NATO STANDARD

AMSP-02

ALLIED FRAMEWORK FOR MODELLING AND SIMULATION AS A SERVICE (MSAAS) CONCEPT OF EMPLOYMENT

Edition A, Version 1

AUGUST 2023

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED MODELLING AND SIMULATION PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

29 August 2023

1. The enclosed Allied Modelling and Simulation Publication AMSP-02, Edition A, Version 1, ALLIED FRAMEWORK FOR MODELLING AND SIMULATION AS A SERVICE (MSAAS) CONCEPT OF EMPLOYMENT, which has been approved by the nations in the NATO MODELLING AND SIMULATION GROUP, is promulgated herewith. The recommendation of nations to use this publication is recorded in STANREC 4794.

2. AMSP-02, Edition A, Version 1, is effective upon receipt.

3. This NATO standardization document is issued by NATO. In case of reproduction, NATO is to be acknowledged. NATO does not charge any fee for its standardization documents at any stage, which are not intended to be sold. They can be retrieved from the NATO Standardization Document Database (https://nso.nato.int/nso/) or through your national standardization authorities.

4. This publication shall be handled in accordance with C-M(2002)60.

Dimitrios SIGOULAKIS
Lieutenant General, GRC (A)
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

INTENTIONALLY BLANK

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]

Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.

INTENTIONALLY BLANK

ACKNOWLEDGEMENTS

The following individuals have participated in the development of this standard or its earlier versions: Wim Huiskamp (NLD), Bharat Patel (GBR), Jose Ruiz (FRA), Lars Jansson (SWE), Niels Krarup-Hansen (DNK), Gerard Konijn (NLD), John Russel Hutt (USA), Brad Friedman (USA), Chris McGroarty (USA), Robert Siegfried (DEU), Andre Hoogstrate (NLD), James Kearse (GBR), Marco Biagini (ITA).

INTENTIONALLY BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

Abbreviation	Definition
AMSP	Allied Modelling and Simulation Publication
AUT	Authority
BM	Business Model
C2SIM	Command and Control Systems and Simulation Systems
C3	Command, Control, and Communication
CAX	Computer Assisted eXercise
CDS	Cross Domain Security
CFBLnet	Combined Federated Battle Laboratories Network
COM	Compliance
CONEMP	Concept of Employment
CP	Command Post
CPX	Command Post eXercise
CSA	Cloud Security Alliance
ENISA	European Union Agency for Network and Information Security
EOL	End of Life
FMN	Federated Mission Networking
GEN	General
HLA	High Level Architecture
IaaS	Infrastructure as a Service
Idam	Identity and Access Management
M&S	Modelling & Simulation
MORS	Military Operational Requirements Subgroup of NMSG
MS3	Modelling & Simulation Standards Subgroup of NMSG
MSaaS	Modelling and Simulation as a Service
MSAB	Multinational Security Accreditation Board
MSCO	Modelling and Simulation Coordination Office
MSCoE	Modelling and Simulation Center of Excellence
MSG	Modelling & Simulation Group
NAF	NATO Architecture Framework
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
NMSG	NATO Modelling and Simulation Group

Abbreviation	Definition
NSO	NATO Standardization Office
OCD	Operational Concept Document
ORG	Organizational
PaaS	Platform as a Service
PPC	NMSG Programming and Planning Committee
SaaS	Software as a Service
SDT	Service Description Template
SEC	Security
SLA	Service Level Agreement
SLAT	Service Level Agreement Template
SOA	Service Oriented Architecture
STANAG	Standardization Agreement
STANREC	Standardization Recommendation
STN	Standards
STO	Science and Technology Organization (NATO)
TRA	Technical Reference Architecture

REFERENCES

[1] NMSG, “AC/323/NMSG(2012)-015: NATO M&S Master Plan Version 2.0,” NATO, 2012

[2] NMSG, “AC/323/NMSG(2012)-016: NATO M&S Implementation Plan Version 2.0,” NATO, 2012.

[3] NMSG, “AC/323/NMSG(2021)-004: Allied Modelling & Simulation Publications (AMSPs) Policy Document (APD) Version 1.0,” NATO, 2021

[4] Harvard University, “Key words for use in RFCs to Indicate Requirement Levels, Network Working Group, March 1997,” https://www.ietf.org/rfc/rfc2119.txt

[5] NMSG, “AC/323/MSG-136)/TP/831: TO-TR-MSG-136-Part-IV: Modelling and Simulation as a Service. Volume 1: MSaaS Technical Reference Architecture,” NATO, 2019

[6] NSO website (https://nso.nato.int/nso/), Accessed 9 November 2017

[7] NMSG, “AC/323/MSG-131/TP/608: Modelling and Simulation as a Service: New Concepts and Service-Oriented Architectures,” NATO, 2015

[8] NATO Allied Command Transformation (ACT) C4ISR Technology & Human Factors (THF) Branch: “C3 Classification Taxonomy”, Baseline 1.0, 15 June 2012

[9] FAA, “System Wide Information Management (SWIM) Governance Policies. Version 3.1” Federal Aviation Administration (FAA), 06 February 2020

[10] NMSG, “AC/323/MSG-136/TP/830: Operational Concept Document (OCD) for the Allied Framework for M&S as a Service,” NATO, 2019

[11] NMSG, “AC/323(MSG-164): Business Model for the Allied Framework for M&S as a Service. Version 1.0”, NATO, 2023

[12] NC3B, “AC/322-D(2018)0002-REV1: NATO Architecture Framework, Version 4.0”, NATO, 2018

[13] NMSG, “AMSP-01 NATO Modelling and Simulation Standards Profile. Edition (E), Version 1”, NATO, 2021

[14] National Institute of Standards and Technology: NIST Cloud Computing Security Reference Architecture, NIST Special Publication 500-292, 08 September 2011.

