The Relationship between Data Protection Legislation and Information Security Related Standards

Martin Meints[1, 2]

[1] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein,
Holstenstr. 98, 24103 Kiel, Germany
ULD61@datenschutzzentrum.de

Abstract. In the last 20 years standards in the context of information security rapidly developed and reached a high level of maturity. Information security also is an important task in the context of data protection, as outlined by the European Data Protection Directive 95/46/EC. However, this Directive does not explicitly relate to standards in the context of information security, security requirements are described quite generally. In this paper it is analysed how on a European level selected standards in the context of information security can be used to fulfill the security requirements described in the Directive 95/46/EC.

Keywords: Directive 95/46/EC, Data Protection Directive, ISO/IEC 27000 series, ISO/IEC 15408, CobiT, ISO/IEC TR 13335-3

1 Introduction

In the Member States of the European Union national data protection legislation is based on the European Data Protection Directive 95/46/EC[3], hereafter called the Directive. Information security measures are referred to by the Directive as an important data protection principle. The Directive describes information security requirements in Recital 46 and Art. 17 only briefly. However, essential requirements for compliance of information security measures with the Directive can be derived from the Recital 46, Art. 17 and – because of special requirements in the case of sensitive data – Art. 8. This text analyses compliance requirements and describes how they can be fulfilled using various standards in the context of information security. In addition it is discussed how far adhering to these standards is necessary to achieve compliance with data protection legislation.

This text is structured as follows: In section 2 general considerations on the relationship between data protection and information security are made, followed by an overview of which security requirements are described in the Directive in section 3. Section 4 gives an overview on information security related standards mainly used in Europe. Section 5 describes which instruments introduced in the standards mentioned can be used to comply with the security requirements described in the

[2] The author wants to thank Diane Whitehouse for her valuable review comments.

[3] Available via http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

Directive. Sections 6 and 7 analyse how these standards relate to state-of-the-art in information security, required by the Directive. The paper closes with a summary and conclusion section.

Please note that "state-of-the-art" in this context explicitly refers to information security in the context of the Directive and is understood as well accepted and established practices by security experts and practitioners. In other technical areas, e.g. operations of applications or operating systems, state-of-the-art may lead to established practices that are from a security point of view clearly not state-of-the-art.[4]

2 General Considerations on the Relationship between Data Protection and Information Security

Data protection and information security are two quite different domains when looking at targets and stakeholders (see e.g. [1]).

Information security mainly is driven by large organisations, with some support by national information security offices (such as U.S. National Institute of Standards and Technology (NIST) or German Federal Office for Information Security). Work in this domain mainly is carried out by technicians with some support by economists. The target of the activity is risk management / risk mitigation in and for *organisations* (governmental institutions/enterprises). As a consequence methodologies and measures developed in this domain are directed towards this target. Increasingly "good" and "best" practice is documented in international standards. In addition to catalogues of technical security measures over the last ten years approaches for integrated Information Security Management Systems (ISMS) and methods for risk assessment and risk treatment have been developed and standardised. These methods and catalogues of technical measures are also increasingly referenced by other domains, e.g. national legislation in the context of financial/tax management, data protection etc.

Data protection is about the protection of fundamental rights of citizens (so called data subjects) and driven mainly by lawyers (with a minor technical support). Risk assessment and mitigation is focused on *data subjects*, not organisations. The results of the risk assessment approaches of information security and data protection may well be conflicting.[5] However, security measures developed to protect the information

[4] An example for this is erasure of data in the context of operating systems and security standards. While state-of-the-art of erasure in operating systems can mean that deleted data basically is hidden from the view of the user and can be restored easily with operating system internal tools or measures, secure erasure in the ISO/IEC 27002 refers to "incineration or shredding [of storage media], or erasure of data for use by another application […]". Indeed the state-of-the-art of secure erasure is not difficult to implement; however, the secure version of erasure is not widely distributed among standard operating systems and applications.

[5] A typical example for such a conflict is the handling of personal data in audit logs. While from the perspective of information security much data may be useful to analyse different

of an organisation also may be effective to protect the data of data subjects and thus to support data protection. These two domains share analyses and understanding and at least sometimes take benefit from each others' experience.

