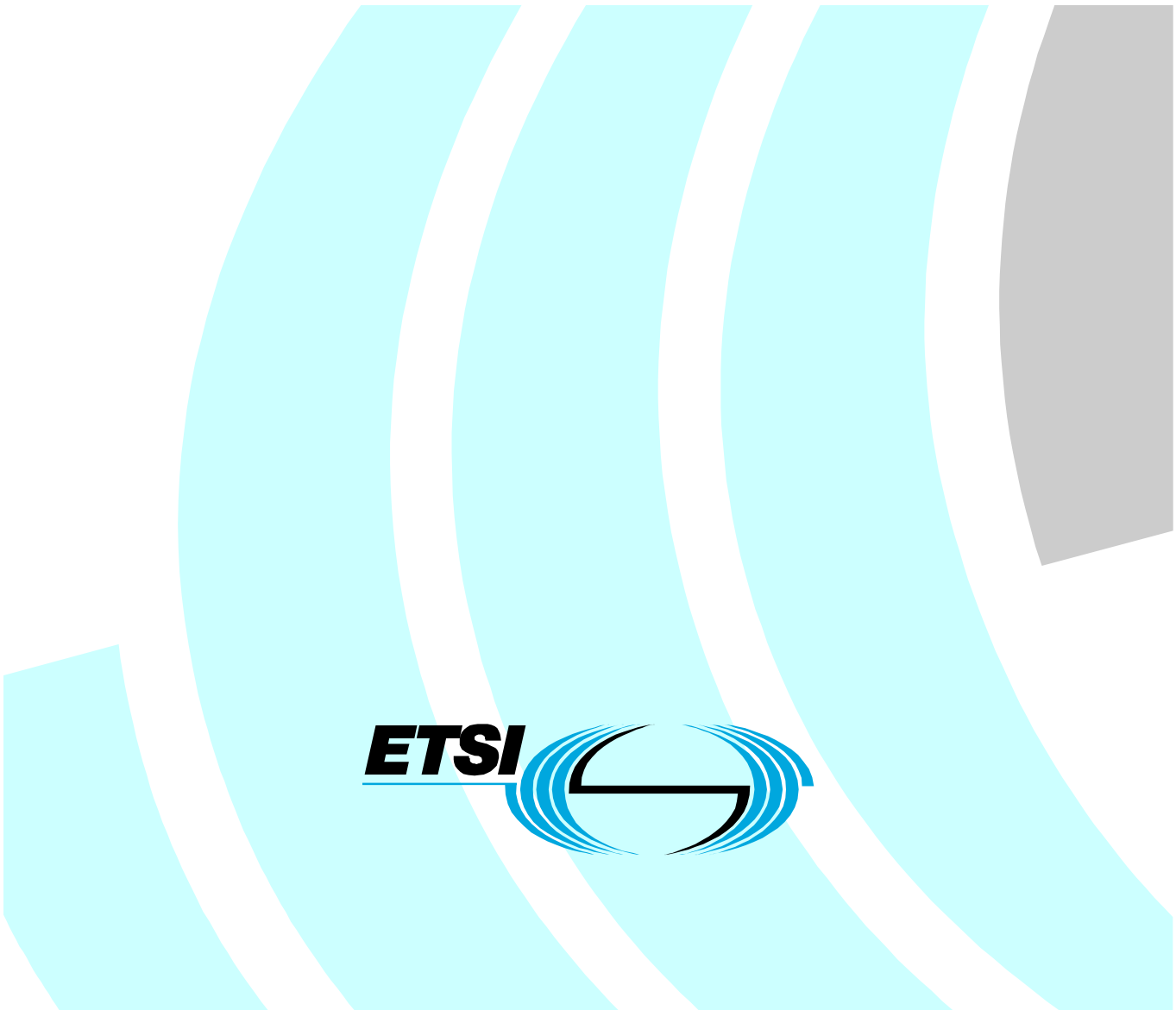
Draft ETSI TR 187023

Technical Report (2

Security Assurance Profile for Secured Telecommunications Operations



Reference
DTR/TISPAN-07049

Keywords
Security,

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

Introduction

An Assurance Profile (AP) document is a formalization of needs in which equipment vendors, solution providers, service integrators, operators and service providers or even final users can define **a common set of security assurance measurement requirements** for a service infrastructure. An Assurance Profile gives a means of referring to this set, and facilitates future evaluation against these needs.

1 Scope

The present document presents the structure of the Assurance Profiles.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references,only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area**.**

[i.1] ISO/IEC 15408 Information technology -- Security techniques -- Evaluation criteria for IT security (also known as Common Criteria).

[i.2] ETSI TS 187 016; "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Identity Protection (Protection Profile)"

[i.3] ETSI TR 187 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN_SEC); Threat, Vulnerability and Risk Analysis"

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Operational Security Assurance: ground for confidence that security controls are running as expected in an operational system.

Security Assurance Measurement Requirements: elements of evidence that need to be measured within a service infrastructure to gain assurance that the security controls are running as expected.

Security Assurance View: specifically focused representation of the security assurance measurement results.

Target of Measurement: minimal part of a service infrastructure where security controls are implemented and for which continuous security assurance measurement is required.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

none

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AP	Assurance Profile
CC	Common Criteria
TOE	Target of Evaluation
TOM	Target of Measurement

4 General concepts and use of Assurance Profiles

4.1 Risk, Trust and Assurance

An assurance profile is the expression of requirements to deploy a security assurance program in order to measure, monitor and maintain security assurance of a telecommunications infrastructure for a particular service.

Such a program can be illustrated in the following diagram where assurance management is a continuation of risk management and an input for trust management. We address in this document security assurance by measurement: infrastructures measured by metrics that generate evidence that leads to assurance.

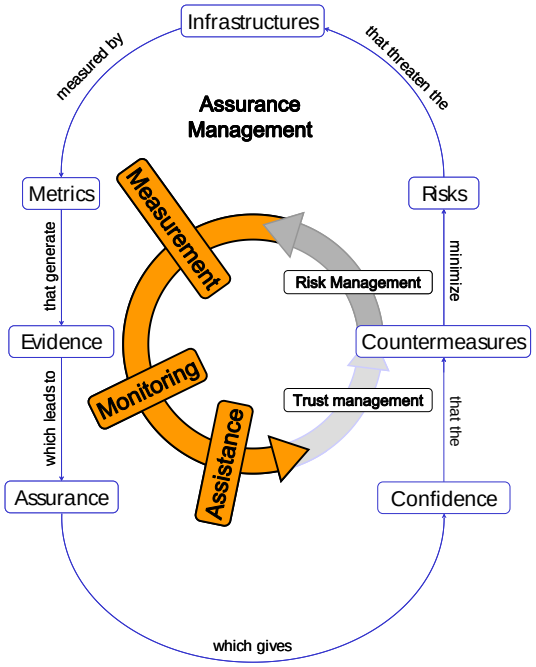


Figure 1 Risk, Assurance and Trust

4.2 Operational Security Assurance

We define operational security assurance, as ground for confidence that security controls are running as expected in an operational system; this is illustrated in the following Figure.

