|  |  |
| --- | --- |
| SESAR_JU | |
| SWIM Compliance Framework Criteria | |
| Document information | |
| Project Title | Operational Requirements & Demands concerning organisation of the ATM Information Management within the scope of the European ATM Enterprise Architecture |
| Project Number | 08.01.01 |
| Project Manager | EUROCONTROL |
| Deliverable Name | SWIM Compliance Framework Criteria |
| Deliverable ID | D49 |
| Edition | 00.01.01 |
| Template Version | 03.00.00 |
| Task contributors | |
| EUROCONTROL, Thales, Frequentis, Noracon, SELEX, DFS, DSNA | |
| Abstract  This document details the SWIM Compliance Criteria used in the SWIM Compliance Framework. The aim of the criteria is to enable objective compliance assessments.  The definition of this Framework has been split in two documents: one defining the Compliance Principles and another one defining the Compliance Criteria for the covered scope.  This version of the SWIM Compliance Framework Criteria targets the “Service Technical Design Description” (STDD). | |

Authoring & Approval

|  |  |  |
| --- | --- | --- |
| Prepared By - Authors of the document. | | |
| Name & Company | Position & Title | Date |
| Pedro Cruellas / EUROCONTROL\* | P08.01.01 Project member | 10-04-2014 |
| Sam Van Der Stricht / EUROCONTROL\* | P08.01 Project manager | 10-04-2014 |
| Mikael Månström / NORACON\* | P08.00 Project Member | 10-04-2014 |
| Les Folds / NORACON\* | P08.03.10 Project Member | 10-04-2014 |
| Eric Roelants / EUROCONTROL | P08.01.01 Project manager | 07-02-2015 |
| Robert Suzic / EUROCONTROL | P08.01.03 Project Member | 27-01-2015 |
| Antonio Strano / SELEX | P14.01.04 Project Manager | 27-01-2015 |
| Hakim Souami / Thales | P14.01.03 Project Member | 27-01-2015 |
| Harald Milchrahm / Frequentis | P14.04 Project Member | 27-01-2015 |
| Tord Pola / Noracon | P08.03.10 Project Manager | 27-01-2015 |
| Dario Di Crescenzo / Selex | P14 Project Co-Leader | 27-01-2015 |
| Oliver Schrempf / DFS | P08.01.03 Project Member | 27-01-2015 |
| Gianluca Marrazzo / SELEX | P08.01.03 Project Member | 27-01-2015 |
| Marc Brochard / EUROCONTROL | WP B4.3 Leader | 15-05-2015 |
| Juliette Engel / EUROCONTROL | B4.3 Project member | 15-05-2015 |
| Ignacio Mesa / NATS | B4.3 Project member | 15-05-2015 |
| FJ Crabiffosse / EUROCONTROL | P08.01.01 Project member | 29-01-2016 |

\* Authoring & approval of previous deliverable D45.

|  |  |  |
| --- | --- | --- |
| Reviewed By - Reviewers internal to the project. | | |
| Name & Company | Position & Title | Date |
| Eric Roelants / EUROCONTROL | P08.01.01 Project manager | 29-01-2016 |

|  |  |  |
| --- | --- | --- |
| Reviewed By – Other SESAR projects, Airspace Users, staff association, military, Industrial Support, other organisations. | | |
| Name & Company | Position & Title | Date |
| Scott Wilson / EUROCONTROL | P08.01.03 Project Manager | 29-01-2016 |
| Antonio Strano / SELEX | P14.01.04 Project Manager | 29-01-2016 |
| Hakim Souami / Thales | P14.01.03 Project Member | 29-01-2016 |
| Tord Pola / Noracon | P08.03.10 Project Manager | 29-01-2016 |
| Harald Milchrahm / Frequentis | P14.04 Project Member | 29-01-2016 |
| Dario Di Crescenzo / Selex | P14 Project Co-Leader | 29-01-2016 |

|  |  |  |
| --- | --- | --- |
| Approved for submission to the SJU By – Representatives of the company involved in the project. | | |
| Name & Company | Position & Title | Date |
| Eric Roelants / EUROCONTROL | P08.01.01 Project manager | 29-01-2016 |
| Oliver Krüger / DFS | P08.01.01 Project Member | 29-01-2016 |
| Stéphane Dubet / DSNA | P08.01.01 Project Member | 29-01-2016 |
| Pedro Fernandez / EUROCONTROL | P08.01.01 Project Member | 29-01-2016 |
| Sam Van Der Stricht / EUROCONTROL | P08.01.01 Project Member | 29-01-2016 |

\* Approval of previous deliverable D45.

|  |  |  |
| --- | --- | --- |
| Rejected By - Representatives of the company involved in the project. | | |
| Name & Company | Position & Title | Date |

|  |
| --- |
| Rational for rejection |
| None. |

Document History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Edition | Date | Status | Author | Justification |
| 01.00 | 01/02/2016 | Draft | FJ Crabiffosse  Eric Roelants | Updates to the SWIM Compliance criteria and minor quality improvements. |
| 01.01 | 22/03/2016 | Final | FJ Crabiffosse | Updates to address SJU comments. |

Intellectual Property Rights (foreground)

This deliverable consists of SJU foreground.

Table of Contents

[Executive summary 7](#_Toc446423598)

[1 Introduction 8](#_Toc446423599)

[1.1 Purpose of the document 8](#_Toc446423600)

[1.2 Intended readership 10](#_Toc446423601)

[1.3 Inputs from other projects 10](#_Toc446423602)

[1.4 Glossary of terms 11](#_Toc446423603)

[1.5 Acronyms and Terminology 13](#_Toc446423604)

[2 The Object under Assessment 16](#_Toc446423605)

[2.1 The OuA in this version 16](#_Toc446423606)

[2.2 General description of the OuA 16](#_Toc446423607)

[3 A summary of the criteria 17](#_Toc446423608)

[4 The result 19](#_Toc446423609)

[4.1 SWIM Compliance Levels 19](#_Toc446423610)

[4.2 SWIM Compliance Assessment Report 20](#_Toc446423611)

[4.2.1 SWIM Compliance Assessment Report template 20](#_Toc446423612)

[4.3 Other things to do 20](#_Toc446423613)

[5 SWIM-related artefacts in the context of Compliance 21](#_Toc446423614)

[6 Information Service Compliance 22](#_Toc446423615)

[6.1 Target of Compliance 22](#_Toc446423616)

[6.2 Compliance Levels 22](#_Toc446423617)

[6.2.1 Information Service Ready 23](#_Toc446423618)

[6.2.2 Information Service Compatible 23](#_Toc446423619)

[6.2.3 Information Service Compliant 23](#_Toc446423620)

[7 Technical Infrastructure (Profile) Compliance 25](#_Toc446423621)

[7.1 Target of Compliance 25](#_Toc446423622)

[7.2 Compliance Levels 25](#_Toc446423623)

[7.2.1 SWIM <Color> Profile Binding Ready 26](#_Toc446423624)

[7.2.2 SWIM <Color> Profile Binding Compatible 26](#_Toc446423625)

[7.2.3 SWIM <Color> Profile Binding Compliant 27](#_Toc446423626)

[8 Information Compliance 28](#_Toc446423627)

[8.1 Target of Compliance 28](#_Toc446423628)

[8.2 Compliance Levels 28](#_Toc446423629)

[8.2.1 Information Ready 28](#_Toc446423630)

[8.2.2 Information Compatible 28](#_Toc446423631)

[8.2.3 Information Compliant 29](#_Toc446423632)

[9 References 30](#_Toc446423633)

[Appendix A SWIM Compliance Assessment Process 32](#_Toc446423634)

[A.1 Introduction 32](#_Toc446423635)

[A.2 Example assessment process 32](#_Toc446423636)

[A.2.1 Roles and responsibilities 32](#_Toc446423637)

