In-House Standardization of Security Measures: Necessity, Benefits and Real-world Obstructions

Eberhard von Faber [1(+2)]

[1] T-Systems
Eberhard.Faber@t-systems.com

[2] Brandenburg University of Applied Science
Eberhard.vonFaber@fh-brandenburg.de

Abstract

The business demands cost reduction, flexible sourcing and customary quality when it comes to getting IT services. Internal and external IT service providers must therefore industrialize their IT production. Industrialization in turn requires standardization of all components in modern IT production. This includes standardizing the security measures that are used to protect the IT service provisioning. Areas and elements are identified that can be standardized. Needs and benefits are described for each. Additionally, this study focuses on real-world obstacles which need to be considered and surmounted in order to secure IT services in an efficient and flexible way. Practical advice is provided to support the standardization of security measures used in-house to protect IT services.

1 Understanding Standardization

First of all it is required to analyze the origin of standardization and the motivation to use standards in general. The term "in-house standardization" is explained. The topic of this paper is further narrowed down by briefly discussing the possible nature of the standards. In the second part of this chapter the term "standard" is defined which is needed in order to discuss benefits later.

1.1 In-house motivation

Many people associate with a standard that they must use it or adhere to it. This understanding leads into the wrong direction. Standards, as being the subject of this paper, are not a "must" – they are not a "law". It is the nature of standards to provide benefits to whom who is using it. As a result, it is simply disadvantageous to ignore the standard. These disadvantages may cause an enterprise to enforce the use of standards and to punish people who are not using them. However, the sequence of causes is important here:

- Standards (as described in this paper) primarily provide benefits such as competitive advantages that should motivate to use them.[1]

1 The obstacles to get these benefits are discussed later.

H. Reimer et al. (eds.), *ISSE 2014 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-06708-3_2,

- If this motivation is not sufficient, enterprises may enforce their use and punish ignorance. We do not assume any external enforcement, pressure or influence.

This is shown on the right hand side in Fig. 1. There are different motivations for standardization such as legislation, regulation or technical reasons which are, however, not considered in this paper. It is assumed that the corporation has an intrinsic interest in standardization of security (raise "competitive advantages"). As a result, the title of this paper refers to "in-house standardization" to emphasize this standardization is driven by the corporation on its own. Standards are based upon agreement. In our context it is sufficient that the agreement holds for one corporation. It is not assumed that the procedure or process is agreed upon or recommended by market players (industry standards) or issued by a standard's organization, the government or any other such authority.

The left hand side of Fig. 1 shows elements that can be standardized. There are two types: real content (called "design patterns") and the way content is provided (called "descriptions"). This paper focuses on standardization of content, i.e. the provisioning of design patterns for security measures that are used by the corporation in order to gain competitive advantages.

