enisa
European Network and Information Security Agency

Shortlisting network and information security standards and good practices

Version 1.0, January 2012

Acknowledgements

We want to express our sincere gratitude to the many people who responded to the survey and the interviews. Their contributions have been invaluable.

The survey and analysis reported in this document were carried out by KPMG Finland, as part of ENISA tender P/28/10/TCD.

About ENISA

The European Network and Information Security Agency (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.

Contact details

For contacting ENISA or for general enquiries on Article 13a, please use the following details:

- E-mail: resilience@enisa.europa.eu
- Internet: http://www.enisa.europa.eu

For questions related to Article 13a, please use the following details:

- E-mail: resilience@enisa.europa.eu

Contents

1 Introduction

This document contains the research results and the raw data of a survey and interviews, which were used to derive a shortlist of the main network and information security standards and good practices relevant for EU Telecom providers.

The security measures in the shortlisted standards and good practices have been categorized in domains and sub-domains, called a meta-framework, or a mapping. The meta-framework was used as input for a working group 'Minimum Security Measures' organized by ENISA to support the EC and the EU member states with the (harmonized) implementation of Article 13a of Directive 2009/140/EC.

Note that this document is published only to provide the reader with the rationale and raw research analysis and results and that it does not reflect the current state of the (related) work in the working group ' Minimum Security Measures'. The final version of the technical guideline on Minimum Security Measures can be found on ENISA's website.

The rest of this document contains the shortlist of common standards and good practices (in Section 2), the survey analysis (in Section 3), and the analysis of the interviews following the survey (in Section 4). The mapping of the standards is published as a separate Excel sheet.

2. Shortlist of standards and good practices

We have derived a shortlist of 20 standards and good practices that are in use in the EU telecommunications market, based on the results of a survey across the EU telecom market.

1 ISO/IEC 27001/2 [I23, I24]

2 ISO/IEC 24762:2008 Guidelines for ICT and disaster recovery services [I12]

3 ISO/IEC 27005 Information security risk management [I25]

4 ISO/IEC 27011 Information security management guidelines for telecommunications [I26]

5 BSI BS25999-1 Business Continuity [I10]

6 ITU-T X.1051 (02/2008) [I29]

7 ITU-T X.1056 (01/2009) [I18]

8 ITU-T X.800 (1991) [I21]

9 ITU-T X.805 (10/2003) [I31]

10 ISF Standard of Good Practice 2007 [I34]

11 CobiT [I27]

12 ITIL Service Support [I15]

13 ITIL Security Management [I15]

14 IT-Grundschutz-Kataloge [G10]

15 KATAKRI (FI) [G5]

16 NIST SP 800-34 [G29]

17 NIST SP 800-61 [G30]

18 FIPS-200 [M50]

19 UK NICC Minimum Standard ND1643 [M46]

20 PCI DSS 1.2 [I28]

Annex 1 provides a longer list of standards and best practices that were used to derive this shortlist, and Annex 2 provides the rationale behind the shortlist.

Meta-framework

The security measures (or controls) in these standards have been categorized in domains and subdomains. This meta-framework (mapping) is published as a separate document (a spreadsheet). The meta-framework was used as input for the technical guideline on minimum security measures (see Introduction).

3. Survey analysis

The questionnaire was sent to 236 potential participants and 25 responses (11%) were received. In this section the survey results are analyzed.

Highlights

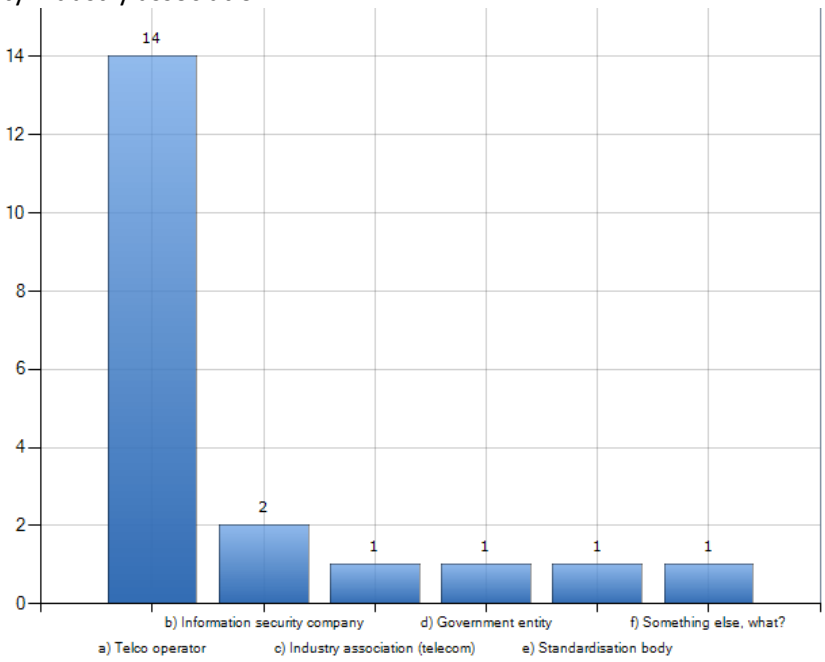
The identification of relevant NIS standards and good practices is based on desktop research, on-line questionnaire and interviews. This section shows some highlights from the survey.

