



PYRAMID Exploiter's Pack Version 4.1

Annex C – Compliance Guide Issue 4.1



Ministry
of Defence

This document has been prepared, as part of the PYRAMID Exploiter's Pack, in order to set out a generic approach to implementation of the PYRAMID Architecture. The PYRAMID Reference Architecture has not been created for any specific system. It is the user's responsibility to ensure that any article created using this document meets any required operational, functional and safety needs. The Author accepts no liabilities for any damages arising due to a failure of the user to verify the safety of any product produced using this document, nor for any damages caused by the user failing to meet any technical specification.

For further information regarding how you can exploit PYRAMID on your project, provide feedback following your review of the PYRAMID Exploiter's Pack V4.1, or have a technical query that you would like answering, please contact the PYRAMID Team using the following email address. PYRAMID@mod.gov.uk

OGL

© Crown owned copyright 2023.

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London, TW9 4DU, or email: psi@nationalarchives.gov.uk

Where we have identified any third party copyright information you will need to obtain permission from the copyright holder concerned.

This publication is available at <https://www.gov.uk/government/publications/pyramid/pyramid-programme>

EXECUTIVE SUMMARY

The MOD's PYRAMID programme introduces a change to the current method of avionic systems design and procurement, aiming to make the next generation of air systems affordable, capable and adaptable by the adoption of an open architecture approach and systematic software reuse.

This document forms part of the PYRAMID Exploiter's Pack and outlines the requirements for compliance by which any component or deployment derived from the PYRAMID Reference Architecture (PRA) should be assessed. PYRAMID compliance confirms that a deployment, or the components within it, meet the rules associated with adopting the PYRAMID approach.

This document provides the definition of component compliance. Component compliance is defined by adherence to the PRA component subject matter. Additionally it provides a template for declaration of component compliance in accordance with the proposed definitions.

This document also provides the definition of deployment compliance. Deployment compliance is defined by adherence to component compliance and compliance of associated component connections (including extension component connections). Additionally it provides a template for declaration of deployment compliance in accordance with the proposed definitions.

The provision of compliance information, and the attained compliance, is intended to support an Exploiting Programme and the wider PYRAMID programme achieving the Single Statement of User Need (SSUN).

CHANGE HISTORY

Date	Issue	Description of Changes
November 2019	1	First Issue
January 2020	1.1	Update from customer review comments
December 2020	2	<p>The PYRAMID Compliance Guide has become an annex to the PYRAMID Exploiter's Pack Ref [1] and so some content of the document has been changed to reflect this.</p> <p>This document has also been updated to align with the new compliance strategy.</p> <p>In addition changes have been made to this document resulting from query answering from both internal and external stakeholders and general maturity improvements.</p>
December 2021	3	<p>The PYRAMID Compliance Guide has been updated to align with the new compliance strategy. This includes:</p> <p>Updates to component compliance to align with Issue 3 of the PYRAMID Exploiter's Pack Ref. [1].</p> <p>The addition of deployment compliance.</p>
October 2022	3.1	<p>Issue 3.1 is a UK OFFICIAL version of Issue 3. No changes to the content of the document have been made other than non-technical changes due to the up-issue of the PYRAMID Exploiter's Pack from Version 3 to Version 3.1 (headers/footers, references etc.).</p>
December 2022	4	<p>The PYRAMID Compliance Guide has been updated to align with updates to Issue 4 of the PYRAMID Exploiter's Pack Ref. [1].</p> <p>The structure of the guide has been updated for readability.</p> <p>Due to feedback received from the CESTIUS Lessons Learnt report, both the Component and Deployment Compliance Statement Templates have been updated.</p> <p>The rules for compliance for both components and deployments have been changed to align with a new paradigm for assessing compliance.</p> <p>In addition, the following new sections have been added to the guide:</p> <ul style="list-style-type: none"> • 2.1 Compliance Goal • 3.2.1 Implemented Provided and Consumed Services • 4.2.1 PYRAMID Scope • 4.2.3 Different PRA Baselines

Date	Issue	Description of Changes
September 2023	4.1	The document has been updated due to now being released via Open Government License v3.