3 Information Security Requirements of the Directive

Among lawyers there seems to be consensus to keep technical details outside European Union (EU) directives, EU regulations and national laws.[6] One important reason is frequent changes in technology requiring a regular update of the corresponding legislation. As security safeguards to a large extent are technically oriented and technically driven in their development, the Directive contains quite general requirements regarding information security. For guidance on concrete implementation data protection relies on other domains of knowledge, e.g. computer science and information security.

Art. 17 of the Directive states the targets of information security which are protection of "personal data against accidental or unlawful *destruction or accidental loss, alteration, unauthorised disclosure or access* […] and against all other unlawful forms of processing". To fulfil this target, "the data controller must implement appropriate *technical and organisational measures* […]". To achieve an appropriate level of information security, (technical) *state-of-the-art, costs*, data protection related *risks* and the *nature of personal data* processed need to be taken into account.

Art. 8 refers to the character of personal data. In this article *special categories of personal data* are described: Data referring to racial or ethnic origin, political opinions, religious or philosophical beliefs, membership in trade unions, health-related data, and data concerning the sex life of the data subject. In Art. 8 it is further stated that Member States shall generally forbid the processing of these data. Cases are described in which processing can be allowed and reference again to suitable safeguards in these cases is made (section 4).

Recital 46 explains Art. 17 and introduces many requirements also to be found later in Art. 17. However, one aspect not explicitly mentioned in Art. 17 is outlined in this Recital: The need to define technical and organisational security measures in a way that they cover the *lifecycles of procedures*[7] in which personal data are processed. Recital 46 refers to "the *time of design* of the processing system and […] the *time of the processing* itself, particularly in order to *maintain security* […]".

The Directive does not provide for a data protection or information security management system. The Directive also does not refer to existing standards. Legal requirements to be met are described, but with respect to the implementation there is

types of attacks over a long period of time, the data minimisation principle asks for a limitation of the amount of personal data stored and the erasure as fast as possible.

[6] See for example [2] for an internationally focused summary on this debate. In the still ongoing debate concerning the modernisation of the German Federal Data Protection Act the integration of concrete technical and management oriented security measures does not play a role at all, see e.g. [3].

[7] In this context a procedure is understood as a governmental or business procedure, covering one or more processes and relating Information and Communication Technology (ICT).

much room for individualised approaches on a national and organisational level. For example the Directive does not suggest whether (a) an integrated management system for security and data protection is required or (b) two separate, but interacting management systems – one for security and one for data protection – can be used. In practice both implementations are commonly found.

The first approach (integrated management systems) seems to be used especially in the public sector and small private companies where security requirements in many cases are mainly driven by compliance with data protection legislation and management resources are limited. This approach has the significant disadvantage of role conflicts between data protection and security management, disabling potentially quality assurance measures.[8], [9] However, for small governmental organisations such as municipalities and small European member states this approach in future will remain relevant. The second approach (separate, but interacting management systems) seems to be implemented frequently predominantly by large organisations in the private sector, especially where security management needs to meet compliance requirements also from other legal or contractual sources (such as the U.S. Sarbanes-Oxley Act (SOX), EuroSOX, contracts with customers etc.).

The Directive also does not refer to other management systems relating to information security management such as Quality Management (e.g. based on the ISO 9000 series) or IT Service Management (e.g. based on the IT Infrastructure Library[10] (ITIL), partly also standardised as ISO/IEC 20000).

National data protection legislation may be more specific concerning security requirements. For example the German Federal Data Protection Act defines eight specific data protection related security goals in the annex to Art. 9.[11] National data protection legislation is not further analysed here as this would exceed the scope of this paper.

[8] In the event of an integrated management system the manager in his data protection role states requirements, implements them in his role as security manager and finally checks in his role as data protection manager whether he himself implemented the requirements sufficiently – the result of this final check is highly predictable. However, this deficiency in the management system can be overcome by additional measures, e.g. regular external audits.

[9] Wherever in this text the masculine gender is used it is meant to encapsulate a person of both genders.