[A.2.2 The process 33](#_Toc446423638)

[A.3 Example of post-condition checks as part of SWIM Compliance 35](#_Toc446423639)

[A.3.1 Post-condition on payload compliance 35](#_Toc446423640)

[Appendix B Compliance with Information Services: Additional information 37](#_Toc446423641)

[B.1 MEP mapping table 37](#_Toc446423642)

List of tables

[Table 1: Compliance Levels per area – Summary 18](#_Toc446423643)

[Table 2: SWIM Compliance Levels – Overview of the Information Service compliance 22](#_Toc446423644)

[Table 3: SWIM Compliance Levels - Compliance with Information Service 22](#_Toc446423645)

[Table 4: SWIM Compliance Levels – Overview of the TI compliance 25](#_Toc446423646)

[Table 5: SWIM Compliance Levels - Compliance with Technical Infrastructure 26](#_Toc446423647)

[Table 6: SWIM Compliance Levels – Information Compliance 28](#_Toc446423648)

[Table 7: Roles-responsibilities and Projects 33](#_Toc446423649)

List of figures

[Figure 1 – SWIM Compliance Framework 8](#_Toc446423650)

[Figure 2 – Compliance Assessment 8](#_Toc446423651)

[Figure 3 – Compliance Criteria and Levels 19](#_Toc446423652)

[Figure 4 – SWIM Compliance Levels - Summary 20](#_Toc446423653)

[Figure 5 – Overview of the SWIM-related artefacts involved in Compliance (S3T artefacts model) 21](#_Toc446423654)

[Figure 6 – Situations to avoid for obtaining SWIM Compliance. 36](#_Toc446423655)

Executive summary

This document provides the SWIM Compliance Criteria; the aim is to enable objective compliance assessments of SWIM Services against well-defined compliance criteria. The definition of this Framework has been split in two documents: one defining the Compliance Principles and another one defining the Compliance Criteria for the covered scope. This document covers the Criteria of the SWIM Compliance Framework.

This version of the SWIM Compliance Framework Criteria targets the “Service Technical Design Description” (STDD).

This document details the SWIM Compliance Criteria used in the SWIM Compliance Framework. The aim of the criteria is to enable objective compliance assessments.

This document is applicable to Services enabled by SWIM.

# Introduction

## Purpose of the document

This document, together with the “D43-SWIM Compliance Framework: Principles” document, defines the SWIM Compliance Framework.

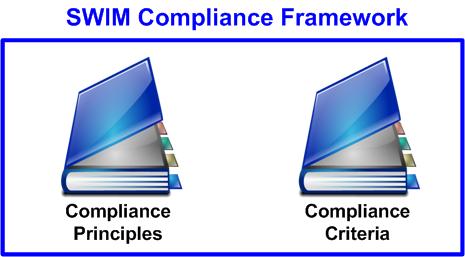


Figure 1 – SWIM Compliance Framework

This document sets out a number of detailed compliance criteria which are used in assessing an ‘Object under Assessment’. The ‘Object under Assessment’ is assessed against the SWIM Compliance Criteria in order to achieve a result. The result of the assessment process is a report outlining the SWIM Compliance Level attained. This simple process is shown in Figure 2.

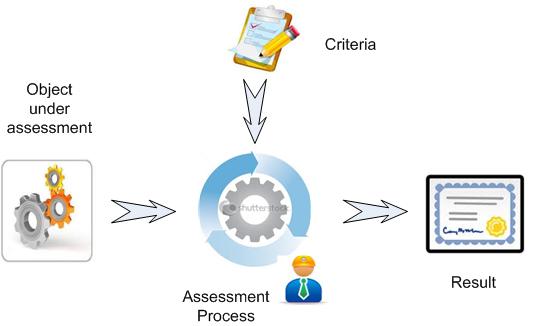


Figure 2 – Compliance Assessment

In order to facilitate the reading and understanding of the criteria, chapters are included which outline the ‘Object under Assessment’ and the compliance report used to record the result of the assessment. Furthermore, a series of annexes are included which add further detail to the assessment process.

The following table lists the references that are used in this version of the document.

| **Reference** | **Rationale / Description** |
| --- | --- |
| AIRM | SWIM shall use a common ATM information reference (AIRM) model as means for achieving (cross-domain) semantic interoperability. For introduction to AIRM see [16]. |
| AIRM Compliance Framework | A set of rules and recommendations on what is required to claim Compliance with AIRM, see [9]. |
| Change Request (CR) on the AIRM | The AIRM is under formal configuration management and governance, called AIRM CCB, see the AIRM Governance Handbook [17] |
| Information Exchange Requirements (IER). | The IER form the basis for the service message and data types and the IER template is embedded in the OSED template and in the SPR template. Feedback can be provided to the SJU if changes in the attributes are needed. The OSED contains the operational characterisation of the IER and the SPR the performance characterisation. |
| ISRM Rulebook [8] | In order to make interoperable service identification and service design possible for multiple stakeholders the work on the model should be governed defined in rules. |
| SESAR European ATM Service Description Document production. [2] | The Service Description Document is the non-formal description of a logical service, its interfaces and operations. |
| SESAR European ATM Service Identification Document template. Ref [4] | The Service Identification Document is an easy to read non-formal extract of the model of identified services with added text. Through a common template all Service Identification Documents have the same structure. |
| SESAR Operational Service and Environment Definition  template Ref [6] (OSED) | The operational requirements for a service should be known to identify and design it. The IER (Information exchange requirements) template is embedded in the OSED template. The OSED contains the operational characterisation of the IER and the SPR the performance characterisation. |
| SESAR Safety and Performance Requirements template Ref [5] (SPR) | The Safety and Performance Requirements for a service should be known to identify and design it. The IER (Information exchange requirements) template is embedded in the SPR template. |
| SWIM ConOps [1] | The SWIM Conops with the high level description and requirements on SWIM should be maintained to explain the benefits, evolution and vision of SWIM. |
| SWIM Profile [10] | The SWIM profiles that define the different characteristics of the infrastructure(s) that the service instance uses to communicate will be one of the standards of SWIM to be maintained. |
| SWIM Profile Specifications | SWIM Profile Technical Specifications (Yellow, Blue, Purple) |
| Templates and Toolbox User Manual. Ref [3] | The document is intended to give the reader an introduction into the SESAR deliverable templates and their layout as well as the Template Toolbox provided with the templates in order to ease the use and enhance the understanding of the templates used in the context of the SESAR Programme. |
| Working\_method\_on\_Services [7] | A process description of the service lifecycle should be required for manageability. |

## Intended readership

This document is intended for all managers and experts in the programme who are involved in SWIM. It concerns all participants in the broad sense, who make or will make use of SWIM to implement, consume, provide or plan to provide, SWIM compliant services.

## Inputs from other projects

Projects P08.01.03, P14.01.04, P14.01.03, P14.04, B04.03 and P08.03.10 are providing input to the document in the form of contributions to and reviews of the document versions.

A team of experts from Work Packages 8 and 14 was built to define the criteria.