- All respondents (100 % of answers) use ISO 27001 for governing information security. Most respondents (65%) also use PCI DSS and ITIL. For Business continuity organisations use BS 25999 (47%). CobiT is also widely (41%) used. Other standards included in the questionnaire are hardly used and open questions did not bring up any other widely used standards either.
- Respondents see maturity models as the best alternative (47%) to cope with different risk profiles and size of organisations.
- Respondents identify advantages in implementing EU-wide information security good practices:
    - For multinational companies, economy of scale and synergies. For citizens, the assurance of minimum level of security in the services across EU. For suppliers, clear rules and solid requirements.
    - Cross-European security platform. This could be a real nightmare for hackers, terrorists and alike.
    - A common security standard can be a "starting point", common to all industries.
    - Fair competition and leaving the technical details to the service providers. Minimum requirements supporting the base-line and secure the interaction between sectors and regions.
    - Structured and systematic approach; evaluation of generic measures per industry sector.
    - Allows one to compare different companies.
    - A set of minimum security requirements would provide a baseline, which would allow organisations to trust other organisations when dealing with sensitive information. The real problem is assessing if these organisations actually meet the claimed level of security.
    - Improved industry wide security if an effective set of minimum standards can be agreed.
    - Why should EU reinvent the wheel? There are good practises out there already today. Minimum requirements would be OK though.
    - Secured end-to-end solution for customers within EU. Aligned security implementations across borders.
    - Easiness of data transfer and data management between EU countries.
- Respondents cite different reasons for using the standards they use:
    - ISO 27001 is considered being the best practice.
    - Implementation of globally accepted best practices/standard.
    - Wide acceptance, availability, need for standardization, no need to reinvent the wheel.

- Good structure and they are widely known.
- Some of them are mandatory (DLG196, PCI/DSS), some others are just well known best practices that are commonly implemented (ISO27001).
- Use of good practice to increase of efficiency; introduction of common language, terms and definitions; identification of common fields of action.
- It makes thing more transparent and understandable for others.
- Those standards are known, informed, trained, experts available.
- 27001 implemented in response to customer demand for specific services.
- ISO 27001 is one reference model.... (others are there as well) - Understood by customers - Some customers even require this (the demand is rising...).
- SOX and PCI DSS because of compliancy needs.
- ISO9001 for certification.
- ISO 27001, ITIL and CobiT as reference and good practice.
- Requirements from customers and the regulator.

Participants industry sector

Of all the respondents, 14 work in the telecom sector, 2 work for information security companies and the rest work for Industry association (telecom), for Government entity, for Standardization body or for security industry association.

