7 Attainment – achieving compliance with ESARIS standards

Introduction and summary: The ESARIS Attainment Model (or: ESARIS Compliance Attainment Model) relates to activities ensuring that the ESARIS security standards are actually implemented and comprise methods for verifying this (Sect. 7.1). In the first place, the ESARIS security standards have to be developed by starting with requirements engineering as the basis (Sect. 7.2). The “Attainment” is organized into five ESARIS Attainment Levels which relate to the achievement of milestones in delivering ICT services according to the methods, procedures, and standards of ESARIS. The first three levels are related to more technical activities (IT engineering, implementation), the set-up for delivery (operations) and include methods for measuring the compliance (Sect. 7.3). The other two levels relate to the integration into portfolio and service catalogs. The portfolio development and the consideration of security in service catalogs (Sect. 7.4) are important for user organizations or even the next party in the internal supply chain of the ICT Service Provider.

7.1 Foundation

Introduction and summary: The ESARIS Attainment Model is an important means for an active security management. It ensures that appropriate security standards are maintained and used. It also provides information if and to what extent the ESARIS security standards are actually implemented. But the information relating to the compliance with ESARIS security standards is moreover important when making any business with user organizations (customers).

The ESARIS Attainment Model describes how security is integrated in the ICT services using ESARIS. This comprises the phase where the ESARIS security standards are being developed as “security design patterns” and the phase where they are applied. In the second phase it is measured if and to what extent an ICT service meets the security standards stipulated in ESARIS. The result is called the ESARIS Attainment Statement and provided in form of so-called Aces. This measurement is a snapshot that measures a current outcome. If practices are still adhered to, the ICT services maintain the quality that has been attained.

The basis for ESARIS attainment assessments are the ESARIS security standards, mainly the ICT Security Standards (Level 4) with the security measures described therein. The ICT Security Baselines (Level 5) provide information on an implementation level including detailed work instructions etc. Refer to Fig. 48.
(1) The standards are used to develop and implement ICT services including their basic constituents such as components and activities. They also provide the design patterns which shall be used to achieve the “secure by design” goal. The ICT Service Provider files the ESARIS security standards in a central **ESARIS Library**. Refer to the figure.

(2) The design and its implementation are compared with the ESARIS security standards from the **ESARIS Library** (step 1). The result is the **ESARIS Attainment Statement** called Ace (see below) which states compliance with and potential deviations from ESARIS security standards. The integration of ICT services and their security features into the service catalogs is also covered by Attainment.

On the one hand, the **ESARIS Attainment Statements** form the basis for an operative security management which identifies possible vulnerabilities and organizes their remediation. Refer to Fig. 48.

On the other hand, the **ESARIS Attainment Statements** provide information about the security features actually being built-in. This information plays an important role in the relationship with user organizations.

(3) When preparing new business with customers it is necessary to verify if the customer’s security requirements are fulfilled. Refer to Fig. 48. To this end, one must know if the ICT service being subject of the contract is compliant with the ESARIS security standards. The **ESARIS Attainment Statements** (in form of Aces) provide the information about the built-in security features and possible deviations from the ESARIS security standards (step 2). Hence, the verification of “attainment” is the basis for a sales promise to customers and for contracting (“Fulfillment”, see Chapter 8).
7.2 Requirements engineering and elaboration and application of ESARIS standards

Introduction and summary: Any verification of compliance with ESARIS security standards assumes that the latter exist and that they are high quality and fit for purpose. The development of security standards starts with requirements collection, analysis and acceptance. It must consider constraints of industrialized IT production. Development of security standards and design of ICT services are often interwoven.

The overall process of implementing security standards comprises three steps.

- Requirements engineering (Step A): The ICT business starts with the identification of relevant requirements and their analysis.
- Provisioning of guidelines (Step B): Then security standards are developed based on the identified requirements. The security standards provide re-usable design patterns for IT production in an industrialized fashion.
- Application of security standards (Step C): The security standards are used for the design of technology and processes and implemented accordingly. Security features become part of the ICT services specification and are used during operations.

Requirements engineering (Step A)

Fig. 49 illustrates the process from the identification of requirements (left) to their consolidation (middle).

Basically, Fig. 49 shows the ESARIS Industrialization Concept (Sect. 6.2). There are two sources of security-related requirements: corporate and market requirements. Note that the two types of requirements do overlap. The focus in this section is on...
customer-independent developments. Customer requirements are requirements that are seen in the market and articulated by actual and potential customers. Corporate requirements are mostly defined to mitigate risks for the ICT Service Provider.