List of Effective Pages

26 pages UK OFFICIAL

26 pages in total

TABLE OF CONTENTS

EXECUTIVE SUMMARY	2
CHANGE HISTORY.....	3
TABLE OF CONTENTS.....	5
TABLE OF FIGURES	6
TERMS AND ABBREVIATIONS USED IN THIS DOCUMENT	7
REFERENCES	8
1 Introduction.....	9
1.1 Scope	9
1.2 Purpose.....	9
1.3 Document Structure	9
1.3.1 PYRAMID Compliance Context.....	9
1.3.2 Component Compliance.....	9
1.3.3 Deployment Compliance.....	10
1.3.4 Component Compliance Statements	10
1.3.5 Deployment Compliance Statements	10
2 PYRAMID Compliance Context	11
2.1 Compliance Goal.....	11
2.2 The Importance of Compliance Declaration	11
2.3 Compliance Guide Use of PRA Lexicon	11
2.4 Compliance Guide Update Roadmap.....	12
2.5 Deployment Programme Lifecycle.....	12
3 Component Compliance	14
3.1 PYRAMID Component Compliance Rule	14
3.2 PYRAMID Component Compliance Supporting Information	14
3.2.1 Implemented Provided and Consumed Services	14
3.2.2 PRA Component’s Subject Matter	14
3.2.3 PYRAMID Compliant Implementations Example.....	16
3.2.4 Extension Components	16
3.3 PYRAMID Non-Compliant Component	16
4 Deployment Compliance	17
4.1 PYRAMID Deployment Compliance Rules.....	17

4.2	PYRAMID Deployment Compliance Supporting Information	17
4.2.1	PYRAMID Scope.....	17
4.2.2	Component Connections.....	18
4.2.3	Different PRA Baselines.....	18
4.3	PYRAMID Non-Compliant Deployment	19
5	Component Compliance Statements.....	20
5.1	Component Compliance Summary	20
5.2	Component Services Declaration	20
5.3	Example Component Compliance Statement Template.....	21
6	Deployment Compliance Statements.....	23
6.1	Deployment Compliance Summary	23
6.2	Deployment Components and Connections Declaration	23
6.3	Example Deployment Compliance Statement Template.....	24

TABLE OF FIGURES

Figure 1: Component Compliance.....	14
Figure 2: Deployment Compliance.....	17
Figure 3: Example PYRAMID Scope	18

TERMS AND ABBREVIATIONS USED IN THIS DOCUMENT

Definitions of project terms, the meaning of acronyms and the meaning of abbreviations used in this document can be found in the PYRAMID Glossary Ref [5].

REFERENCES

The reference numbers are consistent across all the documents in the PYRAMID Exploiter's Pack. This means that in this document, when a reference is not used, the corresponding reference number will not appear in the reference list.

Project Related Document References:

For the avoidance of doubt, all documents referenced below which form part of the PYRAMID Exploiter's Pack are subject to the terms of DEFCON 703.

Reference Title, Document Number, Issue & Date

- | | |
|-----|---|
| [1] | PYRAMID Exploiter's Pack (Main Document), RCO_FUT_23_004, Issue 4.1, September 2023. |
| [5] | PYRAMID Exploiter's Pack Annex D: Glossary, RCO_FUT_23_008, Issue 12.1, September 2023. |
| [6] | PYRAMID Reference Architecture Model, RCO_SYS_0025, Version 4.0.0, December 2022. |

1 Introduction

The MOD's PYRAMID programme introduces a paradigm shift to the current method of avionic systems design and procurement, aiming to make the next generation of air systems affordable, capable and adaptable by the adoption of an open architecture approach and systematic software reuse.

The PYRAMID Exploiter's Pack defines this Reference Architecture in the form of a set of coherent, reusable and well-bounded functional components, along with architectural, specific and support policies and exemplar component interaction views.