## Glossary of terms

| Term | Definition |
| --- | --- |
| **Capability** | The collective **ability to deliver a specified type of effect or a specified course of action**. Within the context of the SESAR Programme a capability is therefore the ability to support the delivery of a specific operational concept to an agreed level of performance**. Source: Common working meeting between B41 EA study and B43 T5. In bold, the NATO Architecture Framework V3 definition** |
| **Governance** | Ability of decision-makers to set policies regarding stakeholders, services, and their relationships |
| **Information Exchange** | A specification of the information that is to be exchanged. An Information Exchange must have a unique identifier. Source: NATO Architecture Framework V3 definition. |
| **Information Exchange Requirement** | An Information Exchange Requirement (IER) is the description, in terms of characteristics, of the requirement to transfer information between two or more end users. The characteristics described include source, recipients, content, size, timeliness, security and trigger. IERs are defined as independent of the communications medium. An IER may express both current and future requirements.  Note: an information element is the descriptor of the content in the IER. Source: (British) Ministry of Defence, Information Exchange Requirements. |
| **Infrastructure profile** | A set of features characterising the enabling infrastructure, including the QoS and security that the infrastructure provides, technical constraints, user behaviour patterns and characteristics.  Profiles relate to legacy and/or new infrastructures such as the SWIM technical infrastructure. Source: B43 T5 study |
| **Means of compliance** | Means to demonstrate that an ‘Object under Assessment’ conforms to a rule (such rule being as e.g., a specification, policy, standard or law) |
| **Node** | **A logical entity that performs Operational Activities specified independently of any physical implementation,** e.g. a stakeholder type providing and/or consuming operational information within a network of other stakeholders. Source: Common working meeting between B41 EA study and B43 T5. In bold, the NATO Architecture Framework V3 Definition. |
| **Object under Assessment** | Item (i.e., [specifications](http://itlaw.wikia.com/wiki/Specification), mechanisms, activities, individuals) upon which an [assessment method](http://itlaw.wikia.com/wiki/Assessment_method) is applied during an [assessment](http://itlaw.wikia.com/wiki/Assessment). |
| **Operational Focus Area** | A limited set of dependent operational and technical improvements related to an Operational Sub-Package, comprising specific interrelated OIs designed to meet specific performance expectations of the ATM Performance Partnership. Source: ATM Lexicon |
| **Policy** | Principle or rule with a view to guiding decisions and achieving one or more rational outcomes |
| **Registry** | The SWIM registry is a trusted, managed, complete and consolidated source of reference for service information and related regulations (policies, standards, certifications and taxonomies). It holds all SWIM metadata regarding:  - stakeholders,  - service definitions,  - service instances,  and the links between them.  Source: Registry ConOps |
| **Service** | The contractual provision of something (a non-physical object), by one party, for the use of one or more other parties. Services involve interactions between providers and consumers, which may be performed in a digital form (data exchanges) or through voice communication or written processes and procedures. Source: ATM Lexicon |
| **Service definition** | The specification of a service as it appears in the Service Description Document and Service Interface Definition. The Service Description Document consists of a mix of textual information and graphics (expressed in a UML notation). The Service Interface Definition consists of machine-interpretable constructs specified according to the selected technical platform, including the necessary technology bindings, e.g. complete WSDL (and XSD), IDL, AMQP, DDS, etc. Source: B4.3 Working Method on Services. |
| **Service interface** | The mechanism by which a service communicates.  Service providers and consumers need to implement service interfaces in order to be able to collaborate. A service interface includes service operations that enable access to the functionality of the services identified, as well as the data used in the service interaction. Source: B43 T5 study. |
| **Service instance** | Service which has been implemented in accordance with its specification in the service catalogue (during the SESAR Development Phase, the service definitions are available in the ISRM) by a service provider (by itself or contracted to a third party). Source: SWIM ConOps |
| **Service level** | A value specification for one or more service attributes indicating the level to which a technical system (or resource if including non-automated services) delivers a service in a particular environment. Example: A “Service Response time” may be defined in relation to a service. A given technical system could have a corresponding Service Level, e.g. ”Less than 3 seconds”. Source: B43 T5 study. |
| **Service consumer** | Stakeholder which consumes service(s) provided by other stakeholder(s) |
| **Service lifecycle** | The lifecycle defines the sequence of phases followed by a service. |
| **Service Payload definition** | The data/information exchange model represented in UML contained in the Service Instance Description. |
| **Service provider** | Stakeholder which provides service(s) that can be consumed by other stakeholder(s) |
| **SWIM** | System-wide information management. SWIM consists of standards, infrastructure and governance enabling the management of ATM information and its exchange between qualified parties via interoperable services. Source: SWIM ConOps. |
| **SWIM Common Component** | A SWIM infrastructure element managed by the ‘SWIM authority’ and implementing a shared capability, e.g. registry, PKI, etc. Source: SWIM ConOps. |
| **SWIM Compliance Assessment Team** | The group of experts who perform the SWIM Compliance Assessment and provide the final SWIM Compliance Level. |
| **SWIM Infrastructure** | The sum of all the SWIM infrastructure elements which are needed to support SWIM services. Source: B43 T5 study. |
| **SWIM Profile** | A SWIM profile is a coherent, appropriately sized grouping of middleware functions/services for a given set of technical constraints/requirements which permit a set of stakeholders to share information |
| **Service Technical Design Description** | A set of one or more published documents that express meta information about a service. The fundamental part of a service contract consists of the service description documents that express its technical interface. These form the Service Technical Design Description (STDD) which essentially establishes an API into the functionality offered by the service.  The service interface definition in the STDD is mainly given as a machine-readable format usually provided in a standard definition language such as IDL, WSDL or others. The STDD also describes such aspects as the message exchange pattern between provider and consumer, plus the chosen SWIM profile and requirements (bindings) on the technical infrastructure.  A STDD can further reference human-readable documents, such as Service Level Agreement (SLA) that describes additional quality-of-service features, behaviours and limitations. |

## Acronyms and Terminology

| Term | Definition |
| --- | --- |
| **AIRM** | ATM Information Reference Model |
| **ADQ** | Aeronautical Data Quality |
| **ATM** | Air Traffic Management |
| **CLDM** | Consolidated Logical Data Model |
| **ConOps** | Concept of operations |
| **DDS** | Data Distribution Service |
| **DOD** | Detailed Operational Description |
| **EA** | Enterprise Architecture |
| **EC** | European Commission |
| **EU** | European Union |
| **ESB** | Enterprise Service Bus |
| **EUROCAE** | European Organization for Civil Aviation Equipment |
| **IBP** | Industry Based Prototype |
| **ICAO** | International Civil Aviation Organisation |
| **ICD** | Interface Control Document |
| **IER** | Information Exchange Requirements |
| **INTEROP** | Interoperability Requirements |
| **IRS** | Interface Requirements Specification |
| **ISO** | International Organisation for Standardisation |
| **ISRM** | Information Services Reference Model |
| **IT** | Information Technology |
| **ITIL** | IT Infrastructure Library (ITIL® provides a Best Practice guidance framework for IT Service Management) |
| **MEP** | Message Exchange Pattern |
| **NAF** | NATO Architecture Framework |
| **NFR** | Non-functional Requirements |
| **OI** | Operational Improvement |
| **OPS** | Operational |
| **OSED** | Operational Service and Environment Definition |
| **OuA** | Object under Assessment |
| **PKI** | Public Key Infrastructure |
| **QoS** | Quality of Service |
| **RPC** | Remote Procedure Call |
| **RTCA** | Radio Technical Commission for Aeronautics |
| **SACG** | SWIM Architect Co-ordination Group |
| **SCG** | Service Coordination Group |
| **SCL** | SWIM Compliance Level |
| **SDD** | Service Description Document |
| **SES** | Single European Sky |
| **SESAR** | Single European Sky ATM Research Programme |
| **SESAR Programme** | The programme which defines the research and development activities and projects for the SJU |
| **SID** | Service Identification Document |
| **SIR** | Service Identification Report |
| **SJU** | SESAR Joint Undertaking (Agency of the European Commission) |
| **SJU Work Programme** | The programme which addresses all activities of the SESAR Joint Undertaking Agency. |
| **SLA** | Service Level Agreement |
| **SOA** | Service Oriented Approach |
| **SOAP** | Simple Object Access Protocol |
| **SoaML** | Service Oriented Architecture Modelling Language |
| **SVA** | Service Activity |
| **SWIM** | System Wide Information Management |
| **SWIM TI** | SWIM Technical Infrastructure |
| **SYS** | System Projects |
| **TAD** | Technical Architecture Description |
| **TS** | Technical Specification |
| **STDD** | Service Technical Design Description |
| **UDDI** | Universal Description, Discovery and Integration |
| **UML** | Unified Modelling Language |
| **WP** | Work Package |
| **WSDL** | Web Services Description Language |
| **XSD** | XML Schema Definition |

# The Object under Assessment

## The OuA in this version

In the ‘SWIM Compliance Framework’ the term ‘Object under Assessment’ (OuA), is used to refer to any “activity, product, process, system, person or body”.