It is important here that the requirements are analyzed with respect to their significance and grouped into
- Standard requirements,
- Optional requirements, and
- Custom requirements.

Standard requirements are accepted as state-of-the-art so that they shall be met on a global basis by all ICT services. Optional requirements need to be met in many cases. But it is too costly to implement the corresponding security measures in every ICT service regardless of whom it is delivered to. For both types of requirements security measures are developed in Step B. Finally, there are requirements that are very specific and only relevant for one customer or a specific group of them. In this case it may not be economic to develop related solutions in advance and to include them into the standard catalog. Such custom security requirements may be realized in customer projects. Consequently, they are out of scope here. Examples are legacy and very high security requirements.

Security requirements differ in scope and relate to different level of abstraction. Hence, the analysis also considers this fact. Refer to Fig. 49.

The security management organization is responsible for the requirements engineering (Step A). However, employees, especially if engaged in deals and in service design, must support this process by identifying security requirements that are not met yet or where standards need to be modified in order to increase the level of standardization or for the sake of general improvements. It might be necessary to identify today’s custom requirements which may become optional or standard requirements in the future if they are requested by more and more customers.

The Security Management organization uses the same process, boards, and roles that are used for the management of security documents. This process covers request, analysis, planning, and approval and is part of the so-called Maintenance System for ESARIS (Chapter 10) which is mainly designed to support the provisioning of guidelines.

**Provisioning of guidelines (Step B)**

The next step comprises the development of security documents and is therefore also straightforward to understand. Refer to Fig. 50.
New or modified requirements (from Step A) result in a formal Change Request that describes what has to be added or modified and where. Then the security standards are developed or modified, respectively. This process results in having security documents that are approved and mandatory. The *Hierarchy of Security Standards* has three levels in which security standards are provided for ICT service on a different level of abstraction (refer to Sect. 3.4).

All security documents are filed in one *ESARIS Library* and made available throughout the ICT Service Provider in this way. Otherwise standardization may not take place.

The business units are responsible to develop and maintain all security documentation which they require for developing, implementing and operating ICT services in an industrialized fashion. This especially covers the *ICT Security Baselines* (Level 5) they are requiring or use. *ICT Security Standards* (Level 4) should also be considered since the security measures stipulated in there are the base for the detailed implementation and operating instructions (Level 5). The Security Management organization supports the development and maintenance of all security documents. But their main responsibility is requirements engineering, approval of security standards, as well as steering and control that the security standards are used and adhered to.

**Application of security standards (Step C)**

The application of security standards covers
- Development (design),
- Implementation (realization), and
- Operations (delivery)

of ICT services. The development, implementation and operations processes are not security-specific and follow the standard processes of the ICT Service Provider.
Fig. 51 shows the application of the ESARIS security standards. All information about implementation and operations should be covered by the design which either provides explicit descriptions or refers to standards. Especially Operations should follow general processes and procedures which are not specific to an ICT service. For the sake of simplicity implementation and operations are not shown in the figure. In terms of security the *ESARIS Library* provides all information that has been agreed in advance and is therefore standardized. In order to provide ICT services in an industrialized fashion these security standards shall be reused as design patterns.

Not all security standards have to be used for a specific ICT service since some information is obviously not relevant. For instance, computing service does not include user workstations such as notebooks. Hence, the relevant standards need to be identified. This is done using the method called *Provider Scope of Control* described in Sect. 4.5. In short, the ICT service specification is analyzed in order to identify all areas where the ICT Service Provider is responsible for. Implemented technologies are identified and it is analyzed how the ICT service is developed and managed. Based on this information the relevant *ICT Security Standards* (and security measures) are selected. The funnel in Fig. 51 represents this. The *ESARIS Security Taxonomy* as a basic element considerably helps to identify the relevant areas. In specific cases, it may additionally be required to verify if all security measures stipulated in a standard actually apply to the ICT service under consideration. The

---

42 This method is not only used for “attainment”. It will be used again when verifying compliance with customer requirements in contracts (“fulfillment”, Chapter 8) and when managing supplier networks (“3rd party integration”, Chapter 9). The *Provider Scope of Control* methodology is a fundamental principle of ESARIS.
result of this analysis is a set of relevant standards (refer to Fig. 51). The relevant standards are mandatory. If not being used, the degree of standardization is decreased which has an impact on industrialized ICT service provisioning. However, it is possible to step out and decide to use other solutions than specified. This step-out process is risk-based and requires a business case. The decision needs to be documented.