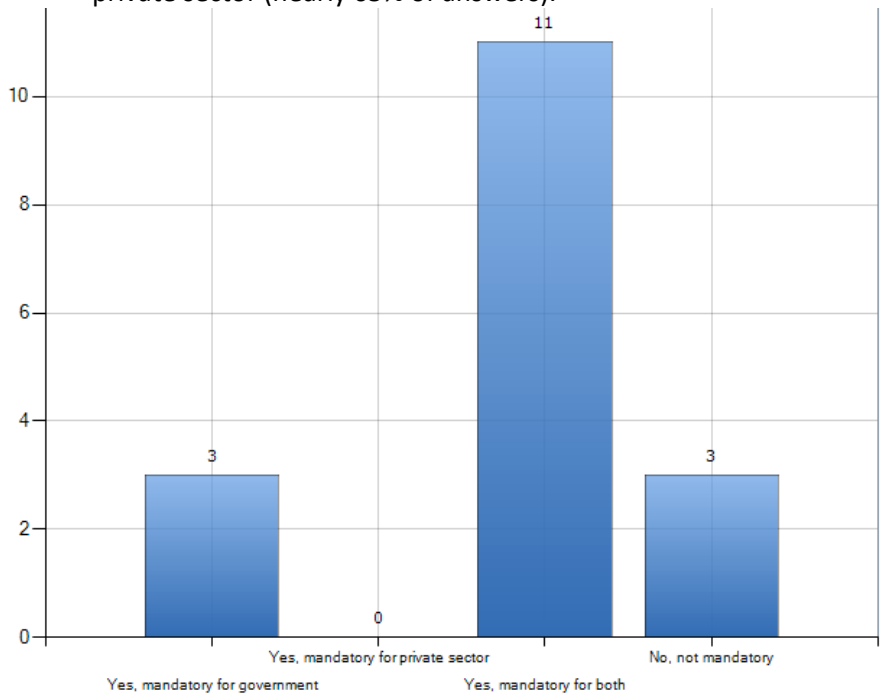


Picture 1: Industry sector

Answers to questions

Whether standards are mandatory

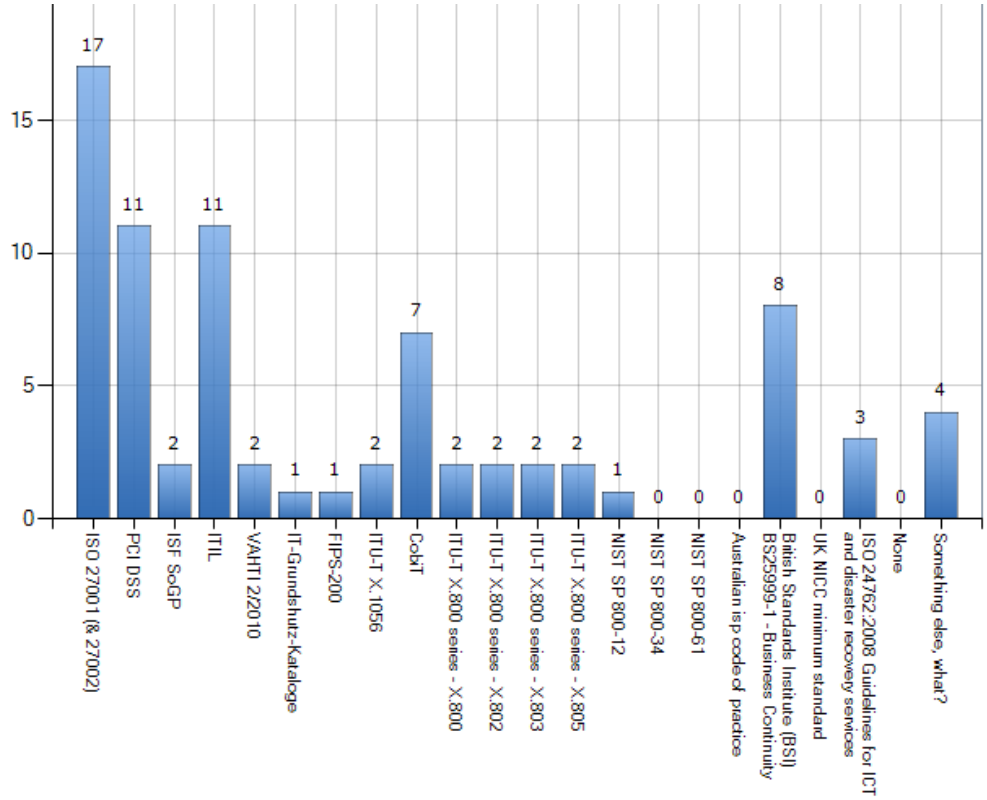
When standards are mandatory they most prominently are mandatory for both public and private sector (nearly 65% of answers).



Picture 2: Whether standards are mandatory

Standards that are mostly widely used by respondents

All respondents (100 % of answers) use ISO 27001 for achieving and maintaining good level of information security. Most respondents (65% for both) also use PCI DSS and ITIL. For Business continuity organisations use BS 25999 (47%). CobiT is also widely (41%) used. Other standard based on the questionnaire are not widely used. Answers to open question mostly listed national legislation relating to privacy and data protection. Those usually are not security standards per say and often do not give any concrete advise or requirements for information security. Sarbanes Oxley act (SOX) was also being mentioned be some respondents.



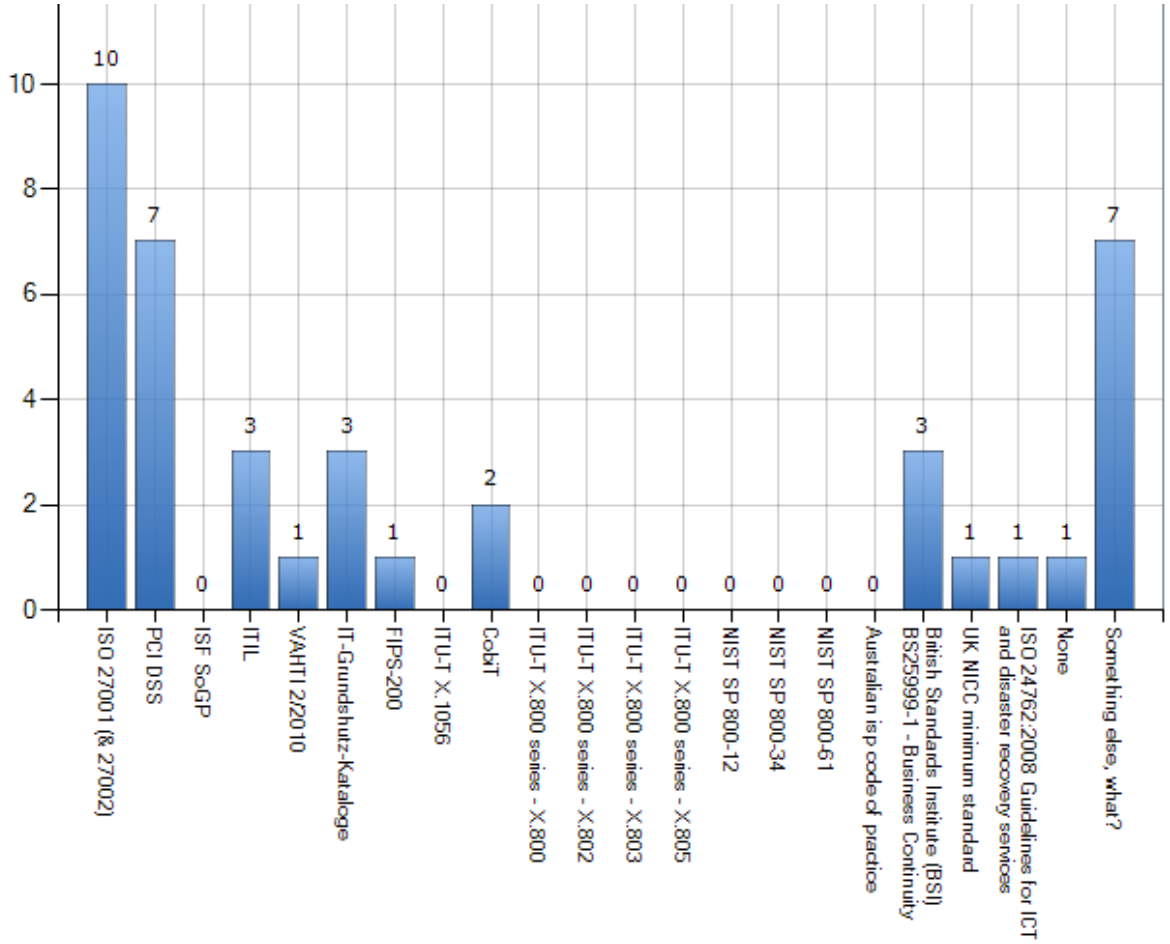
Picture 3: Standards used by organisations