[10] ITIL (Information Technology Infrastructure Library; current version 3.0) is a good-practice Information Technology (IT) Service Management Framework maintained by the U.K. Office for Government Commerce (OGC). ITIL is available via http://www.ogc.gov.uk/guidance_itil.asp.

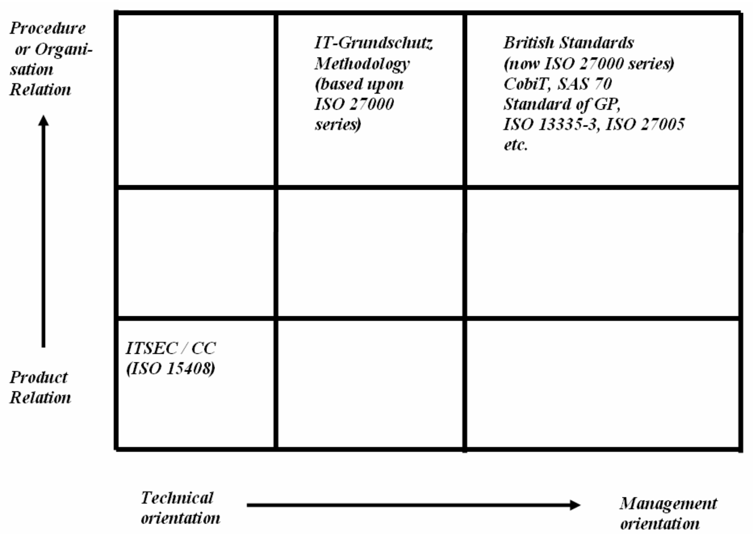
[11] See http://www.bfdi.bund.de/nn_946430/EN/DataProtectionActs/Artikel/Bundesdatenschutzgesetz-FederalDataProtectionAct,templateId=raw,property=publicationFile.pdf/Bundesdatenschutzgesetz-FederalDataProtectionAct.pdf

4 Information Security Related Standards – an Overview

Commonly international security standards refer to three main security goals, referred to as "CIA":

1. **C**onfidentiality,
2. **I**ntegrity (including authenticity and non-repudiation) and
3. **A**vailability.

These standards typically can be classified in three types, based on the orientation toward management or technology on the one hand and the area of application (organisations or products) on the other hand. Figure 1 shows the categorisation of most important standards according to information security:



	IT-Grundschutz Methodology (based upon ISO 27000 series)	*British Standards (now ISO 27000 series) CobiT, SAS 70 Standard of GP, ISO 13335-3, ISO 27005 etc.*
ITSEC / CC (ISO 15408)		

Fig 1: Categorisation of information security related standards based upon [4][12]

Today the most important seem to be the three categories:

1. Information security management systems (ISMS, ISO 27000 series, Standard of Good Practice for Information Security[13], SAS 70[14] etc.), IT

[12] Boxes in the middle are to be understood as "as well category 1 as category 2"

[13] The "Standard of Good Practice for Information Security" is being developed by the Information Security Forum (ISF). The standard is available free of costs via https://www.isfsecuritystandard.com/SOGP07/index.htm.

[14] SAS 70 (Statement on Auditing Standards No. 70) is a certificate for service organisations developed by the (U.S.) American Institute of Certified Public Accountants (AICPA). The certificate contains controls relating to information technology and information security. See http://www.sas70.com/about.htm

Governance Frameworks (CobiT[15]) and methodology standards (especially ISO TR 13335-3 and 27005 for risk assessment and treatment); these standards are kept general with respect to technical security measures.

This means that e.g. the targets of technical and organisational security measures are described in so called "Controls", but the specific technical implementation for operation systems etc. and good practice processes are not specified.