[15] NATO Consultation, Command and Control Board (C3B): “NATO Cloud Computing Policy”, AC/322-D(2016)0001, 7 January 2016

[16] NATO Consultation, Command and Control Board (C3B): “NATO Information and Communications Technology (ICT) Service Management Policy”, AC/322-D(2014)0009, 28 November 2014

[17] European Union Agency for Network and Information Security (ENISA): Security Framework for Governmental Clouds, 26 February 2015, ISBN 978-92-9204-115-1, doi: 10.2824/57349

[18] European Union Agency for Network and Information Security (ENISA): Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, 16 February 2017, ISBN 978-92-9204-203-5, doi 10.2824/456345.

[19] NATO: Annex N To Volume II - Federation, NATO FMN Implementation Plan v3.0, CIS Security (Including Cyber Defence), 8 July 2014

[20] CFBLNet Reference https://community.apan.org/wg/cfblnet/cfblnet_public/

[21] MSAB Reference https://community.apan.org/wg/cfblnet/cfblnet_public/w/cfblnet-guide/

[22] NMSG, “AC/323/NMSG(2022)-177: Terms of Reference for the M&S Standards Subgroup (MS3)”, NATO, 2022

[23] NMSG, “AC/323(MSG) – MORS/11-2017: Terms of Reference for the Military Operational Requirements Sub-Group (MORS)”, NATO, 2017

[24] NATO: STANREC 4800 “NATO Education and Training Network – Federation Architecture and Federation Object Model”. AMSP-04 Edition B. Edition 2. NSO, 26 March 2021

CHAPTER 1 INTRODUCTION AND SCOPE

1.1 BACKGROUND

1. To a great extent, future military training, analysis, and decision-making capabilities will be provided by Modelling and Simulation (M&S). Two main barriers are accessibility and complexity: hardware, software, and personnel necessary to implement and utilize models and simulations can be both time- and cost-intensive.

2. M&S products are highly valuable to NATO and military organizations and it is essential that M&S products, data and processes are conveniently and securely accessible to a large number of users as often as possible. Stand-alone use has to be supported as well as integration of multiple simulated and real systems into a unified simulation environment whenever the need arises.

3. Recent technical developments in cloud computing technology and service-oriented architectures (SOA) offer opportunities to better and securely utilize M&S capabilities to satisfy these critical needs. M&S as a Service (MSaaS) is a concept that takes advantage of those developments, enabling an ecosystem that will supply and provide improved services to discover, compose and execute required simulation environments, using cloud-based computing or deployed to local computer systems or a hybrid of the two.

4. The Allied Framework for MSaaS is the common approach of NATO and Nations towards implementing MSaaS. The Allied Framework for MSaaS or MSaaS ecosystem in the NATO coalition will be based on a federated approach of national and NATO services and service providers that is enabled by a common technical reference architecture, common processes and a common business model. The MSaaS concept is visualised in Figure 1-1.