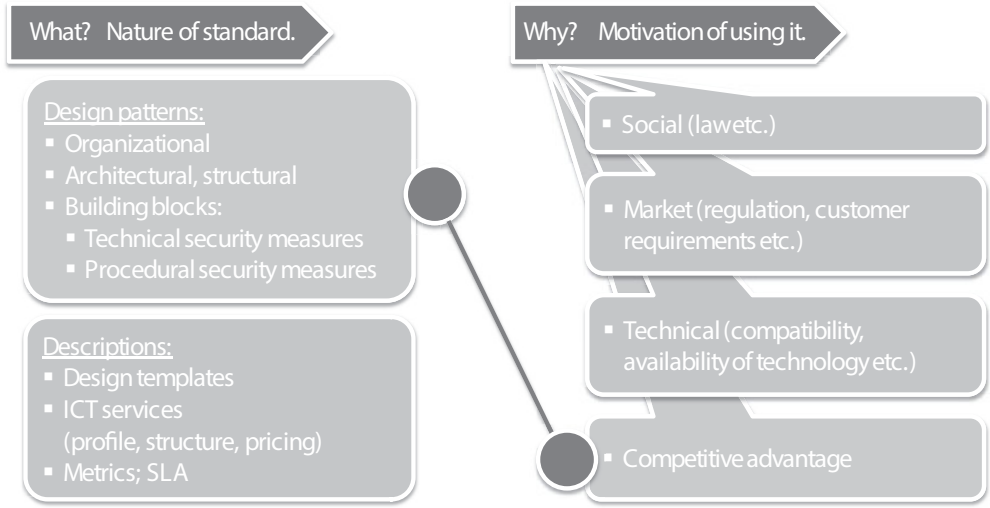

Fig. 1: Nature of standards and motivation to use them

1.2 Definition: standards and norms

What is a standard? The term "standard" is interpreted as something which is

- pre-approved, demonstrably better than other solutions in general and therefore strongly recommended for application and adherence if not prescribed,
- widely recognized or employed, especially because of its excellence,
- preferred and automatically applied as long as there is no serious objection that the standard would not be adequate.

This is shown in Fig. 2. The latter also indicates the opposite of standards. Note that this definition reflects the type of motivation from above: own interests or competitive advantages drive the use

of "in-house standards" (refer to Fig. 1). We do not require specific social or political interests, the need to regulate markets or technical constraints.

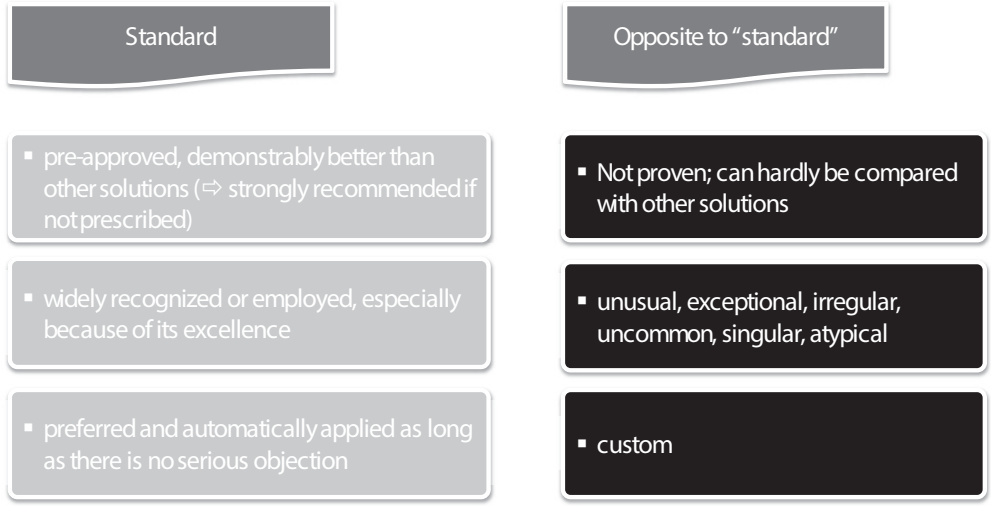

Fig. 2: Standard versus non-standard

Note that the term "norm" has a different meaning. "Norm" rather refers to an average level of achievement or performance, i.e. to a desired status that needs to be achieved. With "standards" one refers to neutral material that is re-used whereas "norm" is not neutral since it rates.

In this paper the neutral term "standard" is used since comparison is not important in our context. The only comparison which can be made is between "standardized" and "not standardized" (or custom). The standardization itself brings the benefits and generates the competitive advantages. This is why this paper is entitled "in-house standardization". It is not important where the standards come from. The motivation for using them is intrinsic: They should be used since they generate value.

2 Necessity and benefits

The above consideration is now applied to standardization of security in an industrial IT production.[2] The term "production" is used in order to emphasize that we only consider the provisioning of IT services on a large scale. IT production is characterized by a high degree of division of labor and by a high degree of specialization of people. The provisioning of the IT services is organized along processes, mostly the ones defined by ITIL[3] or [ISO20000]. Both sources define the IT service management. This chapter describes why standards are to be applied. Hereby necessity and benefits go hand in hand. Refer to Fig. 3 for an overview. The first subchapter describes why standards need to be applied in IT production. The second subchapter describes general outcomes of standardization also of security measures. The third subchapter carves out specific

2 In this paper the term "IT" (information technology) is used. However, this may also include communication services, so that "ICT" (information and communication technology) would have been more precise.
3 ITIL: IT Infrastructure Library

benefits for security professionals namely the CISO.[4] Note that all three parts are important for the CISO since he does his business in a given corporate environment where all the usual business rules and mechanics apply.