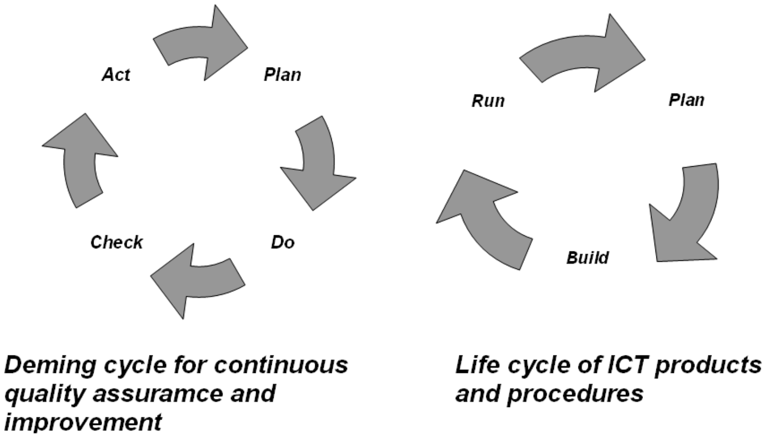
With respect to processes and functional structures ISMS heavily rely on principles and good practice developed in the context of quality management (standardised in the context of the ISO 9000 series). This includes process design (e.g. the use of the Deming cycle[16] for continuous quality assurance and improvement and life cycles of information and communication (ICT) products and procedures and hierarchal process structures containing core and supporting processes), process documentation and improvement (e.g. by use of Key Performance Indicators, KPI).

2. Information Security Management Systems based on ISO 27000 series equipped with a catalogue of technical security measures (e.g. the IT-Grundschutz Methodology of the German Federal Office for Information Security (BSI))[17].
3. Product related security standards with a strong technical orientation (e.g. ITSEC and Common Criteria (ISO 15408)); the Common Criteria contain a number of Security Functions in different classes and families which are to be taken into consideration in product development and operation. Though these Security Functions are described independent of existing implementations, they can be implemented quite concretely.

[15] Control Objectives for Information and related Technology, currently Version 4.1. CobiT is available free of costs via http://www.isaca.org.

[16] The Deming cycle has been established in the context of quality management for more than 50 years, in the context of environment management for more than 15 and in the context of information security management for more than 10 years. All information security management related standards analysed in this text refer to the Deming cycle.

[17] The IT-Grundschutz Methodology contains three BSI standards (BSI 100-1 to 100-3; a fourth standard dealing with business continuity management is in preparation) describing the methodology which is compliant with ISO 27001 and 27005, and the IT-Grundschutz Catalogues (compliant with ISO 27002). These documents are accessible free of costs via http://www.bsi.de/gshb/intl/index.htm



Deming cycle for continuous quality assuramce and improvement

Life cycle of ICT products and procedures

Fig. 2: Cyclic good practice process used in the context of ISMS

5 Standards and Data Protection Requirements

Generally speaking, the standards mentioned are suitable to match the security requirements of the Data Protection Directive. How this could look like in detail, is described in this section.

The security goals referred to in the standards (confidentiality, integrity, availability) are well within the scope of the *security goals* outlined in the Data Protection Directive. To meet the other requirements the approach of two separate but interacting management systems seems to be most suitable [5]. The standards mentioned cover three levels of acting in organisations, namely the strategic (horizon of planning three to five years), tactical (horizon of planning six months to three years) and operational level (horizon of planning up to six months). The following instruments described in the standards mentioned seem especially relevant:

- On the strategic level an *ISMS* covering security aspects of procedures in each phase of the lifecycle. This includes an effective management structure (hierarchy) and good-practice cyclic processes (Deming cycle and lifecycle). Special emphasis in the standards is put on the personal take over of the responsibility for effectiveness of the ISMS by the management of the organisation and *quality assuring measures* (audits). Essential information about the ISMS shall be published in a *security policy*.
- On the tactical level a *security concept* for each procedure, containing (a) a description of the procedure and related ICT (a *network plan* and a *list of assets*[18]), (b) a *risk assessment* and (c) a *risk treatment plan* containing *technical and organisational security measures* (d) a formal declaration that

[18] Assets are understood as anything of value in the context of information processing to the organisation. Assets may contain hardware, software licences, documents and even personal experience, if the information inside people's heads is taken into consideration.