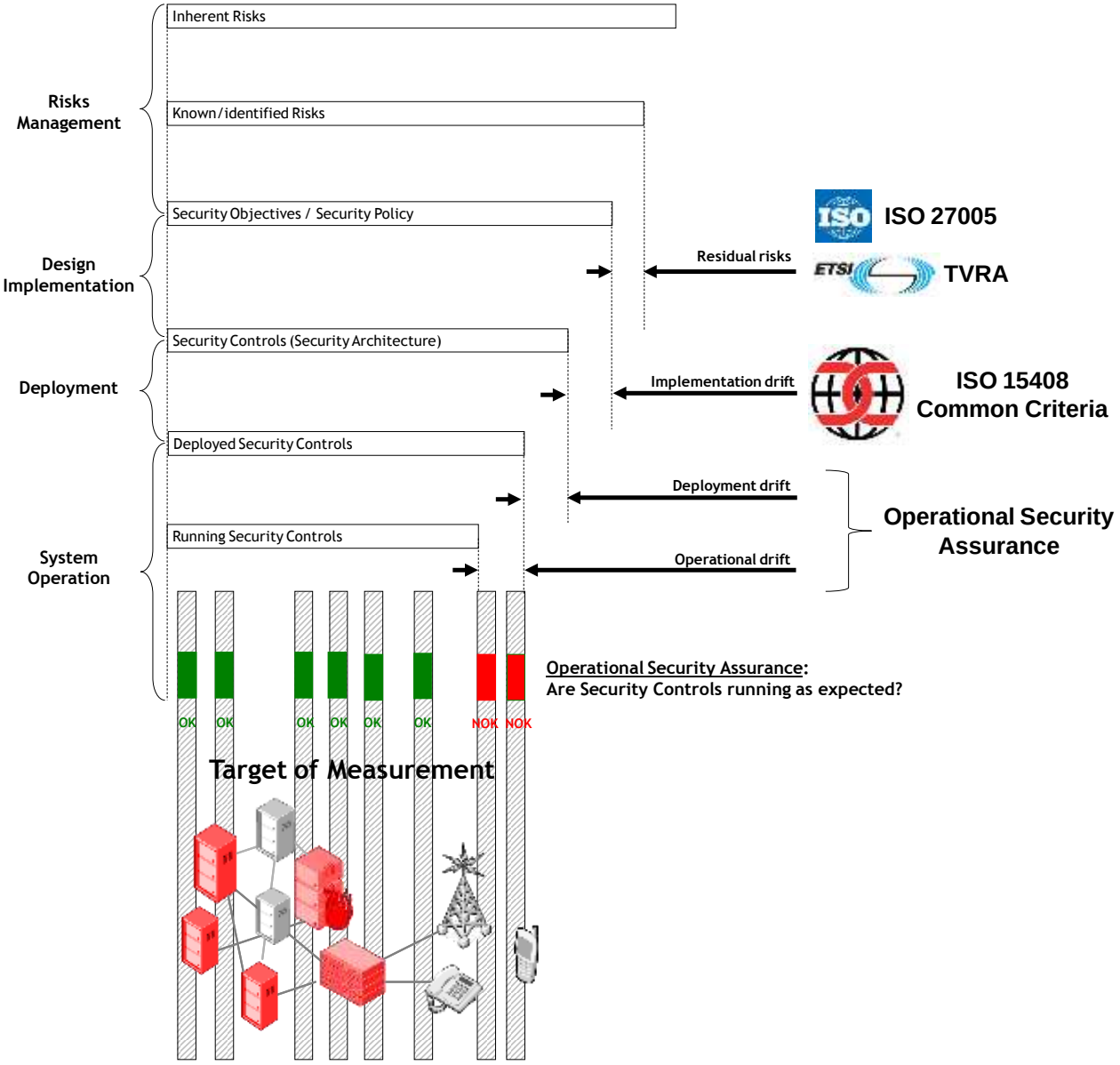


Figure 2 Operational Security Assurance definition

Operational security assurance is the last step in the overall security life cycle process. The diagram presents the different steps and how security assurance is related to all of them. The figure also shows how some of the most relevant standards are related to these different steps.

The first step is called **risk management**. A service infrastructure is exposed to threats and is subject to vulnerabilities (inherent risks). Managing risks consists in first identifying those risks (risk assessment) and then deciding the ones that can be covered by security objectives and those that are considered residual risks (risk treatment and risk acceptance). There are several standards concerned with risk management e.g. ISO 27005 and ETSI TVRA are some of the most appropriate and used standards related to IT and telecommunications infrastructures.

The second step is the **design and implementation of security controls** that will lead to the security architecture. The drift that can occur is called implementation drift and can be measured with ISO 15408 standards that brings assurance that the implemented system achieves expected security objectives.

The third step is the **deployment phase** where security architecture is deployed and configured. During this step, implemented security controls can be deactivated or modified by configuration. Drift that can occur is called deployment drift.

The last step is the **operational phase**. In this phase, an operational drift can occur: procedures could not be applied, configuration of equipments could be modified, equipments could be down, services could be unavailable,... The implementation of a security assurance program allows the evaluation (with more or less precision depending on the assurance level) of this operational drift. To achieve and quantify this drift, measures are performed on the target of measurement.

4.3 Concepts

4.3.1 The Target of Measurement (TOM)

An Assurance Profile (AP) refers to a particular service infrastructure. It defines a Target of Measurement (TOM) as the minimal part of this infrastructure that needs to be measured continuously in order to evaluate the operational security assurance for the service.

The Target of Measurement is in general the minimal set of elements that enforce or contributes to the security of the service.

4.3.2 The Security Assurance Views (SAV)

The Assurance Profile introduces the concept of Security Assurance View (SAV). Each Security Assurance View, defined in an Assurance Profile, gives a particular representation of the measurement results (i.e. information on the operational security assurance of the service). An Assurance Profile contains one or several Security Assurance Views.

Each Security Assurance View has a specific focus (e.g. a regulation, a standard, a security policy or list of requirements etc.). Recommendations for Security Assurance Views are (but not limited to):

- A **functional security assurance view**: this type of view will represent operational security assurance function by function (identification, authentication, access control, etc…). A functional security assurance view can combine various functions or only focus on one function.
- A **security policies assurance view**: this type of view will represent operational security assurance policy by policy (e.g. Mandatory access control policy, personal authentication policies, Secret distribution policy, etc.) A security policy assurance view can combine different policies or only focus on one policy.
- A **regulation/standard security assurance view**: this type of view will represent assurance of compliance for a specific regulation or standard. If the infrastructure is subject to several regulations/standards, the AP may present one combined view of all regulation or a view by regulation.
- A **geographical security assurance view**: this type of view will present operational security assurance by geographical area such as sites, country etc… This depends on the type of service and infrastructure deployment.
- A **set of equipments security assurance** view: this type of view will focus on a particular set of equipment that need special attention or if, for example, the service infrastructure is so complex that it will be easier to regroup equipment under different simpler view rather that a complex one.
- An **application security assurance view**: in this case, the AP will focus on a specific application of the service infrastructure. For example in an IPTV service infrastructure, a specific view can be made for Video On Demand application.

Figure 3 depicts the concepts of Target of Measurement and Security Assurance views, showing the views as a hierarchical structure. It should be noted that this is an illustrative example. This document does not defined any mandatory way to describe Security Assurance Views.

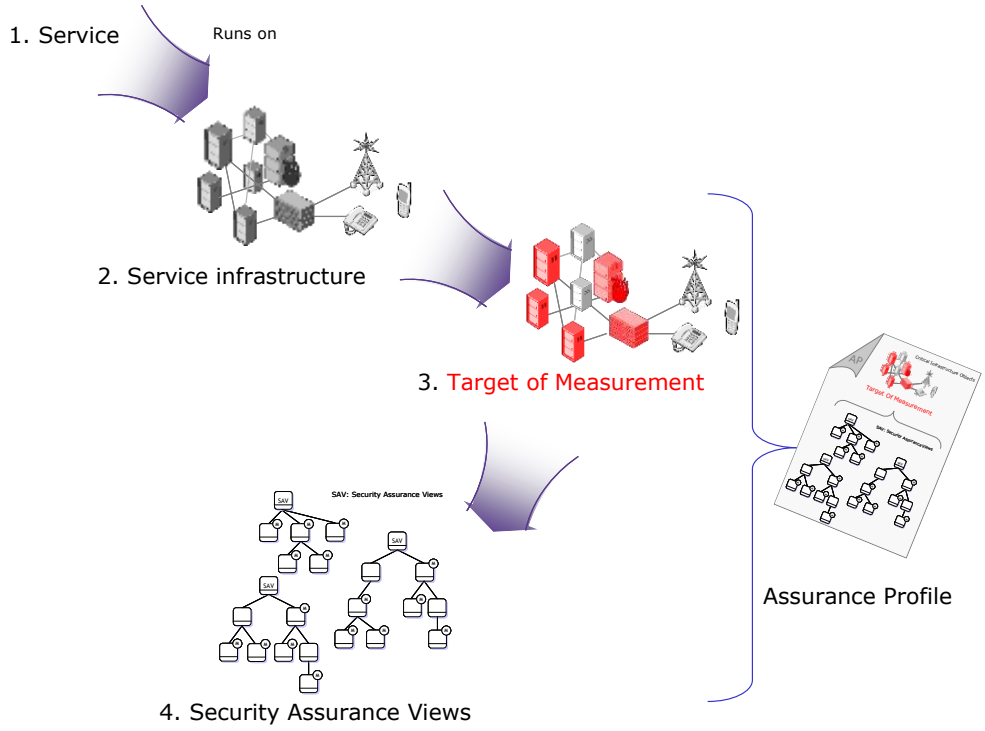


Figure 3 Target of Measurement and Security Assurance Views

4.4 General use of Assurance Profiles

4.4.1 How an AP should be used

An AP is typically a statement of operational security assurance measurement needs implemented by a defined and common set of measurement requirements. The use may differ between different actors.

An AP is a statement of needs in which equipment vendors, solution providers, service integrators and operators define a common set of security assurance measurement requirements on an agreed Target of Measurement. An AP gives a means of referring to this set, and facilitates future evaluation against these needs.

An AP can be considered as one or several specific angles of view for measuring the security assurance of a service infrastructure. Then, an entity (e.g. an operator or a corporate) may choose to implement different monitoring views of the security assurance of a service infrastructure, which may relate to several different Assurance Profiles.

An AP is therefore typically used as:

- Part of requirement specification for a specific consumer or group of consumers, who will only consider buying a specific type of service if it matches the AP.
- Part of a regulation from a specific regulatory entity, who will only allow a specific type of Service to be used if it matches the AP.
- A baseline defined by a group of service providers, who then agree that concerned provided services will conform to the agreed AP.

Though, this does not preclude other uses.

4.4.2 What an AP is not intended to provide

Three roles (among many) that an AP is not intended to provide:

- A security guarantee: an AP cannot be enough to guarantee that a Target of Measurement provides enough security if the AP is used to deploy, manage and monitor the Target of Measurement.

- a detailed infrastructure specification: An AP is designed to provide guidelines in designing security assured infrastructures. Compliance with an AP will not guarantee that the Target of Measurement is properly designed and secured.

- a complete specification of assurance measurement needs: An AP is designed to help the definition of assurance models and metrics for a TOM, not to be an exhaustive specification of assurance needs and measurements. An AP represents a common and coherent understanding on how security assurance should be addressed for a Service and measured within the Target of Measurement.