The mandatory security standards or patterns are the input for the “design” together with a bunch of other material that is not related to security aspects. The “design” incorporates a security conception. Important features from the design are reflected in the “ICT service description” as used in service catalogs. This also holds for security so that the “ICT service description” is expected to also describe security features. Refer to Fig. 51. The “ICT service description” must contain information about security if this is important for the next party using the ICT service (customer or next unit of the ICT Service Provider in the supply chain).

Note that there is a cycle in the relation shown in Fig. 51. If the “design” for some reason leads to a change of the “ICT service” and its “ICT service description”, it may be required to analyze again what standards are actually relevant. This may in turn lead to a changed set of mandatory standards which can have an effect on the design.

The business units are responsible to develop and implement an ICT service. This means that they are also responsible to develop and maintain all design documentation (including those about security). The designers can reuse the security measures stipulated in the ICT Security Standards (Level 4). The related ICT Security Baselines (Level 5) contain further detail which should also be reused. This approach reduces the effort for designing the security part of ICT services. During operations the business benefits from using standards which allows for provisioning ICT services in an industrialized manner.

**Summary:** The overall process is shown in Fig. 52.

Step A: Internal and external requirements are analyzed and it is decided which of them shall be met by all possible ICT services (standard requirements) and which of them shall be considered as possible additions (optional security requirements).

Step B: Solutions are elaborated. This means that design patterns are developed in form of security standards. They are made available in a central library.

Step C: The security standards can now be used. This covers the phases of development or design, implementation as well as operations. Each activity is based on standards and predefined elements that are reused. All information can be considered to be part of the design. The business units are fully responsible for the provisioning of ICT services which includes all security features.
7.3 ESARIS Attainment Levels and verification of compliance

The application of the ESARIS security standards goes along with a “verification process”. It is organized into five ESARIS Attainment Levels which relate to the achievement of milestones in delivering ICT services according to the methods, procedures, and standards of ESARIS. The first three levels are related to the design and implementation of technology and IT management processes but also include “successfully delivered”. The last two stages are related to the management of the service portfolio (called Service Catalog Management in ITIL). The ICT (functionality) and the related IT service management activities shall comply with the ESARIS security standards. The ESARIS Attainment Model (or: ESARIS Compliance Attainment Model) comprises a method to formally verify if and to what extent an ICT service, component or activity complies with the ESARIS security standards. The result is documented in form of an Ace which also contains the ESARIS Attainment Statement.
In order to ensure that the ESARIS security standards are actually used, a verification mechanism is required that checks if and to what extent an ICT service, a component or a activity complies with the relevant security standards. The verification mechanism is an important element of the ESARIS Attainment Model and organized in stages each associated with achieving an ESARIS Attainment Level. The first three stages are related to more technical tasks (engineering and implementation). The last two stages are related to the management of the service portfolio. The ESARIS Attainment Levels are shown in Fig. 53.

| ESARIS Attainment Level | Description                                                                 |
|-------------------------|-----------------------------------------------------------------------------|
| technologically complete| ready for ICT implementation; the ICT components can be provided with security measures defined in ESARIS |
| operations ready        | ready to deliver; this means that the service and security management processes can be provided as defined in ESARIS |
| successfully delivered   | this means that the ICT service has at least once been provided to a customer with security measures as defined in ESARIS |
| integrated into delivery portfolio | this means that ESARIS is part of the ICT service description provided by the Delivery |
| integrated into sales portfolio | this means that ESARIS is part of the ICT service description provided to customers |

The ESARIS Attainment Levels are as follows:

- **Engineering and implementation**
  - Level 1 – Technologically complete (ready to “run”; this means that the ICT is build and functional; the components integrate the security measures defined in the lower half of the ESARIS Security Taxonomy),
  - Level 2 – Operations ready (ready to “deliver”; this means that the service and IT security management processes are in place; the IT service management activities are enhanced as described by the security measures from the upper half of the ESARIS Security Taxonomy),
  - Level 3 – Successfully delivered (this means that the ICT service has at least once been provided to a customer with ESARIS security measures in place),
- **portfolio design and integration**
  - Level 4 – Integrated into delivery portfolio (this means that service catalogs for internal use describe relevant security features explicitly or by referring to ESARIS security standards),
Level 5 – Integrated into sales portfolio (this means that service catalogs which describe ICT services for customers also describe their relevant security features).

A core ICT service with its functionality achieves the ESARIS Attainment Level 1 ("technologically complete") if the security measures from the lower half of the ESARIS Security Taxonomy are applied. A comparison must also exist which shows possible deviations from the ESARIS security standards.

