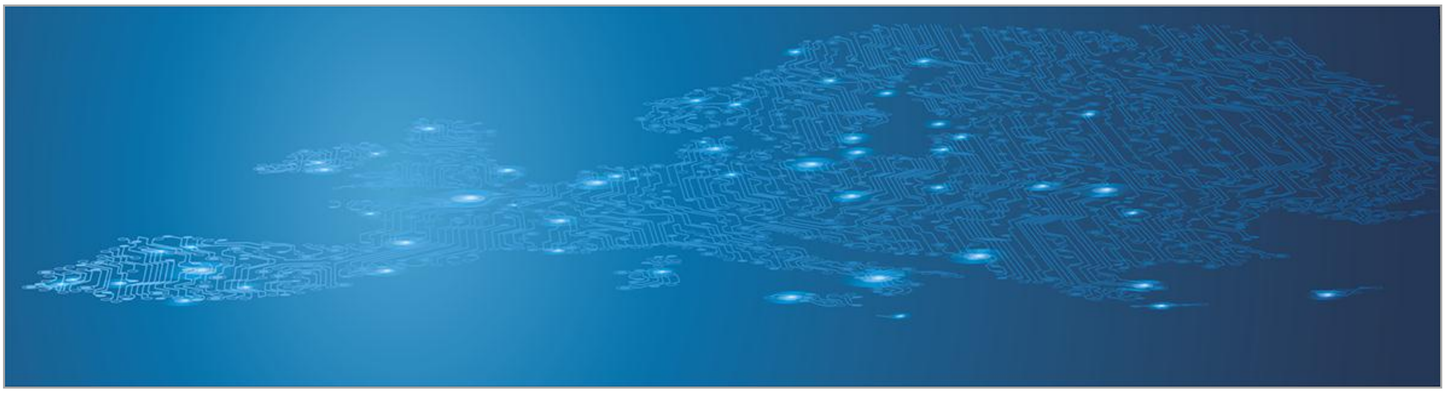

Security certification practice in the EU

Information Security Management Systems - A case study

Version 1, October 2013

European Union Agency for Network and Information Security

www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contributors to this report

This work was partly commissioned by ENISA under the contract ENISA P/18/12/TCD Lot 1, to time.lex. Contributors: Eleni Kosta (time.lex), Jos Dumortier (time.lex), Hans Graux (time.lex).

ENISA project manager: Rodica Tirtea

Acknowledgements

We would like to extend our gratitude to:

- The national correspondents and respondents to the survey for their collaboration.
- The reviewers for their comments, suggestions, feedback.

We also thank a number of people for providing anonymous input.

Contact

For contacting the authors please use sta@enisa.europa.eu .

For media enquires about this paper, please use press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

Table of Contents

1 Executive summary

The recently published Cybersecurity Strategy of the European Union[1] states the need to develop industrial and technical resources for cybersecurity. Among the actions it is mentioned that "*prime focus should be to create incentives to carry out appropriate risk management and adopt security standards and solutions, as well as possibly establish voluntary EU-wide certification schemes building on existing schemes in the EU and internationally*" [2].

This study focuses on two *objectives*: The first objective is to provide expertise from other certification areas to the reform of the European data protection legislation[3], as the new proposed legislation identifies privacy certification as a means to achieve implementation of data protection requirements. The second objective is to identify, based on existing knowledge, recommendations and steps to be followed for achieving the objectives of the aforementioned EU cyberstrategy, namely the development of voluntary EU-wide certification schemes building on existing schemes in the EU. In order to collect experiences from existing certification schemes and given the broad range of existing certification schemes, this study addresses Information Security Management Systems (ISMS) certification.

For the collection of practical experiences of private companies and public organisations for Information Security Management Systems certification a survey was conducted. Based on the available resources, the survey was carried out in a set of Member States (MSs), which account more than 50% of EU population and covered Austria, Belgium, France, Germany, Italy, the Netherlands, Poland, Spain, Sweden, Slovakia, United Kingdom.

The survey provides information on existing accreditation bodies and schemes and on certification bodies and schemes. Further to this administrative perspective, based on the available resources we identify the current practice on the basis of two interviews carried out with one company of the private sector and one organization of the public sector in each surveyed country. Based on the collected information, this study provides a qualitative analysis of certification practices in the area of Information Security Management Systems. Further work will provide a quantitative perspective on the practice in the area of certification by considering a larger sample of companies, which are selected using statistical methods, and such work should not be focusing only on ISMS certification.

Some of the findings of the survey are introduced here:

- In certain MSs national legislation requires information security certification in specific sectors, such as public healthcare.
- National authorities are encouraging the implementation of certification processes for ISMS (e.g. by introducing specific information security certification requirements in case of participation in public procurement).
- Based on the survey, the large majority of companies that own a security certificate consider this as useful for their functioning, as the certification process ensures a regular and systematic identification of risks and evaluation, etc. and also provides competitive advantages.

Between the recommendations of this study are:

[1] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN(2013) 1 final, 7/2/2013, (last accessed on 23.09.2013), available at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667
[2] ibid, p. 12.
[3] European Commission, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 25 January 2012, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last accessed on 23.09.2013)

- There are limitations in the statistics on existing certification processes. **We recommend that policy makers (i.e. the European Commission in case it is regulating the area) or the responsible authorities (i.e. national supervising authorities in the area of accreditation and certification) should demand reliable statistics on certification. The bodies issuing certificates should keep updated public records on certificates that they have issued, on the specific version of products/systems they certified including information on the validity of the certificates.**
- Introducing and possibly *requiring an additional certification related to privacy may be cumbersome especially for SMEs.* **Under the lead of the European Commission, standardization bodies, and responsible stakeholders should work together to develop best practices and standards combining the requirements for security and data protection in order avoid duplication of work for the two certification areas.**
- There is a well-established legislation regarding accreditation and certification in the MSs. **When considering introducing certification for other purposes, i.e. for privacy/data protection, the European Commission together with national policy makers should link such initiatives with existing national accreditation structures.**
- Companies should not be able to get certificates without really having implemented the processes and controls that have been written down in the audited documents. **The national policy makers should ensure enforcement of such requirements for genuine compliance for instance by applying sanctions and/or ad-hoc assessments carried on by third parties.**

2 Introduction

The recently published Cybersecurity Strategy of the European Union[4] states clearly the shared responsibility of all stakeholders and the need for all actors to protect themselves in the context of growing dependency on information and communications technologies. The need to develop industrial and technical resources for cybersecurity is mentioned among the strategic priorities and actions, and in this context "*prime focus should be to create incentives to carry out appropriate risk management and adopt security standards and solutions, as well as possibly establish voluntary EU-wide certification schemes building on existing schemes in the EU and internationally*" [5]

This report aims at providing input for the adoption of a framework on privacy certifications[6], as well as for eGovernment certification in Europe. There are numerous IT security certification schemes across the European Member States that can serve as the basis for the drawing of recommendations on aspects of security certifications that could be applied to privacy and eGovernment services certification. This study addresses Information Security Management Systems (ISMS) certification. An *Information Security Management System* (ISMS) is a systematic approach to managing sensitive company information so that it remains secure. It encompasses people, processes and IT systems.[7]

This study focuses on two *objectives*: The first objective is to provide expertise from other certification areas to the reform of the European data protection legislation[8], as the new proposed legislation identifies privacy certification as a means to achieve implementation of data protection requirements. As such, this study aims at providing 'lessons learned' from security certification to be used for the purpose of developing privacy certification & privacy seals and to support, according to the Work Programme of ENISA[9], related activities initiated by DG JUST and JRC[10]. The second objective is to identify, based on existing knowledge, recommendations and steps to be followed for achieving the objectives of the aforementioned EU Cyber Security Strategy, namely the development of voluntary EU-wide certification schemes building on existing ISMS schemes in the EU.

In order to achieve the goals the report examines current practices regarding security certification in the European Union and provides a short overview of existing information technology security certification schemes in a selection of European Union Member States. In order to collect practical experiences from certification, a survey was carried out on the experiences of private companies and public organisations for ISMS certification. The survey was based on the collection of information

[4] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN(2013) 1 final, 7/2/2013, (last accessed on 23.09.2013), available at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667
The European Commission, the High Representative of the Union for Foreign Affairs and Security Policy, have published a cybersecurity strategy for the European Union. The cybersecurity strategy provides a list of priorities and actions aimed at enhancing cyber resilience of information systems, reducing cybercrime and strengthening EU international cyber-security policy and cyber defence, while promoting values of freedom and democracy and ensuring the safely grow of digital economy.

[5] ibid, p. 12.

[6] In the context of this report certification consists of the "attestation, by an independent third party assessment, that certain requirements and best practices are being observed"[6].

[7] http://emea.bsi-global.com/InformationSecurity/Overview/WhatisanISMS.xalter.

[8] European Commission, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 25 January 2012, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last accessed on 23.09.2013)
The European Commission proposed a regulation on data protection that will replace the existing Data Protection Directive. The proposal for the new regulation contains specific provisions relevant to certification, data protection seals and marks. *"[…]the Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks*".

[9] ENISA Work programme 2013, available at: http://www.enisa.europa.eu/publications/programmes-reports/work-programme-2013 (last accessed on 23.09.2013). See section 3.4.5 "Enabling the Information Society".

[10] EC, JRC, EU privacy seals project, Inventory and analysis of privacy certification schemes, 2013, available at: http://bookshop.europa.eu/en/eu-privacy-seals-project-pbLBNA26190/

from eleven EU Member States, namely Austria, Belgium, France, Germany, Italy, the Netherlands, Poland, Spain, Sweden, Slovakia, United Kingdom. Based on available resources for this study, we aimed at having a representative sample of EU Member States, accounting for over 50% of the European population. These Member States represent different legal, administrative and socio-political cultures and ensure an adequate population and geographic coverage.