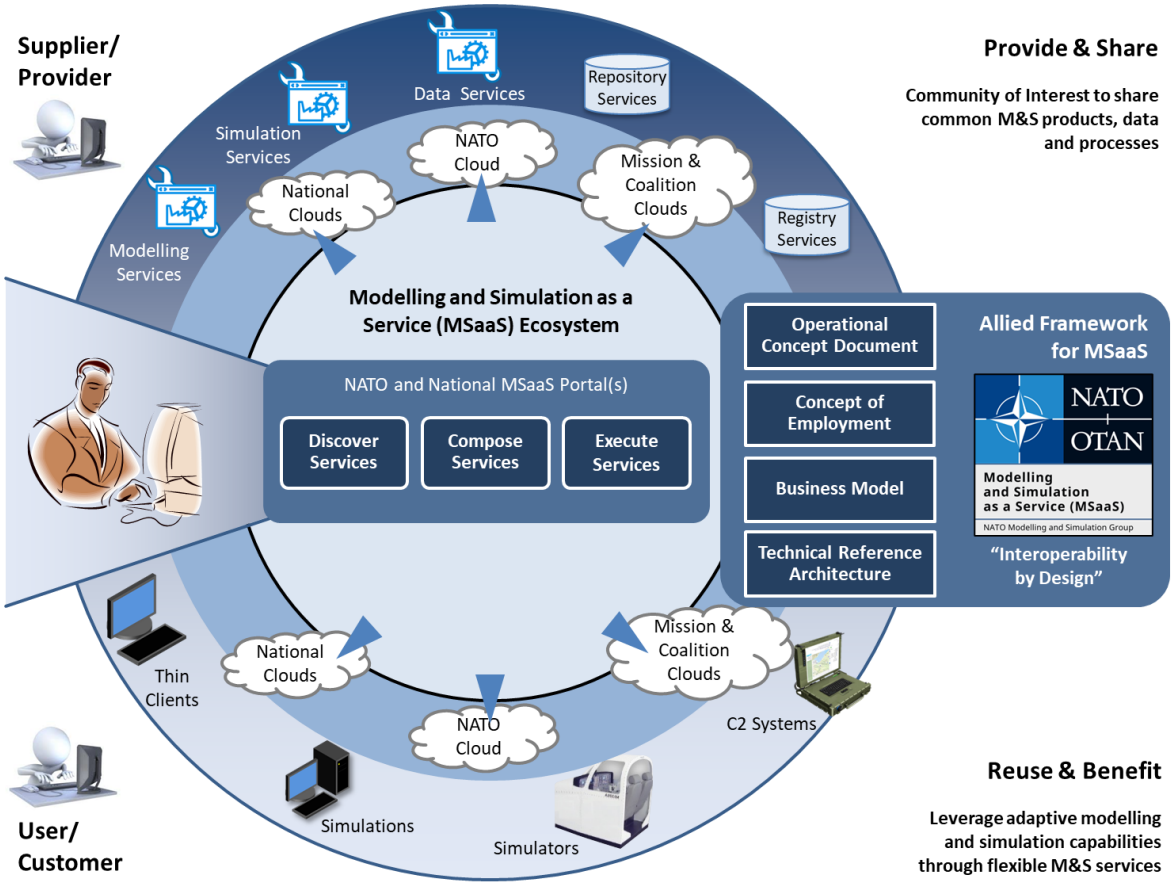

Figure 1-1: Allied Framework for MSaaS

5. The NATO Modelling and Simulation Group (NMSG) mission addresses and supports establishing a common technical framework to foster interoperability and reuse as defined in the NATO M&S Master Plan [1]. This document defines the Allied Framework for Modelling and Simulation as a Service (MSaaS) Concept of Employment (CONEMP) and supports that NMSG mission.

6. Establishing a persistent capability like the Allied Framework for MSaaS requires effective operating procedures. They ensure that all of the independent service-based efforts (i.e. design, development, deployment, or operation of a service) combined will meet customer requirements.

1.2 SCOPE AND APPLICABILITY

1. This document is a guideline for NATO and (multi)-national MSaaS implementations. This document establishes the concept of employment, identifies MSaaS stakeholders and their relationships, describing or referencing operating procedures, and provides guidance and technical refences for implementing and maintaining the Allied Framework for MSaaS as a persistent capability.

2. The operating procedures and technical references in this document are recommended by the NMSG to promote M&S service sharing and interoperability between MSaaS implementations. These operating procedures and technical references are not formally mandated by NATO, unless supported by a specific NATO Standardization Agreement (STANAG). The AMSP-02 will be covered by a Standardization Recommendation (STANREC).

3. The operating procedures and technical references specified in this document should be applied to all current and prospective MSaaS-enabled implementation programs and efforts in NATO and Nations.

1.3 DOCUMENT GOVERNANCE

1. This document was originally produced by the Governance Subgroups of MSG-136 and MSG-164 MSaaS Research Task Groups of NMSG. However, with its publication as AMSP-02, the NMSG takes over as custodian with responsibility for the document. As custodian, the NMSG is responsible for maintaining this document as per Section 5.1 and NATO STO: Allied Modelling and Simulation Publications (AMSPs) Policy Document (APD) [3].

2. The NMSG will conduct informal reviews of this document as new information becomes available or technology changes and process change requests for future consideration in revised products. NMSG may recommend initiating new task groups to conduct the actual update or revision of the document in accordance with NATO STO: Allied Modelling and Simulation Publications (AMSPs) Policy Document (APD) [3].

1.4 ORDER OF PRECEDENCE

1. In the event of a conflict between the text of this document and the references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

1.5 KEY WORDS

1. The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119 [4].

2. These key words are capitalized when used to specify requirements unambiguously. When these words are not capitalized, they are meant in their natural-language sense.

INTENTIONALLY BLANK

CHAPTER 2 TERMS AND DEFINITIONS

1. This chapter summarizes MSaaS-specific key terms, formal definitions are stated in NATO STO: “Modelling and Simulation as a Service (MSaaS) - Technical Reference Architecture”. STO-TR-MSG-164-II, 2021 [5]. Generic definitions and terms are available on the official NATO Terminology Database website (NATOTerm) [6].

2.1 SERVICE

1. This document uses the term “service” always in the sense of “M&S service”, unless stated otherwise, using the following definition:

> “An M&S service is a specific M&S-related capability delivered by a producer to one or more consumers according to well defined contracts including Service Level Agreements (SLA) and interfaces.”

2. A more detailed classification of these M&S services is provided in the MSaaS Technical Reference Architecture [5] in alignment with the NATO C3 Classification Taxonomy [8]. This document uses the term “M&S service” as a generic term in the sense of the NATO C3 Classification Taxonomy’s notion of M&S Capability.

3. A service can be composed out of other services. The composition can be considered as a new service that does not necessarily expose the constituting services. Whenever this document uses the term “service”, it includes “composed services” unless stated otherwise.

2.2 SERVICE LIFECYCLE

1. The ability to effectively manage all stages of the service lifecycle is fundamental to the effectiveness of MSaaS. This document adopts the Service Lifecycle Management Process as defined in Ref. [9] to contain a set of controlled and well-defined activities performed at each stage of a service’s lifecycle for any and all versions of any given service. Table 2-1 lists the sequential service lifecycle stages. Policies relevant to each stage are described more fully in the subsequent chapters.

Table 2-1: Service Lifecycle Stages

Lifecycle Stage	Description
Proposed	The need for a specific service has been identified and it has been assessed whether existing services satisfy this need. If this is not the case, a new service may be proposed.
Definition	The service’s requirements are gathered and the service design is produced based on these requirements.