4.5 Implementing an assurance program using Assurance Profiles

The general use of an Assurance Profile is to help defining and establishing an assurance program and to deploy an associated measurement infrastructure.

4.5.1 Assurance program definition

An assurance program is a process to be implemented in order to be able to evaluate continuously operational security assurance for a service.

4.5.2 Assurance program implementation methodology

To implement an assurance program, the following inputs are necessary:

- Security best practices and expert knowledge: a generic risk analysis, in case of an abstract TOM (i.e. a generic architecture of a service), or a specific risk analysis, for an operational TOM, together with the necessary knowledge (e.g. system administration, security best practices and modeling) required to design and instantiate a relevant model.

- Compliance needs: lists of laws or standards the system or class of system must be compliant with.

- A System and its Services: the operational system running the targeted service to be evaluated.

The relevance of the security control realizations is accepted as the starting point of the assurance program, for which the risk analysis and the conformance claims are the justification.

The implementation of an assurance program is decomposed into 6 steps.

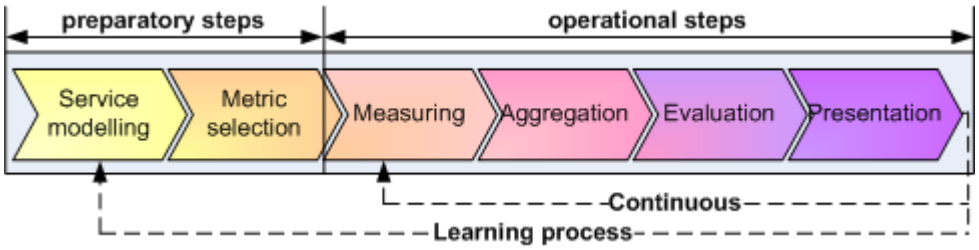


Figure 4 Assurance program 6-steps methodology

Step 1 (Service Modeling)

(I) Security Objectives and Security Requirements: the security controls to be evaluated are defined from known threats and security objectives for the service and the system providing this service. These are the security mechanisms expected to be present and running correctly in the system to fulfill the security objectives and counter the chosen risks, e.g. traffic filtering, configuration files access control, compliant of a specified function with standards, etc. Each security mechanism is decomposed and projected onto the different (abstract) infrastructure objects of the system by formalizing security requirements. The architecture combining the set of (abstract) infrastructure objects on which exists security requirements constitutes the TOM. Classically, infrastructure objects can be of three types: humans (e.g. security guard, HR employee, etc.), cyber (e.g. OS, firewall, anti-virus software, hard drive, log files, database, AAA, etc.) or physical (e.g. doors, locks, fences, etc.).

(II) Assurance Measurement Objectives and Assurance Measurement Requirements: for each security requirement Assurance Measurement Objectives are defined as a high level metric demonstrating that the security requirement is satisfied. Each measurement objective is then further decomposed into one or more Assurance measurement requirements which measure the different dimensions of the corresponding (abstract) infrastructure objects and demonstrate the related security requirement satisfaction. Measurement requirements may be further refined and formalized in (abstract) derived measures by specifying at the lowest possible level the expected result of a base measure to be instantiated in the step 2 by the operational system. Also at this point, contrary to an offline evaluation, the impact of some evolutions over time have to be included in measurement requirements.

(III) Security Assurance Views and Metrics: based on the (abstract) derived measures specified in the measurement requirements we may construct different abstract assurance metrics and security assurance views. Security assurance views are compositions of those metrics used to highlight some specific points of the security assurance evaluation. Various aggregation and composition models may combine their results differently in order to present the result of the assurance evaluation.

Step 2 (Metric Selection)

As opposed to step 1, step 2 is rather bottom-up and aims at instanciating the established model by identifying the system's raw data (i.e. base measures) required to evaluate the derived measures. Those base measures may be extracted from appropriate available data of the system found in Network Operations Center (NOC) or Security Operation Center (SOC) logs, OS files, etc. For data not directly available, dedicated probes should be defined.

The metric selection phase has an important impact on the assurance evaluation, that adds to the difficulty of having generic models which take into account the possible lack of some measurements (due to dynamics, policies or technical constraints). This need for the abstract model to take into account those real measurement constraints constitutes a fundamental difference to the off-line assurance.

Step 3 (Measurement)

(I) The required system probes are installed and activated along with the other measurement framework entities. Probes fetch base measures, while the measurement framework makes this data available for the corresponding processing engine, i.e. the one that manages the assurance model to be evaluated.

(II) Operational assurance has to face all the inherent problem of operational systems, and dynamic measurements in systems. The framework then requires constant management to maintain the proper access to the required derived measures. For a valid assurance assessment at any time, any systems part - just as the targeted security mechanisms - that may change, malfunction, move, crash, be removed, be under management, disappear, slow down, become unavailable, and so on, has to be handled properly by the framework.

Step 4 and 5 (Aggregation and Evaluation)

Each derived measures and metric produces an assurance result, indicating whether the infrastructure object relating to the base measure on the measured device is conformed to the expected result, and an assurance level (called metric capability), correlated to extrinsic (e.g. rigor of base measure interpretation, coverage of relating measurement requirements) and intrinsic (e.g. probe measurement frequency, probe precision, etc.) properties of the measurement framework that produces the results.

Dynamism such as devices appearance/disappearance and mobility in the system (laptops changing locations, mobile terminals) are addressed by the model and the measurement framework, allowing their corresponding derived measures and base measures to also appear/disappear and move inside the system while being still correctly handled.

Among handled dynamism, the evolutions over time of the used probe set (state changes, updates, etc.), which may influence the level of confidence (i.e. assurance level) of the assurance results has to be considered.

Step 6 (Presentation)

This step consists of providing to the users the security assurance evaluation results in relevant views of the system. These views provides, at a central management point, some hints to managers on how the protection mechanisms of the system evolve. From this information, the managers can decide how to adapt or modify the security mechanism to enhance the system and its services.

With the concept of Security Assurance Views, different presentations of the assurance evaluation regarding different security challenges (e.g. network view, files right management view, etc.) are enable, but also the post treatment of the gathered data (e.g. average of measures and/or metrics evaluated to true/false, frequency of measures results changes, alarms based on metric results, etc.).

4.5.3 Use of Assurance Profile

The Assurance Profile as pictured in Figure 5 is addressing preparatory steps of assurance programs.

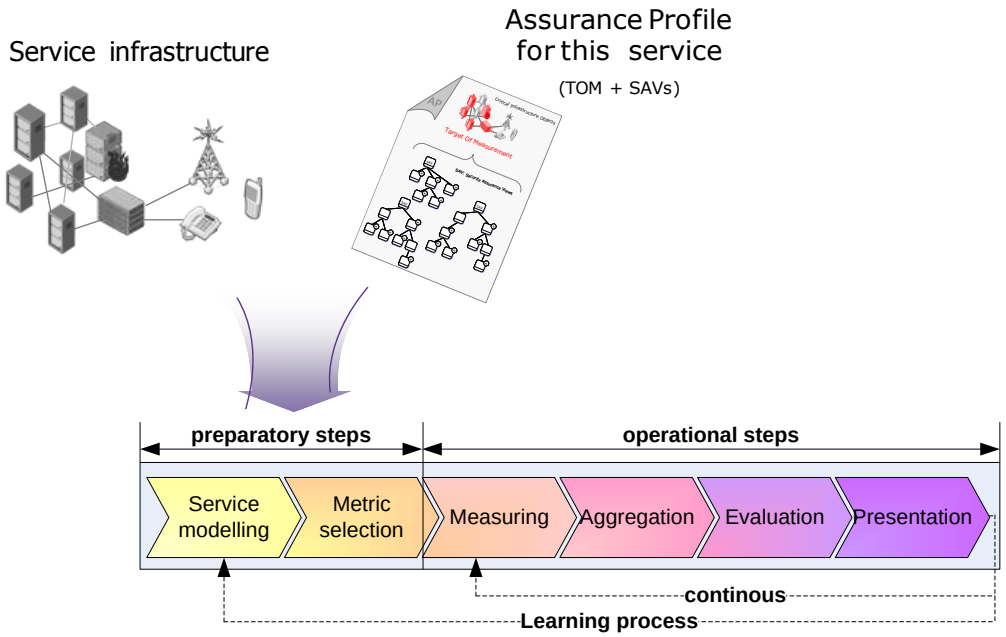


Figure 5 General use of Assurance Profile

When an operator, a service integrator or a group of users or consumers want to establish such a program, they should first look if there is an existing Assurance Profile corresponding to their service. To perform this, they have to check if the deployed infrastructure satisfies applicability requirements for the Target of Measurement. Those applicability requirements may be, for example, specific security architecture for the infrastructure.