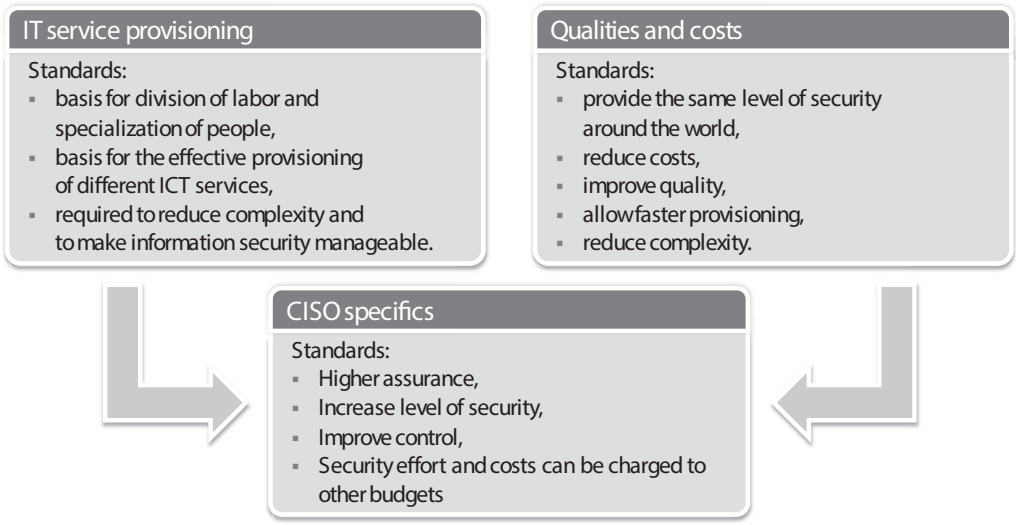

Fig. 3: Necessity and benefits for standardizing security

2.1 Necessity: IT service provisioning

The provisioning of IT services (in an industrial fashion) is of complex nature and characterized by a high degree of division of labor and by the distribution of activities throughout the organization. As a result, many organizational units and business roles have to contribute to protecting the IT services. IT service provisioning on a large scale ("production") requires the standardization of security for the following reasons ([EFWB13b]):

- Industrial production is characterized by a high degree of division of labor and high specialization of people. Industrial production uses defined processes where procedures need to be clearly defined too. This very structured approach requires many elements described in terms of modules (that can often be re-used). Such modules or patterns are the result of standardization. (Perspective: outside-inside.)
- IT service providers mostly maintain a comprehensive portfolio of various IT services including desktop services, communication services, and computing services. The service models (i.e. the division of labor between IT service provider and user organization) may also differ. (Perspective: inside-outside.) Producing these services in an industrial way also requires the modules or patterns from standardization as demanded in the previous bullet.
- Reduction of complexity is required in order to make information security manageable. This is required both to understand and to sell/buy the IT services (perspective: outside-in) and to secure the IT service (perspective: inside-out).

4 CISO: Chief Information Security Officer; head of security in a corporation

Note that in case of large-scale IT production there is a clear split into the demand and the supply side. We call the supply side "IT service provider" regardless if this is an internal or in-house IT department or an external enterprise. We call the demand side "user organization" regardless if this is an enterprise that has outsourced its IT or a business unit that consumes service from its internal IT department. If IT becomes big, it must become an "IT production" which provides IT service on a large scale.

2.2 Benefits: quality and cost improvements

Fig. 2 above provides a "definition" of standards. This definition directly leads to benefits that are produced by standardization. Such advantages are

- Same level of security around the world (important for customers with global business),
- Cost reduction,
- Improved quality,
- Faster provisioning,
- Reduction of complexity.

The first point becomes more and more important. Enterprises are working on a global basis so that they need to use IT services on different continents and in different countries. Though there are local differences in legislation and in industry regulation, global enterprises like to streamline their business as much as possible. This also holds for consuming IT services and for managing IT security risk associated with this. But moreover IT services can be obtained on a global basis. This is a result of deregulation, the rise of global providers and made possible through the development of communication networks and IT.