The ‘Object under Assessment’ in this version of the SWIM Compliance Criteria is the Service Technical Design Description (STDD) for an implemented service.

The ‘Object under Assessment’ (OuA) is the *Service Technical Design Description (STDD)* for the service being validated. The purpose here is to make sure that Service Technical Design Description is meeting the provided compliance criteria.

This version of the SWIM Compliance Framework assumes that:

* The information exchange is implemented as a service.
* The service implementation is described in a STDD.
* The STDD is used as the ‘Object under Assessment’ for assessing compliance against the compliance criteria.
* The compliance is performed actually on the design level and not on the actual implementation level.
* A compliance report is issued for each service wishing to claim SWIM compliance.

## General description of the OuA

A **Service Technical Design Description (STDD)** is comprised of one or more published documents that express metadata about the service. The fundamental part of a STDD consists of the service description documents that express its technical interface.

The STDD is a “design level” artefact that includes:

* A **service interface definition** usually represented in a machine-readable standard definition language such as IDL or WSDL.
* Such aspects as the message exchange pattern between provider and consumer, plus the chosen SWIM profile and requirements (bindings) on the technical infrastructure.

Although the STDD can further reference human-readable documents, such as a Service Level Agreement (SLA) that describes additional quality-of-service features, behaviours and limitations.

For the sake of SWIM Compliance assessment, the prerequisites on the STDD are:

1. The STDD is properly filled in according to an agreed template;
2. The STDD includes or contains an exact reference to:
   1. The SDD (including its version) being defined,
   2. The SWIM TI profile Technical Specification used and
   3. The information exchange model used.

# A summary of the criteria

An object under assessment that wishes to claim SWIM compliance is assessed for four distinct things:

* Technical Infrastructure (Profiles’ Bindings) compliance (to ensure that the STDD is based on the use of a SWIM TI Profile which meets the requirements associated with the transport of the information).
* Information Service compliance (to ensure that the service instance, i.e. the realisation of the service within the used technology context, meets the description of the service).
* Information (AIRM) compliance (to ensure that the service instance is based on the use of the AIRM so to ensure that the semantics of the information is preserved in the information exchange).
* Governance compliance. However, please note that the governance criteria are not yet used for this version of the SWIM Compliance Framework.

Each of these is further defined in its own chapter.

The following table provides the summary of the criteria for this ‘Object under Assessment’. The improvements made for each level, identify the benefits of the next level of compliance.



Table 1: Compliance Levels per area – Summary

# The result

## SWIM Compliance Levels

The “SWIM Compliance Framework: Principles” document defines four SWIM Compliance Levels (SCL):

1. Not compliant,
2. SWIM Ready,
3. SWIM Compatible and
4. SWIM Compliant.

Each SWIM Compliance Level comprises a number of criteria to be met. This matrix is illustrated in Figure 3.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Ready | Compatible | Compliant |
| Information | Condition IN-1 | Condition IN-1 | Condition IN-1 |
|  | Condition IN-2 | Condition IN-2 |
|  |  | Condition IN-3 |
| Information Service | Condition IS-1 | Condition IS-1 | Condition IS-1 |
| Condition IS-2 | Condition IS-2 | Condition IS-2 |
| Condition IS-3 | Condition IS-3 | Condition IS-3 |
|  | Condition IS-4 | Condition IS-4 |
|  |  | Condition IS-5 |
| Technical Infrastructure | Condition TI-1 | Condition TI-1 | Condition TI-1 |
| Condition TI-2 | Condition TI-2 | Condition TI-2 |
| Condition TI-3 | Condition TI-3 | Condition TI-3 |
|  | Condition TI-4 | Condition TI-4 |
|  | Condition TI-5 | Condition TI-5 |
|  |  | Condition TI-6 |
|  |  | Condition TI-7 |

Figure 3 – Compliance Criteria and Levels

In order to reach a specific level of SWIM compliance, all the criteria need to be fulfilled. For example, to be “SWIM Compliant” the STDD shall be: SWIM Profile Compliant, Information Service Compliant and Information Compliant (see table 2 below).

This means that if not all of the criteria for a given compliance level are met, **the SWIM Compliance level is constrained by the minimum level for each of the areas.**

After having checked all criteria, some post-conditions checks may apply. The post-conditions are meant to verify the consistency between the different areas (Information, Information Services and Technical Infrastructure). The next figure shows the ‘consistency’ check, which is called ‘post-condition’. For more information and examples, see Appendix A.



Figure 4 – SWIM Compliance Levels - Summary

## SWIM Compliance Assessment Report

The SWIM Compliance Assessment Report documents the result of the compliance assessment. It gives:

* An overall assessment for the object under assessment (i.e. either: no SWIM Compliance, SWIM Ready, SWIM Compatible or SWIM Compliant).
* An assessment for each of the SWIM Compliance areas (TI Bindings, Information Service, AIRM, governance).
* The gap to be bridged to become the next level of SWIM Compliance.

The details for the compliance assessment for each of the main areas are explained in the chapter ‘detailed compliance criteria’.

### SWIM Compliance Assessment Report template

The SWIM Compliance Assessment Template is available as a separate document, to be filled in by the SWIM Compliance Applicant or by the SWIM Acceptance Team. The filled-in template is the SWIM Compliance Assessment Report that provides an overall assessment.

## Other things to do

In addition to providing the result of the compliance assessment, the SWIM Compliance Assessment Report should provide a statement that the overall assessment results are self-consistent.

# SWIM-related artefacts in the context of Compliance

The SWIM compliance criteria make reference to a number of artefacts to be used as input to the compliance assessment. For example:

* “Information compliance” is assessed against the ATM Information Reference Model (AIRM).
* “Information service compliance” is assessed against a Service Description Document (SDD).
* “Technical infrastructure (profile) compliance” is assessed against the Interface Bindings of a SWIM TI Profile.

The full picture of the key artefacts mentioned in the SESAR Working Method on Services, along with their relationships in the context of SWIM Compliance, is shown in Figure 5.



Figure 5 – Overview of the SWIM-related artefacts involved in Compliance (S3T artefacts model)

# Information Service Compliance

## Target of Compliance

The target versions of Information Service Compliance that are applicable for compliance assessment are:

* Reference Service Model versions defined by Service Foundation[[1]](#footnote-1)

## Compliance Levels

Information service compliance is defined for three compliance levels with the following content:

|  |  |  |
| --- | --- | --- |
| **Information Service Ready** | **Information Service Compatible** | **Information Service Compliant** |
| Operations are mapped  Physical message description is mapped  Chosen MEP is compliant with the one required by the SDD | Operations are mapped  Physical message description is mapped  Chosen MEP is compliant with the one required by the SDD  The service is part of the Reference Service Model | Operations are mapped  Physical message description is mapped  Chosen MEP is compliant with the one required by the SDD  The service is part of the Reference Service Model  The supported NFR given in the STDD are compliant with those required in the SDD |

Table 2: SWIM Compliance Levels – Overview of the Information Service compliance

The Service Technical Design Description is assessed against the SDD. The detailed definition of each compliance level is done in the following chapters.