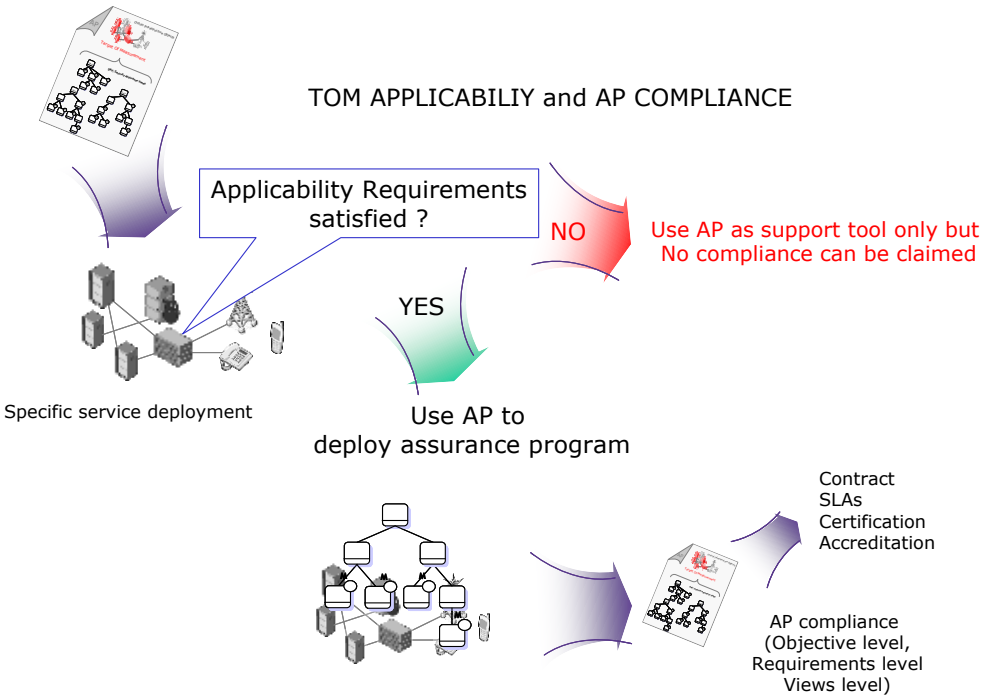


Figure 6 Applicability and compliance

If the infrastructure satisfies the applicability requirements, the Assurance Profile can be used and a compliance with the AP can be claimed. How to state this compliance is explained in Chapter **Error! Reference source not found.**. The operation to be done to use an Assurance Profile is called "Assurance Profile instantiation.

If the applicability requirements are not satisfied, the Assurance profile can only be used as guidance to build the assurance program but no compliance can be claimed.

5 Building an Assurance Profile

The following diagram illustrates how an Assurance Profile is articulated and how to build it. It also shows dependencies and operations to gather information.

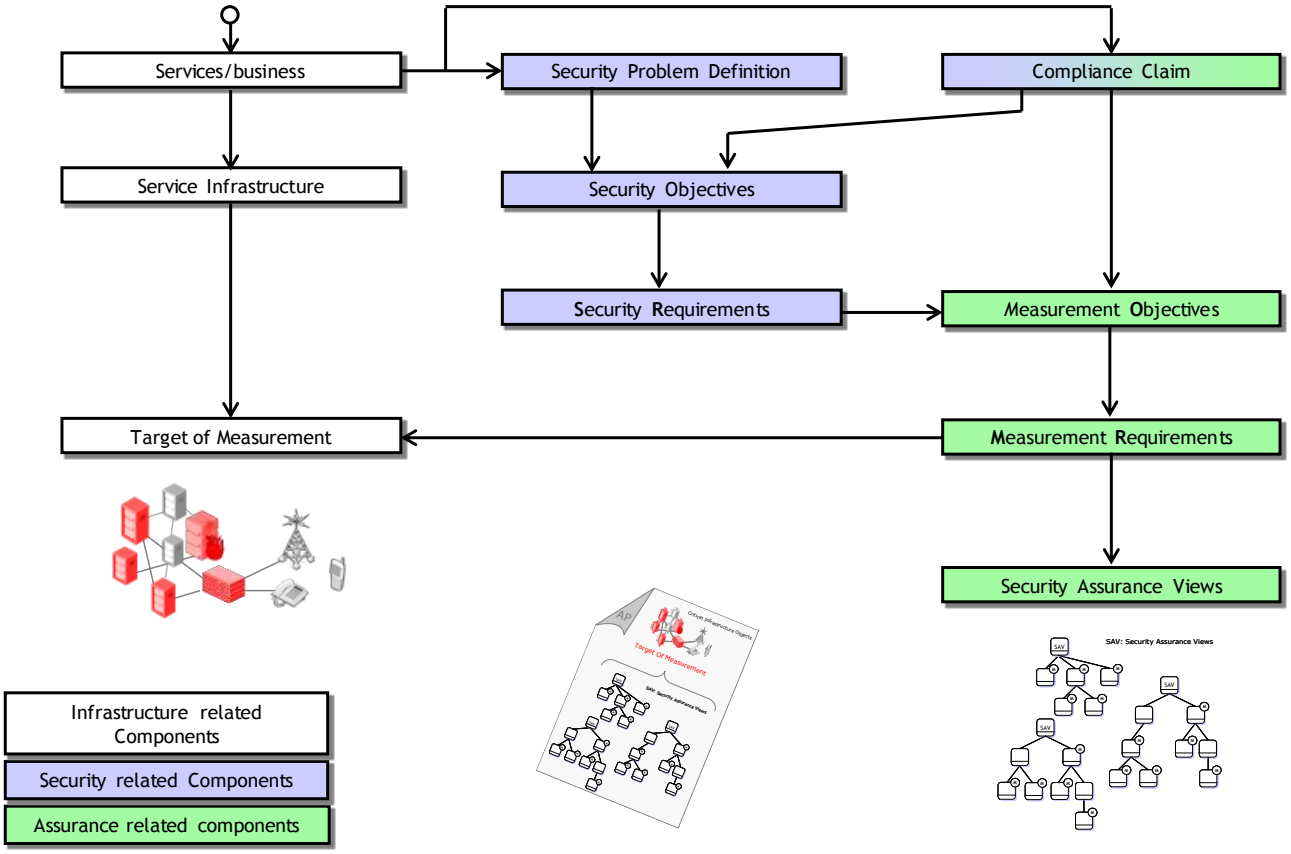


Figure 7 Assurance Profile's structure

The structure of an Assurance Profile is composed of three types of components: 1) infrastructure related components, 2) security related components and 3) assurance related components. All these components are described in details in the next sections.

The structure of an Assurance Profile is top down, from the service to a target of measurement associated with a set of security assurance views.

The entry point of the Assurance Profile is a telecommunication service or a specific business associated with this telecommunication service - e.g. IP-VPN service of a large company or the specific business associated with the VoIP service in the triple-play offer of a Carrier. This service is running on an infrastructure. In order to reduce the complexity, the Assurance Profile will focus only on critical components of this infrastructure on which security safeguards are deployed. The set of critical infrastructure objects that will be measured, defines the Target of Measurement as defined previously.

Concerning **security related components**, the Assurance Profile provides a presentation of the security problem that the service is facing and the security requirements that should be deployed to address those problems. This is addressed

in the “Security Problem Definition” component. This component is refined into Security Objectives. Those Security Objectives may also be derived from the claimed compliance to standards or regulations. Those Security Objectives are then refined into Security Requirements.

Concerning **assurance related components**, the Assurance Profile is providing first a compliance claims which describe which standards, regulations, or any specific document that is relevant to the security assurance for the service. Those compliance claims are derived into Measurement Objectives which also depend on Security Requirements. Measurement objectives are then derived into Measurement Requirements.

Having defined measurement requirements, they are selected and combined to constitute different security assurance views related to the concerned service. All these security assurance views will fully describe what need to be deployed and measured on the TOM to obtain service security assurance.

Creation of a new Assurance Profile that inherits from an existing one is expected to be a common scenario. They are many reasons for why this is likely to occur. For example, evolution of a service infrastructure or a new regulation or even change of the security problem definition can be addressed this way. Basically inheritance consists in reusing components of an existing Assurance profile. If the reuse is massive, the compliance of an AP with another AP can be claimed.

6 Assurance Profile components

This chapter defines the Assurance Profile content, i.e. component requirements. All components have one mandatory requirement and one optional requirement. It is recommended to satisfy optional requirements as much as possible. Indeed, providing additional information then provides enhanced support and help to deploy security assurance measurement programs.

Each component is described on one separate page. Each component has the same structure:

- A dependencies section that defines the components that need to be fulfilled prior the component,
- A requirement section that defines what information is requires. This section indicate what is mandatory and what is optional,
- An explanation section that explains what should be understood from the requirements,
- An example of application of the requirements. The selected examples are based on the Identity Protection as defined in TS 187 016 [i.2].

6.1 Assurance profile reference

An Assurance Profile contains a clear AP reference that identifies a particular Assurance Profile. A typical AP reference consists of:

- Title
- Version
- Authors
- Publication date

6.2 Target of Measurement

6.2.1 Dependencies

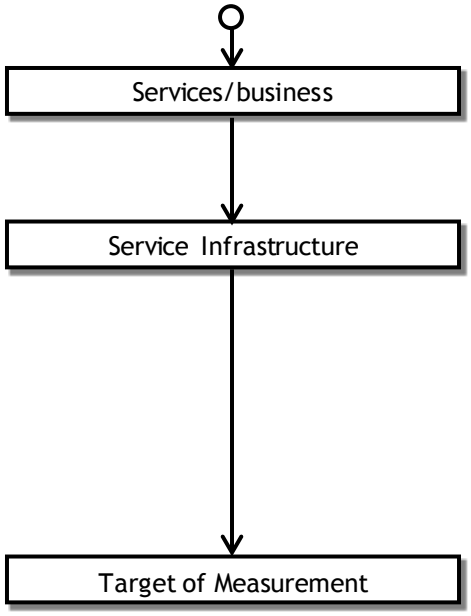


Figure 8 Target of Measurement dependencies

6.2.2 Component requirements

AP_TOM.1 (Mandatory) One or several applicability criteria shall be described.