The reduction of costs (benefit no. 2 in the above list) is the result of re-use which reduces the expenditure or the effort. In modern IT service production scaling effects play an important role. They can only be realized if platforms are identical which in turn requires the implementation of standards.

Improved quality and faster provisioning (no. 3 and 4 in the above list) are also straightforward to understand. Quality is increased since more time and effort can be spent to develop and prove the solution. More experience is available from using it. Faster provisioning is an extra benefit which is very important for the fast-moving information technology and its market. Note that quality is in turn directly correlated to security. Reduction of complexity (no. 5) considerably improves security since complex things are hard to understand and to manage. Simplicity helps to meet the security target.

2.3 CISO specifics

The standardization of security has further benefits that are essential for the security management department and the people being responsible for the security of the IT services, foremost the Chief Information Security Officer. There are at least four benefits or advantages:

- Higher assurance,
- Increase of the level of security,
- Improved control,
- Security effort and costs can be charged to other budgets.

Standardization of security leads to higher assurance. Nowadays user organizations are facing problems obtaining detailed information when investigating the market in order to find third party IT services with the appropriate security or risk profile. They need reliable information about security in order to be able to estimate and manage associated risks. Hence, the IT service providers must deliver appropriate assurance[5] together with their IT services [EvFWB12]. This is made easier or is even enabled through standardization that is as complete as possible.

But more straightforward, standardization increases the level of security. If there are no security standards, the consideration of security maybe left to people with their respective personal opinions and priorities. If using security standards (as security patterns) it is more likely that security is considered at all. Standards also improve the availability of information about the "security". This in turn helps to identify gaps and vulnerabilities. Transparency is essential for an effective security management. Without standards, transparency is hard to achieve in a complex IT production.

Improved control: this fact is very similar. The security management department can concentrate on the standards. The available resources are usually far from being sufficient to control security in a largely heterogeneous environment. In this way, standardization of security also helps to live with the limited resources the CISO may have available.

Good news for the CISO. The security standardization is also a way to integrate security into the day-to-day IT business. This can help the security organization to safe money since the costs are transferred from the security budget to other corporate budgets:

- It is a main principle of ESARIS[6] described in [EFWB13a] that IT security management is integrated with IT service management. One result is that some dedicated security costs become inherent IT costs. Another main principle is: security is everybody's responsibility. This reduces the work load of security professionals.
- However, the main effect of standardizing security are reduced costs for development and maintenance of security measures. The standardization leads to a harmonization of the IT environment which reduces all efforts that are associated with the management of information security.

But security experts should not expect money to be left. Increasing demands will eat up this money. Security experts must standardize security in order to be able to do their job with reasonable quality.

3 What can be standardized

Standardization of security can relate to different kind of things. Examples range from architecture and technical terms all the way to roles and responsibilities and include technical and procedural measures as well. Examples are already shown in Fig. 1. Here we focus on design patterns which comprise:

5 Assurance is the level of confidence that the *ICT service* meets security expectations, more precisely its *security target*. Assurance is established by applying assurance measures (e.g. by following specific security procedures in the life-cycle). Assurance moreover requires providing reliable information about implemented measures and their effectiveness and quality. Therefore, assurance calls for transparency. The reliable information is provided by the ICT service provider and perhaps an external party in addition. The latter can measure effectiveness and quality (third-party assessments).

6 ESARIS: Enterprise Security Architecture for Reliable ICT Services

- Organizational,
- Architectural, structural,
- Terms (also technical ones),
- Building blocks:
  - Technical security measures,
  - Procedural security measures.

The organizational measures comprise principles of governance and control as well as the definition of roles and responsibilities. Basic procedures may also be defined. This is the foundation that organizes the people's activities and ensures that they hopefully cooperate and run in the same direction. Organizational standardization (including principles, roles and responsibilities) aims at providing an environment that is stable over time so that people can get familiar with it and will remain in "best fit status" as long as possible. If the organization and the tasks rapidly change, employees must spend a considerable part of their time to familiarize themselves with the new situation and tasks. Standardization also comprises the definition of roles and job titles which is an often underestimated means for an effective security management.