An ICT service (functionality and included IT service management) achieves the ESARIS Attainment Level 2 ("operations ready") if the security measures from the upper half of the ESARIS Security Taxonomy are applied. This means that all relevant IT service management processes are in place and can be applied to the core ICT service. A comparison must also exist which shows possible deviations from the ESARIS security standards.

An ICT service can reach the ESARIS Attainment Level 3 as soon as it has been successfully delivered to a customer. This level is seen as a reality check since the real business of ICT service provisioning is expected to provide extra knowledge which can be used to review and proof the information gathered for the levels 1 and 2.

While the first three ESARIS Attainment Levels focus on service design and implementation as well as on operations based on standardized processes in the delivery units, the ESARIS Attainment Levels 4 and 5 are related to the organization of sales processes and of the internal supply chain. In general, the ICT Service Provider’s service catalogs cover two types of ICT service: customer-facing ICT services that are to be purchased by the customers and supporting ICT services that are required to deliver customer-facing services. The service catalogs are developed and maintained according to the Portfolio Management process usually by people specialized in this job. In fact, three categories of ICT service exist: those in the pipeline (proposed or in development), those which are currently “for sale” (live or available for deployment), and retired ICT services as well.

An ICT service achieves the ESARIS Attainment Level 4 if appropriate information material about security features (including an appropriate ESARIS Attainment Statement) is integrated in the ICT service description reproduced or referred to in a service catalog for internal use. Obviously, design and operating documentation must also contain such security-related information.

An ICT service achieves the ESARIS Attainment Level 5 if the same is achieved with respect to a service catalog used to sell and deliver ICT services to user organizations (customers of the ICT Service Provider). Highly standardized ICT services may be sold, purchased and deployed over the Internet (user self-provisioning). In such a case, the necessary preparations are subject of this attainment phase.

Both parts as well as the stages may be started or run simultaneously. However, the attainment of ESARIS compliance follows a bottom-up approach. The founda-
tion is built first with ICT and process implementation. The stage “successfully delivered” demonstrates that the implementation works. Portfolio design and integration is put at the end which does not mean that the development process should not follow a top-down approach. It is put at the end here, since the message “ready to deliver” assumes the foundation in technology and IT service management.

The major goal of “attainment” is to ensure that the ESARIS security standards are adhered to through the correct implementation of the design patterns provided by the ESARIS security standards. This needs to be verified. Fig. 54 shows how the compliance with ESARIS security standards is verified. The comparison between “reality” (left in the figure) and “standards in paper” (right-hand side) results in a document called Ace which includes the ESARIS Attainment Statement as a summary. Compliance with ESARIS security standards is documented by means of Aces. An Ace is created for an entity which can be an ICT service, a component, or an activity. Such entities (and their Aces) can be reused when building composite ICT services. Aces are the basis for an operative security management since they contain information about deviations which are to be dealt with.

Fig. 54: Verification of compliance with ESARIS security standards and Aces

The attainment verification is performed for all relevant areas in the ESARIS Security Taxonomy. Hence, the relevant ICT Security Standards (Level 4) need to be identified first. Perhaps, it is necessary to analyze if specific security measures are relevant or not. This selection of standards and measures is done using the method called Provider Scope of Control described in Sect. 4.5.

43 “Ace” is an abbreviation which stands for “Attainment component in ESARIS”. However, the name was mainly chosen to draw the attention of stakeholders to this important instrument and raise the motivation to elaborate one. “Do you have an Ace up in your sleeve?”
The Ace is created during development and provided by the Business Unit ("service owner") responsible for the ICT service design, realization, and provisioning. This approach ensures that the designers are applying the ESARIS security standards and that caring for security is everybody’s obligation and not restricted to the Security Management organization. The finalized Aces are approved by the Security Management organization. The Aces are then centrally stored for future reference and re-use.

An Ace documents the level of compliance with ICT Security Standards and ICT Security Baselines and thus serves as ESARIS Attainment Statement. An Ace for an ICT service, component, or activity consists of a frame document which contains several attachments. The following information is collected in the documents:

- **Ace summary:**
  - Identification and characterization of the ICT service, component, or activity including its supplier and the intended areas of application,
  - Identification of the relevant ESARIS areas (ICT Security Standards) together with an indication of the depth in which the verification or comparison was performed (on Level 4 only or including Level 5).
  - Summary of compliance levels with the security measures from the applicable ESARIS areas and description of major exceptions.