AP_TOM.2 (Mandatory) A list of (abstract) infrastructure objects that compose the Target of Measurements shall be stated.

AP_TOM.3 (Optional) Details of contribution of each identified infrastructure objects of the Target of Measurement toward the service or the security architecture, thus justifying why it is critical for the service and its security.

6.2.3 Explanation

The Target of Measurement description presents in a narrative writing style the abstract infrastructure objects supporting the telecommunication service under continuous security assurance measurement. The Target of Measurement description should provide potential users of the Assurance Profile with a general understanding of the Target of Measurement; the Target of Measurement description may also be used to describe the wider application context into which the Target of Measurement will fit.

The Target of Measurement description discusses the physical or logical (e.g network layers) scope of the Target of Measurement as set of abstract Infrastructure Objects. This should be documented at a level of details that is sufficient to give the reader a general understanding of those parts and confidence on the suitability of the Target of Measurement.

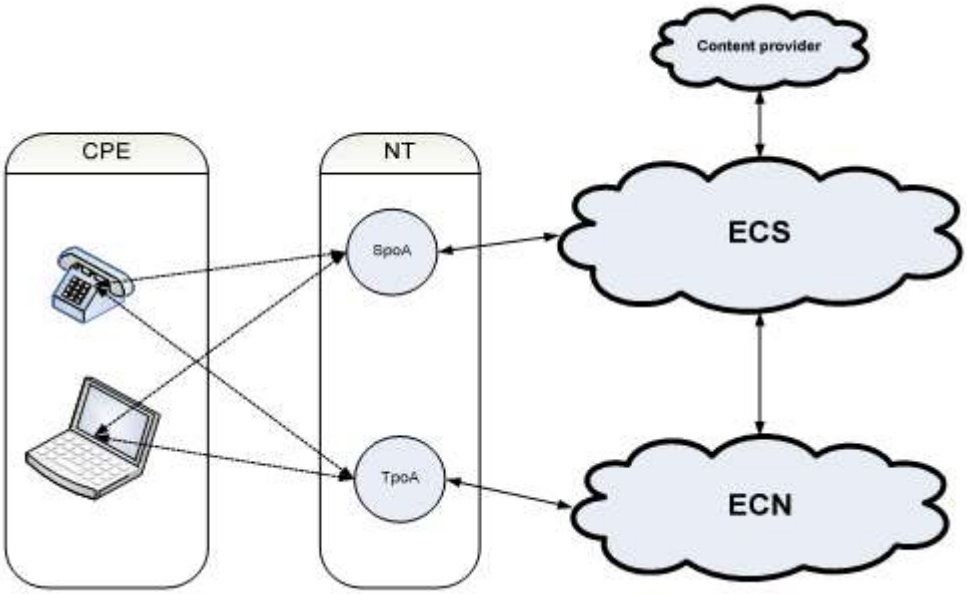
In addition, in order for user to determine if the Assurance Profile is applicable, it should be given some requirements that have to be satisfied by the operational system. If the requirements are not satisfied by the operation, the Assurance Profile should not be used. One example of applicability requirement might be the security architecture of the Target of Measurement. In this case, the architecture should be given at a level of details that is sufficient to give users of the Assurance profile an understanding of the applicability of the Target of Measurement to the infrastructure that will fulfil an assurance program base on the Assurance Profile.

6.2.4 Example of application

Applicability criteria:

This Assurance Profile is applicable for operational systems compliant with NGN-R2 requirements.

List of Infrastructure Objects:



The main Infrastructure objects in NGN-R2 systems are:

- CPE: Customers Premises Equipment
- NT: Network Termination
- ECN: Electronic Communication Network
- ECS: Electronic Communication Service

6.3 Security Problem Definition

6.3.1 Dependencies

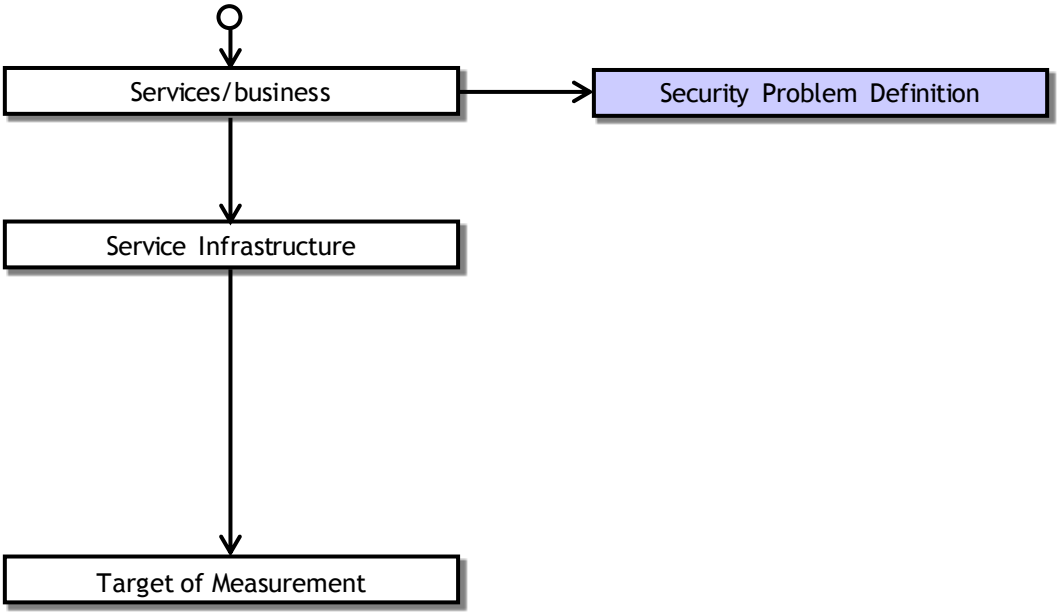


Figure 9 Security Problem Definition dependencies

6.3.2 Component requirements

AP_SPD.1 (mandatory): The identified risks toward the service shall be stated.

AP_SPD.2 (optional): The identified risks shall be explained and the risks analysis shall be provided.

6.3.3 Explanation

This component describes the overall security problem definition, showing the risks (or threats, depending what is known when writing the Assurance Profile) that must be countered, enforced and upheld by the Service and its environment. A risk (or threat) analysis should be performed prior to the AP writing. Although any kind of clearly defined and rational risk analysis methodology can be used, it is recommended to use a methodology that follows the frame of ISO 27005 or ETSI TVRA to perform this analysis.

6.3.4 Example of application

The risks to be covered are defined in TR 187 002 [i.3].

6.4 Compliance CLaims

6.4.1 Dependencies

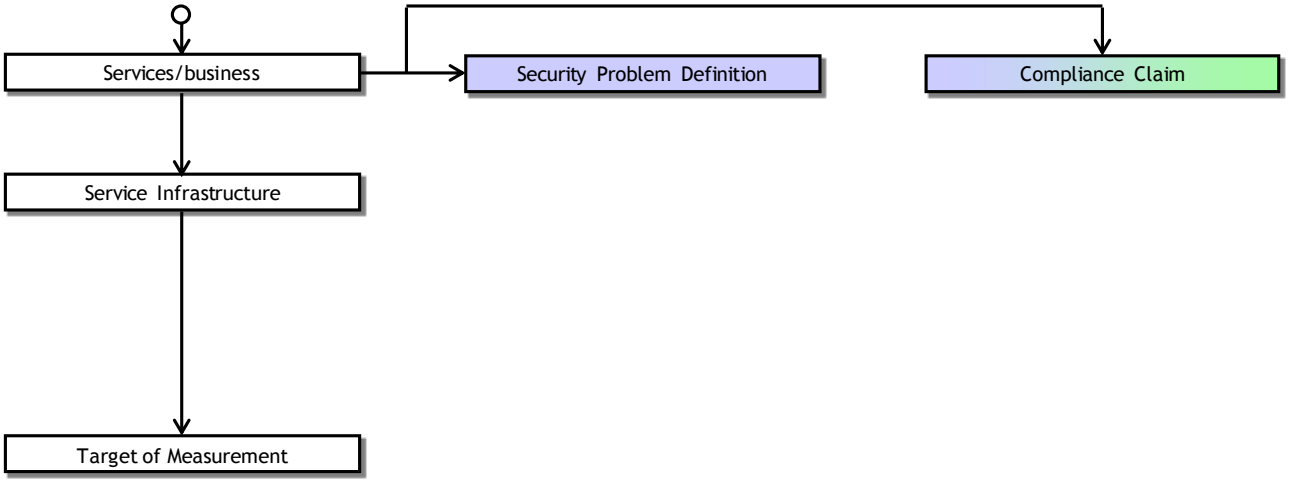


Figure 10 Compliance Claims dependencies

6.4.2 Component requirements

AP_CCL.1 (Mandatory): The claiming of conformance with standard, regulation or other applicable policies shall be stated.

AP_CCL.2 (Mandatory): The claiming of inheritance from other Assurance Profile (if necessary) shall be stated.

AP_CCL.3 (Optional): The claiming of conformance with standard shall be described by deriving standards or regulation requirements where the AP claims compliance. This means that, not only the standards or regulations is stated but a list of Applicable requirements is given.