remaining (or residual) risks are taken over by the management of the organisation. Product related security standards may be used especially in the planning phase when hard- and software are selected.
For the risk assessment ISO 27005 provides two methods relevant also in the context of data protection risks. A risk assessment framework established in the context of privacy and data protection is the *Privacy Impact Assessment (PIA),* a methodology described e.g. by Roger Clarke [6]. Parts of the methodology of ISO 27005, e.g. generation and documentation of results, can easily be integrated in PIA framework. In the context of the risk assessment also *special categories of personal data* need to be taken into consideration. In addition in this context the *cost effectiveness* of technical and organisational security measures can be checked and optimised including the impact of these measures on the market (competitive advantage).
- On the operational level an *implementation plan* and *operational documentation* of implemented measures. This documentation is essential as a reference for internal and external security and data protection audits.

6 Security Standards in Relation to State-of-the-Art

State-of-the-art in accordance with the Directive 95/46/EC in the context of information security is difficult to describe. The reasons for this are mainly:

- The Directive does not refer to standards.
- Changes in the environment in which information is processed, especially the technology used, threats to and vulnerabilities in systems, and requirements and targets of organisations do not allow a long term stable evaluation of practice.
- Requirements and abilities of organisations vary largely so that good practice in or for one organisation does not necessarily suit another. In this context in addition to other influencing factors such as (legacy) system infrastructures etc., the size of an organisation is closely linked to its abilities. Large organisations typically can spend more resources on information security compared to small organisations. In addition it has to be taken into consideration that international standardisation mainly is driven by large organisations that are able to spend resources on this task. Existing standards differ in targets. While some of them, especially certification standards, aim at “best practice” and “excellence” and may exceed state-of-the-art, others summarise “good practice” and state-of-the-art. Important differences between good practice standards and certifications standards are e.g., an explicit (and provable) management commitment, an effective management system containing function bearers able to enforce security, sufficient resources and effective processes, application of a risk assessment methodology compliant to ISO 13335-3 or 27005, and completeness and quality in covering the security controls (or security functions) listed in the standards.

As a result there can be no general and homogeneous judgement as to how standards relate to state-of-the-art. In this section an attempt to classify the most relevant standards relating to information security as “is state-of-the-art” or “is exceeding state-of-the-art” is presented.

6.1 The ISO 27000 Series

The ISO 27000 series contain a number of standards with different targets. As shown in Fig. 3, the standards in the ISO 27000 series can be categorised[19] in three classes (see white boxes):

1. Terminology (aiming at a standardised vocabulary),
2. Requirements containing standards for certification (ISO 27001: ISMS in organisations) and accreditation (ISO 27006: requirements auditors have to meet in order to get certified and licenced with a certification body),
3. Guidance standards, containing good practice and methodologies (currently ISO 27002 “Code of Practice”, containing control objectives and controls together with guidance relating the implementation of the controls and ISO 27005 “Information Security Risk Management”, describing essential elements of a risk management process and related tasks. In addition ISO 27005 describes how qualitative and quantitative risk assessment can be carried out and provides examples for the application of these risk assessment methods.)