The application of technical and procedural standards (see below) requires further instruments. The most important instruments (or enabler) for standardization are architecture and agreed technical terms. Technical terms enable people to actually talk about and work on the same subject. Agreed technical terms provide clarity and reduce ambiguity and bias. The architecture provides relations of subjects as well as structure which in turn enable people to cope with the complexity of security and large-scale IT production.

- A main element of ESARIS described in [EFWB13a] is the *ESARIS Security Taxonomy* which has been discussed in [EFWB13b]. This central ordering schema allows IT professionals to cope with security even if they have no or only limited security knowledge.
- Other examples are models that check and approve compliance. The *ESARIS Fulfillment Model* and the *ESARIS Attainment Model* are examples that define a standardized way to build and verify security conceptions [EvFWB12].

The main point and most important area for security standardization is very specific. Corporations must also standardize technical security measures and procedural security measures. These "building blocks" are to be used whenever any process, procedure or IT system or component is designed and set-up. This approach generates an enormous economic value. But moreover it enables the CISO to manage information security in the IT production environment at all.

An example which realizes the above is shown in Fig. 4. The diagram shows the *ESARIS Security Taxonomy* that defines 31 areas described in so-called *ICT Security Standards* (17 more related to technology, 14 more related to overarching aspects and processes). Each area or *ICT Security Standard* defines about 10-20 security measures. Hence, there are about 500 security measures in total. These measures are used to manage the security of the IT services. They are re-used whenever anything is developed or implemented.

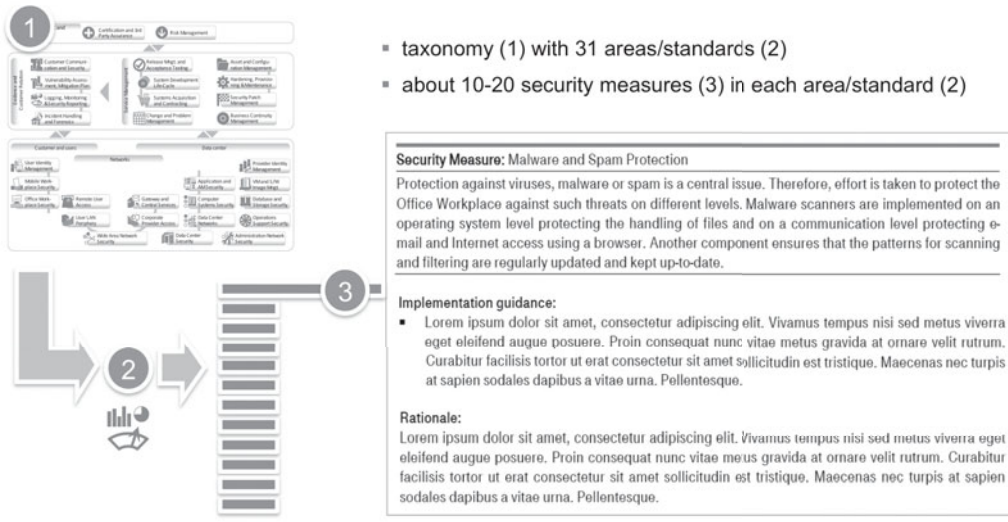

Fig. 4: Taxonomy, standards and about 500 security measures in total

4 Obstacles and solutions

But there are obstacles in the way towards standardization of security measures. These are discussed now. Refer to Fig. 5 for an overview. The obstacles or problems are organized into those which are business related, related to security concerns and those which are related to humans. In other words, business issues hinder standardization of security, human behaviour may hinder standardization of security, but also the aim to increase the security may provide reasons against the standardization of security.