When asked about reasons for using aforementioned standards, respondents gave the following answers:

- ISO 27001 is considered being the best practice.
- Implementation of globally accepted best practices/standard.
- Wide acceptance, availability, need for standardization, no need to reinvent the wheel.
- Good structure and they are widely known.
- Some of them are mandatory (DLG196, PCI/DSS), some others are just well known best practices that are commonly implemented (ISO27001).
- Use of good practice to increase of efficiency; introduction of common language, terms and definitions; identification of common fields of action.
- It makes thing more transparent and understandable for others.
- Those standards are known, informed, trained, experts available.
- 27001 implemented in response to customer demand for specific services.

- ISO 27001 is one reference model.... (others are there as well) - Understood by customers - Some customers even require this (the demand is rising...).
- SOX and PCI DSS because of compliancy needs .
- ISO9001 for certification.
- ISO 27001, ITIL and CobiT as reference and good practice.
- Requirements from customers and the regulator.

Based on the survey ISO 27001 (59%) and PCI DSS (41%) are also most widely used standards for 3rd party compliance i.e. organisations need to comply with those standards since it is required by an external party.



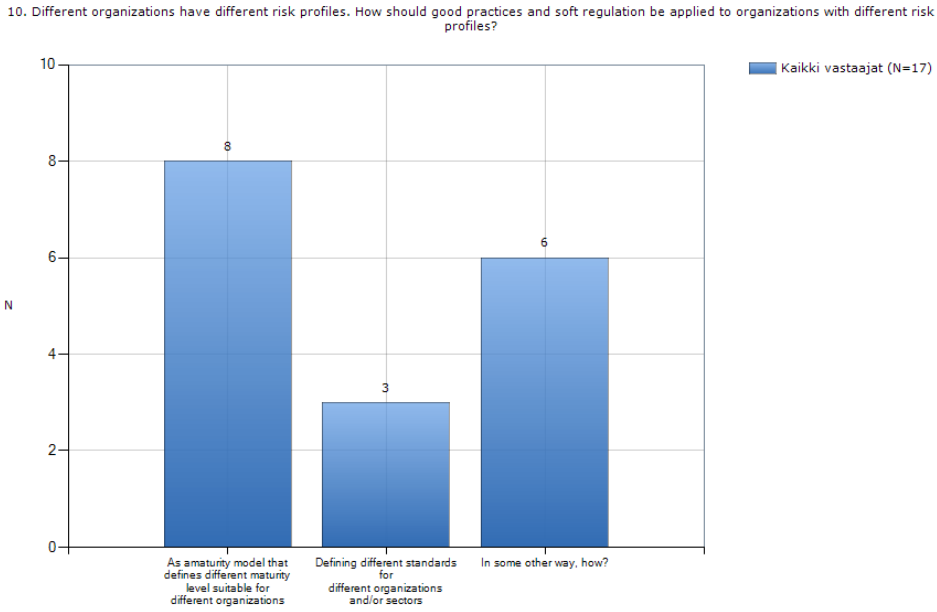
Picture 4: Standards required to be used by organisations

When asked what is your opinion of the added value of using the standard(s)/good practice(s) that you selected related to your environment or sector, respondents gave the following answers:

- ITU and NIST are engineering standards that definitely have their value in that area, ISO is considered best practice, but is not telecom sector specific. Risk environment in the telecom vertical differs significantly, thus requiring changes in the application of ISO 27001.
- Standards are key for the success in managing complex and geographically distributed security environments. Unfortunately there are too much to choose from.
- Holistic approach to information security, Business Continuity etc, implementation framework, monitoring and compliance and so on.
- It is very important to have a standardized and widely accepted approach on security. This will allow for more efficient implementation and communication. Standards have great value in that.
- There is always added value, when the confidentiality of the information of our customers is secured. If there is no security, there is no business.
- They give a good "starting point" for information security; no more no less. The real added value is always given by people and processes.
- Achieve a documented level of security and make the work with governance more effective. Communication externally is also improved and facilitated using established standards.
- Valuable in terms of meeting specific customer requirements.
- It seems that they give somewhat competitive advantage. The demand for certification by our customers is on the rise.
- Good to have defined standards. Standard, same for all companies. Can be used as benchmark. Good basis to ensure security of services.

How to cope with different risk profiles and business requirements

In the survey maturity models were seen as the best alternative (47%) to cope with different risk profiles and size of organisations i.e. if one standard is developed for whole industry it should be a maturity model-type of standard.



Picture 5: How to cope with different risk profiles and business requirements

Costs and benefits of implementing security baselines

When asked about comments on the costs and benefits of implementing security baselines, respondents gave the following answers:

- Implementing security baseline cannot be assessed in terms of cost / benefit in the telecom vertical. Major driver for telecom security is the market position of the carrier.
- Performance metrics should be mandatory. You can't manage what you can't measure. ENISA should lead and establish a common KPI dashboard in Europe to benchmark the different outcome for security.
- The issue is that compliance or rather assurance costs the customer, and this is repeated each time.
- It is very difficult to evaluate any financial indicator in terms of "benefits". By the end of the day, a single security incident can through the company out of business. More or less obvious, the feasible compromise between "do nothing" and "total protection" (which is just something ideal and never touchable) is rather a matter of try & error, than of pure accounting.
- Generally the security baseline if effectively and "early" implemented will give very valuable benefits, not only to comply with the regulation but really value adding. This is important for the marketing positioning also.
- Business need and external demand were main drivers in several divisions and subsidiaries around the world.
- Would be very costly to roll out fully across all aspects of the business. There is an element of administrative overhead to any standard that adds little value.

