting
TRR	Test Readiness Review
WCAG	Web Content Accessibility Guidelines
WCM	Web Content Management
WYSIWYG	What You See Is What You Get

Table 12 List of Acronyms

Distribution List for IFB-CO-115759-DAMS-WCM Amdt 2

Bidders List

NATO Delegations (Attn: Infrastructure Adviser)

Embassies in Brussels (Attn: Commercial Attaché)

NCI Agency – All NATEXs

NCI Agency Internal Distribution (not disclosed)