2.1 Background

In January 2012, the European Commission presented its proposals for the reform of the data protection legal framework of the European Union, proposing the replacement of the Data Protection Directive with a Regulation[11] (hereafter 'draft Regulation'), which was the outcome of consultation and debates of three intense years. The draft Regulation introduces in Article 39 the possibility for the Member States and the Commission to establish data protection certification mechanisms and data protection seals and marks. Such certification mechanisms are seen as transparency mechanisms that will ensure compliance with the rules contained in the draft Data Protection Regulation "allowing data subjects to quickly assess the level of data protection of relevant products and services"[12]. More specifically Article 39 - "Certification" - reads as follows:

"1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.
2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.
3. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2)."

Based on the requirements mentioned in Article 39 of the draft Regulation, this study aims at providing 'lessons learned' from security certification to be used for the purpose of developing privacy certification & privacy seals and to support, according to the Work Programme of ENISA[13], related activities initiated by DG JUST and JRC[14].

This survey is complemented with a paper addressing the security and usability issues of trust indicators on websites, more concrete analysing the human behaviour and interaction with seals, trustmarks, and indicators[15].

2.2 Description of the survey

The area of Information Security Management Systems certification schemes is very rich. Therefore a survey on the Information Security Management Systems (ISMS) schemes and practical

[11] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the Protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final - 2012/0011 (COD), 25.01.2012.
[12] Recital 77 draft Data Protection Regulation.
[13] ENISA Work programme 2013, available at: http://www.enisa.europa.eu/publications/programmes-reports/work-programme-2013 (last accessed on 23.09.2013). Seee section 3.4.5 "Enabling the Information Society".
[14] Link to JRC/DG JUST project on privacy seals.
[15] The paper will be available at: http://www.enisa.europa.eu/activities/identity-and-trust/library/publications

experiences was carried out, the outcomes of which can be used as the basis for the development of privacy and data protection certification schemes that are promoted by the European Commission. The survey was based on the collection of information from eleven EU Member States, namely Austria, Belgium, France, Germany, Italy, the Netherlands, Poland, Spain, Sweden, Slovakia and the United Kingdom. Based on available resources for this study we aimed at having a representative sample of EU Member States, accounting for over 50% of the European population. These Member States represent different legal, administrative and socio-political cultures and ensure an adequate population and geographic coverage.

Austria and **Germany** are two countries with an Austrian-German legal system. **France** has a strong continental Napoleonic law tradition, while the **United Kingdom** is the largest common-law country in the European Union. **Italy** and **Spain** are two countries from the South of Europe. **The Netherlands** and **Belgium** are two Northern European countries, while **Sweden** is a Scandinavian country. Finally, **Slovakia** and **Poland** are two Central European countries.

These countries form an interesting mix of experiences with ISMS, and furthermore contain both common law and continental law, western and central European jurisdictions on larger and smaller territories.

The information was collected through a questionnaire that was dispatched to and collected from a selected list of representatives in these Member States (see Annex I). Besides providing the legal background and an overview of accreditation bodies and certification practice in the selected MSs, the national representatives carried out two interviews. The national representatives selected one company from the private sector and one organization from the public sector in each surveyed country, using their expertise, choosing from entities that were subject to certification. Although the number of interviews will not allow for general findings, they do provide a good indication of current practices in the area of ISMS certification. The answers focused on providing information

a) on the number and type of organisations accredited under ISMS certification,

b) on the number and type of organisations certified – by these or other accredited organisations – on the basis of the ISMS certification standards and

c) on the practical experience with the certification process both in the private and the public sector.

2.3 Structure of the study

Following the Introduction (Section 2), Section 3 of the study provides an introduction to certification, focusing on IT certification in Europe and on privacy seals and other privacy certification schemes. The next two sections are dedicated to the survey carried out in eleven European Member States on Information Security Management Systems (ISMS) schemes and practical experiences, the outcomes of which can be used as the basis for the development of privacy and data protection certification schemes that are promoted by the European Commission. Section 4 provides information on existing accreditation, as well as certification bodies and schemes. Section 5 analyses certification practices in the area of Information Security Management Systems on the basis of two interviews carried out with one company of the private sector and one organization of the public sector in each surveyed country (sections 5.1 and 5.2 respectively). The findings of the survey, followed by a number of recommendations, are summarized in section 6.

3 Certification

Certification schemes cover business-to-business (B2B) and business-to-consumer (B2C) processes and products based on their performance according to the baseline requirements specified in the scheme of reference (See Table 1).

Type of attestation	Self-certified	Third-party	
Audience	B2C	B2C	B2B
Object	Products and processes	Products and processes	Mostly management systems
Contents	Mostly above baseline requirements	Mostly above baseline requirements	Baseline and above baseline requirements

Table 1: Categories of certification schemes (Source: European Commission (2010)[16])

3.1 IT security certification

In an ENISA study published in 2007 the authors define certification as ”the successful conclusion of a procedure to evaluate whether or not a professional activity actually meets a set of requirements”.[17] The main objective of certification is to inspire trust. A certification scheme can be defined as the collection of requirements, procedures and means available for obtaining a certificate.

Certification often means compliance with a standard. ISO defines an official standard as follows: *“[d]ocument established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context”*[18]. However, “standards” can also be set *de facto*, by private actors. By way of illustration, the so-called ‘Common Criteria’ is a certification scheme where the security level of a product is evaluated according to a set of criteria defined in the international standard ISO/IEC 15408.

Certification, as defined in the ENISA study of 2007, is the final stage of a longer process. This process is usually designated with the term “conformity assessment.” During a conformity assessment a person or a body will evaluate compliance of persons, products and/or processes with a given set of requirements. It is important to emphasize that 1) the evaluation, and 2) the certification, are not necessarily performed by the same body.

IT security certification schemes have been developed by international, regional and national organisations. At international level, schemes with broad acceptance in practice have been deployed by the International Organisation for Standardization (ISO), by the information Systems Audit and Control Association (ISACA) or the Information Systems Security Association (ISSA). According to a 2012 information security breaches survey, 41% of the customers of large organisations and 13% of small organisations asked companies to comply with a recognised international standard, such as ISO 27001.[19]

[16] European Commission, “Commission Communication — EU best practice guidelines for voluntary certification schemes for agricultural products and foodstuffs”, 2010/C 341/04, OJ C341/5 (16.12.2010), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:341:0005:0011:en:PDF.

[17] C. Casper & A. Esterle, Information Security Certification. A Primer: People, Products, Processes, ENISA, December 2007, p. 2.

[18] See http://isotc.iso.org/livelink/livelink.exe/fetch/2000/2122/687806/Glossary.htm?nodeid=2778927&vernum=0

[19] PriceWaterhouseCoopers, in collboration with BIS, “Information security breaches survey - Technical report 2012”, available online at http://www.pwc.co.uk/en_UK/uk/assets/pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf.

At national level several organisation are developing IT security certification schemes. Organisations that have been involved in the deployment of IT security certification scheme at national level are, for instance, the US National Institute for Standards and Technology (NIST) or the British Standards Institute (BSI).

Evidently, it is impossible to provide an overview of all possible certification schemes related to information security. Usually a distinction is made between certificates for a) persons, b) products and c) organizations.

a) Persons

Certification of information security experts often concludes a training programme. Programmes and certificates can be provided by private companies, professional associations, educational institutions, etc. Well-known are also the information security certification schemes provided by specialized institutions such as GIAC[20], International Council of Electronic Commerce Consultants (EC-Council)[21], ISC[22]or by professional associations such as ISACA.[23] In the framework of ISO, specific certification can be obtained by ISO 27001 auditors or by information security officers who wish to implement the ISO 27001 standard. This ISO certification is provided by accredited certification bodies or unaccredited ones.

b) Products

Typical examples of certification schemes for products are the schemes available for the payment sector.[24] The "Common Criteria" is a certification scheme where the security level of a product is evaluated according to a set of criteria defined in the international standard ISO/IEC 15408.[25] A "certified product" does not necessarily mean that the (security of a) product has been tested and approved by an independent body. There are four types of certification, and they are based on who does the certifying: vendor certification, market certification, user (self) certification, and independent certification. While independent certification is generally recommended, it is often not realistic due to the rapid turnover and the continuous launch of new product generations.

c) Organisations

Certification of organisations can take various forms. In the first place it is important to mention that the absence of certification does not necessarily mean that this organisation has not been – or is not – audited and monitored, whether or not by external and/or independent experts. The security of a critical networks and operations, e.g. in the financial sector or the transport sector, is often submitted to permanent security monitoring. Secondly, organisations often engage in certification processes for specific applications or for their most critical operations. Certification doesn't necessarily mean that the organisation is being certified as such. Thirdly one needs to distinguish between general information security management certification and the certification of specific security-related activities. Very specific auditing or certification schemes exist, for example, for data hosting services (data centres) or for so-called third-party trust providers.

3.2 Approaches to achieve auditable information security management

Based on the above discussion, one can distinguish between at least five different approaches to information security management certification: 1) the "ISO Conformity Assessment" approach; 2)

[20] http://www.giac.org
[21] http://www.eccouncil.org
[22] http://www.isc2.org
[23] http://www.isaca.org/certification/
[24] See, for example: https://www.pcisecuritystandards.org/
[25] http://www.commoncriteriaportal.org/

the ISAE 3000 approach; 3) the AICPA approach; 3) the ISAE 3402 approach and 5) the ISRS 4400 approach on "agreed upon procedures".