In order to show that the PYRAMID approach has been adhered to, compliance rules have been defined for components and deployments. This guide aims to present an unambiguous definition of compliance and how it is assessed. Where this guide discusses compliance, it is always referring to PYRAMID compliance.

Although this guide provides direction on how to declare compliance, the process for claiming compliance is out of scope of the PYRAMID Exploiter's Pack.

The potential future changes to PYRAMID compliance are included, in order to minimise their impact on users of this guide.

1.1 Scope

The PYRAMID Compliance Guide explains what compliance is and outlines the requirements for compliance by which any component or deployment derived from the PRA should be assessed.

1.2 Purpose

This document explains how an Exploiting Programme can assess, in order to declare, PYRAMID compliance.

1.3 Document Structure

This document has the following sections:

1.3.1 PYRAMID Compliance Context

This section provides an overview of PYRAMID compliance.

This includes an explanation of the PYRAMID compliance goal, importance of compliance declaration, use of PRA lexicon within the Compliance Guide, roadmap for compliance, and how compliance fits within the lifecycle of a development programme.

1.3.2 Component Compliance

This section details the rule for assessing compliance of components, and the definition of the component compliance attainable. This section also provides supporting information for this rule.

1.3.3 Deployment Compliance

This section details the rules for assessing compliance of a deployment and the definition of the deployment compliance attainable. This section also provides supporting information for these rules.

1.3.4 Component Compliance Statements

This section details the information that is expected in a component compliance statement. This section also contains a component compliance statement template.

1.3.5 Deployment Compliance Statements

This section details the information that is expected in a deployment compliance statement. This section also contains a deployment compliance statement template.

2 PYRAMID Compliance Context

This section provides context for PYRAMID compliance, including its goal and how this fits into the lifecycles of Exploiting Programmes.

2.1 Compliance Goal

The goal of PYRAMID compliance is to help ensure that an Exploiting Programme realises the benefits provided by the PRA in order to support the strategic imperatives outlined in the PYRAMID Single Statement of User Need (SSUN). In particular, compliance seeks to preserve the separation of concerns, a concept that has been adopted by PYRAMID to enhance the rapid upgradability of future platforms. Therefore, PYRAMID compliance is based on the absence of subject matter pollution. Each PRA component represents a discrete area of subject matter. Consequently, subject matter pollution occurs when a PYRAMID component includes any subject matter of a PRA component that it is not based on. A PYRAMID compliant deployment should have no subject matter pollution.

2.2 The Importance of Compliance Declaration

In providing compliance information (on a compliance declaration), an Exploiting Programme communicates in a consistent manner:

- An understanding of whether a specific component's services align with the PRA definition.
- That the deployment has been achieved in a PYRAMID compliant way.

The provision of compliance information, and the attained compliance, is intended to support an Exploiting Programme seeking to re-use a deployment or component.

Compliance declaration is intended to provide a consistent way to document information that will help to:

- Support the ease of integration of components and deployments.
- Improve the ability to re-use components between differing deployments.
- Improve the ability to efficiently insert and update capability of a deployment rapidly and with reduced risk.

In order to generate an argument to support that a deployment, or the components within it, has been developed with the PYRAMID approach, it is essential for exploiters to be able to declare compliance against the PRA definition.

2.3 Compliance Guide Use of PRA Lexicon

The common language provided by the PRA can be used in compliance declarations to make it easier for Exploiting Programmes to compare existing components against their requirements. Compliance can be assessed against the PRA at any phase of an Exploiting Programme's implementation lifecycle, whether that be at the design concept stage, software specification, executable software, or a set of deployed components. The compliance assessment defined in this guide can be applied to any use of the PRA, for example, for an air platform mission system or a mission planning system.

The PRA has been designed around a service modelling approach to system development and a similar approach to development of PYRAMID compliant software is recommended. For ease of reading, this Compliance Guide has been written based on the assumption that a service modelling approach will be adopted by PYRAMID exploiters. Should an exploiter wish to adopt an alternative approach the principles outlined in this guide would still apply with references to 'services' replaced by the appropriate artefact for the approach taken.