Lifecycle Stage	Description
Development and Maintenance	The service specifications are developed and the service is built or maintained to include Verification and Validation.
Compliance	The service is inspected and/or tested to confirm that the service complies with the prescribed set of standards and regulations and is approved for use.
Production	The service is available for use by its intended users.
Deprecated	The service will no longer be available to new users or supported to existing users and will be phased out until retired.
Retired	The service is disposed of and is no longer used.

2.3 ALLIED FRAMEWORK FOR M&S AS A SERVICE

1. The combination of service-based approaches (i.e. M&S services) with ideas taken from cloud computing is known as “Modelling & Simulation as a Service” (MSaaS). This document uses the following definition:

> “M&S as a Service (MSaaS) is an enterprise-level approach for discovery, composition, execution and management of M&S services.”

2. Enterprise level refers to the fact that MSaaS satisfies the needs of a broader community rather than individual service consumers. This definition stresses the fact that MSaaS is not only a technical solution, but also includes organizational and governance aspects on the enterprise level (e.g., overarching management, funding and oversight).

3. The “Allied Framework for MSaaS” is the common approach in the NATO coalition towards a federated MSaaS ecosystem consisting of national and NATO MSaaS implementations, underpinned by a common technical reference architecture, common processes and a common business model.

4. The Allied Framework for MSaaS is defined by the following documents (see also Figure 1-1):

a. Operational Concept Document: The OCD describes the general vision and concepts of MSaaS, the intended use, key capabilities and desired effects of the Allied Framework for MSaaS from a user’s perspective [10].

b. Business Model: The BM describes how MSaaS will manage and enable the intended use, key capabilities and desired effects of the Allied Framework for M&S as a Service from a stakeholder’s perspective in the multi-government business space [11].

c. Technical Reference Architecture (TRA): The Technical Reference Architecture describes the architectural building blocks and patterns for realizing MSaaS capabilities [5].

d. Concept of Employment (CONEMP): The Concept of Employment [this document] identifies MSaaS stakeholders and their relationships and provides guidance for implementing and maintaining the Allied Framework for MSaaS as a persistent capability.

2.4 MSAAS IMPLEMENTATION

1. The Allied Framework for MSaaS defines the blueprint for stakeholders to implement MSaaS. The specific solution architecture of MSaaS may be different for each implementation:

a. An MSaaS Implementation is the specific realization of M&S as a Service by a certain stakeholder. An MSaaS Implementation includes both technical and organizational aspects.

b. An MSaaS Solution Architecture is the architecture of a specific MSaaS implementation and is derived from the Operational Concept Document and the Technical Reference Architecture. A synonymous term for “Solution Architecture” is ‘’Target Architecture’’ or “Project Architecture” (NAF parlance) [12].

2. MSaaS documents, data and tools should be managed through an MSaaS Portal as outlined in the MSaaS Operational Concept Document [10]. This will include dissemination of documents, services, datasets (e.g., databases, imagery) and tools (e.g., federate compliance testing tools), dealing with feedback, implementation issues etc. that are addressed in updates and maintenance activities.

3. Users of these MSaaS services, tools, data and processes may access an MSaaS Portal to find resources or information. Dedicated workspaces could be made available through the MSaaS Portal to prepare and execute specific events.

2.5 STAKEHOLDERS

4. The stakeholders in MSaaS are defined by their roles as described by the MSaaS Operational Concept Description (OCD) [10] and based on their MSaaS business and operational needs and interactions.

5. At the top level, the stakeholders can be classified as Service Producers and Service Consumers. These two categories can be further divided into respectively, Suppliers / Providers and Customers / Users.

6. The stakeholders are explained in the following sections. Figure 2-1 visualises the stakeholders and their relationships.