1) The "ISO Conformity Assessment" approach

Within the International Organization for Standardization (ISO), the conformity assessment policy development committee ISO/CASCO is both responsible for developing and making recommendations on conformity assessment policy to the ISO/CASCO membership and for developing conformity assessment standards and guides. Particularly relevant ISO standards include (a) ISO 17021 "Conformity assessment: Requirements for bodies providing audit and certification of management systems" (where the ISO 17000 series replaces EN 45000), and (b) ISO 27006 Requirements for bodies providing audit and certification of information security management systems.

Certification of an entity against a specific set of requirements or standard (e.g. ISO 27001) is performed by a certification body "accredited" for performing conformity assessments against such a specific set of requirements or standard by an Accreditation Body. Such an accreditation means that the accredited certification body has the authority, expertise and knowhow to go into organisations and assess them against the target requirements. Only certification bodies can be accredited. It is a common misconception that organisations think that they can become e.g. ISO 27001 "accredited" (instead of "certified"). Accredited certification bodies undergo periodic assessments by their accreditation bodies, usually their National Accreditation Body.

2) The ISAE 3000 approach

The International Federation of Accountants (IFAC) operates the International Auditing and Assurance Standards Board (IAASB). This IAASB issued the "International Standard on Assurance Engagements (ISAE) No. 3000, Assurance Reports on Controls at a Service Organization" originally in June 2000. The current version is "ISAE 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information - International Standard on Assurance Engagements (ISAE)".[26] ISAE 3000's core part focuses on the requirements that allow a practitioner (i.e. an auditor) to express a degree of assurance over a subject matter. Much attention is devoted to selecting the appropriate criteria to audit the subject matter (the topic of the audit), and to obtaining and evaluating evidence. ISAE 3000 offers the state-of-the-art framework in auditing, based on worldwide consensus. To convince customers that the organisation uses the most advanced routines, controls and processes, also in the area of information security, providers often try to obtain a ISAE 3000 assurance statement. For example in the area of cloud services, providers sometimes refer to "ISAE 3000 compliance" in order to demonstrate that the data of the customer are securely stored and only accessible for duly authenticated persons.

3) The AICPA approach

Historically, the AICPA's "Statement on Auditing Standards No. 70: Service Organizations", commonly abbreviated as SAS 70 was a popular auditing statement issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) with its content codified as AU 324. SAS 70 was recently replaced by two standards: (a) ISAE 3402: International Standard on Assurance Engagements No. 3402, Assurance Reports on Controls at a Service Organization, which is the international standard adopted by the International Auditing and Assurance Standards Board (IAASB), and (b) SSAE 16: Statement on Standards for Attestation Engagements No. 16 , Reporting on Controls at a Service Organization, which is the "local" standard adopted by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA).

[26] http://www.ifac.org/publications-resources/

To help Certified Public Accountants (CPAs) selecting the appropriate standard for a particular engagement, the AICPA has introduced the SOC (Service Organization Control) reporting concept, and identified 3 different engagements (SOC 1 relevant to user entities' internal control over financial reporting, SOC 2 focusing on security, availability, processing integrity, confidentiality, or privacy and SOC 3 on trust service principles and criteria).[27] SOC reports are internal control reports on the services provided by a service organization providing information that users need to assess and address the risks associated with an outsourced service.[28]

4) The ISAE 3402 approach

The IFAC International Auditing and Assurance Standards Board (IAASB). Issued in December 2009 the “International Standard on Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization”.[29] ISAE 3402 was developed to provide an international assurance standard to allow public accountants to issue a report for use by user organizations and their auditors on the controls at a service provider that are likely to impact or be a part of the user organization’s system of internal control over financial reporting. Its focus is on financial reporting. In principle, the procedure is as follows: a) The user organization is an entity that outsourced part of its business to a service organization. b) Formal agreements regarding the outsourced services are recorded in a contract and/or Service Level Agreement (SLA). c) Under the ISAE 3402 standard the external auditor has five responsibilities:

1 Prepare and present a complete an accurate description of the ‘system’ (i.e. the internal control framework).

2 Specify the control objectives.

3 Identify the risks that threaten the achievement of the control objectives.

4 Design, implement and maintain controls to provide reasonable assurance that the control objectives will be achieved.

5 Provide a written assertion to accompany the description as to the completeness and accuracy of the information provided and state the criteria used as a basis for making the assertion.

The external auditor shall subsequently determine if all relevant aspects of the ISAE 3402 standard are adequately addressed by the system description. In addition, the service auditor determines if mentioned controls exist, are adequately designed and operated effectively (only type II) during a certain period. The service auditor provides an opinion to the ISAE 3402 report. The auditor of the user (internal auditor) can subsequently rely on the external auditor opinion, when auditing the user organization financial statements.

5) The approach on “Agreed upon procedures”

Finally, an approach can be based upon procedures agreed between the service provider and the auditor. Such an approach allows fine-tuning of scope and audit objectives to the largest extent possible. It is typically used to provide comfort to the service provider internally. It is less suitable to provide assurance towards external parties. [30]

[27] See http://www.ssae16.org/white-papers/aicpa-soc-reports--introduction.html
[28] See further http://www.cohnreznick.com/soc-report-faqs
[29] http://isae3402.com
[30] For an example, see http://www.pscpa.com/assurance/agreed-upon-procedures

3.3 Privacy seals and privacy certification

As mentioned in the Introduction, one of the objective of the study is also to provide ‘lessons learned’ from security certification to be used for the purpose of developing privacy certification & privacy seals[31] Therefore, this section presents a short introduction to privacy seals and privacy certification.

Certification of privacy seals and other privacy certification schemes present a problem of adverse selection[32] that arises when less trustworthy companies would use means to pretend that they are trustworthy taking advantage of the existing information asymmetry on the market. Online interactions reflect a two-sided market, with companies actively making decisions about how to present themselves. Good companies want to demonstrate their integrity. Nevertheless, as usual in adverse selection, less trustworthy companies also have an incentive to pretend that they are good.

There is currently a lax approach toward privacy certification, which can give rise to adverse selection, resulting in a situation where the companies that seek and obtain trust certifications are actually less trustworthy than others.[33]

Control measures, regulation and best practices in the area have been set to address possible issues along the certification process, for instance by guaranteeing the independency of certifiers, and granting them enforcement powers (See Figure 1).

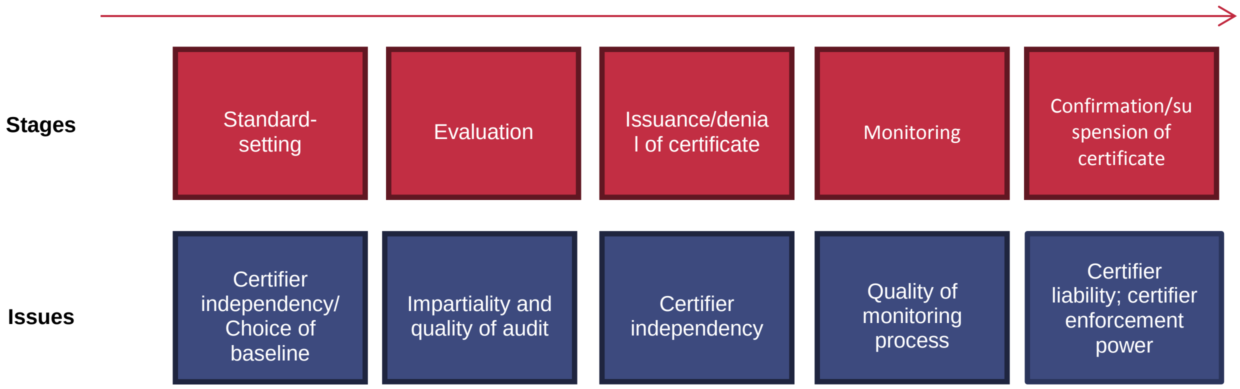
Stages
Standard-setting
Evaluation
Issuance/denial of certificate
Monitoring
Confirmation/suspension of certificate
Issues
Certifier independency/ Choice of baseline
Impartiality and quality of audit
Certifier independency
Quality of monitoring process
Certifier liability; certifier enforcement power

Figure 1: The certification process

The following aspects generally describe the solidity of a (privacy) certification scheme[34]:

1. **Certifier independency**: The certifier should be an independent entity, with no conflicts of interest towards the certified entity. In the framework of member-funded and profit-oriented certification initiatives, a further check of the impartiality of the certifier can be constituted by the cost structure of the service.
2. **Choice of standards:** The baseline to which the certification relates is a fundamental element of the process. Its conceivability and transparent representation allows users to understand the principles that the privacy seal summarizes in one pictogram.

[31] Privacy seal is an identifiable symbol or logo, voluntarily displayed on a Web site, which graphically asserts that the site has implemented and complies with specified privacy practices: Definition by Andrew Tan at http://www.slideshare.net/acc626tan/privacy-seals-8465052.

[32] Herschel I. Grossman, Adverse Selection, Dissembling, and Competitive Equilibrium, The Bell Journal of Economics, Vol. 10, No. 1 (Spring, 1979), pp. 336-343, available online at http://www.jstor.org/stable/300333.

[33] B. Edelman, Adverse selection in online ‘‘trust’’ certifications and search results, in *Electronic Commerce Research and Applications* (2010) http://www.benedelman.org/publications/advsel-trust-se.pdf

[34] Paolo Balboni, *Trustmarks: Third-Party Liability Of Trustmark Organisations In Europe*, Doctoral Thesis, University of Tilburg, 2008 http://arno.uvt.nl/show.cgi?fid=90317

3. **Impartiality in auditing procedure:** Audits can be conducted internally based on internal or third-party standards, or externally by a third party, such as auditing firms.
4. **Active monitoring of the certified company:** The certification system should address the question of ongoing monitoring and periodic re-assessment of the company.
5. **Certifier enforcement power:** In order for certificates to guarantee the standards on which they are based, the certification system has to enable the certifier to withdraw or suspend the certificate in cases when the certified service departs from the pre-established standards.
6. **Certifier accountability**: The certificate informs the customer of certain quality aspects of a product or service and thus of its use. Certifier liability towards third parties motivates the certifier to provide the most accurate information possible and enhances trust in the certifying system itself.[35]

The deployment of a privacy seals and privacy certification scheme should take into account these characteristics.