Within this document 'component' refers to a component which has been developed from the PRA, where reference is being made to a component definition from the PRA the term 'PRA component' is used.

2.4 Compliance Guide Update Roadmap

As a part of the PYRAMID Exploiter's Pack, this guide will be subject to updates. This document will be updated in accordance with each release of the PRA. A compliance declaration should be against a specified issue of the PRA.

Future updates will consider the inclusion of:

- Enhancements based on feedback from industry and the application to their Exploiting Programmes.
- Compliance to policies.
 - Although the PRA policies are considered optional, as they should only be applied if appropriate for the needs of the component or deployment design, it can be seen that a clear understanding of the use of the policies may support the goals of compliance (e.g. the application of the Data Driving policy in support of the enablement of rapid capability insertion).
 - While it is accepted that the use of policies by a component or deployment will impact some of the objectives of using PYRAMID, it is not currently mandated. While not assessed in this issue of the guide, it is strongly suggested that all policies should be considered for appropriateness in any component or deployment design.

It is intended that compliance in future issues will build upon the rules detailed in this issue, thereby maintaining clear backwards compatibility between issues.

2.5 Deployment Programme Lifecycle

Development of a component can be considered within the process of a specific programme or system development. An Exploiting Programme should declare its compliance at its key programme milestones.

Showing how a component is compliant at differing stages of its lifecycle supports its design reviews being conducted at appropriate programme maturity reviews, ensuring the programme's progress is consistent with achievement of PYRAMID compliance.

Therefore, it is probable that compliance reviews would be held alongside an Exploiting Platform's design reviews.

Component compliance may be stated for a component at any stage of development. For example, compliance may be declared for platform independent component design, platform specific component design, or a delivered single component product.

Deployment compliance may be stated for a deployment at any stage of development. For example, compliance may be declared for platform specific deployment design, or a delivered deployment.

It is recommended that compliance of component connections (including extension component connections), within the deployment, should be assessed at the design concept stage, i.e. early in the deployment lifecycle. This is because it is likely to be difficult to assess compliance of the software providing the component connections at later stages of the lifecycle.

3 Component Compliance

This section defines the rule and supporting information that are to be used to determine if a component is compliant with the PRA definition.

How the compliance should be declared is defined in section [5 - Component Compliance Statements](#).

3.1 PYRAMID Component Compliance Rule

A component can be declared as either compliant or non-compliant.

Developed components are assessed for compliance against the PRA definition. [Figure 1: Component Compliance](#) shows how compliance with the PRA definition affects the component's compliance attainment.

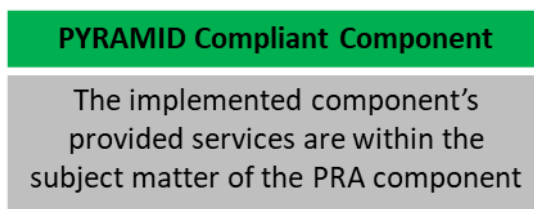


Figure 1: Component Compliance

3.2 PYRAMID Component Compliance Supporting Information

3.2.1 Implemented Provided and Consumed Services

In order to declare a component PYRAMID compliant, only the implemented provided services must be assessed against the component compliance rule. However, it is likely that in a future version of this guide (as the consumed services defined in the PRA become more mature), PYRAMID component compliance will consider both the provided and consumed services of the component.

Therefore, it is recommended that any compliance assessment also considers the consumed services. The purpose for which the component is consuming the service should be within the subject matter of the consuming component.