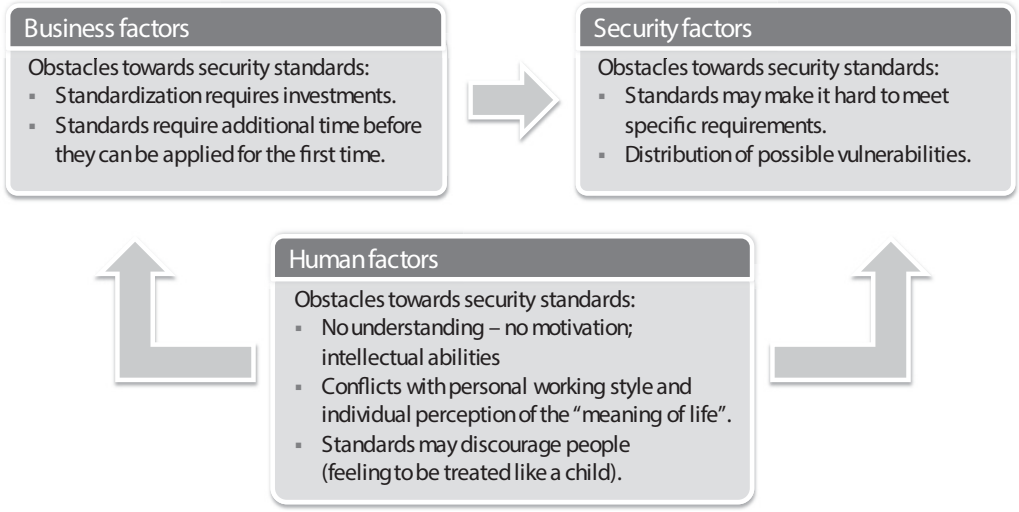

Fig. 5: Obstacles and problems towards standardization of security

4.1 Business factors

Standardization of security requires investments. There are fixed costs before any economies of scale or any other improvement becomes visible. In many cases it is not easy to justify the investments. Everybody seems to know that there is no other way but the go-ahead for the investment in standardization requires a well calculated business case where often only numbers count. In practice, too many people hesitate to develop the business case and some managers are reluctant to make the only reasonable decision. Even more critical, the standardization also means delay. The standards need to be developed and approved before they can be used. This takes time. Ad-hoc implementations are much faster. People tend to prefer fast ad-hoc solutions and the management mostly demands fast completion of projects. Standardization only takes place if the corporation is lucky enough to have an informed management that is also willing to make a decision.

The situation with the business is shown in Fig. 6 (schematically only). The figure shows the function of the total effort spent over the elapsed time. There are two cases: Without standardization the effort decreases only slightly over time. The decrease is due to practice. – Now standardization is considered. The effort is initially higher. But after having elaborated the standards the effort is lower than in the first curve. The area between the two curves indicate the investment and the savings, respectively. These simple graphs show the following:

- Firstly, the CISO must prolong its planning horizon beyond the break-even. If the planning horizon is shorter, no standardization will take place.
- Secondly, the investment costs. No problem if the CISO's budget is increased so that it also covers the extra investments for standardization. But in most cases this will not happen. The only way to master the standardization is a budget shift: Reserve 10% of the total budget or so for standardization. This means stop about 10% of other activities and live with the security chaos (that will not occur). *Alternatively*, oblige every security project and longer lasting security activity to produce about 15-20% results that can be re-used as standards.

