2 Environment

Introduction and summary: The *Enterprise Security Architecture for Reliable ICT Services (ESARIS)* does not organize all security-related activities in a corporation. For example, all larger corporations including ICT Service Providers require an Information Security Management System (ISMS) for steering the security management by defining the organizational structure and procedures used. Such systems form the so-called *Frameworks for ESARIS* in which ESARIS is embedded (Sect. 2.1). ESARIS concerns only the security of ICT services and not of the corporation as a whole. The two perspectives corporate and ICT service security are discussed in Sect. 2.2 and a general governance model is given further clarifying interdependences with respect of using ESARIS.

Fig. 8 summarizes what ESARIS is about. Note that ESARIS is neither a sole conceptual tool nor a means for planning only. It is a realization of a tool box which provides a classification, organization and standardization schema which will be used by every employee in the company (when it comes to security). It provides a collection of practical security standards designed to meet the needs of a large-scale IT production. It does not only tells what to do, but provides detailed guidance how to do it. The concepts, methods and measures are tried and proven and actually applied in practice.

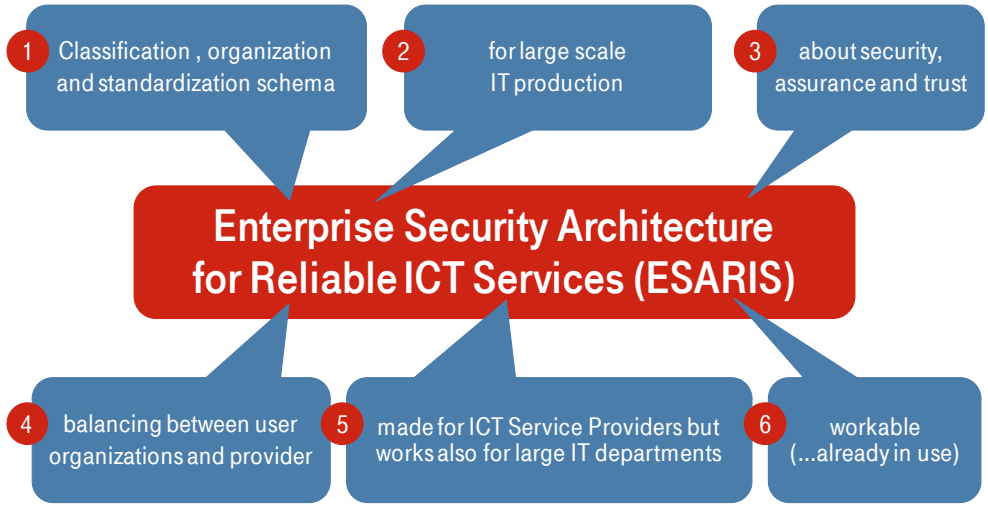

Fig. 8: Characteristics of ESARIS

E. von Faber, W. Behnsen, *Secure ICT Service Provisioning for Cloud, Mobile and Beyond,* Edition <kes>,
DOI 10.1007/978-3-658-16482-9_2

2.1 Frameworks for ESARIS

Introduction and summary: The ESARIS approach – the subject matter of this book – does not cover all the activities within an enterprise that relate to information security and IT risks. Firstly, a security management organization and processes for it on a corporate level are required. This Information Security Management System (ISMS) build or maintain the so-called *Enablement Framework for ESARIS*. Secondly, one must manage the relations to standards, industry and other best practices. The collection and classification of security measures or controls is the subject of the so-called *Endorsement Framework for ESARIS*. This framework also maintains a mapping between all existing security measures from the different sources as required for the Internal Control Framework of the ICT Service Provider and its customers.

An environment and conditions need to be defined in which the *Enterprise Security Architecture for Reliable ICT Services (ESARIS)* is used. The security-related "set of environmental conditions" is referred to below as the "Framework for ESARIS". Other conditions exist, but only those relating to information security are considered in the following.

The Framework for ESARIS consists of two parts (refer to Fig. 9). The *Enforcement Framework for ESARIS* provides the capabilities whereas the *Endorsement Framework for ESARIS* provides input for ESARIS and manages relations to different sources:

- The *Enforcement Framework for ESARIS* can be considered the *Information Security Management System (ISMS)* of the ICT Service Provider since it provides the organization, the processes and other resources and is built to establish, implement, operate, monitor, review, maintain and improve information security. An ISMS which is largely defined in ISO/IEC 27001 [14] is used by many large organizations and implemented on a corporate level.
- The *Endorsement Framework for ESARIS* builds the part that manages relations of ESARIS to norms, industry standards and best practices as well as legislation and regulation. This framework looks in detail at security implementation standards, namely ISO/IEC 27002 [15] or PCI-DSS [16]. It also comprises a mapping between the security measures defined in ESARIS and the security controls stipulated in the environment.