3.2.2 PRA Component's Subject Matter

Component compliance is assessed against the PRA component's subject matter. Each PRA component represents a discrete area of subject matter. Subject matter pollution occurs when a PYRAMID component includes any subject matter of a PRA component that it is not based on. More information on subject matter can be found in the PYRAMID Reference Architecture Model Ref [6] section:

Architecture > Domains > Introduction > Introduction Text

The definition of a PRA component defines its subject matter. Therefore, the different artefacts of the component are different views of its subject matter, e.g. responsibilities, subject matter semantics, services, etc. Each PRA component's definition can be found in the PYRAMID Reference Architecture Model Ref [6] section:

Architecture > Domains > Component Set > [component_name]

To understand a component's subject matter, the key parts of the component definition are the subject matter semantics and the services. The semantics give an overall view of information and the concepts the component reasons about, whereas the services give a more detailed view of the behaviour exhibited by the component and the information at the component interfaces. For compliance assessment, it is recommended that an exploiter understands both of these artefacts as this should enable understanding of the PRA component's subject matter.

3.2.2.1 PRA Component's Subject Matter Semantics

Each component includes a definition of its subject matter semantics, specified in the PYRAMID Reference Architecture Model Ref [6] section:

Architecture > Domains > Component Set > [component_name] > Subject Matter Semantics

The component's subject matter semantics defines the scope of the component by showing its entities (artefacts that model concepts that may or may not exist in the real-world). This section also includes a semantics diagram, showing the relationships between these entities.

3.2.2.2 PRA Component's Services

The PRA component's services give detailed information on component behaviour and an abstract view of the data needed to achieve it. The behaviour exhibited by a PRA component is defined by its provided services. What the component depends on (from another component) to achieve this behaviour is defined by its consumed services.

Services are formed of interfaces and activities. Information on services and service elements can be found in the PYRAMID Reference Architecture Model Ref [6] section:

Architecture > Domains > Introduction > Introduction Text > Services

A PRA component's services are specified in the PYRAMID Reference Architecture Model Ref [6] section:

Architecture > Domains > Component Set > [component_name] > Services > Service Definitions

where [component_name] refers to the name of the component under analysis.

Not all of a PRA component's services will be required for all developed components.

Attributes on service interfaces and service interfaces themselves are expected to be made specific to a developed component. For more detail, see the PYRAMID Reference Architecture Model Ref [6] section:

Architecture > Domains > Introduction > Introduction Text > Services > Service Diagrams > Interfaces

3.2.3 PYRAMID Compliant Implementations Example

A component can have various implementations, all of which may be compliant. The implementation will be dependent on the requirements of the deployment.

For example, the Jettison component may be implemented in two different deployments that both require the Jettison component's Requirement service.

In the first deployment, the Requirement service requires three service interfaces: Requirement, Criterion and Jettison_Achievement.

In the second deployment, the Requirement service only requires two interfaces: Requirement and Jettison_Achievement. The Criterion service interface has not been included in the second deployment as it is not a requirement of this deployment to assess the quality of a jettison solution.

For any given developed component service derived from the PRA, not all of a PRA component's service interfaces are required. Therefore, both of the examples can be compliant as long as they adhere to the component compliance rule outlined in section [3.1 - PYRAMID Component Compliance Rule](#).

3.2.4 Extension Components

As stated in the PRA, any component based design can use extensions. More detail on component extensions can be found in the PYRAMID Reference Architecture Model Ref [6] section:

Architecture > Architectural Policies > Modelling Principles > Component Extensions

An extension component is a component that fulfils the needs of an extension point. It is still a component like any other in a deployment. However, an extension component's subject matter should only be a subset of the PRA component that its parent component is based on.

3.3 PYRAMID Non-Compliant Component

If any of the component's provided services do not pass the rule defined in section [3.1 - PYRAMID Component Compliance Rule](#), the component will be non-compliant.

4 Deployment Compliance

This section defines the rules and supporting information that are to be used to determine if a deployment is compliant with the PRA definition.

How the compliance should be declared is defined in section [6 - Deployment Compliance Statements](#).

4.1 PYRAMID Deployment Compliance Rules

A deployment can be declared as either compliant or non-compliant.

Deployments are assessed for compliance against the PRA definition. [Figure 2: Deployment Compliance](#) shows how compliance with the PRA definition affects the deployment's compliance attainment.