[35] Y Danidou and B. Schafer, Legal Environments for Digital Trust: Trustmarks, Trusted Computing and the Issue of Legal Liability, in *Journal of International Commercial Law andTechnology*
Vol. 7, Issue 3 (2012) p. 212 http://jiclt.com/index.php/jiclt/article/viewFile/156/154

4 General information on accreditation for ISMS

4.1 Accreditation bodies in the surveyed EU MS

The European Regulation 765/2008 was adopted in July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products.[36] According to the Regulation, "Since the purpose of accreditation is to provide an authoritative statement of the competence of a body to perform conformity assessment activities, Member States should not maintain more than one national accreditation body and should ensure that that body is organised in such a way as to safeguard the objectivity and impartiality of its activities"[37]. Table 2 depicts the national accreditation bodies in the surveyed Member States and the relevant legal framework in which they were created.

COUNTRY	NATIONAL ACCREDITATION BODY	LEGAL FRAMEWORK
Austria	Akkreditierung Austria[38]	Federal Accreditation Act 2012[39]
Belgium	BELAC[40]	Royal Decree of 31 January 2006[41]
France	Cofrac (Comité français d'accréditation)[42]	Decree n°2008-1401 dated December 26, 2008 related to accreditation and to the conformity assessment adopted pursuant to Article 137 of the Law 2008-776 of August 4, 2008[43]
Germany	DAkkS (Deutsche Akkreditierungsstelle)[44]	Accreditation Body Act (AkkStelleG) of 31 July 2009[45]
Italy	ACCREDIA[46]	Decrees of 22 December 2009 of MiSE (Ministry of Economic Development) – - "designation of Accredia as the only Italian national body authorized to carry out activities for accreditation and market surveillance"[47] - "requirements for the organization and operation of the only national body authorized to carry out accreditation in accordance with EC Regulation 765/2008"[48]

[36] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, L218/30, 13.08.2008, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0030:0047:en:PDF.

[37] Recital 15 of European Regulation 765/2008.

[38] http://www.bmwfj.gv.at/TechnikUndVermessung/Akkreditierung/Seiten/AkkreditierungsstellePIZ.aspx

[39] Bundesgesetz über die Akkreditierung von Konformitätsbewertungsstellen (Akkreditierungsgesetz 2012 – AkkG 2012, Federal Law Gazette I No. 28/2012 (National Council: GP XXIV RV AB 1712 page 148. Federal Council: AB 8699 page 807), available at http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2012_I_28/BGBLA_2012_I_28.pdf. Unofficial translation in English: http://www.en.bmwfj.gv.at/technicalaffairsandsurveying/Accreditation/Documents/Accreditation%20Act%202012_Austria.pdf

[40] http://economie.fgov.be/en/entreprises/life_enterprise/quality_policy/Accreditation/

[41] Koninklijk besluit van 31 januari 2006 tot oprichting van het BELAC accreditatiesysteem van instellingen voor de conformiteitsbeoordeling, http://economie.fgov.be/en/binaries/20060131_AR_creation_du_systeme_BELAC_FR_tcm327-56341.pdf (text only available in Dutch and French)

[42] http://www.cofrac.fr/

[43] Décret n° 2008-1401 du 19 décembre 2008 relatif à l'accréditation et à l'évaluation de conformité pris en application de l'article 137 de la loi n° 2008-776 du 4 août 2008 de modernisation de l'économie, available in French at http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000019992087.

[44] http://www.dakks.de/en/content/legal-basis

[45] Akkreditierungsstellengesetz vom 31. Juli 2009, BGBl. I S. 2625, http://www.dakks.de/sites/default/files/AkkStelleG.pdf

[46] http://www.accredia.it

[47] Decreto 22 dicembre 2009 'Designazione di ACCREDIA quale unico organismo nazionale italiano autorizzato a svolgere attività di accreditamento e vigilanza del mercato' Gazzetta Ufficiale della Repubblica Italiana 20/26.01.2010, available in Italian at: http://www.accredia.it/UploadDocs/484_Decreto_GU_20100126.pdf

[48] Decreto 22 dicembre 2009 'Prescrizioni relative all''organizzazione ed al funzionamento dell' unico organismo nazionale italiano autorizzato a svolgere attivita di accreditamento in conformita al regolamento (CE) n. 765/2008', Gazzetta Ufficiale della Repubblica Italiana 19/25.01.2010, available in Italian at http://www.accredia.it/UploadDocs/485_Decreto_GU_20100125.pdf

Netherlands	RvA (Raad voor Accreditatie)[49]	Law of 29 October 2009 on the designation of a National Accreditation Organisation[50]
Poland	PCA (Polskie Centrum Akredytacji/Polish Centre for Accreditation)[51]	Act of 30 August 2002 on conformity assessment system[52]
Slovakia	SNAS (Slovak National Accreditation System)[53]	Law of 27 October 2009 No. 505/2009 Coll. on Accreditation of Bodies Responsible for Conformity Assessment and on Amendment of Certain Acts[54]
Spain	ENAC (Entidad Nacional de Acreditación)[55]	Royal Decree 1715/2010[56]
Sweden	SWEDAC (Swedish Board for Accreditation and Conformity Assessment)[57]	Conformity Assessment Act[58] and the Conformity Assessment Ordinance[59]
United Kingdom	UKAS (United Kingdom Accreditation Service)[60]	Accreditation Regulations 2009[61]. UKAS operates under a Memorandum of Understanding with the Government through the Secretary of State for Business, Innovation and Skills[62]

Table 2 List of national accreditation bodies in the surveyed Member States

Within Europe, the European cooperation for Accreditation (EA)[63] is the main institution that oversees the interactions and interoperability between the different European players, mainly the national accreditation bodies. This network is well established, in particular in the area of ISO 27001, which is the main international standard for an Information Security Management System (ISMS). With regard to Information Security Management Systems, the national accreditation bodies have accredited certification bodies in the area of ISMS. The number of certification bodies that have been accredited in the area of ISMS varies significantly between the surveyed countries: The Austrian and Belgian accreditation bodies have certified only one company each in the area of ISMS,

[49] www.rva.nl

[50] Wet van 29 oktober 2009, houdende regels omtrent de aanwijzing van een nationale accreditatie-instantie in verband met de implementatie van EG-verordening nr. 765/2008 (Wet aanwijzing nationale accreditatie-instantie), available in Dutch at http://wetten.overheid.nl/BWBR0026591/geldigheidsdatum_01-09-2013

[51] http://www.pca.gov.pl/english/?page=akredytacja_en

[52] Ustawa z dnia 30 sierpnia 2002 r.o systemie oceny zgodności, Off. J. of 2002, No 166, item 1360, with subs. changes), consolidated text in Polish available from: http://isap.sejm.gov.pl/DetailsServlet?id=WDU20021661360.

[53] http://www.snas.sk/index.php?l=en

[54] 505 ZÁKON z 27. októbra 2009 o akreditácii orgánov posudzovania zhody a o zmene a doplnení niektorých zákonov, Strana 3853, Čiastka 177, available at http://www.sgpstandard.cz/editor/files/tech_poz/tech_poz/sr/zakon/505_2009_zz.pdf, Unofficial translation in English available at: http://snas.sk/e/files/pdf/Act_505_2009%20.pdf.

[55] http://www.enac.es/

[56] Real Decreto 1715/2010, de 17 de diciembre, por el que se designa a la Entidad Nacional de Acreditación (ENAC) como organismo nacional de acreditación de acuerdo con lo establecido en el Reglamento (CE) nº 765/2008 del Parlamento Europeo y el Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) nº 339/93, Off. Gaz. 7/08.01.2011, pp.1670-1673, available in Spanish:http://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-398. Royal Decree 2200/1995, of December 28, modified by the R.D 338/2010, of March 19, and complementing the Royal Decree 2584/1981 of 18 September 1981, recognizes establishment of ENAC and mentions that Ministry of Industry and Energy can give it support (http://www.boe.es/boe/dias/1996/02/06/pdfs/A03929-03941.pdf).

[57] http://www.swedac.se/en/

[58] Lag (2011:791) om ackreditering och teknisk kontroll, available at http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Lag-2011791-om-ackrediterin_sfs-2011-791.

[59] Förordning (2011:811) om ackreditering och teknisk kontroll, available at http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Forordning-2011811-om-ackre_sfs-2011-811.

[60] http://www.ukas.com/

[61] Accreditation Regulations 2009 (SI No 3155/2009), http://www.legislation.gov.uk/uksi/2009/3155/introduction/made

[62] Memorandum of Understanding between Department for Business, Innovation and Skills and United Kingdom Accreditation Service, available at http://www.ukas.com/library/About-Accreditation/About-UKAS/UKAS-BIS%20MoU%20June%202013.pdf.