- **Detailed ESARIS Statement of Compliance document (attachment):** Evaluation of compliance with security measures defined in the ICT Security Standards for each of the relevant ESARIS areas. Any deviation from security measures is identified and forwarded to the evaluation of potential risks implied by this noncompliance.

- **List of related ICT Security Baselines (Level 5) which actually have been incorporated in the design and therefore been considered in the Attainment evaluation (attachment).**

- **List of referenced Ace(s) of sub-components in case of a composite Ace (attachment).** A composite Ace relates to an ICT service, component or activity which is composed of other ICT services, components or activities already evaluated so that Aces exist.

It is worth to note two things. First, the business is responsible for the comparison of reality with standards and the evaluation of compliance. Templates exist. Though, security experts may do the work and consult the Security Management organization too, the business manager ("service owner") is responsible for the result. The Ace is signed by him or her. This also holds if the Ace is elaborated under the auspices of the Security Management organization or initiated by it. Second, deviations from ESARIS security standards are possible for several reasons. Some may be tolerated. However, deviations which result in exposing the ICT Service Provider or the user organization (customer) to a significant risk are tracked and require treatment according to common risk management practices.
Modularization is important for an industrialized IT production. As a consequence, ICT Service Providers follow a modular approach in providing ICT services. The service offering portfolio is hierarchical and modular which supports combining different elements. The composition is based on a set of building blocks and uses a hierarchy of standardized ICT delivery components as illustrated in Fig. 55. This needs to be taken into account when considering the management of ESARIS Attainment Statements (Aces) since all yellow elements in the figure may have an associated Ace.

An industrialized IT production uses a composition schema in which ICT services are combined with options and are aggregated to ever more complex ICT services. This means that “production elements” are used to build Standard Delivery Elements (SDE), the SDE are used to build ICT services, and the ICT services can be used to build “service chains”.

Fig. 56 shows the aggregation of ICT services again. Each ICT service has an ICT service specification and a design. The design comprises a security conception which in turn provides information about compliance with the ESARIS security standards in terms of the ESARIS Attainment Statement in the form of an Ace. If the ICT Service Provider works on the next level of aggregation it is not necessary to analyze compliance with ESARIS from scratch. Instead the Aces from the reused ICT services can be reused where available. This is shown in Fig. 56. If Aces are not yet available, they need to be requested from the service owner in a recursive process to get all required Aces. Of course, the attainment statements are not only collected and summed up. They are aggregated requiring a step where the integration is being analyzed.
In order to avoid multiple checks and verifications of ESARIS Attainment Statements, it is usually only required to step down to the next lower level of the composition hierarchy and refer to the Aces available at that level. In case that further detailed information needs to be reviewed, the references to underlying ICT Security Baselines (Level 5) or additional Aces on even lower composition levels can be retrieved from the information collected within the Aces.

### 7.4 Service offering portfolio integration

**Introduction and summary:** The collection of available ICT services and their specification together form the so-called service offering portfolio of an ICT Service Provider. The security measures specified in ESARIS security standards must be implemented in the ICT services. Their service specifications must reflect this fact and also describe relevant security features. In this way, security is one element in service catalogs. The latter are an important instrument for managing the relationships along the complete supply chain. The structure of the ESARIS security standards is the perfect input for the service portfolio management and the elaboration of service catalogs. This relates to the achievement of the ESARIS Attainment Levels 4 and 5.

The Service Portfolio Management (or Service Offering Portfolio Management) is a complicated process interwoven with several other processes. For example, almost all ITIL processes are directly affected, including Service Strategy (SS), Service Design (SD), and Service Transition (ST). Continual Service Improvement (CSI) and Service Operation (SO) are involved rather indirectly. Merely the result of the process is therefore shown in the following instead of describing all the necessary steps in the standard Portfolio and Offering Management process.
It has been mentioned, that the ICT Service Provider’s service catalogs cover two types of ICT service: customer-facing ICT services that are to be purchased by the customers and supporting ICT services that are required to deliver customer-facing services. It has also been mentioned, that two types of service catalogs exist relating to two types of portfolio. There are service catalogs that describe the delivery and are used by the ICT Service Provider only internally to organize the internal supply chain. And there are service catalogs which are given to the customers and describe the sales portfolio with the corresponding ICT services. Both types of service catalogs may contain both customer-facing services and supporting services. Note that supporting services may optionally supplement customer-facing services and require an order from customers in this case. This means, that the portfolio (and service catalog) integration relates to the achievement of both ESARIS Attainment Levels 4 and 5. Service catalogs (and offering portfolios) are structured in a modular way which corresponds to and is necessary for an industrialized IT production. In the following, no distinction is made between delivery and sales portfolio because the differences are not essential in the context given.\textsuperscript{44}

The offering portfolio consists of individual, predefined ICT services each being described by a service specification. Security is one characteristic or feature among others and must therefore also be part of the service description. The principle is shown in Fig. 57 using a simple example of a managed workplace service.