---

[14] ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Requirements, 2013 [5]

[15] ISO/IEC 27002 – Information technology – Security techniques – Code of practice for information security management, 2013 [6]

[16] PCI Standards Council: PCI DSS (PCI Data Security Standard); Version 3.2 as of 2016 [13]

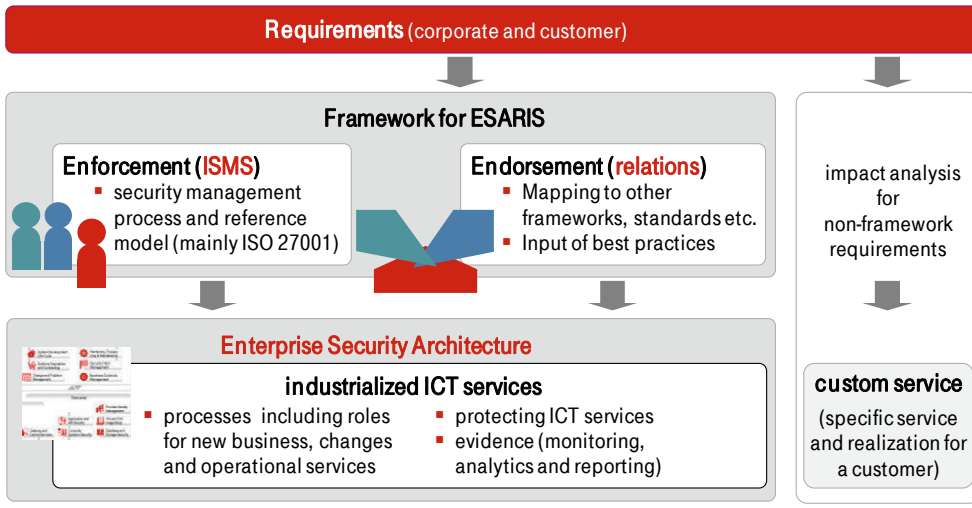

Fig. 9: Role and content of the Framework for ESARIS

The *Endorsement Framework for ESARIS* comprises participating in standardization boards (such as ISO), industry associations (such as the Information Security Forum, ISF, and the Cloud Security Alliance, CSA). It also deals with the analysis of legislation and regulation. As a result, it delivers material for the development of ESARIS and its security standards.

ESARIS is built to fulfill corporate and customer security requirements using predefined controls. It may be, however, that some specific customer requirements cannot be met by controls which are foreseen and selected beforehand. Those requirements are called "non-framework requirements" (right in Fig. 9). In such cases, a business impact analysis is performed in order to decide the following:

- the existing security will be advanced so that the "non-framework requirements" will no longer be "non-framework" ones,
- the customer's request will be rejected,
- a customer specific service will be built.

The modification of the ESARIS security standards will result in an improvement which can be used for subsequent businesses with other customers (case 1). The alternatives are a "no-go decision" (case 2) and a full-custom solution (case 3). Note that a custom solution may or may not balance between security level and costs. However, such a decision can affect the provider's business as a whole. Hence, an impact analysis is necessary and the decision is taken on a rather corporate or board level (refer to Fig. 9).

Though custom solutions are out of the scope of ESARIS, they should be built, as far as possible, using elements taken from the industrialized ESARIS services. A "no-go decision" is not the preferred choice for the customer or the provider. Often there are other ways to solve the problem if special customer requirements cannot

be met by an ESARIS control in the first place. The following example may demonstrate this: The customer requests access to firewall management systems to control specific activities. This request must be rejected due to the ICT Service Provider's policy restrictions. But a customized firewall report can be created for the customer as an alternative and compensating response, so that the user organization is able to get the necessary information about firewall activities. In this case it may turn out that this alternative solution is already covered by ESARIS so that no custom solution has to be built and maintained.

Enforcement Framework for ESARIS

The *Enforcement Framework for ESARIS* is defined, controlled and maintained by the Security Management of the ICT Service Provider on a corporate level. As already mentioned, ISO/IEC 27001 [17] is often used as a basis. This standard defines the same requirements for security management in enterprises of all types and sizes.