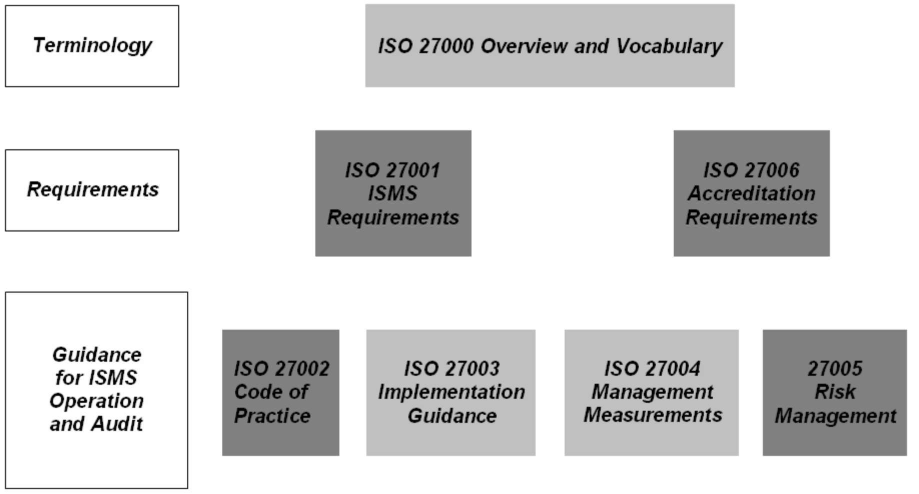

Terminology
ISO 27000 Overview and Vocabulary
Requirements
ISO 27001 ISMS Requirements
ISO 27006 Accreditation Requirements
Guidance for ISMS Operation and Audit
ISO 27002 Code of Practice
ISO 27003 Implementation Guidance
ISO 27004 Management Measurements
27005 Risk Management

Fig. 3: Overview on existing and planned standards in the ISO 27000 series (non-comprehensive overview)[19]

[19] This categorisation was presented by the German Federal Office for Information Security in the ISO 27001 auditors training 2007 and 2008 (documentation not publically accessible).

While the standards in dark grey boxes already exist, the standards in light grey boxes are still in preparation.

The standards in the categories 1 (terminology) and 3 (guidance) aim at “good practice” and state-of-the-art. They allow an adaptation of the implementation of technical measures and methods to the specific requirements of different types of organisations.

The standards in the category 2 (requirements) aim at certificates and “best practice”. They exceed partially state-of-the-art (e.g. ISO 27001 in the completeness of documentation and the implementation of controls), while other parts, especially the design and implementation of ISMS, clearly describe “good practice”. However, partial implementation of the ISO 27001, especially when carried out by small organisations, still can be state-of-the-art.

6.2 IT-Grundschutz Methodology

The IT-Grundschutz[20] Methodology consists of three important parts:

- The description design an operation of an ISMS in compliance with the ISO 27001,
- A specific risk assessment approach based on qualitative risk assessment as described in ISO 27005,
- The IT-Grundschutz Catalogues, a collection of risks and technical and organisational security measures. This catalogue is based on ISO 27002, but exceeds this standard in technical concreteness and reference to existing implementations e.g., concerning operating systems and applications.

The reference to the IT-Grundschutz Methodology and the content of the IT-Grundschutz Catalogues can be considered to be state-of-the-art.

For the IT-Grundschutz Methodology also a certificate issued by the German Federal Office for Information Security is available, based on ISO 29011 and ISO 27006. This certificate again aims at “best practice” and exceeds state-of-the-art.

6.3 CobiT

CobiT is designed as an IT governance framework and currently does not support the certification of organisations. CobiT essentially is a collection of relevant control objectives and controls exceeding the scope of the ISO 27002 by integrating aspects of IT service management and quality management. Full and partial implementation of CobiT also can be considered to be state-of-the-art.

[20] The IT-Grundschutz Methodology, formerly and unclearly translated as baseline protection methodology, is an approach to start the development of a security concept with an initial set of security measures, covering for a “standardised” organisation a related set of initial risks sufficiently. The concretely needed security level for a “real”, existing organisation is derived from this initial security level in a qualitative risk assessment.

6.4 ISO 13335-3, now ISO 27005

This standard was withdrawn in June 2008, as the security standards were being restructured by ISO and the content was modernised and shifted to ISO 27005. Both standards describe different methods for carrying out risk assessments and risk treatment. This includes three methods for risk assessment for organisations:

- qualitative,
- quantitative risk assessment, and
- the baseline protection approach.

The qualitative risk assessment contains the evaluation of risks for an organisation based on a qualitative estimation (e.g. based on a scale from 1 to 5) of potential impact and likeliness or frequency of occurrence. Based on an organisation specific risk policy, a decision is made whether the risks analysed are acceptable or not (in the latter case they need to be dealt with).

The quantitative risk assessment provides a method to evaluate risks as an Annual Loss Expectancy (ALE). In case these losses are not acceptable, a treatment of the corresponding risks is required.

The baseline protection approach in the originally described way is not supported in ISO 27005 any more. The successor methodology, the IT-Grundschutz Methodology, is a qualitative risk assessment approach.