Major obstacles and difficulties in implementing different security measures

When asked about obstacles and difficulties in implementing different standards, respondents gave the following answers:

- Typical IT environments are significantly more complex than typical industry IT architectures. Responsibilities typically are oriented on revenue streams not IT systems.
- Budget cuts. Lack of liability for the staff in case of negligence. Legal harmonization in fighting cybercrime. Lack of authority to enforce international regulations.
- When it comes to money, you always have to produce a convincing business case. Despite the hype created by various security incidents, it is not an easy task to get the approval in advance (of something bad happening to you). The difficulties start with evaluating the impact (not always having all relevant data or being able to make reasonable assumptions), and continue with assessing the risk.
- When information security is 100%, there is no way to utilize any information. Changing processes from into ones that actually require more work, is never easy.
- We use several (and sometimes old) technologies and we also deal with many people (IT Admins) and some of the countermeasures have a strong impact on day by day work (just think to strong authentication).
- Products and services being more and more complex and usage profiles are constantly changing. International harmonisation is not common.
- Measuring benefit especially in the retail business; finding a way for using measures as differentiator in the regulatory environment.
- Change resistance, lack of knowledge, time slots for trainings.
- There are no obstacles and difficulties except financials.
- Funding, documentation and rollout.
- Finding the right solutions. Allocating funds and resources. One cannot give any return on investment figures, there is no business case.
- Very difficult to measure the benefits of implementing security baselines. Certain baselines have to be implemented because certain laws require them, other because we estimate it's important to protect our customers and the company . Not always easy to find the good balance.
- Implementing the requirements into standard processes including training is time and resource consuming.

Biggest obstacles of defining and implementing EU-wide IT security standard

When asked about the biggest obstacles of defining and implementing EU-wide information security good practices, respondents gave the following answers:

- Security is a competitive factor. Incumbent telecoms are not willing to give up their high-price high-security position while younger competitors are not willing to invest in security while damaging their price-leadership strategy.
- This could be seen as 'another yet standard'.
- Ensuring they are one size fits all - which is impossible.
- There are different perceptions about security even between individuals, departments, companies, etc. it is very hard at this level. Main reasons: culture, in general, knowledge specifically. There is also a tendency to mix.
- Different types of businesses have different type of requirements.
- Plenty of industries, plenty of interests, plenty of people. It will be really difficult to find a common EU-wide information security good practice.
- International competition and the lack of level playing field. Changing and detailed requirements.
- Agreement on baseline security and threat catalogues; exchange of information.
- Cultural change resistance ambiguity in vocabulary & implementation. Why another standard if there are already ISO standards.
- Mostly such regulation are either very abstract or very detailed. Both approaches are not good. Better method would be to define only some basic security measures a little bit more exactly as "you should.
- Good practices and "soft" regulations provide useful guidance but are generally unenforceable across member states, ministries and private sector organisations. In many countries, even those with minimum security requirements, there is a great deal of discretion permitted in how requirements are implemented. Developing a set of minimum good practice requirements is achievable but must take into account the many different operating environments and must recognize that implementation will vary from member state to member state, ministry to ministry and organisation to organisation.
- Impact on commercial aspects - i.e. risk of pushing up costs to operators and also customers.
- Alignment of governments and laws within all EU countries.
- Different maturity levels of EU countries. Combining common and national requirements.

Biggest benefits of defining and implementing EU-wide IT security standard

When asked about the biggest benefits of defining and implementing EU-wide information security good practices on minimum security requirements and measures, respondents gave the following answers:

- For multinational companies, economy of scale and synergies. For citizens, the assurance of minimum level of security in the services across EU. For suppliers, clear rules and solid requirements.

- Cross-European security platform. This could be a real nightmare for hackers, terrorists and alike.
- The standards we refer and apply today, are generally EU-wide.
- To deal with a common security standard it's always useful to draw a "starting point" or a "minimal security strategy" that is common to all industries.
- Fair competition and leaving the details to the service providers and let the market choose according to needs and availability of level of security. Minimum requirements supporting the base line and secure the interaction between sectors and regions.
- Structured and systematic approach; evaluation of generic measures per industry sector.
- You can compare different companies.
- A set of minimum security requirements would provide a baseline against which organisations could assess whether or not other organisations meet an acceptable level of security. This would allow organisations to trust or not to trust others with sensitive information. The real problem is not in developing the minimum requirements but in assessing whether other organisations actually meet the claimed level of security.
- Improved industry wide security if an effective set of minimum standards can be agreed.
- Why should EU reinvent the wheel? There are good practises out there already today. Minimum requirements would though be ok.
- Secured end-to-end solution for customers within EU. Aligned security implementations across borders.
- Easiness of data transfer and data management between EU countries.

4. Interview analysis

An invitation to participate to interview was sent to 196 potential participants and in the end 5 people (3%) were interviewed. In this section the results of the interviews are analyzed. Responses to questions are included as an annex (Annex 2).

What security measures, processes and controls are used in your organisation to implement or to support information security, network integrity and business continuity?