---

\textsuperscript{44} ITIL moreover distinguishes between pipeline (planned ICT services), catalog (ICT services that are currently delivered), and retired ICT services (delivered in the past).
ESARIS security standards (right in the figure) provide the pattern both for the design (lower left) and the service specification (upper left). In the example, the workplace is equipped with appropriate means for boot protection, container-encryption and malware protection. And the software is fully managed. IT service management includes the maintenance of the software based on a secure initial set-up of the machines (using a software image). Both types of security aspects are covered by ICT Security Standards (Level 4, ESARIS Orchestration Layer). This is visualized by two red boxes in Fig. 57 that frame specific ICT Security Standards which specify the security measures in detail. In the above example, the Office Workplace (OWS) standard is providing the re-usable patterns for the service specification and the high-level design (Level 4). The underlying ICT Security Baselines (Level 5) are used for the low-level design. Note that the service specification in the service catalog directly reflects the description of the security measures stipulated in the relevant ICT Security Standards. Utilizing the underlying ICT Security Baselines (Level 5) ensures that the security measures are correctly implemented resulting in reliable service catalogs. The same is done regarding the aspects of IT service management.

In an industrialized IT production environment, IT service management and other services are defined and set up once and then used for almost all ICT services. This results in a modular service offering portfolio and, more important, in higher quality and lower costs. Two examples are discussed in the following.

The first example is shown in Fig. 58. The ICT Service Provider has standardized the security support for cloud and other computing services. Three aspects are shown on the left-hand side of the figure: security scanners, use of root accounts and a basic virus protection. All three have their equivalent in ESARIS security standards shown on the right-hand side. The figure shows more detail for the last…

Fig. 58: ICT service specification (standard support) versus ESARIS security standards
aspect: The text in the ICT service specification (left) is a copy or a shortened version of the text specifying the security measure in the ICT Security Standard about computer systems in data centers. The document ID (ESARIS-L4-S14) is indicated but explained later in Chapter 10. There is a complete set of design patterns specifying how this virus protection is implemented. The document ID “ESARIS-L5-S14-xyz” refers to these ICT Security Baselines.

The second example is shown in Fig. 59. Most large companies are organized along business processes though people still belong to legal entities. These business processes are a mixture of processes from general business administration (or Enterprise Resource Planning, ERP), typical business processes and others relating to the life-cycle of the products or services offered by the company. A diagram with such a process map is shown in the upper left of Fig. 59. The upper half of the ESARIS Security Taxonomy (upper right in the figure) relates to the life-cycle activities of the ICT services, more specifically to the IT service management activities.

Fig. 59: Set-up of processes and practices versus ESARIS security standards

The ESARIS security standards provide design patterns (lower right in Fig. 59) that are to be reused. If new processes are designed or existing ones are modified (lower left in the figure), the ESARIS security standards must reflect these additions or changes and vice versa.

There are several reasons for, on the one hand, having security integrated in the portfolio and the process landscape and for explicitly specifying security in ESARIS security standards. First, managing security in a complex environment requires having one defined set of documents which can be looked at and analyzed. Gaps cannot be found if the information is distributed amongst an undefined series of documents which may also be updated or revoked quite independently. That’s why the ESARIS security standards, namely the ICT Security Standards (Level 4), are required even if the same contents would also be part of
process documents. Second, the ESARIS security measures need to be implemented. Therefore, the security aspects need to be described or referred to in the primary process documents. IT personnel will expect all relevant information to be provided by the primary work instructions they are using, either in form of directly workable instructions or as a reference to other such material (e.g. *ICT Security Baselines* (Level 5)). Third, customers need to be informed and to be provided with a complete picture about all relevant security measures in place. Contracts need to have a common basis. Hence, descriptions of security measures are required that are unique, not ambiguous and not providing room for interpretation. This can only be achieved by having one centrally managed set of ESARIS security standards. Note that for the same reason, ICT service specifications are centralized and made available by means of service catalogs. Both the security standards on Level 4 and the service catalogs are highly modular, well-structured and provided in a formalized form.