Table 3 shows which Information Service Compliance Level is required as a minimum for each SWIM Compliance level.

|  |  |  |
| --- | --- | --- |
| **SWIM Ready** | **SWIM Compatible** | **SWIM Compliant** |
| Information Service Ready | Information Service Compatible | Information Service Compliant |

Table 3: SWIM Compliance Levels - Compliance with Information Service

Common pre-requisites for all levels are the following:

1. The Service Technical Design Description has a reference to a designed logical service.
2. The referenced logical service has an SDD with a specific version approved by the Service Foundation.
3. In case of a service offering multiple interfaces covering multiple MEPs, the SDD shall contain an explanation about which interfaces (or groups of) are mandatory, or which are interpreted as alternative options for downstream technical design. As a consequence, it will be clear which operations (or groups of) are mandatory and which are optional for downstream technical design.

### Information Service Ready

A Service Technical Design Description can obtain the compliance level “**Information Service Ready**” when the following conditions are met:

1. The operations described in the STDD are mapped to the operations required by the SDD, i.e. each operation in the SDD is mapped from an operation in the STDD fulfilling the same operational purpose. The STDD must state which interface(s) it implements and must implement all mandatory operations of the chosen interface(s) from the SDD. Evidence: A reference to the mapping or the mapping itself is provided in the Compliance Report.
2. For all the operations mapped as per IS-1, the physical message description given in the STDD shall be mapped to the logical service description in the SDD, i.e. each element in the SDD payload is put in correspondence with an element in the STDD payload having the same meaning. All the entity item attributes of the SDD payload shall be covered. Evidence: A reference to the mapping or the mapping itself is provided in the Compliance Report.
3. For all the interfaces involved in the mapping as per IS-1, the messaging exchange patterns (MEPs) stated in the STDD are matched to the MEPs required by the SDD, according to a certain ruleset found in B.1. Evidence: Text describing the mapping between MEPs and the reference to the applied rules from the SWIM foundation.

In case any of the conditions above cannot be met due to gaps or errors in the SDD then an exception must be justified and a corresponding change request must be raised towards the proper governance body.

### Information Service Compatible

A Service Technical Design Description can obtain the compliance level “**Information Service Compatible**” when the following conditions are met:

1. as defined in 6.2.1
2. as defined in 6.2.1
3. as defined in 6.2.1
4. The referenced logical service is part of the Reference Service Model. Evidence: The SDD describing the logical service provides a version of the Reference Service Model that contains this service..

In case any of the conditions above cannot be met due to gaps or errors in the SDD/ Reference Service Model then an exception must be justified and a corresponding change request must be raised towards the proper governance body.

### Information Service Compliant

A Service Technical Design Description can obtain the compliance level “**Information Service Compliant**” when the following conditions are met:

1. as defined in 6.2.1
2. as defined in 6.2.1
3. as defined in 6.2.1
4. as defined in 6.2.2
5. For all the interfaces involved in the mapping as per IS-1, all NFRs required by the SDD are mapped to either NFRs in the STDD or fulfilled by design decisions. Evidence: A reference to the mapping or the mapping itself is provided in the Compliance Report.

In case any of the conditions above cannot be met due to gaps or errors in the SDD/Reference Service Model then an exception must be justified and a corresponding change request must be raised towards the proper governance body.

# Technical Infrastructure (Profile) Compliance

## Target of Compliance

The versions of the SWIM Profiles that are applicable compliance assessment are either:

* SWIM Profiles 3.1 or later

## Compliance Levels

|  |  |  |
| --- | --- | --- |
| **Profile Binding Ready** | **Profile Binding Compatible** | **Profile Binding Compliant** |
| SWIM Profile Color and version to which STDD applies is clearly defined  A known MEP is provided in the STDD  Technologies used in the Protocol Stack for service implementation are among those found in the Interface Bindings Catalogue of the SWIM Profile used | SWIM Profile Color and version to which STDD applies is clearly defined  A known MEP is provided in the STDD  Technologies used in the Protocol Stack for service implementation are among those found in the Interface Bindings Catalogue of the SWIM Profile used  The STDD includes a complete Interface Binding that is technically compatible with one of the Interface Bindings included in the SWIM Profile used  The STDD includes a service interface definition provided in a machine-readable format using a standard service definition formalism/language | SWIM Profile Color and version to which STDD applies is clearly defined  A known MEP is provided in the STDD  Technologies used in the Protocol Stack for service implementation are among those found in the Interface Bindings Catalogue of the SWIM Profile used  The STDD includes a complete Interface Binding that is technically compatible with one of the Interface Bindings included in the SWIM Profile used  The STDD includes a service interface definition provided in a machine-readable format using a standard service definition formalism/language  The STDD includes one of the Interface Bindings available in the SWIM Profile used  Requirements associated to the chosen bindings used have been verified. |

Table 4: SWIM Compliance Levels – Overview of the TI compliance

Three levels of compliance are defined for STDD in relation to Technical Infrastructure criteria.

In particular, such levels are:

* SWIM <Color> Profile Binding Ready
* SWIM <Color> Profile Binding Compatible
* SWIM <Color> Profile Binding Compliant

<Color> “placeholder” depends from available profile names which, at the time of writing (February 2016) they are; Yellow, Blue and Purple.

A service instance consumer and/or provider who wishes to claim SWIM Compliance with the Technical Infrastructure shall be assessed according to the assessment process described in the following sections.

The mapping between the physical message description included in the STDD and the AIRM is part of the Information compliance. Therefore, this aspect is not covered by SWIM Technical Infrastructure compliance criteria.

The mapping between the STDD and the SDD is part of the Information Service Compliance. Therefore, this aspect is not covered by SWIM Technical Infrastructure compliance criteria.

A SWIM catalogue of MEPs is available on the SWIM-TI TAD for Iteration 3.1 [11]. MEPs descriptions/references included in the STDD will have to refer to those included in Annex B.1. For simpler access, the interface binding catalogue can be found in [15].

Table 5 shows which TI Compliance Level is required as a minimum for each SWIM Compliance level.

|  |  |  |
| --- | --- | --- |
| **SWIM Ready** | **SWIM Compatible** | **SWIM Compliant** |
| Profile Binding Ready | Profile Binding Compatible | Profile Binding Compliant |

Table 5: SWIM Compliance Levels - Compliance with Technical Infrastructure

### SWIM <Color> Profile Binding Ready

Pre-requisite:

1. The Service Technical Design Description has a reference to the technical specifications of the SWIM TI profiles.

The Service Technical Design Description is assessed against the technical specification of the SWIM TI profiles.

A Service Technical Design Description can obtain the compliance level “**SWIM <COLOR> Profile Binding Ready[[2]](#footnote-2)**” when all of the following conditions are met:

1. The STDD clearly indicates which is the version of the SWIM <COLOR> Profile it refers. Note: Once the <COLOR> is chosen, it applies to (and constraints) all the subsequent criteria (i.e. it is not legal to mix evidences for a same STDD mixing requirements from different Profiles). Evidence: The STDD contains the applicable SWIM <COLOR> Profile version information.
2. The messaging exchange pattern (MEP) provided in the STDD is selected from the MEPs catalogue. Evidence: The provided MEP (code) exists in the MEPs catalogue.
3. The STDD clearly indicates the technologies of the Protocol Stack used to provide the service. The technologies included in the provided Protocol Stack can be selected independently from each other from the catalogue available in the SWIM <COLOR> Profile specified in TI-1. Evidence: A complete Protocol Stack is provided in the STDD. Note: The Technologies included in the Protocol Stack provided in the STDD shall be among those already foreseen in the SWIM <COLOR> Profile Interface Catalogue Binding but the grouping of such technologies into the stack may differ among those included in the available Interface Bindings.

### SWIM <Color> Profile Binding Compatible

The Service Technical Design Description is assessed against the technical specification of the SWIM TI profiles.