In the event that risks are not acceptable, four different treatment options can be chosen:

- Reduction of risks by technical and organisational security measures aiming at the reduction of the likeliness to occur or the reduction of the impact in case an incident happens until the remaining risk is acceptable;
- Avoidance of risks e.g. by redesigning the system to avoid existing threats or vulnerabilities;
- Transfer of risks, typically by insuring them; or
- Acceptance, in which the risk turns into a remaining or residual risk.

In practice these options also can be combined. Frequently risks are reduced by implementing organisational and technical security measures and then the remaining risk is transferred e.g. to an insurance company.

The application of the described risk assessment methods can be considered to be state-of-the-art in security. However, these methods also can be applied in the context of specific privacy and data protection risks and can be used in the context of the Privacy Impact Assessment (PIA, [6]) as well.

6.5 Common Criteria (ISO 15408)

The Common Criteria (CC)[21] are designed as a certification standard for information security related products. Today relatively few products are certified only, so that the existence of CC certificates cannot be considered to be state-of-the-art. In addition the manufacturer applying for a CC certificate has a significant influence which security functions are assessed on which level in the certification process. As a result the sheer existence of a CC certificate does not mean that the product is suited for any thinkable application in the area of certification. More precisely, CC certificates need be evaluated carefully when looking for security solutions. Nevertheless, if suited to the purpose for which they are meant to be used, CC-certified products should be preferred in the context of procurement procedures.

The CC also provides an overview on security functions categorised in so called classes and families relevant for certified products. One example for this is the family FAU_GEN summarising security requirements for audit logging in applications [7]. These security functions also can be used in the context of procurement or development of own solutions. They can be classified as state-of-the-art.

6.6 Summary

The following table sums up how the standards analysed relate to state-of-the-art:

Standard	**Content and remarks**	**Considered to be state-of-the-art in security**	**Considered to exceed state-of-the-art in security**
ISO/IEC 27001	Information Security Management Systems (ISMS)	X (partial implementation, especially concerning hierarchy and processes of the ISMS)	X (certificates)
ISO/IEC 27002	Code of Practice, catalogue of generic information security measures	X	
ISO/IEC 27005	Information Security Risk Management	X (risk assessment methods also can be applied in the context of data protection risks and the Privacy Impact Assessment (PIA))	
ISO/IEC	Accreditiation		X (certificates)

[21] Currently (November 2008) CC version 2.3 are standardised as ISO/IEC 15408 while the current version 3.1 still is in the standardisation process at the International Organization for Standardization (ISO).

27006	Requirements; covering certificates for auditors and requirements for Certification Bodies (CBs)		
ISO/IEC TR 13335-3	Risk Assessment Methodology; withdrawn in June 2008	X (see ISO/IEC 27005)	
IT-Grundschutz Methodology	Three BSI-Standards and the IT-Grundschutz Catalogues	X (ISMS, risk assessment methodology and security measures in the Catalogues)	X (certificates)
CobiT V4.1	IT governance framework	X	
ISO/IEC 15408	Security certificates and protection profiles for ICT products	X (security functions)	X (certificates)

Tab. 1: Overview of the categories of standards analysed

7 State-of-the-Art in Relation to Security Standards

One question in the relationship between state-of-the-art and security standards is still open: Can state-of-the-art be fulfilled without – possibly unwittingly – making use of the content of these standards? The answer clearly is no. Today there seems to be no good technical or management practice that completely does not either relate to or map with the standards mentioned. This is also true for security white papers concerning products, manufacturers, or vendors' issues for their customers, as they refer at least implicitly to standards. The reference in many cases is quite explicit when looking into the IT-Grundschutz Catalogues, as reference to established products in the context of operating systems and applications is made. Examples which come from the white papers can be found for example in the context of networking equipment, operating systems or multi-purpose printing devices.[22] But in some cases the link to the standards mentioned is not made explicitly in the security white papers. It is often up to the readers to establish these links.