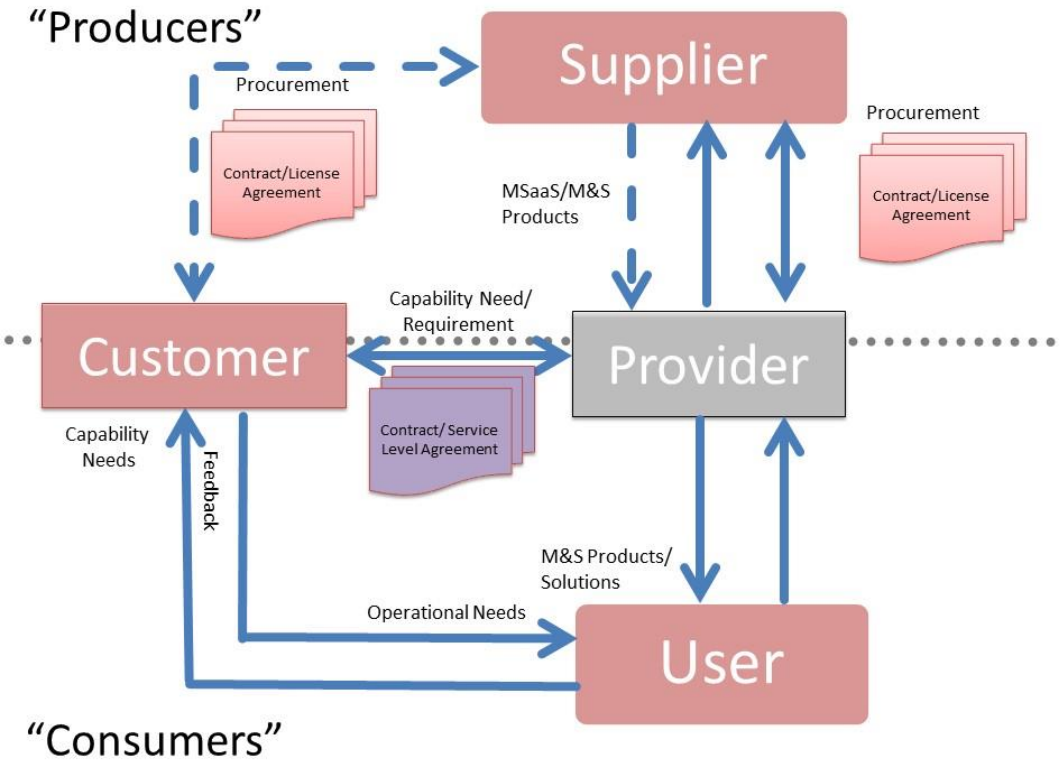

Figure 2-1: Stakeholders and Interactions

Solid arrows indicate general case of stakeholder relationships/interactions, dashed lines indicate additional relationships/interactions in the special case of Enterprise Licences or Government-off-the-Shelve services

7. The identified stakeholders in MSaaS represent generic roles required for implementing MSaaS as a persistent capability. Each nation or organization that implements MSaaS should map these generic roles to its specific organizational structures. Depending on the actual organizational structures, it may be the case that some of the stakeholders identified are actually represented by the same organizational entity. Generic roles can be mapped onto one or more real people or organizational entities. Depending on the organisation size, one real person could fulfil multiple roles, unless prevented by other guidelines.

2.5.1 CUSTOMER

1. As a consumer of M&S services using the The Allied Framework for MSaaS, the MSaaS Customer is a defense organization with an operational need (e.g., training, mission planning, acquisition), and is the budget holder. The Customer may include a NATO Nation/HQ/Agency or group of Nations or international entities.

2.5.2 PROVIDER

1. As a producer of M&S services, the MSaaS Provider makes M&S products and services (including integrated services such as executable simulations) available to Users of the Allied Framework for MSaaS in accordance with Customer SLAs. Therefore, the MSaaS Provider needs to manage and maintain a core set of secure M&S services to comply with the SLAs. These services include the use of MSaaS Portal services (e.g. for registering and discovering services) to maintain visibility and availability of M&S products, either already owned by defense organizations or available from Suppliers through a license agreement, purchase order, a legal contract or agreement. The MSaaS Provider takes responsibility for the composition and integration of M&S products and services in accordance with Customer requirements.

2.5.3 USER

1. As a consumer of M&S products and services, the User (e.g. Operational End User) is responsible for providing data and feedback on performance and functionality of the Allied Framework for MSaaS to the Customer. The user must comply with relevant security policies and other agreements.

2.5.4 SUPPLIER

1. MSaaS Suppliers develop and provide M&S products. This includes maintaining M&S products and making these available to MSaaS providers as part of the Allied Framework for MSaaS either via a product procurement or license agreement. Examples of Suppliers include large defense contractors, small and medium enterprises, and academic institutions, in addition to government organizations.

INTENTIONALLY BLANK

CHAPTER 3 GENERAL POLICIES

1. This chapter specifies the general policies for MSaaS implementations. These policies are further elaborated in CHAPTER 4 of this document.

2. To avoid ambiguity and to enable convenient referencing, all policies defined in this document are identified by a unique identifier. The identifiers are made up by three letters to indicate the type of policy (e.g., GEN for a general policy) and a two-digit number.

3. [GEN-01] An MSaaS implementation SHALL conform to the principles as identified and established in the NATO M&S Master Plan [1].

4. [GEN-02] An MSaaS implementation SHALL be aligned with the NATO M&S Standards Profile AMSP-01 [13]. The AMSP-01 includes recommended M&S standards and STANAGs/STANRECs.

5. [GEN-03] An MSaaS implementation SHALL conform to the practices, architectural principles, and operating procedures as identified and established by this document.

6. [GEN-04] An MSaaS solution architecture SHALL comply with the MSaaS Technical Reference Architecture [5]. This includes access to the services through a Portal (or a federation of Portals) and support for a federated MSaaS ecosystem with multiple solution architectures.

7. [GEN-05] Any M&S service from a NATO MSaaS implementation that is provided or consumed by a NATO body, Nation or Organization SHOULD comply with the policies defined in this document as formalised by its related STANREC.

8. [GEN-06] The federated MSaaS ecosystem SHALL include a NATO MSaaS Portal (see Section 2.4) provided by a NATO assigned organization.

INTENTIONALLY BLANK

CHAPTER 4 DETAILED POLICIES

4.1 ORGANIZATIONAL POLICIES

4.1.1 Service Identification Policies

1. [ORG-01] All MSaaS M&S capabilities SHALL be defined and provided as services and managed in accordance with this document.

2. [ORG-02] The NMSG SHALL hold the responsibility of enterprise architect for MSaaS in accordance with the NMSMP and define all services in the context of a M&S service landscape description.

4.1.2 Service Level Agreement Policies

1. [ORG-03] Each (composed) service SHALL be provided according to certain conditions formalized in a Service Level Agreement (SLA). The agreement may apply to a specific phase in the lifecycle of a service.