[63] EA members: AUSTRIA – **BMWFJ,** BELGIUM – **BELAC,** BULGARIA – **BAS,** CROATIA – HAA, CYPRUS – **CYS-CYSAB,** CZECH REPUBLIC - **CAI,** DENMARK – **DANAK,** ESTONIA – **EAK,** FINLAND – **FINAS,** FRANCE – **COFRAC**FYROM – **IARM,** GERMANY – **DakkS,** GREECE - **ESYD** HUNGARY - **NAT,** IRELAND - **INAB,** ITALY - **ACCREDIA,** LATVIA - **LATAK,** LITHUANIA - LA, LUXEMBURG – **OLAS,** MALTA – **NAB-MALTA,** NETHERLANDS - **RvA,** NORWAY - NA, POLAND - **PCA,** PORTUGAL – **IPAC,** ROMANIA – **RENAR,** SERBIA – **ATS,** SLOVAKIA – **SNAS,** SLOVENIA – SA, SPAIN – **ENAC,** SWEDEN – **SWEDAC,** SWITZERLAND – **SAS,** TURKEY – **TURKAK,** UNITED KINGDOM - **UKAS.**

while the German one has certified seventeen and the UK twenty-three. Table 3 below provides an overview of the number of certified bodies in the area of ISMS in the surveyed Member States, while a list of the certified bodies in the area of ISMS in the surveyed Member States can be found in Annex 2.

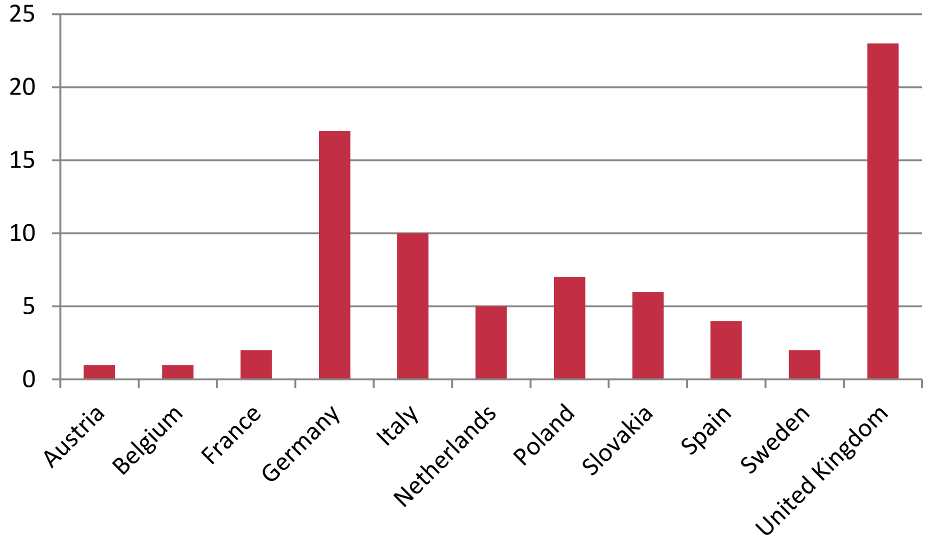

Table 3 Number of ISMS certification bodies

It is interesting to note that the Netherlands Standardization Institute (NEN) has specified the NEN 7510:2011 'Health Informatics - Information security management in health'.[64] NEN is currently working on a certification schema for NEN 7510. As far as known the Dutch national accreditation organisation (RvA) is not involved.

Summary of findings: The number of certification bodies that have been accredited in the area of ISMS *varies significantly* between the surveyed countries, ranging from only one, as in the case of Austria and Belgium, to twenty-three in the United Kingdom.

4.2 Accredited certification bodies and schemes/ISMS certifications in the surveyed countries

All certification bodies provide ISMS certification for compliance with the ISO 27001 standard (ISO/IEC 27001:2005).[65] Many of them provide certification with other relevant standards as well, as for instance the French LSTI that provides ISMS certification for compliance also with ISO 27005 (Security Risk Manager).

The number of certificates issued in each surveyed country varies significantly and unfortunately for the majority of the surveyed countries there are no statistics. The International Register of ISMS Certificates[66] mentions a fraction only of the ISMS certificates. For instance the Register mentions only 3 certified companies in **Belgium**, while the authors are aware of at least fifteen ISMS certified organisations. Some ISMS certification companies provide information about the organisations they certify, but this information is also not complete. In **Sweden**, the certification bodies accredited by SWEDAC must be able to present to which companies they have issued a certificate. SWEDAC,

[64] http://www.nen.nl/NEN-Shop/Norm/NEN-75102011-nl.htm
[65] http://www.27000.org/iso-27001.htm
[66] http://www.iso27001certificates.com/

Intertek Certification AB and the "Swedish Association for Testing, Inspection and Certification"[67] refer to a public search engine of certified companies in Sweden. The register is according to SWEDAC's website "the most complete at present" and list 30 companies certified for compliance with ISO 27001, although this number may not be accurate.

A survey of certifications to ISO management system standards was carried out in 2012 by ISO[68], where data on ISO/IEC 27001 for information security were also collected. Table 4 illustrates the number of certificates issued in 2012, according to the ISO survey.

Country	Number
Austria	28
Belgium	31
France	71
Germany	488
Italy	495
Netherlands	190
Poland	279
Slovakia	127
Spain	805
Sweden	32
United Kingdom	1701

Table 4 Number of certificates accredited by national accredited bodies against ISO/IEC 27001 in 2012[69]

Summary of findings: The number of certificates issued in each surveyed country varies significantly and unfortunately, for the majority of the surveyed countries there are no official statistics. Certification companies provide information about the organisations they certify, but this information is also not complete.

4.3 Validity and revocation of ISMS certificates

The ISMS certifications are based on ISO/IEC 17021. The certification is subject to surveillance audits and recertification. The audit programme shall include a two-stage initial audit, surveillance audits in the first and second years, and a recertification audit in the third year prior to expiration of certification. The three-year certification cycle begins with the certification or recertification decision.

The surveillance audit programme shall include, at least

a) internal audits and management review,
b) a review of actions taken on nonconformities identified during the previous audit,
c) treatment of complaints,
d) effectiveness of the management system with regard to achieving the certified client's objectives,
e) progress of planned activities aimed at continual improvement,
f) continuing operational control,

[67] SWETIC, http://www.swetic.org/en/swetic-swedish-association-for-testing-inspection-and-certification-1
[68] ISO survey conducted in 2012 , http://www.iso.org/iso/home/standards/certification/iso-survey.htm.
[69] http://www.iso.org/iso/database_iso_27001_iso_survey.xls.

g) review of any changes, and
h) use of marks and/or any other reference to certification.

The ISO/IEC 27001 certification is usually divided in a two-stage external audit process defined by the ISO/IEC 17021 and ISO/IEC 27006 standards, while a third stage involves follow-up audits that are carried out in order to verify that the organisation remain compliant to the standard. Stage 1 is dedicated to the review of the documented ISMS against the standard and Stage 2 to the review of the implementation of the ISMS within the business and evidence of adherence. The third stage, as mentioned above involves follow-up audits that are carried out in order to verify that the organisation remain compliant to the standard. In the majority of the surveyed countries, the ISMS certificates are granted for a three-year period, during which certified bodies need to be annually audited to ensure on-going compliance with the standards. The certification can be renewed for subsequent three-year periods. However this timeframe depends on scheme requirements.

The certificate can be revoked if the annual audit finds reasons for it. The ISO/IEC 17021 (which regulates the activities of Certification Bodies) regulates both suspension and revocation of issued certificates. Motivations are coded and described - at standard regulation level - by each Certification Body. The certification body shall suspend certification in cases when, for example, the client's certified management system has persistently or seriously failed to meet certification requirements, including requirements for the effectiveness of the management system, the certified client does not allow surveillance or recertification audits to be conducted at the required frequencies, or the certified client has voluntarily requested a suspension.

Summary of findings. In the majority of the surveyed countries, the ISMS certificates are granted for a three-year period, during which certified bodies need to be annually audited to ensure ongoing compliance with the standards. The certificate can be revoked if the annual audit finds reasons for it.

4.4 Costs for an ISMS certificate

In practice, many certification bodies follow the guidance in ISO/IEC 27006 on the number of days (Auditor Time Chart in annex C[70]) for calculating the minimum duration of an audit, for usage of Certification and Accreditation Bodies. The cost will then be determined by applying the appropriate daily rates to the days needed. According to the findings of the survey, the costs for the certification depend on a number of factors, such as the type and size of the organisation, the scope of the certification, the location of workplaces and operations. Only one national correspondent provided an estimate for the cost, stating that the auditor’s daily fee can vary between 800 and 1.000 EUR. In addition to the costs for the certification audit, there is significant cost associated with the effort to implement the ISMS in the organisation, to set up processes to gather and store evidence and to train the employees.

Summary of findings. The costs for an ISMS certificate depend on the number of days needed (depending on the size and the type of organisation or the scope of the certification), the tariff scheme of the certification body and the expertise/experience of the auditors applied.

4.5 Additional information on seals and certification schemes

Some of the surveyed countries provided information on other security seals and security certification schemes that are delivered by accredited certification bodies. The **French** National Agency of Information Security (ANSSI) recently published a document enlisting requirements applicable to audit service providers regarding the security of information systems (the PASSI

[70] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=59144

standard). Such standard covers the following activities: architecture audit, configuration audit, source code audit, intrusion tests, organizational and physical audit. The PASSI standard will be integrated into the next version of the general security standard RGSv2. Upon the RGSv2's publication, public administrations shall refer to audit service providers complying with such standards.[71]

In the **Netherlands** the Privacy-Audit-Proof certificate has been developed by the Dutch Data Protection Authority[72], while NEN 7510[73] is a national Dutch standard for healthcare information security management. Finally the **Swedish** Certification Body for IT Security (CSEC) is the certification body accredited by SWEDAC[74] and operates as Sweden's national certification body for IT security in products and systems according to Common Criteria for Information Technology Security Evaluation[75].