AP_CCL.4 (Optional): The claiming of inheritance from other Assurance Profile shall be described by giving specific components of the inherited AP with which the Assurance Profile reuses.

6.4.3 Explanation

This component describes if the AP:

- Claims inheritance with other APs or is composed of Security Assurance views of other APs, in this case as pictured in Figure 15. Some component of the Assurance profile can just be given by a reference to component to inherited Assurance Profile.
- Claims conformance with any standards, regulations or other applicable policies

If there is no standard or regulation, the component should state the Assurance Profile does not comply with any standard or regulation.

Claiming compliance with standard or regulation increase the overall security assurance as security requirements and measurement requirements will be based on sound and recognized requirements.

Optionally, it might be necessary to claim compliance with existing operational security policies that have to be addressed by the infrastructure in general and the target of measurement in particular.

6.4.4 Example of application

Conformance with standard, regulation or other applicable policies:

As explained in TS 187 016 [i.2] section 5, the NGN must ensure the rights and freedom of natural persons with regard to the processing of personal data and, in particular, their right to privacy as specified by Directive 95/46/EC (Data protection Directive).

Inheritance from other Assurance Profile:

The Assurance Profile does not claim any inherence from another Assurance Profile.

6.5 Security Objectives

6.5.1 Dependencies

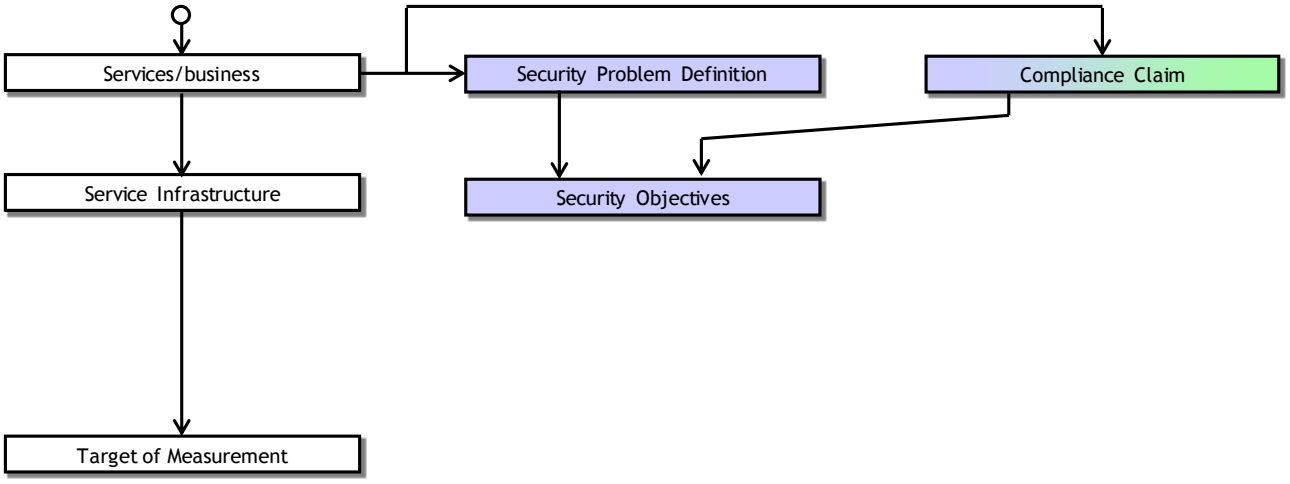


Figure 11 Security Objectives dependencies

6.5.2 Component requirements

AP_SSO.1 (Mandatory): The security objectives to be achieved shall be stated. This statement should be done with a service resolution.

AP_SSO.2 (Optional): The security objectives to be achieved shall be described together with how they cover identified risks and comply with standards.

6.5.3 Explanation

This component describes the Security Objectives that have to be achieved in order to counter risks identified for the Service or to be compliant with standard or operational policies. References to any standard can be given. Optionally, security objectives will be justified by identifying which AP, standard or regulation is addressed and if AP-CCL.2 has been chosen, the AP_SSO.2 will indicate precisely on each specific requirements of the AP, standard or regulation, the service security objectives apply.

6.5.4 Example of application

Security objectives related to Identity Management defined in TS 187 016 [i.2] are:

- Access to NGN services should only be granted to users with appropriate authorization
- The identity of an NGN user should not be compromised by any action of the NGN
- No action of the NGN should make an NGN user liable to be the target of identity crime
- No change in the ownership, responsibility, content or collection of personal data pertaining to an NGN user should occur without that user's consent or knowledge

- Personal data pertaining to an NGN user should be collected by the NGN using legitimate means only
- An audit trail of all transactions having an impact on personal data pertaining to NGN users should be maintained within the NGN
- The identity of an NGN user should not be compromised by any action of the NGN
- No action of the NGN should make an NGN user liable to be the target of identity crime
- The NGN shall comply with the European regulations on privacy (EC Directives 2002/58/EC and 2006/24/EC)
- The NGN shall comply with the European regulations on data protection (EC Directive 95/46/EC)
- The NGN shall comply with the requirements to support law enforcement (EC Directive 2006/24/EC and COM 96/C 329/01)

6.6 Security Requirements

6.6.1 Dependencies

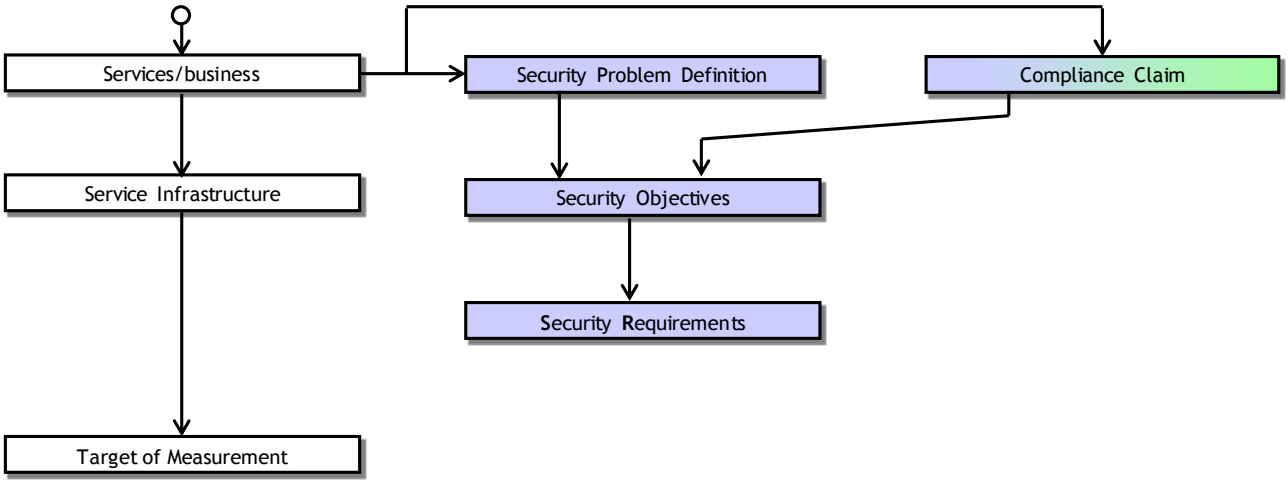


Figure 12 Security Requirements dependencies

6.6.2 Component requirements

AP_OSR.1 (Mandatory) Security Requirements to be satisfied shall be stated.

AP_OSR.2 (Optional): Security Requirements to be satisfied shall be described together with how they participate to achieve the Security Objectives identified in AP_SSO.1.

6.6.3 Explanation

This component describes the Security Requirements to be satisfied by the service infrastructure. Optional information will describe the link between those requirements and list of objectives identified at service level in the AP_SSO component thus providing more confidence in the correctness of the Assurance Profile.

6.6.4 Example of application

Examples of security requirements related to Identity Management defined in TS 187 016 [i.2] are:

Functional requirement	**Functional class**
Security Objective 1: Access to NGN services should only be granted to users with appropriate authorization	

1.1	An NGN operator shall be the only entity able to create the identifiers in class 2	Access control policy
1.2	An NGN operator shall be the only entity able to destroy identifiers in class 2	Access control policy
1.3	An NGN shall support the secure transfer of identifiers and identities between CSPs	Export to outside TSF control
1.4	An NGN shall be able to enforce the use of NGN provided secrets for authentication	Specification of secrets

6.7 Measurement Objectives

6.7.1 Dependencies

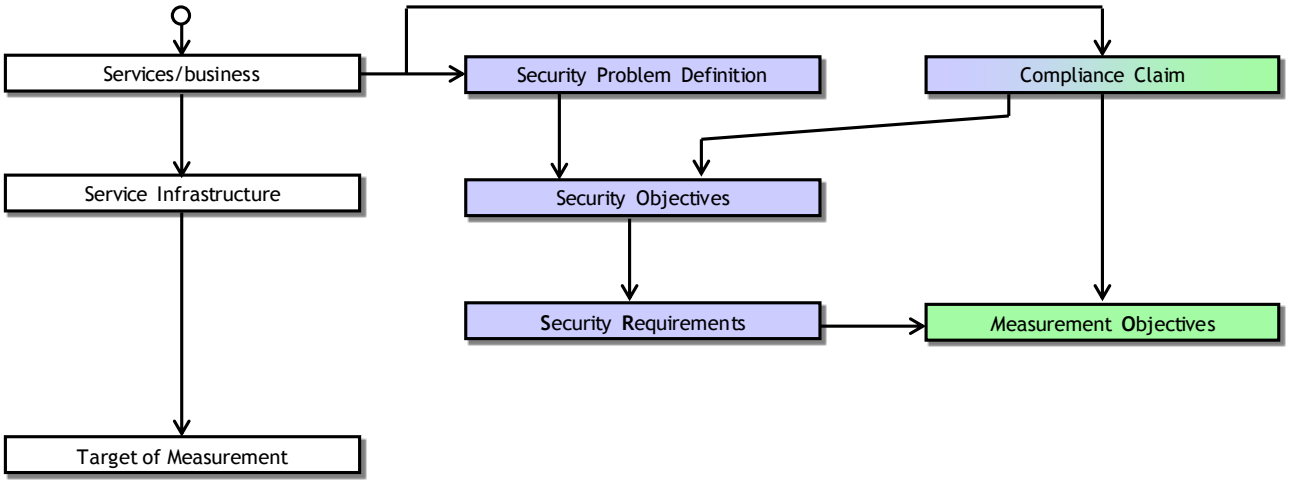


Figure 13 Measurement Objectives dependencies

6.7.2 Component requirements

AP_SMO.1 (Mandatory) Measurement objectives shall be stated.