PYRAMID Compliant Deployment
All of the components within the deployment are compliant, as determined by the PYRAMID component compliance rule.
All of the component connections within the deployment do not contain subject matter* defined within the scope of a PRA component.
Where extension components exist within the deployment, only the parent components have access to the provided services of their extension component(s). An extension component can consume services from elsewhere as long as they are compatible with the parent's services.

Figure 2: Deployment Compliance

*The component connections within the deployment should not contain any subject matter defined within the scope of a PRA component, beyond that required for data translation to bridge the semantic gap between the components. Therefore, a PYRAMID compliant component connection does not contain any behaviour defined within a PRA component's subject matter.

4.2 PYRAMID Deployment Compliance Supporting Information

4.2.1 PYRAMID Scope

The scope of a deployment for which compliance will be assessed belongs to the Exploiting Programme. However, as the PRA is only concerned with application software, it is highly likely that a deployment is never going to be exclusively derived from PYRAMID. Only the parts aligned to the PRA can be PYRAMID compliant. This section of the deployment is called the PYRAMID scope. [Figure 3: Example PYRAMID Scope](#) shows the PYRAMID scope section of an example deployment. As shown in the diagram, the PYRAMID scope includes PYRAMID components and the component connections between these components. Exploiters should identify the PYRAMID scope section of their deployment early on in the deployment lifecycle.

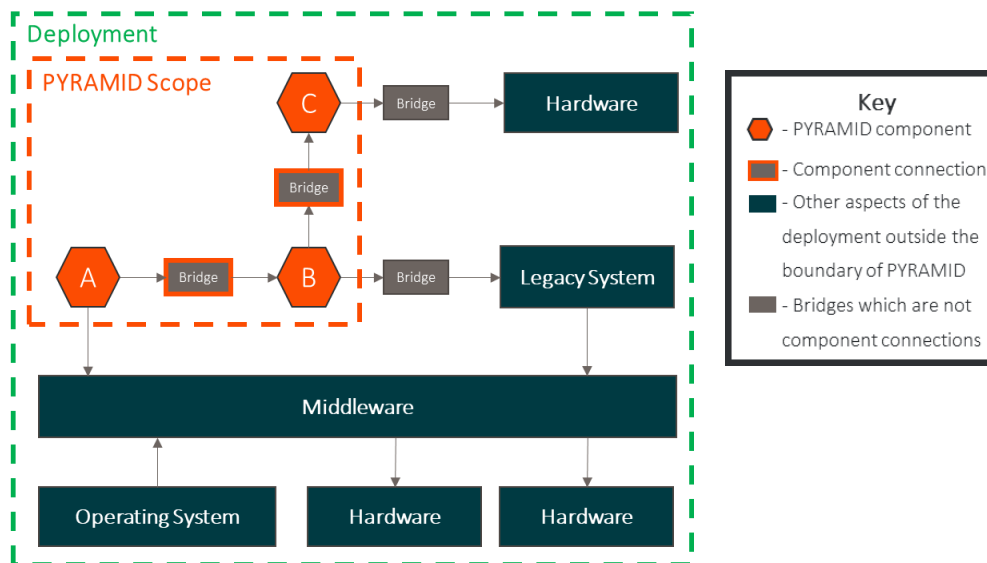


Figure 3: Example PYRAMID Scope

4.2.2 Component Connections

Component connections allow components to work together within a deployment. This includes mapping and translating between component services. More detail on component connections can be found in the PYRAMID Reference Architecture Model Ref [6] section:

Architecture > Architectural Policies > Modelling Principles > Component Connections

The design and implementation of component connections should be appropriate to the specific needs of the deployment.

4.2.2.1 Extension Component Connections

Extension components are integrated into the system through the use of component connections (including any interactions with their parent component).

More detail on extension component connections can be found in the PYRAMID Reference Architecture Model Ref [6] section:

Architecture > Architectural Policies > Modelling Principles > Component Extensions > Rules for Extensions

4.2.3 Different PRA Baselines

All implemented components and component connections within the deployment must each be compliant to a version of the PRA (from v3 onwards).

While a deployment which uses components and component connections which align to different PRA baseline versions may still be compliant, it is recommended that exploiters attempt to use the same baseline wherever possible, to minimise the small risk of pollution due to changes in component scopes between issues.