Summary of findings. Some countries have developed national certification schemes for specific sectors. For instance in **France** ANSSI, the National Agency of Information Systems' Security defined a document enlisting requirements applicable to audit service providers regarding the security of information systems (the PASSI standard), which is applicable to public authorities in terms of information systems' security. In the **Netherlands** the Privacy-Audit-Proof certificate has been developed by the Dutch Data Protection Authority[76], while NEN 7510[77] is a national Dutch standard specific for healthcare information security management.

[71] Further information can be found at: http://www.ssi.gouv.fr/fr/menu/actualites/publication-du-referentiel-d-exigences-applicable-aux-prestataires-d-audit-de.html.
[72] http://www.dutchdpa.nl/downloads_audit/PrivacyAuditFramework.pdf
[73] http://www.nen7510.org
[74] http://www.fmv.se/en/Our-activities/CSEC---The-Swedish-Certification-Body-for-IT-Security/About-CSEC/.
[75] http://www.commoncriteriaportal.org
[76] http://www.dutchdpa.nl/downloads_audit/PrivacyAuditFramework.pdf
[77] http://www.nen7510.org

5 Practical experiences with the ISMS certification process

5.1 Private sector

5.1.1 Surveyed companies

In order to gather information about the practical experiences with the ISMS certification process in the private sector and identify potential key success elements for European certification bodies, national correspondents from the selected eleven European Member States[78] carried out personal interviews with companies from the private sector that have experiences with going through ISMS certification. The surveyed companies were all active in the IT industry and their profiles varied as follows: two companies were IT service providers, two were trust service providers offering digital certificates, two were IT consultancy companies, a communication service provider, a data centre (outsourcing) provider, an identity service provider, a company active in product and people identification and one specialised in the reuse of computers and equipment. The companies cover a broad range of size (from 11 to 5.000 employees) and all companies were interviewed on their experiences for ISMS certification according to the ISO 27001 standard. The interviews[79] were carried out with specialised employees from each company, who had the position of (Chief) Information Security Officer, (Chief) Security Officer, Security Manager, Coordinator of Information Security Management System or Risk Management Director. Thus they were highly qualified to provide answers on the experiences of their company with ISMS certification.

Eight of the surveyed companies had **prior experience with certification**. All of them had gone through the process of obtaining ISO 9001, while two of them had experience with ISO 20000 that targets IT systems in general, but has also security part. Some of the companies have also experiences with specific sector certification processes.

The certification processes covered in the majority of the examined countries all core processes and services provided by the company. One of the examined companies excluded only two specific controls concerning electronic commerce in the certification process. In three cases, ISMS certification was pursued for specific processes, such as the deployment, supply and support of managed information and communication technology services on different sites, outsourcing, software development, deployment of LANs and WLANs, maintenance, or design, development, implementation and administration of software.

Only one company had used security **seals** on their website, as they were WebTrust for CAs, while the one company had acquired the official national seal for ISO27001.

5.1.2 Motivation for undergoing ISMS certification

The reasons for which the surveyed companies decided to obtain ISMS certification were very similar among all companies and ranged from internal (e.g. improvement in quality) to external (e.g. meeting clients expectations).

More specifically, the certification is seen as integrated into the company's quality approach. In the phase of preparation for the certification, all services of the company as are checked, which leads to an **improvement in quality**. One company found that even the ordinary management of security was greatly improved by having a formal system in place. One company also stated that the certificate raises the **security-awareness of the employees**.

[78] See Annex I for a list of the national correspondents.
[79] Due to the sensitivity of the information relating to ISMS certification, the interviewees preferred to remain anonymous.

Another incentive for the acquisition of an ISMS certificate is that it represents a **marketing** and **competitive advantage**. The companies that obtained a certificate did not only aim at keeping their existing customers satisfied, but also at gaining new ones. Actually, the use of certification as a means to **meet customer expectations** has been mentioned as the most important incentive by the surveyed companies. Obtaining the certificate has led to an **increased assurance level** perceived by customers. In many cases, the clients actually requested the demonstration, with an acknowledgment by an independent entity, that certain safeguards with regard to ISMS are met. One of the surveyed companies stated that the customers are requesting every year more and more for the so called "big 3" certificates (9001, 20000 and 27001), putting companies that have them at a competitive advantage. One surveyed company actually decided to obtain the certification, because it was working with government authorities that requested a managed security process from them.

Another reason for which the surveyed companies acquired the certificate is due to the fact that the requirement to be certified is set in a growing number of **procurement procedures**.

Finally one company found that the decision to obtain certification under ISO 27001 was a natural choice as it forms a good **base for other assurance schemes**.

5.1.3 Time period required for the preparation of the company in view of the certification

The time period required for the preparation of a company in order to undergo certification *depends on a number of factors*, such as for example if the company has obtained another certificate or whether several of the controls are already in place in the company. The time period that was required for the surveyed companies in order to prepare for the certification varied between 3 and 18 months. The majority of the companies required about 6 to 12 months in order to complete the preparation. Companies that already had experience with certification were already familiar with the process and needed less time for preparation. For example one company already had experience from the certification of quality management systems as it was ISO 9001 certified and it needed about six months. One of the companies explained that while the preparation phase took approximately six months, 3-4 months were dedicated to the gathering of evidence of adherence. Finally, two companies stated that the preparation took about 18 months, which included two-stage reviews for quality checks on the way to the certification audit.

5.1.4 Time period required for the actual certification process

The time period required for the actual certification process *did not exceed a week* for the surveyed companies. The duration of the actual certification process depends of course on the size of the organisation and the scope of the audit. The certification audit normally took two to six days, while yearly audit took between one and three days. The time was longer in companies that were certified for other/more standards at the same time. Often the certification was divided in two stages that were carried out on different time periods: Stage 1 for a review of the documented ISMS against the standard and Stage 2 for a review of the implementation of the ISMS within the business and evidence of adherence.

5.1.5 Cost for certification

The *cost for the certification*, in the sense of the audit itself, in the case of majority of the surveyed *companies did not exceed the amount of 10.000 EUR*, which in most cases was characterised as less than 1% of the annual turnover.[80] In all cases, however, the surveyed companies found that the cost of the audit and certification is low compared to the added value for the company.

[80] One company did not provide financial information due to their company policy.

5.1.6 Experiences from ISMS certification

One may think that companies, especially start-ups or SMEs, may find an ISMS certification as an unwanted necessity and excessive cost to meet customer requirements. However, the survey that was conducted in eleven European Member States revealed that all surveyed companies had very good experiences with ISMS certification. One of the companies found that ISMS certification brings together "a wealth of industry experience and knowledge", while another company characterised ISMS certification as possibly "the company's main strategic business asset".

All surveyed companies found that the actual preparation of the company for the certification *increased internal awareness* and contributed to the improvement of the processes and the offered services. Two companies stressed especially the importance of the fact that that the certification was not a snapshot at a certain moment in time. Not only are there annual follow-up audits, as foreseen by ISO 27001, but the changes in processes, controls and infrastructure are so drastic that it wouldn't be possible to put everything in place during the audit and not continue to implement it further on, especially since it involves continuous improvement due to the annual auditing. One company found that even the ordinary management of security was greatly improved by having a formal system in place

All surveyed companies also had very positive experiences with the *acceptance of the certification* by their customers. The certification contributed to an increased assurance level perceived by customers and also opened new business opportunities. Finally, the certification was found very useful in *public procurement procedures*, even when the certification was not obligatory requirement.

5.2 Public sector

5.2.1 Surveyed companies

In order to gather information about the practical experiences with the ISMS certification process in the public sector and identify potential key success elements for European certification bodies, national correspondents from the selected eleven European Member States[81] carried out personal interviews with public bodies and agencies that have experiences with going through ISMS certification. Eleven public organisations, one from each surveyed country, were surveyed. ISMS certification is the public sector aims at raising the quality of the services that are offered to citizens. However, ISMS certification of public bodies or agencies is not yet so widespread compared to the private sector.[82] Therefore it was not possible for all national correspondents to find an organisation from the public sector that had acquired ISMS certification. Three of the surveyed companies (Belgium, Germany, Spain) are in the preparation phase in order to obtain an ISMS certification. Nevertheless they provided valuable information on their experiences so far in order to prepare for the certification.

Few of the surveyed organisations had any previous experience of security certification schemes. The **French** organisation was already familiar with the General Security Database ("Référenciel Général de Sécurité" or the "RGS") issued by ANSSI ("Agence Nationale de la Sécurité des Sytèmes d' Information", the National Agency of Information Systems" Security). RGS defines a set of security rules applicable to the public authorities in terms of information systems' security. The **Dutch** organization had prior experience with a "Privacy Audit Proof" certificate[83], which is a Dutch privacy

[81] See Section I for the list of MSs and the rationale of the selection.
[82] According to the ISO 2011 survey, out of the 6.314 ISO 27001 certificates that were obtained in 2011, only 106 fell under the category. 'public administration' (http://www.iso.org/iso/database_iso_27001_iso_survey.xls).
[83] https://www.privacy-audit-proof.nl/.

certification scheme based on a privacy audit framework developed under the auspices of the Dutch Data Protection Authority. None of the organisations had used security **seals**.

The activities of the surveyed public organisations covered a broad range: the directorate general for IT of a ministry and a ministry of transport, two municipalities, a health insurance body, a public service in charge of employment, an organisation involved in the infrastructure of electronic health cards, an organisation managing IT and data transmission infrastructure for specific functions, regional land registers, an organisation providing bailiff, process serving and credit management services and an agency that depends on ministry of industry.

Ten out of the eleven surveyed organisations were interviewed on their experiences for ISMS certification according to the ISO 27001 standard. In one case, the public organisation had to comply with a national certification scheme, which is actually very similar to the ISO 27001 certificate.