Organisations seemed to have information security management systems implemented and the most important areas of information security identified. The measures, processes and controls varied from interview to interview.

What are the top three information security requirements/standards in use?

ISO-27000 series was mentioned in all interviews. Other mentioned requirements/standards were PCI-DSS, BS-2599, ISO-14001, ISO-9001, ISO-18001, SOX, CobiT and ITU standards.

If you use those standards to support the security work in your organisation, what are the benefits of using those standards?

There is a customer requirement for ISO 27001 and PCI-DSS. Other reasons that were mentioned are:

- They have good structure and they are widely known
- Customer confidence
- Doing business with other parties so that information security can be demonstrated
- One single document simplifies the process of fulfilling regulations
- Standards are the best tools against reinventing the wheel

What is your opinion of the added value of using the standard(s)/good practice(s)?

The usage of the standards and good practices were seen to provide the following added value to organisation:

- Someone has already thought through the actions that must be done
- Helping to maintain the same level of requirements
- Helping to quantify the work that has been done in the company
- Save time and potentially money as well

What are the major obstacles and difficulties you met in implementing security requirements (that you are forced implementing by external parties or are implementing voluntarily)?

The most important obstacle was money. Another common difficulty is that implementing security requirements reduces flexibility.

Do you use security standards because it is mandatory or for some other reason?

The only mandatory requirement that was mentioned is PCI-DSS. Other reasons were that it adds business value and reduces risk.

Different organisations have different risk profiles. How should good practices and soft regulation be applied to organisations with different risk profiles?

Many interviewees identified the need to have baseline controls that are applied to every organisation. Additionally, the need to have additional controls that should be implemented based on risk analysis was also identified.

What would be the biggest obstacles of defining and implementing EU-wide information security good practices and soft regulations?

The most important obstacles based on the interviews are:

- Different types of businesses could have different set of requirements
- Companies at the moment have different risk management methodologies
- Enisa might not have enough power to enforce implementation
- Mandatory standards will increase costs and the costs will be passed to customers

What would be the biggest benefits of defining and implementing EU-wide information security good practices on minimum security requirements and measures?

Based on the interviews the biggest benefit would be that it would harmonise the requirements, which would:

- Help co-operation
- Protect the weakest links in the co-operative situations
- Make the audits easier

If EU-wide information security good practice or standard would be created, what standard (if any) it should be based upon?

Based on the interviews the EU-wide security good practise should be based on ISO 27001/27002 standards. If business continuity requirements will be implemented, those should be based on BS 25999. The idea of different sets of requirements for different kinds of businesses should be adopted from PCI-DSS.

Annex 1: Full overview of identified standards and best practices

Good practices in the EU Member States, EFTA and OECD countries

Australia

[G1] HB 231:2004 Information security risk management guidelines, COMMERCIAL
Generic guide for the establishment and implementation a risk management process for information security risks.
http://infostore.saiglobal.com/store2/Details.aspx?ProductID=568847

[G2] ISM – Information Security Manual
Standard governing the security of government ICT systems.
http://www.dsd.gov.au/infosec/ism/index.htm

[G3] INTERNET SERVICE PROVIDERS VOLUNTARY CODE OF PRACTICE
http://iia.net.au/images/resources/pdf/icode-v1.pdf

Austria

[G4] Österreichisches Informationssicherheitshandbuch (Austrian Information Security Handbook)
Document positioning itself between general standards such as ISO/IEC 27001/27002 and more detailed handbooks such as BSI's "IT Grundschutz Catalogues".
https://www.sicherheitshandbuch.gv.at/

Finland

[G5] KATAKRI VAHTI-ohjeet (Information Security Guidance by the Finnish Ministry of Finance's VAHTI group)
http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/09_Tietoturvallisuus/02_tietoturvaohjeet_ja_maaraykset/index.jsp

[G6] Sisäverkko-ohje, VAHTI 3/2010 (Information security guidance for internal networks)
Guidance unifying and enforcing proper methods of building internal networks and supporting the selection of a suitable security level at the organisation.

[G7] Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010 (Guidance for organisations to fulfill the requirements of the State Council's statute concerning information security in public administration)

[G8] ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin VAHTI 2/2009 (ICT operation continuity and preparation for disturbances and special circumstances)
Guidance improving and strengthening the ICT continuity and recovery planning within the public administration.

Germany

BSI-Standards
https://www.bsi.bund.de/cln_165/ContentBSI/EN/Publications/BSI_standards/standards.html

[G9] BSI Standard 100-4: Business Continuity Management (PDF, 1.16 MB)
Standard introducing a systematic way to develop, establish and maintain an agency-wide or company-wide internal business continuity management system.

[G10] IT-Grundschutz-Kataloge
Document including numerous controls both in the technical and administrative areas of security.
https://www.bsi.bund.de/cln_165/ContentBSI/grundschutz/kataloge/kataloge.html

Italy

[G11] Guidelines for applying Common Criteria (ISO/IEC 15408) in the Italian ICT Security Certification Scheme
http://www.ocsi.isticom.it/index.php/documentazione/linee-guida-provvisorie

[G12] Procedure for the conformity assessment of secure signature creation devices according to requirements laid down in Annex III of the Directive 1999/93/EC
http://www.ocsi.isticom.it/index.php/dispositivi-di-firma/procedura-di-accertamento

DigitPA

[G13] Guideline for operational continuity in the Public Administration
http://www.digitpa.gov.it/sites/default/files/CNIPA_Quaderno_28.pdf

[G14] Guideline for Digital Signature
http://www.digitpa.gov.it/sites/default/files/GuidaFirmaDigitale2009_a_0_0.pdf

Netherlands

[G15] National Continuity Forum - Guide for providers of critical telecom services - guidance on continuity planning & crisis management. *The guide (finalised and informal agreed upon in end 2002) is based on ISO9000 en Emergos.*

[G16] National Continuity Forum - Guide for providers of critical telecom services – guidance on incident reporting.