2. [ORG-04] Each SLA SHALL be documented according to the Service Level Agreement Template (SLAT) as defined in ANNEX A. The SLAT captures information about individual services and provides a well-defined and unambiguous description of a service level for each service (e.g., regarding availability, resource consumption, solutions and escalations in case of unforeseen issues or calamities).

3. [ORG-05] Service providers and customers SHALL agree on a Service Level Agreement (SLA) prior to service usage.

4.1.3 Service Description Policies

1. The policies in this section are concerned with methods and tools to describe services and their interfaces.

2. The Service Description Template (SDT) as defined in the Technical Reference Architecture [5] captures information about individual services and provides a well-defined and unambiguous description of a service. The SDT aims to enable a machine-readable registry of services that are discoverable in an automated way.

3. [ORG-10] Each M&S service SHALL be described as specified by the Service Description Template (SDT).

4. [ORG-11] Each M&S service description SHALL be made available in a registry and SHALL be accessible through the MSaaS Portal(s) (see Section 2.4).

5. [ORG-12] Each M&S service SHOULD be made available in a repository and SHOULD be accessible through the MSaaS Portal(s).

6. [ORG-13] Each M&S service that is provided NATO-wide SHALL be classified in accordance with the C3 Classification Taxonomy.

7. [ORG-15] M&S service users SHALL be able to provide feedback (rating, comments, etc.) to the service Provider and the community of interest via the MSaaS Portal(s).

8. [ORG-16] All service providers SHALL indicate the forecasted retirement date of (a specific version) of a service (End of Life (EOL)) as part of the metadata of a service.

9. [ORG-17] The service provider SHOULD include technical information of using a service (interfaces, network setting) in the metadata of service.

4.1.4 MSaaS Business Model

1. [ORG-20] Each MSaaS implementation SHALL define the associated business model (ecosystem) as defined in [1], including the description of the following topics:

   a. Value proposition,

   b. Stakeholder segments,

   c. Stakeholder channels,

   d. Key partners,

   e. Key activities,

   f. Key resources,

   g. Customer relationship,

   h. Cost structure,

   i. Revenue Streams

4.2 TECHNICAL POLICIES

1. None.

4.3 SECURITY POLICIES

1. The policies in this section address security concerns and the safeguard of all MSaaS stakeholders (Suppliers, Providers, Customers, and Users) by employing a secure environment, for their services, data, account information and personally identifiable information (PII).

2. [SEC-01] Any MSaaS implementation SHALL be compliant with the hosted security environment measures (technical, procedural, as well as organizational).

3. [SEC-02] Any MSaaS implementation SHALL be compliant with the hosted security's measures to include CyberSecurity for the purpose of the protection of cyberspace and use of it against any sort of crime related to information Confidentiality, Integrity and Availability.

4. [SEC-03] All products and services developed by industry SHALL provide the required nation certifications as fit for use and adhere to NIST (Cloud Security Reference Architecture [14]) best practices.

5. [SEC-04] Any MSaaS implementation SHOULD adhere to the MSaaS Technical Reference Architecture Document [5], to provide specific end-to-end data flow examples of where specific security controls (e.g., Cross Domain Security (CDS) solutions) shall be imposed.

6. [SEC-05] The stakeholders involved in managing an MSaaS implementation and in providing technical services SHALL be responsible for ensuring they address the users' areas of concern regarding security and secure hosting infrastructure. This includes but is not limited to:

   a. Risk Management

   b. Account Management

   c. Authentication & Authorization

   d. Monitoring and Reporting

   e. Physical Security

   f. Data-at-rest / Data-in-transit / Data-to-remove

   g. Compliance with National and International/Industry Standards on Security

7. The approach to securing an MSaaS implementation is intrinsically related to the underlying infrastructure which may utilize different cloud computing service models (SaaS, PaaS, or IaaS) and deployment model (Public, Private, Hybrid, or Community). For each component it is necessary to evaluate the particular security requirements in the specific MSaaS solution architecture, and to map them to proper security controls and practices in technical, operational, and management classes.

8. [SEC-06] All MSaaS data, data exchanges, data transfers, output (ex. After Action Review) in the same security domain SHALL be at the same classification level. Aggregation of data may result in a higher classification and needs to be examined and re-classified before execution.

9. [SEC-07] The stakeholders involved in managing an MSaaS implementation and in providing technical services SHALL apply best practices for security and comply with specific regulations from involved accreditation authorities. Important references include, but are not limited to:

a. NATO Cloud Computing Policy [15]

b. NATO Information and Communications Technology (ICT) Service Management Policy [16]

c. NIST Cloud Security Reference Architecture [14]

d. ENISA Guidelines [17], [18]

e. CSA Best Practices, see https://cloudsecurityalliance.org/;

f. FMN Security/IdAM [19]

g. CFBLnet [20]

h. Multinational Security Accreditation Board (MSAB) [21]

10. [SEC-08] The practices to be implemented SHALL be selected by the MSaaS provider based on the national or other specific organisational security requirements. Selected practices and compliance with them SHALL be documented by the MSaaS provider and SHALL be provided upon request to other parties.

CHAPTER 5 AUTHORITIES AND RESPONSIBILITIES

1. This chapter defines how to sustain (maintain and update) the Allied Framework for MSaaS.

5.1 AUTHORITY

1. The mission of the NATO Modelling and Simulation Group (NMSG) is to develop and exploit M&S for the benefit of the Alliance and its Partners. The NMSG is the delegated NATO tasking authority for M&S standards. The NMSG has established the Modelling and Simulation Standards Subgroup (MS3) as the permanent body responsible for M&S standards [22]. MS3 is the custodian for technical standards as defined by [3].