The interviews[84] were carried out with specialised employees from each company, who had the position of (Chief) Information Security Officer, (Chief) Security Officer, Data Protection and Security Officer, IT Security Officer. Thus the interviewed experts were highly qualified to provide answers on the experiences of their company with ISMS certification. One of them, specialist in internal security, was actually certified Lead Auditor ISO27001: 2005.

5.2.2 Motivation for undergoing ISMS certification

All surveyed public organisations decided to obtain ISMS certification, because on the one hand they realised the importance of information management in a secure way, and on the other hand they wished to strengthen the confidence of citizens, or of companies that collaborate with them, in the security of the IT and data management processes. One organisation highlighted that the certification was used in order to promote customer take up for services that they were developing. Another organisation stated that they decided to obtain the ISMS certificate because they did not want security to be a separate process but rather to be integrated throughout their business processes. The surveyed organisations that are active in the in area of health and deal with health data considered ISMS certification as essential both for the citizens, as well as for their partners (medical sector, health insurers…). In Germany, Slovakia and Spain national legislation required the certification of information security processes in the sectors in which the surveyed organisations are active.[85] One organisation admitted that they obtained the ISO 27001 certification as part of complying with the requirement to adhere to a sector scheme and that they would probably have not pursued ISO 27001 certification alone otherwise.

5.2.3 Time period required for the preparation of the organisation in view of the certification

The time period required for the preparation of an organisation in order to undergo certification *depends on a number of factors*, such as for example if the organisation has obtained another certificate or whether several of the controls are already in place. The time period that was required for the surveyed public sector organisations in order to prepare for the certification varied between 3 months and two years. Three of the interviewed organisations are still in the preparatory phase for certification, while one prepared for the ISO 27001 together with ISO 9001 and therefore could not estimate the preparation period that was required for the ISMS certification. Two organisations had already prior security schemes in place and this shortened the preparation time they needed for the

[84] Due to the sensitivity of the information relating to ISMS certification, the interviewees preferred to remain anonymous.

[85] In **Germany**, the electronic health card system is specified by an organisation called Gematik, according to the requirements of which an ISO27001 certification for the electronic health card infrastructure is required. Regulation of the **Slovak** Ministry of Finance 312/2010 contains requirements fr information security for public administration. In **Spain**, Public Administration Organisations are obliged to comply with ENS, the National Security Scheme before 30 January 2014 (www.minhap.gob.es).

certification. Two organisations needed about 8 months, one 15 months, one 18 months and one 2 years.

5.2.4 Time period required for the actual certification process

The time period required for the actual certification process varied between the surveyed companies, while three of the surveyed organisations have not been certified yet. The duration of the actual certification process *depends on the size of the organisation and the scope of the audit*. Often the certification was divided in two stages that were carried out on different time periods: Stage 1 for a review of the documented ISMS against the standard and Stage 2 for a review of the implementation of the ISMS within the business and evidence of adherence. The certification audit normally took between 2 days and 2 weeks, while one organisation spent 4 weeks for the certification process. More specifically, two organisations spent 2 days, two spent 7 days, one spent 10 days, two organisations spent 2 weeks, and one spent 4 weeks. The time was longer in organisations that were certified for other standards at the same time.

5.2.5 Cost for certification

The cost for the certification, in the sense of the audit itself, varies depending on the size of the organisation, to processes that are being certified and the experience of the auditor. For less than one third of the surveyed organisations the cost did not exceed the amount of 10.000 EUR. For one third of companies the cost was above 10.000 EUR and the remaining companies did not provide values. Three of the surveyed organisations have not been certified yet and did not provide any data on cost.

5.2.6 Experiences from ISMS certification

The overall experiences of the surveyed public organisations with ISMS certification were **positive**. The ISMS itself is a process-oriented management system and permits standardised management and control of the required information security in the processing of comprehensive data sets as defined in existing statutory provisions. The ISMS certification ensures a regular and systematic **identification of risks** to information security, and the evaluation and reduction of such risks to an acceptable and feasible degree by means of suitable security measures. In addition, the certification permits to proceed to an annual audit of the organization's good practices, which requires **continuous assessment** with the aid of numerous system and process audits and leads to **improvements of the implemented system** and thus **improvements to the organisation** of work. Thanks to the calculation of security indicators reflecting the efficiency of the system, continuous adjustment and **further evolution** in line with changing requirements can be achieved. ISMS certification also allowed the **management of information** in a much more rigorous and deliberate way than before. Moreover, this certification ensures **sustainable security and safety** in the organization's processes, which would not be possible without such certification. In short, ISMS certification brought the organisation a lot of **structure** and strongly improved **system availability**. With regard to the handling of personal data, on organisation found that ISMS certification preserves the compliance of rules for the processing and handling of **personal data**. The certified ISMS introduced also **policy access rights** to information systems and management of security incidents and vulnerabilities to the surveyed organization.

One company referred to the **limits** of ISO 27001 certification, stating that an organisation could get certified without really having implemented the processes and controls that have been written down in the audited documents.

5.3 Summary of findings from the interviews with private companies and public organisations

The interviews with private companies that had experiences with ISMS certification revealed the following findings:

- The *time period* required for the *preparation* of a company in order to undergo ISMS certification *depends on a number of factors*, such as for example if the company has obtained another certificate or whether several of the controls are already in place in the company. The time period that was required for the surveyed companies in order to prepare for the certification varied between 3 and 18 months. The majority of the companies required about 6 to 12 months in order to complete the preparation.
- The *time period required for the actual certification process did not exceed a week* for the surveyed companies. The duration of the actual certification process depends of course on the size of the organisation and the scope of the audit.
- the *cost* for the certification, in the sense of the audit itself, in eight of the surveyed companies *did not exceed the amount of 10.000 EUR*, which in most cases was characterised as less than 1% of the annual turnover. In all cases, however, the surveyed companies found that the cost of the audit and certification is low compared to the added value for the company.
- The use of certification as a means to *meet customer expectations* has been mentioned as the most important incentive by the surveyed private companies. However, private companies actually underwent ISMS certification when this was required either in order to *ensure collaboration with government authorities* that requested a managed security process from them or because the requirement to be certified is set in a growing number of *procurement procedures*.
- All surveyed companies found that the actual preparation of the company for the certification *increased internal awareness* and contributed to the improvement of the processes and the offered services. All surveyed companies also had very positive experiences with the *acceptance of the certification by their customers*.

The interviews with public organisations that had experiences with ISMS certification revealed the following findings:

- All surveyed public organisations decided to obtain ISMS certification, because on the one hand they realised the *importance of information management* in a secure way, and on the other hand they wished to *strengthen the confidence of citizens, or of companies* that collaborate with them, in the security of the IT and data management processes
- The *time period* required for the preparation of an organisation in order to undergo certification *depends on a number of factors*, such as for example the size of the company, if the organisation has obtained another certificate or whether several of the controls are already in place. The time period that was required for the surveyed private companies in order to prepare for the certification varied between 3 and 18 months, while the time period that was required for the surveyed public sector organisations *varied between 3 months and 2 years.*
- The duration of the actual certification process *depends on the size of the organisation and the scope of the audit*. The certification audit normally took between two days and two weeks, while one organisation spent four weeks for the certification process.
- The overall experiences of the surveyed public organisations with ISMS certification were *positive*. The ISMS itself is a process-oriented management system and permits standardised

management and control of the required information security in the processing of comprehensive data sets as defined in existing statutory provisions.

6 Conclusions and recommendations

The number of certification bodies that have been accredited in the area of ISMS *varies significantly* between the surveyed countries, ranging from only one, as in the case of Austria and Belgium, to twenty-three in the United Kingdom. Similarly, the number of certificates issued in each surveyed country varies significantly and unfortunately, for the majority of the surveyed countries there are no official statistics. Some certification companies provide information about the organisations they certify, but this information is also not complete.

The main findings of the survey are:

- There are no reliable statistics on the number of certificates and certified companies.
- Certain MSs national laws require an information security certification in certain sectors, such as public healthcare.
- National authorities are encouraging the implementation of certification processes for ISMS (e.g. by introducing specific information security certification requirements in case of participation in public procurement).
- Some MSs have developed national certification schemes for specific sectors.
- Based on the survey, the large majority of the interviewed companies, which were awarded an information security certificate, consider this useful for their functioning, as the certification process ensures a regular and systematic identification of risks and evaluation, etc. and also provides competitive advantages.
- The *costs* for an ISMS certificate depend on the number of days needed (depending on the size and the type of organisation or the scope of the certification), the tariff scheme of the certification body and the expertise/experience of the auditors applied.
- In the majority of the surveyed countries, the *ISMS certificates are granted for a three-year* period, during which certified bodies need to be annually audited to ensure ongoing compliance with the standards. The certificate *can be revoked* if the annual audit finds reasons for it.
- The initial certification process requires more resources (especially for the preparation stage) in the case of the first certification. The preparation stage requires between 3 months and 2 years, while majority of the companies required 6 to 12 months. The actual certification process takes two to six days for private companies and between two days to two weeks for public organisations.

One may think that companies, especially start-ups or SMEs, may find an ISMS certification as an unwanted necessity and excessive cost to meet customer requirements. This survey, conducted in eleven European Member States, revealed positive perspective on ISMS certification for the case of the surveyed companies.

The concluding remarks and recommendations are listed below:

- There are limitations in the statistics on the existing certification processes. **We recommend that policy makers should demand reliable statistics. The bodies issuing certificates should keep updated public records on certificates that they have issued, on the specific version of products/systems they certified, including information on the validity of the certificates.**
- Introducing and possibly *requiring an additional certification related to privacy may be cumbersome especially for SMEs.* **Under the lead of the European Commission, standardization bodies, and responsible stakeholders should work together to develop**

best practices and standards combining the requirements for security and data protection in order avoid duplication of work for the two certification areas.