The development of the ISMS and its activities can be planned along the "Plan-Do-Check-Act" cycle (PDCA) though such an approach is not described in the standard. Furthermore, this framework ensures that activities are supported through the central provisioning of processes, tools and methods. It provides a foundation for the achievement of an appropriate security level of the enterprise and defines and standardizes activities throughout all departments and units of the enterprise. An example for grouping the activities is shown in Fig. 10.

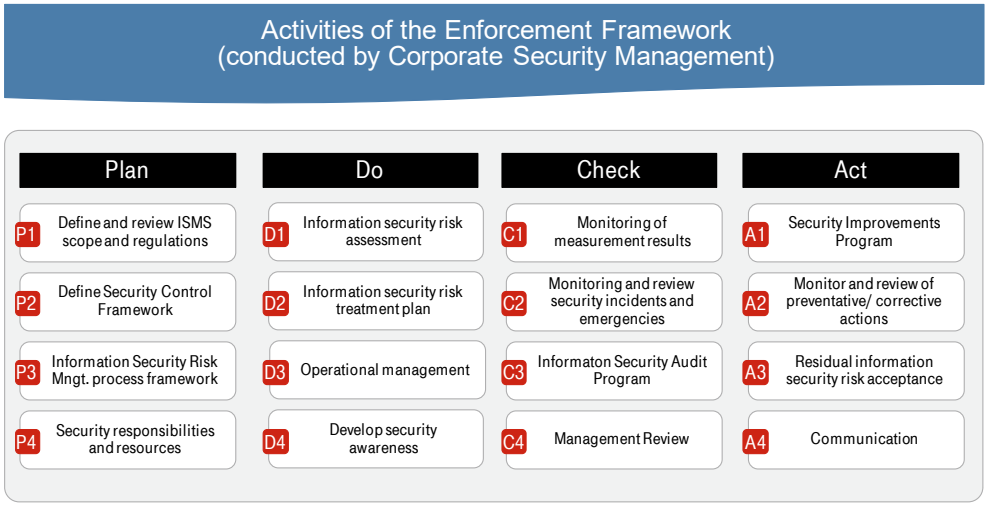

Fig. 10: Activities within the Enforcement Framework for ESARIS

Although most activities are intended to enable the ICT Service Provider to meet security requirements, some activities can also be considered a control. For in-

[17] ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Requirements, 2013 [5]

stance, "developing security awareness (D4)" can enable persons (make them capable) or cause them to act (being a measure).

Endorsement Framework for ESARIS

The framework comprises

- consideration of norms, industry standards and best practices as well as legislation and regulation, and
- mappings between the security measures defined in ESARIS and the security controls stipulated in the environment.

The main sources for best practices are security implementation standards from the ISO (e.g. ISO/IEC 27002 [18]), the ISF (e.g. the SOGP[19]), ENISA (e.g. about cloud computing[20]), the Federal Office for Information Security (BSI, Germany, e.g. IT-Grundschutz[21]), the Cloud Security Alliance (e.g. security guidance[22]), the NIST (e.g. the handbook for managers[23]) and the PCI Security Standards Council.[24] In addition, organizations must adhere to legislation and consider regulation. Moreover, an ICT Service Provider regularly learns from its customers. All these sources are collected and classified as shown in the upper half of Fig. 11. The sources (represented by the braces in the figure) define single security measures (represented by the grey bricks below them). These measures may exist also in other sources whereas specific security measures may be unique to one source.

A main function of the *Endorsement Framework for ESARIS* is to maintain a mapping between all security measures just mentioned (upper half in Fig. 11) with the security measures laid down in ESARIS security standards (lower half in Fig. 11). Such mappings are required for the Internal Control Framework of the ICT Service Provider. The ICT Service Provider can also use the mappings when providing evidence to the customers that their security requirements are met.

---

18 ISO/IEC 27002 – Information technology – Security techniques – Code of practice for information security management, 2013 [6]

19 Information Security Forum (ISF): The Standard of Good Practice for Information Security 2016 [25]

20 European Network and Information Security Agency (ENISA): Cloud Computing Information Assurance Framework; November 2009 [22]

21 Federal Office for Information Security (BSI): IT-Grundschutz-catalogues; Version 13, 2013 [24]

22 Cloud Security Alliance (CSA): Security Guidance; Version 3.0, Nov. 2011 [31]

23 Pauline Bowen, Joan Hash and Mark Wilson: Information Security Handbook: A Guide for Managers, Recommendations of the National Institute of Standards and Technology; NIST Special Publication 800-100, October 2006 (updated 2007) [15]