AP_SMO.2 (Optional) Measurement objectives shall be described with the justification on how measurement could permit to demonstrate that the security requirements are running and how to comply with standards and regulations identified in AP_CCL.1.

6.7.3 Explanation

This component describes measurement objectives that need to be achieved to demonstrate that security requirements are running as expected. Optionally, the component should describe how these objectives address and demonstrate compliance with standard as identified in AP_CCL.1.

If AP_CCL.1 has been chosen, the link will just indicate which AP, standard or regulation is satisfied by the service assurance measurement objective.

If AP_CCL.2 has been chosen, AP_SMO.2 will explain precisely on which specific requirement of AP, standard or regulation it specific applies.

Measurement objectives are generally specified as following: *To check if [Security Requirement] is [running as expected]*

where [Security Requirement] is a Security requirement from the AP and [running as expected], the reference to be used during the measurement to decide if it can be considered that the security requirement is enforced or not.

6.7.4 Example of application

Examples of measurement objectives related to Identity Management and based on examples or security requirements stated in 6.6.4 are:

- To check if the NGN operator is the only entity able to create the identifiers in class 2
- To check if the NGN operator is the only entity able to destroy identifiers in class 2
- To check if the NGN supports the secure transfer of identifiers and identities between CSPs
- To check if the NGN is able to enforce the use of NGN provided secrets for authentication

6.8 Measurement Requirements

6.8.1 Dependencies

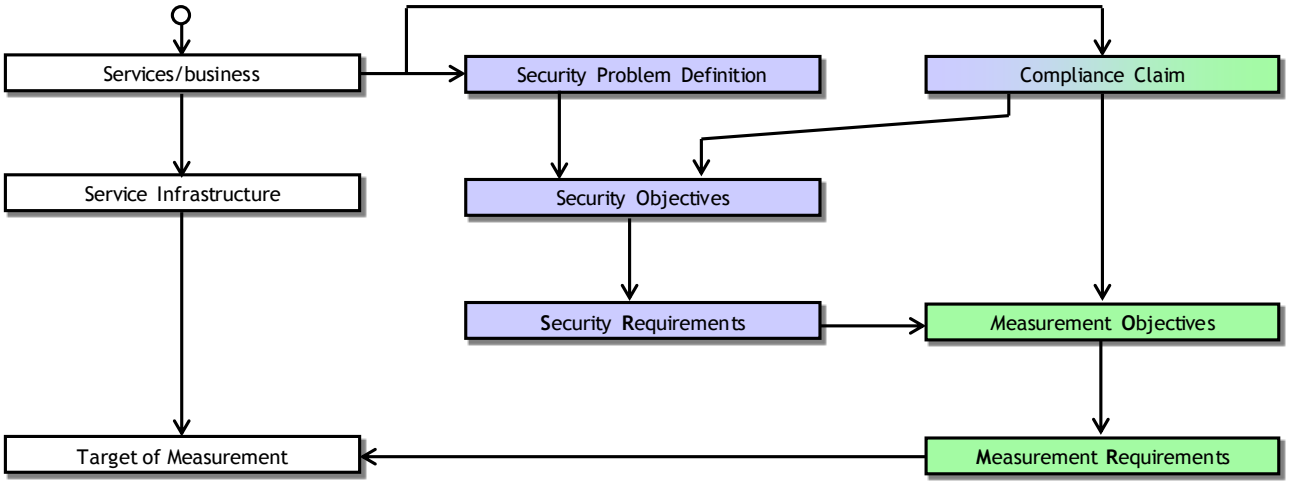


Figure 14 Measurement Requirements dependencies

6.8.2 Component requirements

AP_OMR.1 (Mandatory) Measurement Requirements shall be stated. The statement shall indicate the infrastructure object concerned by the measurement.

AP_OMR.2 (Optional) Measurement Requirements shall be described with the justification on how Measurement Requirements satisfy Measurement Objectives.

6.8.3 Explanation

Usually security and measurement objectives are written in natural language and at high level. Measurement requirements are formalized requirements for measurement and are iterated for each infrastructure object on which measurement has to be done.

The measurement requirement shall be a question with a YES/NO answer.

A taxonomy has been developed to formalize these requirements. Each requirement has to be formalized as following:
Is [taxonomy domain] of [concerned security requirement] on [concerned Infrastructure Object] [as expected]?

The [taxonomy domain] is a combination of the following statements:

- The concerned security requirement realization that is a combination of:

- **The security requirement** concerned by the measurement objective linked to the measurement requirement.
- **The scope**: has the measurement to be done on the Infrastructure Object concerned by the security requirement or on its environment? Syntax: "IO" or "IO environment".
- **The domain**: is the concerned Infrastructure Object a physical object, a social object or a cyber object? Syntax: "Physical", "Social", "Cyber".

- The properties of the measurement requirement that is a combination of:
  - **The temporal property**: does the measurement concern the configuration or the execution of the security requirement? Syntax: "Configuration" or "Execution".
  - **The specificity**: is the expectation generic or specific to the system implementation? Syntax "Generic" or "Specific"

The [concerned security requirement] is the security requirement concerned by the measurement objective linked to the measurement requirement.

The [as expected] statement is the reference with which the measurement result will be evaluated to obtain the answer YES/NO for the requirement.

6.8.4 Example of application

Examples of measurement requirements related to Identity Management and based on examples or measurement objectives stated in 6.7.4 are:

Reference	**Security requirement realization**			**Properties**		**Expectation**
	Security requirement	**Supporting IO**	**IO Type**	**Temporal**	**Specificity**	
To check if the NGN operator is the only entity able to create the identifiers in class 2						
MR-1	An NGN operator shall be the only entity able to create the identifiers in class 2	NGN operator	Social	Configuration	Generic	An access control policy exists stating that the NGN operator is the only entity able to create the identifiers in class 2
MR-2	An NGN operator shall be the only entity able to create the identifiers in class 2	NGN	Cyber	Configuration	Specific	The access control system is configured to allow only NGN operator to create the identifiers in class 2
MR-3	An NGN operator shall be the only entity able to create the identifiers in class 2	NGN operator	Social	Execution	Specific	An audit is regularly performed to confirm that the the NGN operator is the only entity able to create the identifiers in class 2

6.9 Security Assurance Views

6.9.1 Dependencies

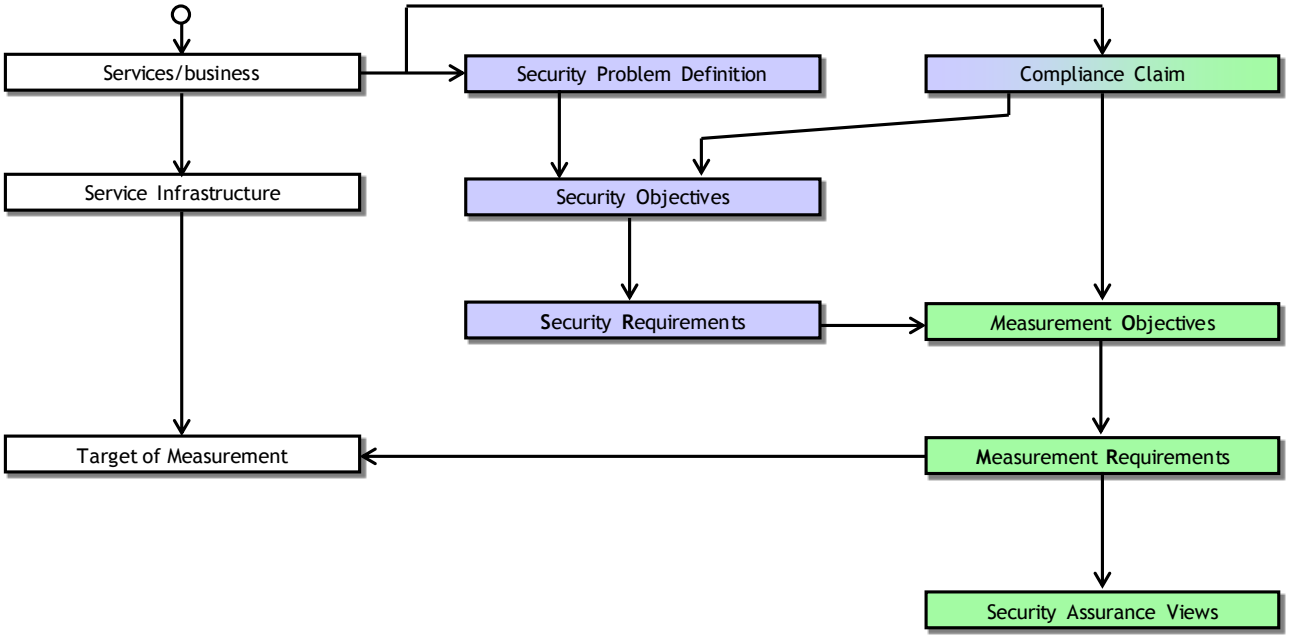


Figure 15 Security Assurance Views dependencies

6.9.2 Component requirements

AP_SAV.1 (mandatory): One or several Security Assurance Views shall be described.