Where a deployment does contain components or component connections which are compliant to different PRA baselines, it is advised that analysis is carried out to determine if there is subject matter pollution within the deployment. This can be declared in the Deployment Compliance Statement, see section [6.3 - Example Deployment Compliance Statement Template](#). Although this is not required to attain PYRAMID compliance, it will be useful to support the PYRAMID compliance goal being achieved, e.g. ease of upgrade.

4.3 PYRAMID Non-Compliant Deployment

If a deployment does meet all of the rules defined in section [4.1 - PYRAMID Deployment Compliance Rules](#), the deployment will be non-compliant.

5 Component Compliance Statements

This section details what is expected of a statement of component compliance, such that it can be used to appraise a specific component against the PRA definition using the PYRAMID component compliance rule. It specifies how compliance should be declared.

A component compliance statement supports the understanding of the implemented component's compliance against the definition of the PRA component.

The component compliance statement will contain the following at this version:

- Component compliance summary.
- Component services declaration.

The component compliance statement is constructed of sections for each of the required details. These sections are defined in the following subsections. A component compliance statement template is provided in section [5.3 - Example Component Compliance Statement Template](#).

5.1 Component Compliance Summary

A component compliance summary provides an overview of the component and should include the following:

- Reference to the version of the PYRAMID Exploiter's Pack used.
- The attained compliance for the component in line with section [3.1 - PYRAMID Component Compliance Rule](#).
- Details of the component under analysis, including but not limited to its name, role and interfaces (e.g. services).
- Details of the component specific to the developer organisation, e.g. technical authority, unique component reference, and component version.

5.2 Component Services Declaration

The component service declaration lists the services provided by the component and the PRA services that have been excluded from implementation. It also supports the provision of a rationale as evidence to support compliance (see section [5.3 - Example Component Compliance Statement Template](#)).

5.3 Example Component Compliance Statement Template

This following Component Compliance Statement template is provided to support component compliance declarations.

Component Compliance Summary

Developer's Component Reference: (Unique Component Reference)	Component Developer: (Company Name or Programme)
Component Development Stage: (e.g. Component Specification, Component Design, Software Design, Deployable Component, etc.)	
Component Version:	
Statement Security Classification: (e.g. Official, Official Sensitive, etc.)	
Number of Sheets In Statement:	
PYRAMID Exploiter's Pack Issue No:	
Component Name: (e.g. Jettison)	
Compliance Attainment: (Compliant / Non-Compliant)	
Role (e.g. The role of Jettison is to coordinate the jettison of physical items from the platform.)	

Component Service Declaration

Implemented Services		PRA Services Not Implemented	
Services Name & Details	Compliance Attainment Rationale	PRA Service Name & Details	Rationale
<i>e.g. Package Jettison - This service identifies jettison activities involving the Jettison Package, consumes the declared achievability, and identifies any changes to these activities.</i>	<i>e.g. The implemented service is within the subject matter of the PRA Jettison component and is therefore PYRAMID compliant.</i>	<i>e.g. Location – This service identifies activities related to the required vehicle location to support jettison, consumes the declared achievability, and identifies any changes to these activities.</i>	<i>e.g. Jettison will be manual and any allowable locations will be operator dependent.</i>
<i>etc.</i>			

6 Deployment Compliance Statements

This section details what is expected of a statement of deployment compliance, such that it can be used to appraise a specific deployment against the PRA definition using the PYRAMID deployment compliance rules. It specifies how compliance should be declared.

A deployment compliance statement supports the understanding of the deployment's compliance against the definition of the PRA.

The deployment compliance statement will contain the following at this version:

- Deployment compliance summary.
- Deployment components and connections declaration.

The deployment compliance statement is constructed of sections for each of the required details. These sections are defined in the following subsections. A deployment compliance statement template is provided in section [6.3 - Example Deployment Compliance Statement Template](#).