Slovakia

[G17] National Strategy for Information Security of the Slovak Republic

[G18] Education System in the Information Security Area in the Slovak republic

[G19] Intent of Implementation of CSIRT.SK

[G20] Legislative Intent on Act of Information Security

[G21] Legislative Intent on Act of eGovernment

Spain

[G22] NATIONAL INSTITUTE FOR COMMUNICATION TECHNOLOGY (INTECO)
http://www.inteco.es/national_communications_technology_institute/ (English version)

INFORMATION SECURITY OBSERVATORY
http://www.inteco.es/Security/Observatory

Guides and Handbooks http://www.inteco.es/Security/Observatory/manuales_en/

- Guía práctica para PYMES:cómo implantar un Plan de Continuidad de Negocio 10/27/2010
- Guide to the use of information technologies in the working environment 12/18/2007
- Legal guide to digital identity and electronic ID cards 11/06/2007
- Guide to privacy and secrecy in telecommunications 09/26/2007
- Guide for the legal response to attacks against the Information Security 04/30/2007
- Guide to Electronic Commerce and e-Trust 04/18/2007

[G23] PILAR (Risks Analysis and Management Tool)
http://rm-inv.enisa.europa.eu/methods_tools/t_EAR_Pilar.html

[G24] MAGERIT (Risks Analysis and Management Methodology)
http://rm-inv.enisa.europa.eu/methods_tools/m_magerit.html

Sweden

[G25] Swedish Post and Telecom Agency Code of Statutes, PTSFS 2007:2, 25 April 2007

United Kingdom

[G26] CPNI telecoms resilience
http://www.cpni.gov.uk/Docs/resilience-guide.pdf
http://www.cpni.gov.uk/Docs/Telecommunications-resillience-v3.pdf

[G27] CPNI BGP filtering guidelines
http://www.cpni.gov.uk/Docs/Border_Gateway_Protocol_v2.pdf

United States

NIST: Special Publications (800 Series), http://csrc.nist.gov/publications/PubsSPs.html

[G28] SP 800-12 An Introduction to Computer Security - The NIST Handbook
Handbook providing assistance in securing computer-based resources (including hardware, software, and information) by explaining important concepts, cost considerations, and interrelationships of security controls. The document illustrates the benefits of security controls, the major techniques or approaches for each control, and important related considerations.
http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/index.html

[G29] SP 800-34 Contingency Planning Guide for Federal Information Systems (Errata Page - Nov. 11, 2010)
Guidance providing background information on interrelationships between information system contingency planning and other types of security and emergency management-related contingency plans, organisational resiliency, and the system development life cycle (SDLC). The document provides guidance to help personnel evaluate information systems and operations to determine contingency planning requirements and priorities.
sp800-34-rev1_errata-Nov11-2010.pdf

[G30] SP 800-61 Computer Security Incident Handling Guide
Publication seeking to assist organisations in mitigating the risks from computer security incidents by providing practical guidelines on responding to incidents effectively and efficiently. The document includes guidelines on establishing an effective incident response program, but the primary focus of the document is detecting, analyzing, prioritizing, and handling incidents.
SP800-61rev1.pdf

[G31] COSO Enterprise Risk Management (ERM) Integrated Framework (2004), COMMERCIAL
Framework defining essential enterprise risk management components, discusses key ERM principles and concepts, suggests a common ERM language, and provides clear direction and guidance for enterprise risk management. The document introduces an enterprise-wide approach to risk management as well as concepts such as: risk appetite, risk tolerance, portfolio view. This framework is now being used by organisations around the world to design and implement effective ERM processes.
http://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/InternalControls/COSO/PRDOVR~PC-990015/PC-990015.jsp

[G32] US NSTAC reports http://www.ncs.gov/nstac/nstac_publications.html

Mandatory and binding minimum measures in the EU Member States, EFTA and OECD countries

Canada

SIDM Policy Instruments, http://www.tbs-sct.gc.ca/sim-gsi/pc-cd/documents/dev-ela-eng.asp

[M1] Policy on Government Security
Government security is the assurance that information, assets and services are protected against compromise and individuals are protected against workplace violence. The extent to which government can ensure its own security directly affects its ability to ensure the continued delivery of services that contribute to the health, safety, economic well-being and security of Canadians.

[M2] Standard on Business Continuity Planning
An essential element of governance is the development of departmental BCP Program policy to apply GSP requirements to new and existing departmental programs and operations, pursuant to any constituent or other legislative requirements.

[M3] Standard on Security Organisation and Administration
This document establishes the operational standard for the organisation and administration of security as required by the Security policy.

[M4] Standard on Management of Information Technology Security (MITS)
Standard defining baseline security requirements that federal departments must fulfill to ensure the security of information and information technology (IT) assets under their control.

Mandatory Government of Ontario Information Technology Standards, Guidelines, Policies and Procedures; 7. Security Standards http://www.mgs.gov.on.ca/en/IAndIT/STEL02_047303.html

[M5] GO-ITS 25 General Security Requirements Version 1.1.
Document defining general security requirements for the protection of the integrity, confidentiality and availability of Government of Ontario networks and computer systems.