24 PCI Standards Council: PCI DSS (PCI Data Security Standard); Version 3.2 as of 2016 [13] (PCI: Payment Card Industry)

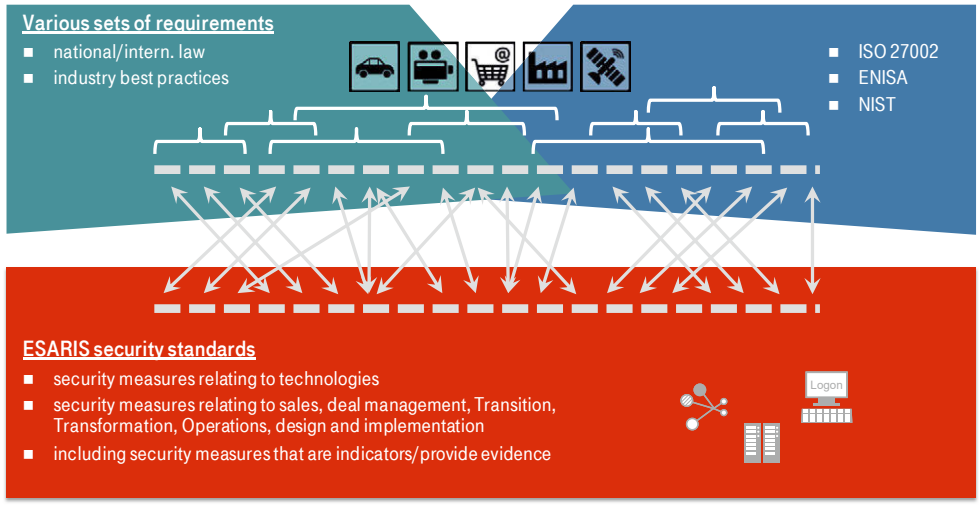

Fig. 11: Endorsement Framework as the mediator from requirements to controls

2.2 Perspectives: corporate versus product security

Introduction and summary: Information security is a discipline that affects many other realms. At a large ICT Service Provider, almost all departments, business processes and the technologies and tools used could have an impact on the achieved level of security and are affected by requirements that relate to information security. Hence, there are several departments and roles that are responsible for reducing risks that arise through the use of ICT. This section looks at two perspectives and distinguishes between the corporate and product perspective, resulting in a Corporate and a Product Security Management. This distinction is necessary since ESARIS focuses on the ICT service or product security only whereas the risk management of the ICT Service Provider must consider product security as one but important element of corporate security.

Leading ICT Service Providers are far too large and complex for strategy and goals to be easy and obvious. They have different departments and the division of labor is very distinct. This makes an organization very powerful, but requires the coordination of different interests. In terms of security, there are two possible perspectives:

- Corporate Security Management
  - which is responsible for the overall security of the enterprise
  - including information security for which an Information Security Management System (ISMS) is operated,
- Product Security Management
  - which is responsible for ensuring that the enterprise's products (and services) are secure and meet the customers' requirements

- using rules and methods from Corporate Security Management as well as those specifically defined for securing products/services.

The situation is shown in Fig. 12.

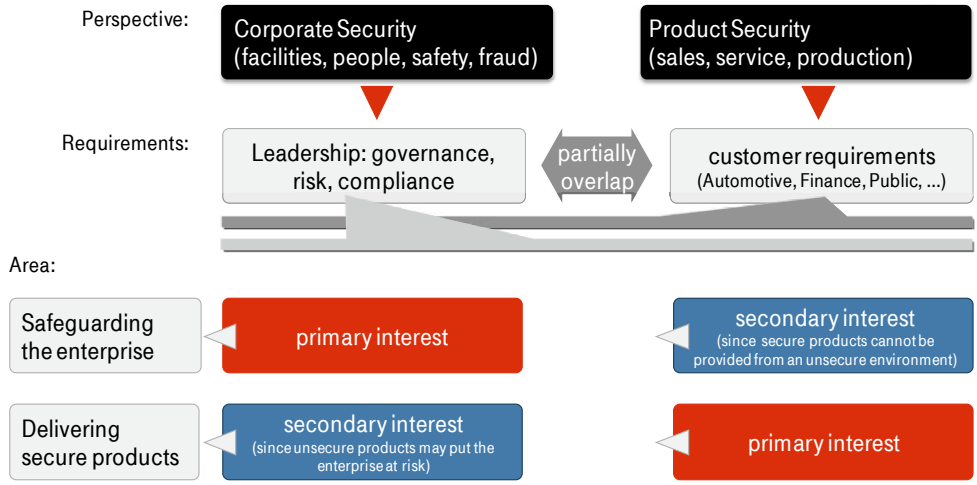

Fig. 12: Two interwoven security perspectives

Corporate Security Management must ensure reliable and efficient leadership and control through the implementation and maintenance of a system for control and regulation as well as corporate organization and processes (Governance). Corporate Security Management must also ensure the systematic identification and assessment of the risks which the enterprise is exposed to and the realization and control of counteracting measures (risk management). Furthermore, Corporate Security Management must ensure adherence to legal and other requirements as well as internal policies and contractual duties (compliance). This task includes the identification, definition and update of regulations as well as their enforcement and control.