AP_SAV.2 (optional): A rationale of choice of Security Assurance View shall be given explaining the choice of the different views and how they relate to each other if possible.

6.9.3 Explanation

A Security Assurance View is an (organized) composition of Measurement Requirements. Such composition permits to represent the results of the Measurement Requirements or aggregated results in a view perfectly adapted to the user concern. For example if a service is supported in two distant geographical areas, the Assurance Profile can describe two security assurance views, one for each site. A security assurance view can also be an organisation of a company, a specific department, a vertical view of an organisation, but also a process, etc

We recommend aligning and describing views regarding the choice made in Target of Measurement, in Security Problem Definition, or in Compliance Claims sections. Measurements requirements aggregated by Infrastructure objects permits to identify objects identified by non-conformity. If compliance to a specific standard is expressed, it should be interesting to have a view dedicated to this compliance. If there is a major risk for the service, it could be interesting to describe a view for this specific major risk.

6.9.4 SAV Objects

Security Assurance views may differ due to their different natures. A regulation views for example will be a flat organisation where other views such as functional or policy oriented ones may require hierarchical representation.

In a hierarchical representation, each node of the tree is called a Security Assurance View Object (or SAVObject).

A description of relations between the SAVObjects of the chosen representation that express the global assurance within the representation, such as an aggregation function, should be given if possible.

6.9.5 Metrics

A Metric is a process that enables to gather raw data from infrastructure objects and to derive a normalized metric result used to gauge some quantifiable component of the service security assurance.

In the SAVs, metrics are specified by a combination of Measurement Requirements with an aggregation function. This aggregation function will be used to aggregate measurement results when the AP will be instantiated in the operational system.

One or several metrics can be attached to a SAVObject.

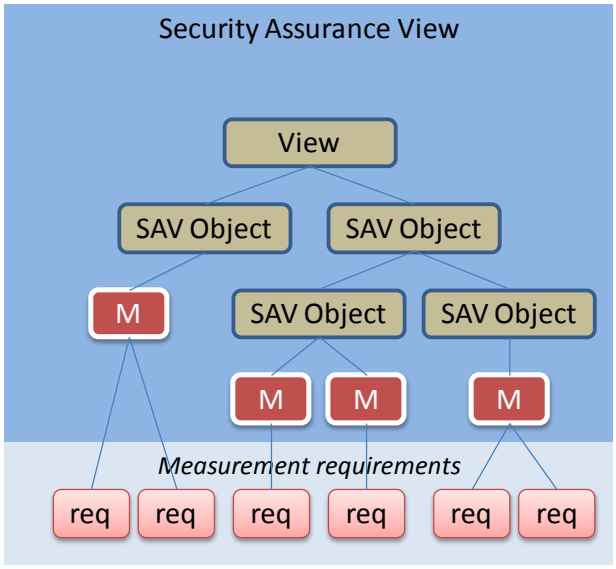


Figure 16 Security Assurance Views content

6.9.6 Example of application

A simple examples of Security Assurance View is a view where a metric is defined for each measurement requirement. Another provided example is to group measurement requirements by concerned infrastructure objects.

If reusing the examples related to Identity Management stated in 6.8.4 are:

Views	**SAV Objects**	**Metrics**	**Measurement requirements**
Standard View	Default SAV object	MR-1 metric	MR-1
		MR-2 metric	MR-2
		MR-3 metric	MR-3
Infrastructure Objects view	NGN operator SAV object	NGN operator metric	MR-1
			MR-3
	NGN SAV object	NGN metric	MR-2

7 Claiming compliance with an Assurance Profile

Compliance with an Assurance Profile is the result of the process consisting in claiming and justifying that a security assurance program implemented for an operational service is based on one or several Assurance Profiles. It can be also use to claim the compliance of an AP with another AP.

Such compliance gives the opportunity to a service provider to demonstrate to service customers that the security and measurements concerns described in the Assurance Profile have been taken into account and that operational security assurance information are available.

Compliance with an Assurance Profile can be declared in a Service Level Agreement (SLA) document or a similar contract. It permits to assure that both service provider and service customer agree on sensible security and measurement requirements defined by a community of experts.

Compliance with an AP can be defined at three levels:

1. Objectives,
2. Requirements,
3. Views.

The three levels are defined as illustrated in the following Figure:

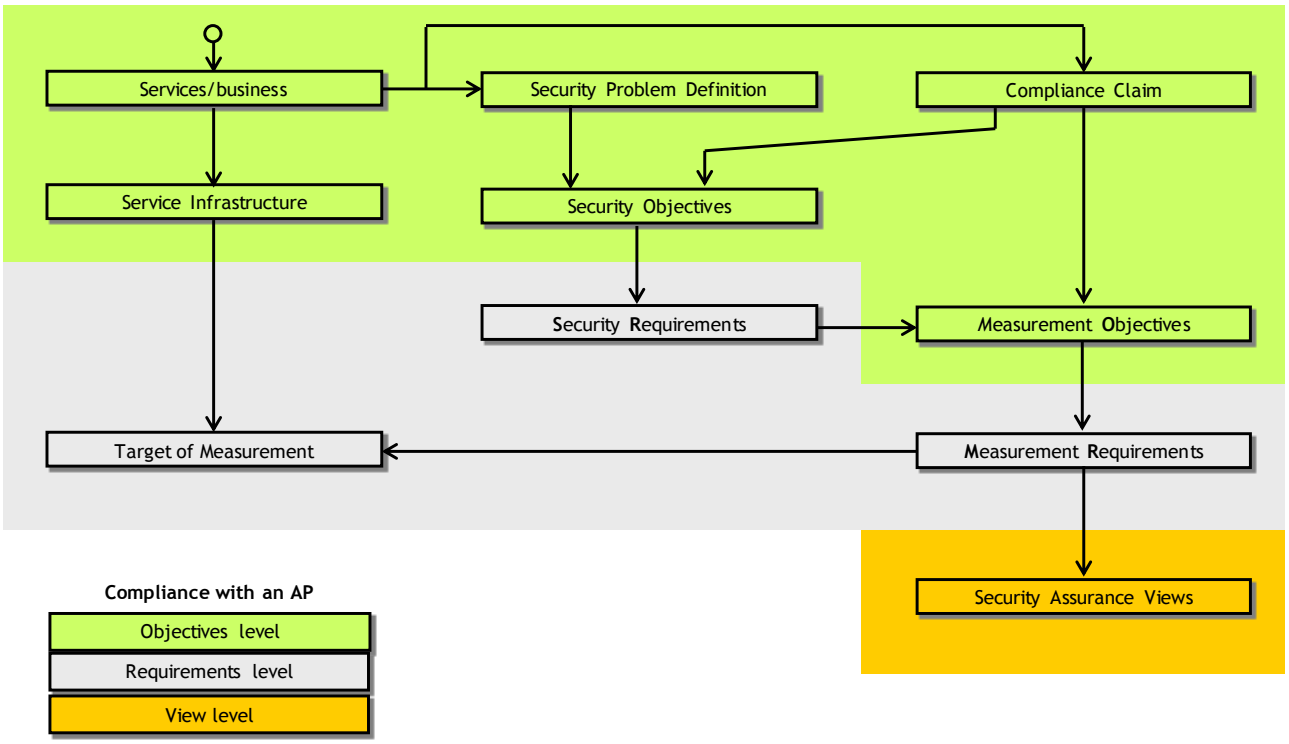


Figure 17 AP compliance level

Claiming compliance at Objectives level requires, at the minimum that the deployed service and associated infrastructure are similar to the ones described in the AP, and that all Security Objectives and Measurement Objectives specified in the AP are implemented in the operational assurance program.

Claiming compliance at Requirements level requires compliance at Objectives level and in addition that all Security and Measurement Requirements specified in the AP are implemented in the operational assurance program. This compliance implies that abstract Infrastructure Objects described in the AP correspond to real objects in the operational infrastructure.

Claiming compliance at Views level requires compliance at Requirements level and in addition that all Views specified in the AP are implemented in the operational assurance program.

History

Document history		
<Version>	<Date>	<Milestone>
V0.0.1	January 2011	Early draft
V0.1.0	June 2011	First draft
V0.2.0	Septembre 2011	Draft for approval
V.0.2.1	Septembre 2011	editorial changes