[22] See e.g. https://secure.sophos.de/security/whitepapers/index.html (Virus protection solutions by Sophos), http://www.microsoft.com/Downloads/details.aspx?FamilyID=90ec8abb-08c7-4706-b730-9a1f9fcf2d9f&displaylang=en (Microsoft Windows Vista, especially the integrated "Windows Security Center") and http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml (VLAN Security White Paper for Cisco networking devices)

8 Summary and Conclusions

Regarding information security, the Data Protection Directive 95/46/EC contains general requirements only. The international standards for information security and related management systems investigated here can be used to implement these requirements. However, as the Directive does not refer to standards, the fulfilment of the security requirements listed in the Directive is possible without directly and explicitly referring to information security related standards. In addition, standards aiming at certification of management systems or products exceed state-of-the-art when they are implemented completely, as they aim at “best practice”. Today these certificates are not requested by Data Protection Commissions as a proof of compliance with security requirements set up in relation to the Data Protection Directive.

Nevertheless, explicit or implicit reference of security measures implemented to proceedings and guidance provided by international standards can be considered to fulfil the state-of-the-art requirement of the Directive. On the other hand, the state-of-the-art implementation of the Directive in complete avoidance or violation of the content of these standards today seems to be impossible.

So far a Europe wide harmonised guidance on how to use information security related standards in the context of the implementation of the Directive does not exist. In the interest of the harmonisation of the European market this could well be a worthwhile task. But how could it be achieved?

In the context of harmonisation of the implementation of data protection in Europe the Article 29 Data Protection Working Party (Art29DPWP)[23] is important; it is composed of national Data Protection Commissions and other authorities (e.g. on a federal state level). Harmonised guidance on the application of data protection legislation typically is given in so called “Working Papers”. A Working Paper on the application of information security related standards could help to give the guidance missing so far. This paper could serve as a contribution to such a Working Paper. Clearly, this issue (and thus the Working Paper) needs to be reconsidered regularly, as standards (and, of course, the technical background) change.

Another approach currently is taken in the European initiative “EuroPrise”[24], offering a European Privacy Seal for products and services. In this context a catalogue of technical criteria was developed based on information security related standards. Targets of Evaluation (ToE) need to fulfil the requirements of this catalogue in order to gain the privacy seal. The maintenance of this catalogue is planned to be supported by the so called “European Privacy Seal Board”. To guarantee European coverage and acceptance of this seal the establishment of this board in close connection to the Art29DPWP, e.g. as a sub-working group, could be a good approach which would ensure the coherence of this catalogue with the suggested Working Paper and other European standardisation approaches in the area of data protection.

[23] See http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm for an introduction, an overview on current members and adopted Working Papers.

[24] See https://www.european-privacy-seal.eu/

References

1. German Federal Data Protection Commission (ed.), Data Protection Module for the IT-Grundschutz Catalogues, Berlin 2007. Available via http://www.bsi.de/gshb/baustein-datenschutz/index.htm
2. Dumortier, J., 'Hat das Fachgebiet "Recht und Informatik" noch Zukunft?' In Taeger, J., Wiebe, A. (eds.), Informatik – Wirtschaft – Recht; Regulierung in der Wissensgesellschaft, pp. 59-70, Nomos Verlag, Baden-Baden 2004.
3. Roßnagel, A., Pfitzmann, A., Garstka, H., Modernisierung des Datenschutzrechts, Opinion by order of the German Federal Ministry of Interior, Berlin 2001. Available via http://www.computerundrecht.de/media/gutachten.pdf
4. Initiative D21, IT-Sicherheitskriteriensysteme im Überblick, Bonn, Germany 2001.
5. Müller, G., Wohlgemuth, S. (eds.), FIDIS Deliverable D14.2: Study on Privacy in Business Processes by Identity Management, pp. 42-47, Frankfurt a.M., 2007. Available via http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp14-del14.2-study_on_privacy_in_business_processes_by_identity_management.pdf.
6. Clarke, R., Privacy Impact Assessment, Canberra, Australia 1998. An updated version of this text is available via http://www.anu.edu.au/people/Roger.Clarke/DV/PIA.html
7. Meints, M., Thomsen, S., "Protokollierung in Sicherheitsstandards," Datenschutz und Datensicherheit, vol. 31, no. 10, pp. 749-751, Vieweg-Verlag, Wiesbaden 2007.