6.1 Deployment Compliance Summary

A deployment compliance summary provides an overview of the deployment and should include the following:

- Reference to the version(s) of the PYRAMID Exploiter's Pack used.
- The attained compliance for the deployment in line with section [4.1 – PYRAMID Deployment Compliance Rules](#).
- Details of the deployment specific to the developer organisation, e.g. technical authority, unique deployment reference, and deployment version.

6.2 Deployment Components and Connections Declaration

The deployment components and connections declaration provides information about the components and connections within the deployment (see section [6.3 - Example Deployment Compliance Statement Template](#)).

6.3 Example Deployment Compliance Statement Template

This following Deployment Compliance Statement template is provided to support deployment compliance declarations.

Deployment Compliance Summary

Developer's Deployment Reference: <i>Unique Deployment Reference</i>	Deployment Developer: <i>Company Name or Programme</i>
Deployment Development Stage: <i>e.g. Deployment Specification, Deployment Design, Software Design, Delivered Unit, etc.</i>	
Deployment Version:	
Statement Security Classification: <i>e.g. Official, Official Sensitive, etc.</i>	
Number of Sheets In Statement:	
PYRAMID Exploiter's Pack Issue(s) used: <i>e.g. Issue 3 and Issue 4</i>	
Compliance Attainment: <i>Compliant/Non-Compliant</i>	
Compliance Attainment Rationale: <i>e.g. The deployment includes several components which are PYRAMID compliant to Issue 4 of the PYRAMID Exploiter's Pack and one component that is PYRAMID compliant to Issue 3. All of the component connections within the deployment are PYRAMID compliant to Issue 4 of the PYRAMID Exploiter's Pack. Therefore, the deployment is PYRAMID compliant.</i> <i>Additional analysis has been carried out to determine if there is subject matter pollution within the deployment due to the use of components from multiple PRA baselines. As there has been a change in the subject matter of Release Aiming between Issue 3 and 4 of the PYRAMID Exploiter's Pack, the implemented Release Aiming component is polluted with another PRA component's subject matter at Issue 4. However, this does not affect the compliance attainment.</i>	

Deployment Components and Connections Declaration

Components		
Component Name	Component Compliance Attainment and PYRAMID Exploiter's Pack Issue No.	Subject Matter Pollution Details
<i>e.g. Release Aiming</i>	<i>e.g. PYRAMID Compliant to Issue 3</i>	<i>e.g. The implemented Release Aiming component contains an In_Store_Progress_Prediction service. This service conveys subject matter that at Issue 4 is in the subject matter of the Trajectory Prediction component. However, this functionality is not being used within this deployment.</i>
<i>e.g. Path Demands</i>	<i>e.g. PYRAMID Compliant to Issue 4</i>	<i>e.g. No subject matter pollution</i>
<i>etc.</i>		

Component Connections			
Connection Details	Connection Compliance Attainment and PYRAMID Exploiter's Pack Issue No.	Subject Matter Pollution Details	Extension Component Connection Details
<i>e.g. Release Aiming to Path Demands</i>	<i>e.g. PYRAMID Compliant to Issue 4</i>	<i>e.g. The connection does not contain any subject matter (beyond that required to bridge the semantic gap) that is defined as belonging within the scope of a PRA component.</i>	<i>e.g. N/A as the connection does not include an extension component.</i>
<i>e.g. Tasks to Tactics Extension</i>	<i>e.g. PYRAMID Compliant to Issue 4</i>	<i>e.g. The connection does not contain any subject matter (beyond that required to bridge the semantic gap) that is defined as belonging within the scope of a PRA component.</i>	<i>e.g. The Tasks parent component has access to the provided services of the Tactics Extension component.</i>
<i>e.g. Threats to Tactics Extension</i>	<i>e.g. PYRAMID Compliant to Issue 4</i>	<i>e.g. The connection does not contain any subject matter (beyond that required to bridge the semantic gap) that is defined as belonging within the scope of a PRA component.</i>	<i>e.g. The Threats component only communicates with consumed services of the Tactics Extensions component.</i>
<i>etc.</i>			