- There is a well-established legislation regarding accreditation and certification in the MSs. **When considering introducing certification for other purposes, i.e. for privacy/data protection, the European Commission and the national policy makers should link such initiatives with existing national accreditation structures.**
- There should be no possibility for an organisation to be certified without actually implementing the processes and controls that have been described in the audited documents. Furthermore, due to the relatively long duration of the preparation stage, there is a high probability that the updated versions of systems are not certified right away after their implementation/deployment. **The national policy makers should ensure enforcement of such requirements for genuine compliance for instance by applying sanctions and/or ad-hoc assessments carried on by third parties.**

7 Annex I: National correspondents for study on ISMS

National correspondents for study on Information Security Management Systems

COUNTRY	NAME	ORGANISATION
Austria	Helga Spacek-Stangl	Secure Information Technology Center – Austria (A-SIT)
Belgium	Jos Dumortier	Time.lex CVBA
France	Annabelle Richard & Diane Mullenex	Ichay & Mullenex Avocats
Germany	Markus Mackenbrock Marian Arning	Bundesamt für Sicherheit in der Informationstechnik Rechtsanwalt Marian Arning
Italy	Paolo Fabbrizi	
Netherlands	Ron van Paassen & Robin de Haas Koen Versmissen	TNO, Organisation Applied Scientific Research Privacy Management Partners
Poland	Dariusz Adamski	University of Wroclaw
Slovakia	Zuzana Halásová	National Security Authority
Spain	Aljosa Pasic	Atos
Sweden	Patric Sporrong	TST Management AB
United Kingdom	Richard Trevorah	tScheme Limited

8 Annex II List of the certified bodies in the area of ISMS in the surveyed states

List of the certified bodies in the area of ISMS in the surveyed Member States

COUNTRY	CERTIFIED BODIES IN THE AREA OF ISMS[86]
Austria	1. CIS - Certification & Information Security Services GmbH (www.cis-cert.com)
Belgium	1. Vinçotte (www.vincotte-certification.com/en/info-technology/isoiec-27001/)
France	1. AFNOR, the French Association of Standardisation (www.afnor.org/en/group/about-afnor/about-us) 2. LSTI (www.lsti-certification.fr)
Germany[87]	1. Comgroup GmbH (www.comgroup.de) 2. DEKRA Certification GmbH (www.dekra.com) 3. Deloitte Certification Services GmbH (www.deloitte.de) 4. DQS GmbH - Deutsche Gesellschaft zur Zertifizierung von Managementsystemen (www.dqs.de) 5. IFAZ Institut für Auditierung und Zertifizierung GmbH (www.ifaz.net) 6. Technischer Überwachungs-Verein Thüringen e. V. Zertifizierungsstelle für Systeme und Personal (www.tuev-thueringen.de) 7. TÜV AUSTRIA Deutschland GmbH (www.tuv-ad.de) 8. TÜV NORD CERT GmbH (www.tuev-nord.de) 9. 9. TÜV Rheinland Cert GmbH (www.de.tuv.com) 10. TÜV Saarland e.V. TÜV SAAR CERT Zertifizierungsstelle Managementsysteme (www.tuev-saar-cert.de) 11. TÜV SÜD Management Service GmbH (www.tuev-sued.de) 12. TÜV-Zertifizierungsstelle der TÜV Technische Überwachung Hessen GmbH (www.tuevhessen.de) 13. UIMCert GmbH (www.uimcert.de) 14. Zertifizierungsstelle der PERSICON cert AG (www.persicon-cert.com) 15. TÜV Rheinland Cert GmbH (www.de.tuv.com) 16. datenschutz cert GmbH (www.datenschutz-cert.de) 17. TÜV SÜD Management Service GmbH (www.tuev-sued.de)
Italy	1. CERMET Soc. Cons. a r.l. (http://www.cermet.it/) 2. CERTIQUALITY S.r.l. (http://www.certiquality.it/) 3. CSQA Certificazioni S.r.l. (http://www.csqa.it/) 4. DASA RÄGISTER S.p.A. (http://www.dasa-raegister.com) 5. Det Norske Veritas Italia S.r.l. (http://www.dnvba.it/) 6. ICIM S.p.A. (http://www.icim.it/) 7. IMQ S.p.A. (http://www.imq.it/) 8. RINA Services S.p.A. (http://www.rina.org) 9. S.C. ALL CERT SYSTEMS S.r.l. (http://www.allcert.ro) 10. TÜV Italia S.r.l. (http://www.tuv.it/)
Netherlands	1. Duijnborgh(C590) (www.dbcert.nl) 2. Ernst&Young (C466) (www.ey.com/GL/en/Services/Specialty-Services/CertifyPoint) 3. PWC (C203) (www.pwc.nl/nl/pwc-certification/informatiebeveiliging.jhtml) 4. BSI (C122) (www.bsigroup.nl) 5. Dekra (C013) (www.dekra-certification.nl)
Poland	1. Polski Rejestr Statków S.A. (www.prs.pl/management-systems-certification.html) 2. Polskie Centrum Badań i Certyfikacji S. A. Zakład Certyfikacji Systemów Zarządzania (www.pcbc.gov.pl/index.php?option=com_content&view=article&id=2&Itemid=5) 3. Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego, Zakład Systemów Jakości i Zarządzania (http://www.zsjz.pl/en/About_Us/History.html and http://www.zsjz.pl/en/Certification/ISO/IEC_27001.html) 4. Bureau Veritas Certification Polska Sp. z o.o. (www.bureauveritas.pl/wps/wcm/connect/bv_pl/Local/Home/Clients/Wnioski-warunki-certyfikacji/) 5. TUV Nord Polska Sp. z o.o. (www.tuv-nord.pl/Certyfikacja_ISO27001.htm)

[86] As of 01.06.2013.

[87] List available at http://www.dakks.de/en/node/1155.

	6. Germanischer Lloyd Polen Sp. z o.o. (www.gl-polen.pl/certyfikacja/proces-certyfikacji-cel-i-zasady) 7. TUV Rheinland Polska Sp. z o.o. (www.tuv.com/pl/poland/uslugi/systemy_zarzdzania/it_telekomunikacja/iso_27001_pl/iso-27001.html)
Slovakia	1. SKQS - Slovenská spoločnosť pre systémy riadenia a systémy kvality, Ltd.. (www.skqs.sk) 2. PQM, Ltd. – COMS (Management Systems Certification Body) (www.pqm.sk/en) 3. Hungarian Standards Institution (MSZT.) MSZT provides a wide range of services for the distribution of standards as well as accredited certification activities (one of them is the accreditation in Slovakia for certification of ISMS) (www.mszt.hu) 4. TÜV SÜD Slovakia, Ltd. (www.tuv-sud.com/slovakia/en/) 5. Vinçotte Slovakia Ltd. (www.vincotte.sk/) 6. ASTRAIA Certification, Ltd. (www.astraia.sk/index.php?page=en)
Spain	1. Asociacion Española de Normalizacion y Certificacion (AENOR) [Spanish Association for Standardization and Certification] (www.en.aenor.es/) 2. Bureau Veritas Certification (www.bureauveritas.es) 3. Laboratorio General d'Assaigs i Investigacions (LGAI) [LGAI technological Center] (www.appluslaboratories.com) 4. OCA Instituto de Certificacion (www.ocacert.com/certificacionISO27001.html)
Sweden	1. Det Norske Veritas Certification AB, part of DNV Business Assurance (http://www.dnvba.com/Global/certification/management-systems/Information-Security/Pages/default.aspx) 2. Intertek Certification AB, part of Intertek Group PLC (http://www.intertek.com/auditing/iso-27001/)
United Kingdom[88]	1. ACS Registrars Limited Also trading as ICS Registrars (www.ACSRegistrars.com) 2. AJA Registrars Limited (www.ajaregistrars.co.uk) 3. Ascertiva Group Limited Trading As NQA (www.ascertivia.com) 4. BM TRADA Certification Limited trading as BM TRADA (www.bmtrada.com) 5. BSI Assurance UK Limited (www.bsigroup.com) 6. Bureau Veritas Certification Holding SAS - UK Branch (www.bureauveritas.com) 7. Certification Europe (UK) Limited (www.certificationeurope.co.uk) 8. Certification International (UK) Ltd (www.cert-int.com) 9. China Certification Center Inc (www.ccci.com.cn) 10. DAS Certification Limited (www.dascertification.co.uk) 11. DNV Certification Ltd (www.dnv.co.uk/certification) 12. Intertek Certification Ltd (www.intertek.com) 13. ISOQAR Limited (www.isoqar.com) 14. Japan Audit and Certification Organization for Environment and Quality (www.jaco.co.jp) 15. Japan Quality Assurance Organization (www.jqa.jp) 16. KPMG Audit Plc (http://rd.kpmg.co.uk/WhatWeDo/19147.htm) 17. Lloyds Register Quality Assurance Limited (www.lrqa.com) 18. Marketing Quality Assurance Limited (www.mqa-ltd.co.uk) 19. Perry Johnson Registrars Inc (www.pjr.com) 20. Registrar of Standards (Holdings) Ltd, trading as United Registrar of Systems, Registrar of Standards Ltd & Global Registrars Inc (www.urscertification.com) 21. SGS United Kingdom Limited (www.sgs.co.uk) 22. SIRIM QAS International Sdn. Bhd. (www.sirim.my) 23. The APM Group Limited (www.apmgroup.co.uk) 24. The Audit People Limited (www.theauditpeople.com)

[88] http://www.ukas.com/about-accreditation/accredited-bodies/certification-body-schedules-ISMS.asp

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vassilis Sofias,
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
info@enisa.europa.eu
www.enisa.europa.eu