Pre-requisite:

1. The Service Technical Design Description has a reference to the technical specifications of the SWIM TI profiles.

A Service Technical Design Description can obtain the compliance level “**SWIM <COLOR> Profile Binding Compatible[[3]](#footnote-3)**” when all of the following conditions are met:

1. as defined in section 7.2.1
2. as defined in section 7.2.1
3. as defined in section 7.2.1
4. The STDD provides a complete Interface Binding that is “technically compatible” with one of the Interface Bindings provided by the SWIM <Color> Profile and version defined in TI-1. Evidence: An Interface Binding that matches one of the Interface Bindings provided by the SWIM <Color> Profile defined in TI-1 is automatically compatible. If differences exist, a reference to a proof of compatibility between differing technologies is sufficient (e.g. [HTTP 1.1](https://tools.ietf.org/html/rfc7230) and [HTTP 2.0](https://tools.ietf.org/html/rfc7540); HTTP 2.0 states that it is backward compatible with HTTP1.1). If the standard/technology does not indicate such compatibility, it is concluded that the condition is not fulfilled.
5. The STDD includes a service interface definition provided in a machine-readable format using a standard service definition formalism/language. The service interface definition must be coherent with the selected binding (e.g. it is provided as a WSDL and XSD if a Web Service binding using SOAP is selected, it is provided as a WADL if a REST Web Service binding is selected…). Evidence: A reference to a document reporting this service interface definition or the service interface definition itself is provided in the Compliance Report.

### SWIM <Color> Profile Binding Compliant

The Service Technical Design Description is assessed against the technical specification of the SWIM TI profiles.

Pre-requisite:

1. The Service Technical Design Description has a reference to the technical specifications of the SWIM TI profiles.

A Service Technical Design Description can obtain the compliance level “**SWIM <COLOR> Profile Binding Compliant[[4]](#footnote-4)**” when all of the following conditions are met:

1. as defined in section 7.2.1
2. as defined in section 7.2.1
3. as defined in section 7.2.1
4. as defined in section 7.2.2
5. as defined in section 7.2.2
6. The STDD identifies an Interface Binding that is part of the catalogue of Interface Bindings of the SWIM Profile and version specified in TI-1. Evidence: The provided Binding Identifier (Requirement code) exists in the SWIM <COLOR> Profile Interface Bindings Catalogue.
7. The Service defined by the STDD can be instantiated on a SWIM Technical Infrastructure implementation that meets the specific requirements[[5]](#footnote-5) derived from TI-6 and defined in the SWIM-TI Technical Specifications (whose version must be as the one provided at TI-1). Evidence: A document, or a reference to a document, where specific coverage of the identified requirements is demonstrated.

# Information Compliance

## Target of Compliance

The versions of AIRM that are applicable for compliance assessment are:

* AIRM v4.0.1 or later, see [19] for latest version.

## Compliance Levels

The Table 6 provides a general summary of the Information compliance criteria and its use is only for introductory purposes since the AIRM Compliance Framework [9] contains detailed, i.e., a full set of, compliance requirements including the criteria needed for each level of the compliance. An AIRM Compliance Handbook [21] is available to guide the Applicant in producing the mappings required by the information compliance criteria.

|  |  |  |
| --- | --- | --- |
| **Information Ready** | **Information Compatible** | **Information Compliant** |
| A documented mapping is made available which represents a semantic correspondence between the (service) physical messages and the AIRM at Entity level. | A documented mapping is made available which represents a semantic correspondence between the (service) physical messages and the AIRM at Entity level.  A documented mapping is made available which represents a semantic correspondence between the (service) physical messages and the AIRM at Property level. | A documented mapping is made available which represents a semantic correspondence between the (service) physical messages and the AIRM at Entity level.  A documented mapping is made available which represents a semantic correspondence between the (service) physical messages and the AIRM at Property level.  A documented mapping is made available which represents a semantic correspondence between the (service) physical messages and the AIRM at Datatype level and Contraints/Business Rules are satisfied. |

Table 6: SWIM Compliance Levels – Information Compliance

### Information Ready

A Service Technical Design Description can obtain the compliance level “**Information Ready**” when the following conditions are met:

1. A documented mapping representing a semantic correspondence between the (service) physical message(s) and the AIRM is fulfilling the compliance requirements stated in the AIRM Compliance Framework [9] needed for achieving the AIRM Compliance Level 1. The evidence for the AIRM Compliance Level 1 shall fulfil the requirement that there is a documented mapping between each OuA’s Entity and a corresponding AIRM Element, at its minimum.

### Information Compatible

A Service Technical Design Description can obtain the compliance level “**Information Compatible**” when the following conditions are met:

1. As defined in 8.2.1.
2. A documented mapping representing a semantic correspondence between the (service) physical message(s) and the AIRM is fulfilling the compliance requirements[[6]](#footnote-6) stated in the AIRM Compliance Framework [9] needed for achieving the AIRM Compliance Level 2. The evidence for the AIRM Compliance Level 2 shall fulfil the requirement that there is a documented mapping between each OuA’s Entity and OuA’s Attribute on one hand and the corresponding AIRM Element on the other hand, at its minimum.

### Information Compliant

A Service Technical Design Description can obtain the compliance level “**Information Compliant**” when the following conditions are met:

1. As defined in 8.2.1.
2. As defined in 8.2.2.
3. A documented mapping representing a semantic correspondence between the (service) physical message(s) and the AIRM is fulfilling the compliance requirements[[7]](#footnote-7) stated in the AIRM Compliance Framework [9] needed for achieving the AIRM Compliance Level 3. The evidence for the AIRM Compliance Level 3 shall fulfil the requirement that there is a documented mapping between each OuA’s “Entity, Attribute, DataType and BusinessRule/Constraint” on one hand and the corresponding AIRM Element on the other hand, at its minimum.

# References

1. 08.01.01 D42 – SWIM ConOps   
   <https://extranet.sesarju.eu/WP_08/Project_08.01.01/Project%20Plan/DEL08.01.01-D42-SWIM%20conops.doc>
2. European ATM Service Description Template <https://extranet.sesarju.eu/WP_08/Project_08.03.10/Other%20Documentation/95%20active%20foundation%20documents/European%20ATM%20Service%20Description%20Template%200_2_0.docm>
3. Templates and Toolbox User Manual [https://extranet.sesarju.eu/Programme%20Library/Toolbox%20User%20Manual.doc](https://extranet.sesarju.eu/Programme%20Library/Templates%20and%20Toolbox%20User%20Manual.doc)
4. SESAR European ATM Service Identification Document template <https://extranet.sesarju.eu/Programme%20Library/SESAR%20European%20ATM%20Service%20Identification%20Document.dot>
5. SESAR Safety and Performance Requirements template <https://extranet.sesarju.eu/Programme%20Library/SESAR%20Safety%20and%20Performance%20Requirements.dot>
6. SESAR Operational Service and Environment Definition  template <https://extranet.sesarju.eu/Programme%20Library/SESAR%20Operational%20Service%20and%20Environment%20Definition.dot>
7. B.04.03-D81 SESAR Working Method on Services Edition 2013 <https://extranet.sesarju.eu/intraprogman/Assessment%20Library/D81%20-%20SESAR%20Working%20Method%20on%20Services%20Edition%202013%20-%20released.doc>
8. 08.03.10-D44 ISRM Foundation Rulebook, edition 00.07.00 <https://extranet.sesarju.eu/WP_08/Project_08.03.10/Project%20Plan/ISRM%20Foundation%2000.07.00/ISRM_Foundation_Rulebook.docx>
9. 08.01.03 AIRM Compliance Framework, Ed. 02.02.06, November 2015 <https://extranet.sesarju.eu/WP_08/Project_08.01.03/Project%20Plan/AIRM_Compliance_Framework.doc>
10. 14.01.03-D38 SWIM Profiles for Iteration 3.1, Ed 00.01.00 <https://extranet.sesarju.eu/WP_14/Project_14.01.03/Project%20Plan/P14.1.3-D38%20SWIM%20Profiles%20for%20Iteration%203.1.doc>
11. 14.01.03-D37 SWIM Architectural Definition for Iteration 3.1, Ed 00.01.00