2. The Military Operational Requirements Subgroup (MORS) is the permanent body of the NMSG responsible for identifying and prioritizing operational needs in the area of M&S capabilities [23].

3. NMSG task groups, NATO bodies or nations may also identify technical needs related to M&S capabilities (e.g., interoperability issues) or identify technical innovations that may benefit NATO or the national technical community (e.g., service-oriented architectures). These technical opportunities or needs will also be reported through the NMSG Programming and Planning Committee (PPC) and in consultation with MS3 this can lead to recommendations for new task group activities to address short-term and long-term technical gaps.

5.1.1 Operational Authority

1. [AUT-01] NMSG SHALL be the custodian of the MSaaS OCD [10], with regard to MSaaS operational needs.

2. [AUT-02] NMSG SHALL be the custodian of the AMSP-02 MSaaS CONEMP (this document), with regard to MSaaS governance recommendations. NMSG SHOULD provide relevant input in order to keep the information updated and in accordance with the MSaaS OCD.

5.1.2 Technical Authority

1. [AUT-03] NMSG SHALL be the custodian of the MSaaS Technical Reference Architecture [5] and implementation recommendations.

2. This AMSP-02 MSaaS CONEMP refers to existing standards, procedures, etc. where applicable. These referred standards are typically included in AMSP-01 the NATO M&S Standards Profile [13]. NMSG will ensure that AMSP-02 and MSaaS Technical Reference Architecture [5] are updated with technical improvements and enhanced guidelines that are or were developed and validated by (future) NMSG task groups.

3. NMSG will review all proposals for updates or modifications to AMSP-02 MSaaS CONEMP (this document) and release new versions of the document as needed. NMSG should also review existing documents (e.g. AMSP-03 standard 'NATO Reference Architecture for Distributed Synthetic Training') and recommend possible integration actions.

5.2 STANDARDS IMPLEMENTATION

1. The AMSP-02 MSaaS CONEMP is aimed at use of MSaaS in NATO and multi-national context and therefore refers to the MSaaS Technical Reference Architecture that includes recommendations for the use of specific (versions of) standards. This could mean that AMSP-02 or MSaaS Technical Reference Architecture (TRA), in comparison with AMSP-01, refers to an earlier version of an M&S standard to address the reality of existing legacy tools. AMSP-02 will generally prefer validated and proven processes and technology, where AMSP-01 also provides recommendations with regard to interoperability innovations (i.e. emerging standards).

2. [STN-01] The AMSP-02 MSaaS CONEMP SHALL be NATOs general guideline for MSaaS in accordance with NMSGs role as NATO's delegated tasking authority for M&S standards.

3. [STN-02] The MSaaS Technical Reference Architecture SHALL be NATOs technical guideline for MSaaS in accordance with NMSGs role as NATO's delegated tasking authority for M&S standards.

5.3 COMPLIANCE TESTING

1. Compliance testing service for individual components of a NATO or multi-national simulation environment is the ultimate responsibility of the participating organizations. The NMSG provides oversight of the Compliance Testing service.

2. [COM-01] Any M&S service SHALL comply with the practices and recommendations for Integration, Verification and Compliance Testing as defined by and in accordance with existing STANAG/STANRECs [24].

3. It is expected that specific conformance targets and conformance test cases are defined by future task groups, taking into account experiences of first MSaaS implementations.

ANNEX A SERVICE LEVEL AGREEMENTS TEMPLATE

1. The stakeholder diagram identifies a formal agreement between customer and provider regarding the service that a user will receive. Noting that all partners in the agreement have certain obligations. That agreement is known as Service Level Agreement (SLA). This paragraph discusses a template for an example SLA. It should cover the description of the service (e.g. CGF entity service), identify the names/POCs for the different parties in the SLA, but also include performance (e.g. max nr of entities, max nr of instances, update rates etc.) and other performance aspects (e.g. guaranteed/best-effort uptime, scalability etc.). It could be a long list of topics that need to be covered.

2. The SLA template must be tailored according to the specific technical requirements (e.g. functionality, performance), availability requirements (e.g. Demo, Exercise or persistent Training Capability) and business conditions (e.g. liability, metering and cost). The template below may serve as guideline.

3. MSG-164 collected some practical experience by developing an example SLA for the planned CA2X2 Forum and future experiments or exercises (e.g. Viking). The EXP and GOV/OPS conducted the process involving agreement between the ‘’Customer’’ and the ‘’Provider’’ on technical aspects, including inputs from business developers, purchasing department and legal reviewers. Obviously, this was just be done to gain experience and not have any financial, legal etc. consequences in the context of MSG-164, but it should serve as guideline for MSaaS in everyday practice that we hope to see in the near future. The SLA template should be evaluated through more examples (either real experiments or mental exercises) as part of MSaaS Phase III.