Thus, Corporate Security Management is primarily addressing the protection of the enterprise as a whole. Of course, unsecure products or services that are delivered to customers may also put the enterprise at risk and such products or services may lead to noncompliance. Refer to Fig. 12.

An enterprise has several organizational units that are responsible for delivering products or services to customers. The delivery of products and services is the main purpose and mission of an enterprise. Hence, the enterprise must also care for secure delivery and for the security of products and services. The corresponding requirements are considered as those of the customers since they are driven by the business objectives and the market.

Thus, Product Security Management primarily focuses on making products (and services) secure in order to meet market requirements. Of course, weaknesses in the enterprise, e.g. in the way of working in processes, in the organization and in

the tools and other methods that are used, may not allow delivery of secure products (and services). Hence, Product Security Management is also interested in the security of the enterprise as a whole. Refer again to Fig. 12.

The necessity and existence of the two perspectives as well as their interwoven way of working is called *ESARIS Duplex Security Management Concept*. Note that the two perspectives are not distinct from each other. They do overlap.

Fig. 13 shows this situation once again. The left-hand side shows the GRC ("Governance, Risk and Compliance") approach and interests. The business with Product Security Management adheres to the corresponding requirements but must meet the requirements of customers while taking technological and business constraints into account. The right-hand side shows the genuine tasks of the business including the sales, service and production departments, which are responsible to secure product and service delivery. Corporate Security Management generally overrules Product Security Management. Examples are compliance issues (e.g. legislation and regulation). In other cases, conditions and constraints shown in the figure may count: Corporate security requirements may only overrule others if this is possible from a business point of view (e.g. strategy, investment, operating costs, margins).

This principle is called the *ESARIS Governance Model*. The ICT Service Provider's Security Management organization must consider these facts.

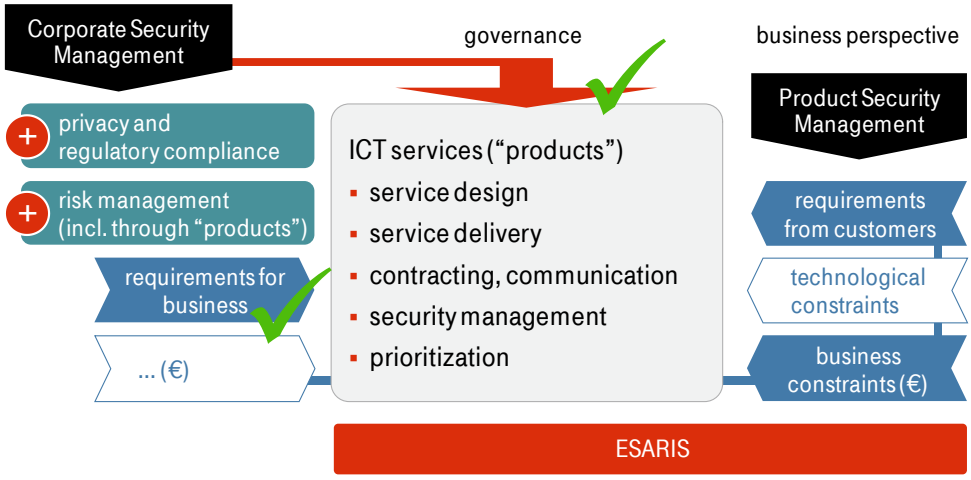

Fig. 13: ESARIS Governance Model

The majority of security measures maintained by an ICT Service Provider are defined, enforced, controlled, improved and maintained for Product Security. Product or service security management is the main focus of ESARIS.

http://www.springer.com/978-3-658-16481-2

Secure ICT Service Provisioning for Cloud, Mobile and Beyond
ESARIS: The Answer to the Demands of Industrialized IT Production Balancing Between Buyers and Providers
von Faber, E.; Behnsen, W.
2017, XIV, 369 p. 159 illus. in color., Hardcover
ISBN: 978-3-658-16481-2