<https://extranet.sesarju.eu/WP_14/Project_14.01.03/Project%20Plan/P14.1.3-D37-SWIM%20Architectural%20Definition%20for%20Iteration%203.1.doc>

1. 14.01.04-D43-005 SWIM-TI Blue Profile Technical Specification 3.1, Ed 00.01.00 <https://extranet.sesarju.eu/WP_14/Project_14.01.04/Project%20Plan/14.01.04.D43-005-SWIM-TI%20Blue%20Profile%20Technical%20Specification%203.1.doc>
2. 14.01.04.D43-004 SWIM-TI Yellow Profile Technical Specification 3.1, Ed 00.01.00 <https://extranet.sesarju.eu/WP_14/Project_14.01.04/Project%20Plan/14.01.04.D43-004-SWIM-TI%20Yellow%20Profile%20Technical%20Specification%203.1.doc>
3. 14.01.04.D43-006 SWIM-TI Purple Profile Technical Specification 3.1, Ed 00.01.00 <https://extranet.sesarju.eu/WP_14/Project_14.01.04/Project%20Plan/14.01.04.D43-006-SWIM-TI%20Purple%20Profile%20Technical%20Specification%203.1.doc>
4. 14.01.04.D43-SWIM Profiles Interface Bindings Catalogue, Ed. 00.01.00 <https://extranet.sesarju.eu/WP_14/Project_14.01.04/Project%20Plan/14.01.04.D43-SWIM%20Profiles%20Interface%20Bindings%20Catalogue.xls>
5. 08.01.03 AIRM Primer , Edition 00.06.00<https://extranet.sesarju.eu/WP_08/Project_08.01.03/Project%20Plan/8.1.3.D13_AIRM_Primer.doc>
6. 08.01.03 AIRM Governance Handbook , v. 00.01.02, <https://extranet.sesarju.eu/WP_08/Project_08.01.03/Project%20Plan/AIRM_Governance_Handbook.doc>
7. 08 01 01-D49-SWIM Compliance Report Template.docx <https://extranet.sesarju.eu/WP_08/Project_08.01.01/Project%20Plan/D49%20SWIM%20Compliance/08%2001%2001-D49-SWIM%20Compliance%20Report%20Template.doc>
8. 08.01.03 AIRM UML Model, Latest version, check tag “latest version” on <https://extranet.sesarju.eu/WP_08/Project_08.01.03/Project%20Plan/Forms/AllItems.aspx>
9. 08.01.03 AIRM UML Model, Old versions <https://extranet.sesarju.eu/WP_08/Project_08.01.03/Project%20Plan/Forms/AllItems.aspx?RootFolder=%2fWP%5f08%2fProject%5f08%2e01%2e03%2fProject%20Plan%2fArchived%5fDeliverables&FolderCTID=0x0120007EC74F8ECFBFEE44AED953B358AC3FC8&View=%7b7ECD364A%2dF9BA%2d4F75%2d815F%2dCC078CA44BEC%7d>
10. AIRM Compliance Handbook, Ed. 0.3, Early Draft, March 2015 <https://extranet.sesarju.eu/WP_08/Project_08.01.03/Other%20Documentation/Working_Area/Service_and_System_Support_Team/Guidance%20Documents/AIRM%20Compliance%20Handbook%200%203.doc>

1. SWIM Compliance Assessment Process
   1. Introduction

Figure 2 includes an “assessment process” icon. Obviously, defining a process that can be used by all compliance applicants is difficult. Each applicant may have a different starting point and different internal working arrangements.

This appendix defines a detailed process and roles based on the experience gathered from SESAR Release 5 V&V Exercises, a similar process can be followed outside of the scope of SESAR by redefining appropriately Governance bodies and roles.

* 1. Example assessment process
     1. Roles and responsibilities

The process makes reference to the following roles and responsibilities. As a reference, the column giving the SESAR Release 5 perspective is also included.

These roles are logical roles and some of them could be combined, e.g. the SWIM Support could overlap with the Applicant.

|  |  |  |
| --- | --- | --- |
| **Role** | **Responsibility**  **(from SWIM compliance point of view)** | **SESAR Project name/**  **Example**  **(Release 5 PoV)** |
| **SWIM Compliance Applicant** | 1. Decides if the system or service documentation or its implementation is *mature enough* for the purpose of compliance; e.g., does the service need an update to be able to satisfy maturity requirements? 2. assess maturity and request improvement of service. 3. provides documentation of the claimed compliance level 4. Asks for advice of “**SWIM Support**” 5. Is ultimately responsible for compliance of service 6. Keeps informed by “**SWIM Acceptance Team**” progress 7. has the ownership and final responsibility to check that the service or system meets the user requirements 8. Responsible for service or systems lifecycle including its maturity 9. Disseminates and gathers feedback from the team of Service/Information/Infrastructure Architects gathered in “**SWIM Support**”   Minimum **competence required**: Management about User requirements | OPS and SYS projects (WP4,WP5,WP6,WP7, WP 9, 10, 12, 13, 15) |
| **SWIM Acceptance Team[[8]](#footnote-8)** | 1. assesses the SWIM Compliance Report correctness in regards to SWIM Compliance Criteria 2. Provides the final SWIM compliance levels to the OuA 3. Require updates, clarifications to the “**SWIM Compliance Applicant**”   Minimum **competence required**:  Compliance competence | A team assigned from WP 8 and 14 |
| **SWIM Support:**  Information Architect, Service Architect,  TI (Infrastructure) Architect, | 1. Supports the all roles defined in this table 2. Collects lessons identified for each release 3. Elevates level of knowledge about compliance in different forums     Minimum **competence required**:  Compliance competence **and**  at least one of other technical competences: Service/Information/Infrastructure Architect) | A team assigned from WP 8 and 14 |

Table 7: Roles-responsibilities and Projects

* + 1. The process

**Initiation**

The compliance applicant contacts SWIM Support to start the SWIM compliance assessment process. The compliance applicant makes the object under assessment available to SWIM Support.

**Maturity Assessment**

SWIM Support gives feedback on the maturity of the object under assessment and asks for integrations and additional material in order to support the assessment process.

Based on this maturity assessment it may be decided not to continue with the full SWIM Compliance Assessment at this time.

**Compliance Assessment**

If the object under assessment is deemed to be mature, the compliance applicant, with the help of the SWIM Support, starts filling the Compliance Report Template Section 2 by listing all the general information such as the OuA versions, the versions of AIRM, Reference Service Model and TI and so on.

The compliance applicant, with the help of the SWIM Support, collects the evidence needed to ascertain all the conditions stated in Section 6-8 and fills in the corresponding sections in the Compliance Report Template accordingly. The process proceeds in two parallel threads:

* Thread 1: Collecting Information and Service Compliance Evidence. This is a stepwise activity to be done in the following order:
  + step 1: Information Service Compliance.
    - The compliance applicant, supported by SWIM Support, builds all the mapping evidence between OuA and SDD/Reference Servide Model as required to meet conditions IS-1 to IS-5 explained in Section 6.
    - The compliance applicant documents all the evidence in the Compliance Report Template sections 3.3.1 ad 3.3.2.
    - Finally, based on the available evidence, the Applicant decides to apply for an Information Service Compliance Level according to the criteria explained in Section 6, and records his decision as “claimed” Assessment Result in Template section 3.3.3.
  + step 2: Information Compliance
    - Depending on the targeted level of compliance the compliance applicant, supported by SWIM Support, provides the mapping evidence between the OuA and the targeted version of AIRM as required by conditions IN-XX explained in Section 8. In particular:
      * If the payload is based on a standardised information exchange model for which a compliance report is published, the Applicant just provides a link to it and fills in the Compliance Report Template section 3.4.2.
      * If the payload is not based on a standard model then the Applicant uses as input the evidence already provided in IS-2 (payload mapping between STDD and SDD) and the AIRM tracing already present in the SDD, in order to derive the mapping to AIRM. In case the input is not correct or it does not satisfy AIRM Compliance Framework, the Applicant performs AIRM mapping anyway and notes down issues for consideration in the post-conditions check.
    - The Applicant documents all the evidence in the Compliance Report Template section 3.4.
    - Finally, based on the evidence, the Applicant decides an Information Compliance Level according to the criteria explained in Section 8, and records his decision as “claimed” Assessment Result in Template section 3.4.5.
* Thread 2: Collecting TI Compliance Evidence
  + The Applicant, supported by SWIM Support, builds all the evidence between as required to meet conditions TI-1 ... TI-7 explained in Section 7.
  + The Applicant documents all the evidence in the Compliance Report Template section 3.5.
  + Finally, based on the evidence, the Applicant decides the TI Compliance Level according to the criteria explained in Section 7, and records his decision as “claimed” Assessment Result in Template section 3.5.