A.1. Service Level Agreement – *<Name of Service>*

A.1.1. Change History

Date	Version	Updated by	Changes to this version

A.1.2. Service Level Agreement

A.1.2.1. Parties

	Provider	Customer
Organization		
Responsible <contact details>		
Business Relationship Manager <contact details>		
Administrator <contact details>		

A.1.2.2. Validity, Review and Monitoring

Validity Period <Defines between which dates this service is valid. If needed define different periods for different phases in relation to an exercise, e.g. preparation, execution, review>	**From** Click here to enter a date.	**Until**
Review and Renewal <Describes procedures for scrutiny and any revision or renewal of this service>		
Termination <Describes procedures for termination of the agreement (if applicable, also rules regarding early termination of the agreement)>		
Monitoring <Describes procedures for monitoring and reviewing how the service has been delivered in relation to specified requirements in this document, for example customer or user satisfaction surveys, availability and performance reports>		

A.1.2.3. Description

Functional scope of the service <Describes the functional scope of the service. Business processes/ activities on the customer side supported by the service.>	
Utility of the service <Desired outcome in terms of utility (example: ”Field staff can access enterprise applications without being constrained by location or time”).>	
Warranty of the service <Desired outcome in terms of warranty (example: ”High availability required during office hours in locations …”)>	
Functional Options <Describes functional options, e.g. software tools, supported standards and interfaces>	
Access to Service <Describes who / where the service is accessible, e.g. role, organizational, geographical. Include reference to network diagrams to support detailed description of the agreed connectivity and access.>	
Information Classification <Describes what information classification the service can handle. Include information classification description regarding the service itself, its design, system set-up>	
Service Reporting <Describes contents and intervals of service reports to be produced by the service provider>	
Service Constraints < Specify required/expected information from the customer/consumer e.g. scenario data, terrain data etc. may be provided by the customer to allow the service to function and not provided by the service itself.>	

Pricing Model<Describes cost for the service provision, rules for penalties/ charge backs>	

A.1.2.4. Service Call Deliveries

Lead time for Service calls (service requests) <Defines maximum lead time for call-off per types of support e.g. on-site support, remote support>	**Type of call-off**				**Lead Time**			
Recovery times for incident management <Defines maximum time to restore service from identified incident. Level 1 to level 4 can be defined here or in an appendix. This concerns the service environment.>	**Level 1 Acute**		**Level 2 Important**		**Level 3 Normal**		**Level 4 Low**	
	Lead time	**Target (%)**	**Lead time**	**Target (%)**	**Lead time**	**Target (%)**	**Lead time**	**Target (%)**
		90 %		90 %		90 %		90 %
Specific Management <Defines audiences with specific needs>								
Service Desk <Describes service desk and define service levels such as opening hours and response times. Describe agreements related to reporting the progress of resolving issues and the logging of issue handling >								
The user's responsibility for delivery <Describes activities that the user must perform in order for the service to work, e.g. follow instructions in reference guide or safety instructions, Security aspects to be observed when using the service (if applicable, references to relevant Security and/or IT Security Policies)>								

A.1.2.5. Escalation Matrix in case of incident

1. For incidents of level 1, 2, special escalations may be of organizational and / or functional nature. This is described in the matrix below.

Escalation Matrix <Refers to incident levels 1 and 2 >	**Organizational Escalation**	**Functional Escalation**
<First escalation level>	<Appointed incident manager> via <mail / telephone number / other>	<Appointed incident manager> via <mail / telephone number / other>
	<Description of report content>	<Description of report content>
	To <Position / department / section> via <mail / telephone number / other>	To <function / role> via <mail / phone number / other>
<Second escalation level>		

A.1.2.6. Availability

Availability Definition <Conditions under which the service is considered to be available resp. unavailable (e.g. if the service is offered at several locations)>	
Availability Slots <Timeslots when the service is required to be available during the given period, Exceptions (e.g. weekends, public holidays, scheduled maintenance). Also consider different time-periods, e.g. for preparation or conducting the exercise where there may be different availability requirements.>	
Average time between service breakdown <Shortest permissible average time between breaks. (Mean time between failure (MTBF) or MTBSI (Mean Time Between Service Incidents)>	
Average downtime <Maximum allowed average time to restore (required by some customers, usually defined as MTRS (Mean Time to Restore Service)>	

Maintenance Interrupt <Planned Downtimes for maintenance (number of allowed downtimes, pre-notification periods). Restrictions on maintenance, e.g. allowed maintenance windows, seasonal restrictions on maintenance, and procedures to announce planned service interruptions>	

A.1.2.7. Criticality and Risk management

Business Criticality <Describes the vital Business Functions (VBFs)and critical assets supported by the service and estimated business impact caused by a loss of the service>	
Continuity Management <Describes the activities that to ensure continuity of service delivery should the service not be available>	

A.1.2.8. Performance

Response Time <Required response time and minimum proportion of calls answered within required time. Agreements on response times for simulation services may also reference federation agreements regarding response times, dead reckoning etc. Different functions may also have different response time requirements and the template should support documenting performance agreements for each identified function. Different functions in a composition may have different dimensioning factors.>	**Response Time**	**Target (%)**
Dimensioning Factor <Defines total load that the service can handle simultaneously, e.g. 1000 users, interactions per second>		

Scalability <Requirements for scalability, delays in dynamic scaling of performance, assumptions for the medium and long-term increase or decrease in workload and service utilization and options to address these needs>	

A.1.2.9. Technical standards/ specification of the service interface

<Mandated technical standards and specification of the technical service interface>	

A.1.2.10. Miscellaneous

<any additional concerns or agreements that need to be captured>	

A.1.2.11. References

1. *<e.g. to higher-level SLAs on the corporate or customer level which also apply to this agreement)>*

A.1.2.12. Glossary

1. *<if applicable>*

AMSP-02(A)(1)