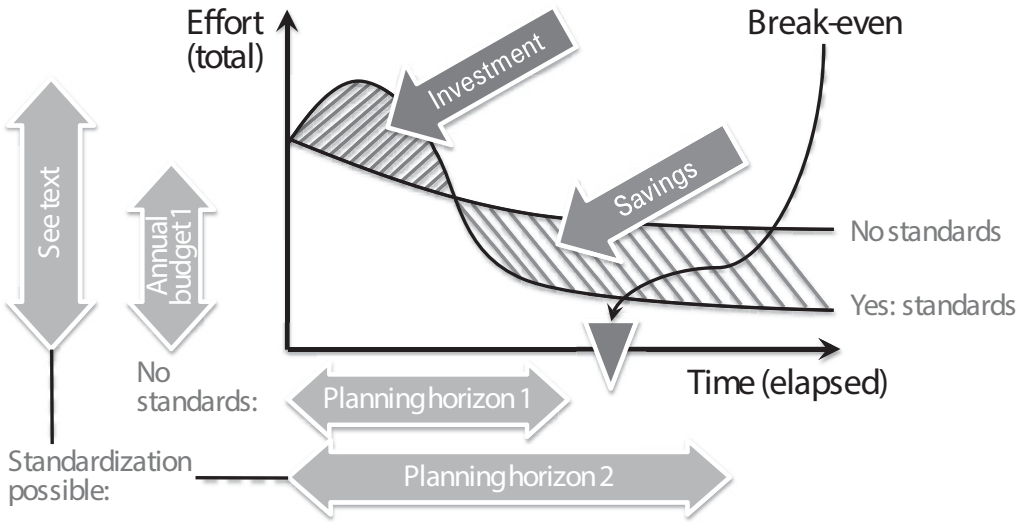

Fig. 6: Standardization as investment

4.2 Security factors

Security concerns may also hinder the standardization of security. The very first and most frequent objection is the lack of flexibility and the belief that requirements cannot be met. To make it short, this is not true. In the 1990ies, user organizations may have insisted that their ideas are exactly realized and their requirements are exactly used as the basis. Time has changed. Cost cutting etc. has lead to a situation where even complex applications are moved to cloud computing environments that are highly standardized and do not provide many options. Optional security measures can be used to meet specific (uncommon) requirements [EFWB13a]. These optional security measures are added to the standardized environment. It's worth noting that these optional security measures are also pre-defined and standardized. That's why the objection is not correct.

In terms of security, standardization is double-edged. On the one hand it raises the quality and strength of a mechanism if it is widely investigated and proven. On the other hand, it is best practice not to put all eggs into one basket. Standardization means using the same technology. If there is, for example, a vulnerability in the technology, the IT service provider gets more vulnerable if the measure is distributed through its IT infrastructure by applying standards. Not without reason, there is the rule to better combine technology or solutions of different manufacturers in order to get a good result. If one fails the other(s) can maintain the security. Note that, however, a standard can exactly define the use of different technologies.

But in fact, the level of security can be decreased when the degree of standardization becomes too high. Fig. 7 (schematically only) shows the degree of standardization and its effect on quality and security.

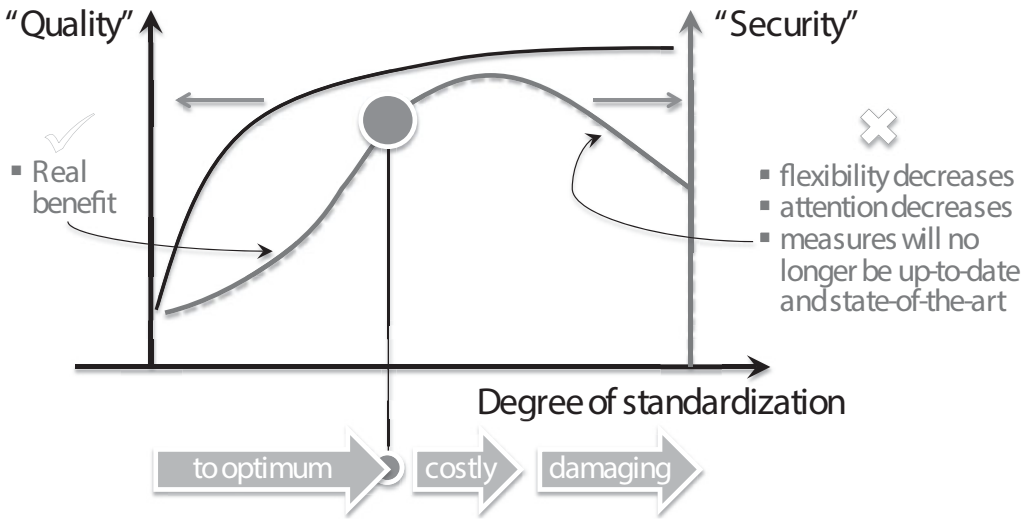

Fig. 7: Quality and security versus degree of standardization

The quality raises with the degree of standardization. But there is a saturation at high values. The "level of security" does not follow this curve directly. There is a delay instead since many things are interwoven in security and need to be fixed altogether. If the degree of standardization be-

http://www.springer.com/978-3-658-06707-6

ISSE 2014 Securing Electronic Business Processes
Highlights of the Information Security Solutions Europe 2014 Conference
Reimer, H.; Pohlmann, N.; Schneider, W. (Eds.)
2014, XIII, 274 p. 100 illus., Softcover
ISBN: 978-3-658-06707-6