**Finishing Off**

After having checked all criteria, having documented all related evidence and having made a statement on the “claimed” level of compliance for the three compliance domains, the Applicant must check all post-conditions (see section below)[[9]](#footnote-9):

* Post-Condition on payload compliance.
  + The Applicant shall document in the Compliance Report section 3.6.1 how to compare the available evidences for payload mappings collected in information and information service compliance.
  + In case the check fails because of an error in the SDD-AIRM tracing, the Applicant raises a CR to the SDD via the Service Foundation and writes the CR codename in the Compliance Report section 3.6.1.

In any case, if the Applicant finds problems hindering compliance assessment in any of the three domains, and if these problems are related to gaps or errors in AIRM, Information Service or TI. The Applicant should report this in the respective section of the Compliance Report and raise a change proposal to the proper governance body (e.g. AIRM CCB, Service Foundation CCB, TI CCB[[10]](#footnote-10)).

**Delivering the SWIM Compliance Assessment Report**

The Applicant delivers the Compliance Report filled in with all the information above to the SWIM Acceptance Team.

**Acceptance by the SWIM Acceptance Team**

The SWIM Acceptance Team assesses the Compliance Report correctness and completeness eventually requiring updates or clarifications to the Applicant.

The SWIM Acceptance Team provides a final Compliance Level for the three domains and documents them in tables in sections 3.3, 3.4 and 3.5 of the Compliance Report, by confirming or amending the level previously claimed by the Applicant. When the judgement differs, the SWIM Acceptance Team also may also indicate in the "remarks" field the reason of the discrepancy and make proposals to the Applicant on how to fill in the gaps in order to obtain the claimed compliance level.

The SWIM Acceptance Team finally confirms the overall SWIM Compliance Level in Section 2 of the Compliance Report according to the criterion stated in Section 3.

The SWIM Acceptance Team delivers the Compliance Report.

* 1. Example of post-condition checks as part of SWIM Compliance

It is assumed that the post condition check happens after the evidences of compliance for the three domains are completed. This section describes different kinds of post conditions that need to be met in order to reach a certain SWIM compliance level.

* + 1. Post-condition on payload compliance

Compliance criteria described in sections 6 and 8 require that the OuA payload has documented mappings to the SDD and to the AIRM respectively. However there is no guarantee that these two mappings are coherent with each other, therefore a subsequent level of checks needs to be done.

The various mappings on A.2.2 have different meanings, they serve different purposes[[11]](#footnote-11) and they are built by different people at different time. But in order to fulfil SWIM compliance, the different mapping paths for a same STDD attribute must be coherent and cannot contradict each other. In Figure 6 two problematic cases are shown in order to describe the problems which may occur and which must be avoided. An explanation is added for each of them.

|  |  |
| --- | --- |
| **Case A: semantic ambiguity** | **Case B: scope ambiguity** |
|  |  |
| The same STDD attribute has two possible semantics in terms of AIRM, depending on the traversed mapping path. | The same STDD attribute is in- or out-of-AIRM scope depending on the traversed mapping path. |

Figure 6 – Situations to avoid for obtaining SWIM Compliance.

Therefore for any level of SWIM Compliance the following post-condition must be met:

**Payload Compliance post-condition:** *for each and any STDD payload attribute, the target AIRM element(s) determined via its AIRM Compliance assessment and the target AIRM element(s) determined indirectly via SDD mappings must coincide. Evidence must be provided to prove this in the Compliance Assessment Report. The same evidences provided for compliance assessment in the AIRM and Information Service domains shall be reused for that purpose. Any exception must be documented in the Report and duly justified. It is up to the SWIM Acceptance Team to decide if this has an impact on the overall SWIM assessment outcome.*

1. Compliance with Information Services: Additional information

Some information needed for the Information Service Compliance is for the time being provided here.

* 1. MEP mapping table

For the compliance check of the messaging exchange patterns (MEPs) stated in the STDD the following table is used to match these MEPs to the MEPs required by the SDD.

Deviations are possible but should be thoroughly justified and documented in the STDD.

This justification will be assessed by the compliance assessor.

|  |  |
| --- | --- |
| **Information Service MEP in SDD** | **SWIM-TI MEP in STDD** |
| Synchronous request/reply | Synchronous Request/Reply |
| Asynchronous request/reply | Asynchronous Request/Reply |
| Fully Decoupled Request/Reply |
| Publish/Subscribe Push | Observer Push |
| Publish/Subscribe Push |
| Publish/Subscribe Pull | Observer Pull |
| Publish/Subscribe Pull |
| One way asynchronous request/reply | Asynchronous Fire & Forget |

END OF DOCUMENT-

1. In the context of SESAR R5 V&V the Service Foundation role was performed by ISRM CCB. [↑](#footnote-ref-1)
2. *<COLOR> text will have to be substituted by existing SWIM Profile Codes (i.e. Yellow, Blue, Purple).* [↑](#footnote-ref-2)
3. *<COLOR> text will have to be substituted by existing SWIM Profile Codes (i.e. Yellow, Blue, Purple).* [↑](#footnote-ref-3)
4. *<COLOR> text will have to be substituted by existing SWIM Profile Codes (i.e. Yellow, Blue, Purple).* [↑](#footnote-ref-4)
5. *TI-6 targets Interface Bindings. The Interface Binding, in turn, implies a number of SWIM TI requirements. Such requirement traceability is provided in SWIM TI Technical Specifications.* [↑](#footnote-ref-5)
6. It should be noted that the satisfaction of IN-2 implies the satisfaction of IN-1 by definition. [↑](#footnote-ref-6)
7. It should be noted note that the satisfaction of IN-3 implies the satisfaction of IN-2 and hence also IN-1 by definition. [↑](#footnote-ref-7)
8. *Note that a same person cannot in a given service compliance context play both Role of Applicant and Acceptance Responsible.*  [↑](#footnote-ref-8)
9. *Currently (April 2015) only one post-condition on payload mapping is required to be checked.* [↑](#footnote-ref-9)
10. *In the context of SESAR Release 5 the role of TI CCB was played by projects P14.1.3 and P14.1.4.* [↑](#footnote-ref-10)
11. *The STDD-AIRM and the SDD-AIRM data mappings are “semantic” mappings done according to, and obeying the AIRM Compliance Framework. The STDD-SDD mapping instead, is an “operational” mapping, namely SDD is based on operational requirements about the payload content that the STDD must fulfil. Nevertheless, this “operational” mapping also implies a “semantic” mapping, in the sense that the target attribute in the SDD must have the same operational meaning of the source attribute, otherwise the operational compliance itself would not be satisfied. Therefore the STDD-SDD tracing can be understood as an “inherited” semantic mapping as well.* [↑](#footnote-ref-11)