[M6] GO-ITS 25.11 Security Design Requirements Version 1.0.
Document outlining an approach for network organisation and describes mandatory requirements for Security Design.

Denmark

[M7] Executive Order on Emergency Preparedness Planning for Electronic Communications Networks and Services

[M8] Executive Order on Planning and Implementation of Emergency Preparedness for Electronic Communications Networks and Services

[M9] Executive Order on the National Telecom Agency's Fees and Charges in 2005 - No. 1494 of 16 December 2004

[M10] Executive Order on Auction of Licences for 3rd Generation (3G) Mobile Networks Word | pdf

[M11] Executive Order Amending the Executive Order on Auction of Licences | pdf

[M12] Executive Order on the Use of Radio Frequencies without a licence and on Radio Examinations and Call Signs etc. Word | pdf

[M13] Executive Order on the Provision of Electronic Communications Networks and Services

[M14] Executive Order on Number Information Databases

Finland

[M15] Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681 (State Council's statute concerning information security in public administration)
Statute regulating the general information security requirements concerning the

classification and handling of official documents.
http://www.finlex.fi/fi/laki/ajantasa/2010/20100681

[M16] Viestintäviraston määräys tietoturvaloukkausten ilmoitusvelvollisuudesta yleisessä teletoiminnassa (Finnish Communications Regulatory Authority's statement concerning the oblication for telecommunications sector to disclose information security incidents)
http://www.ficora.fi/attachments/suomiry/5m3uFvOS8/Viestintavirasto09D2009M.pdf

[M17] Viestintäviraston määräys teleyritysten tietoturvallisuuden hallinnasta teletoiminnassa (Finnish Communications Regulatory Authority's statement concerning the information security management in the telecommunications sector)
http://www.ficora.fi/attachments/suomiry/5rhRbUPns/Viestintavirasto47C2009M.pdf

[M18] Viestintäviraston määräys viestintäverkkojen ja -palvelujen varmistamisesta (Finnish Communications Regulatory Authority's statement concerning the continuity of communications networks and services)
http://www.ficora.fi/attachments/suomiry/5vB4GW4xt/Viestintavirasto542008M.pdf

Greece

[M19] Strengthening the legal framework for ensuring the secrecy of telephone communication (Law 3674/2008)
http://www.adae.gr/portal/fileadmin/docs/nomoi/N.3674.2008.pdf

[M20] Electronic communication law (Law 3431/2006)
http://www.eett.gr/opencms/opencms/admin/downloads/telec/N3431.pdf

[M21] Regulation on General Authorizations (EETT Decision no 390/3/31-6-06)
http://www.eett.gr/opencms/export/sites/default/EETT_EN/Electronic_Communications/Telecoms/Licensing/Licensing_Docs/Decision_390_3_2006.pdf
(the regulation with the amendments only in Greek:
http://www.eett.gr/opencms/export/sites/default/admin/downloads/telec/apofaseis_eett/kanonistikes_apofaseis_eett/AP_390_3_2006.pdf)

[M22] Electronic signatures

- "Regulation on the Provision of Electronic Signature Certification Services", Decision 248/71 (FEK Issue 603/B/16-5-2002)"
- Regulation on the Designation of Bodies for the Conformity Assessment of Secure-Signature-Creation Devices and Secure Cryptographic Modules and on the Designation of Bodies for the Conformity Assessment of Certification Service Providers using the Voluntary Accreditation Criteria, Decision of the Hellenic Telecommunications & Post Commission under the Protocol No. 295/63.
- Regulation on the Conformity Assessment of Secure Signature Creation Devices and Secure Cryptographic Modules, Decision of the Hellenic Telecommunications & Post Commission under the Protocol No. 295/64.

- Regulation on the Voluntary Accreditation of Certification Service Providers, Decision of the Hellenic Telecommunications & Post Commission under the Protocol No. 295/65.

http://www.eett.gr/opencms/opencms/EETT_EN/Electronic_Communications/DigitalSignatures/LawFramework.html

[M23] Secrecy Assurance Regulations for Telecommunication Services, ADAE Regulation http://www.adae.gr/portal/index.php?id=302&tx_ttnews[tt_news]=63&tx_ttnews[backPid]=282&cHash=95487a25d464b6e7044ec99778ce6db7

[M24] Secrecy Assurance Regulations for Internet Telecommunications, ADAE Regulation http://www.adae.gr/portal/index.php?id=302&tx_ttnews[tt_news]=62&tx_ttnews[backPid]=282&cHash=6a3a2897e47f2d0a03c3aa7ea66af3e5

Italy

[M25] Technical and Security Requirements for Public Administration System Network (Prime Minister Decree – april 1° 2008), DigitPA http://www.digitpa.gov.it/sites/default/files/normativa/DPCM_01-apr-08.pdf

Netherlands

[M26] The Telecommunications Act (no english version available online) http://wetten.overheid.nl/BWBR0009950/geldigheidsdatum_16-02-2011

Romania

[M27] ANCOM Decision no. 338/2010 on the general authorization regime for providing electronic communications networks and services http://www.ancom.org.ro/DesktopDefault.aspx?tabid=1130

Slovakia

[M28] Act on Information Systems of Public Administration, July 1, 2006

[M29] Edict on Information Systems of Public Administration, July 15, 2010

[M30] Act on Electronic Communications, April 1, 2004

[M31] Act on e-Signature, May 1, 2002

[M32] Act on e-Commerce, February 1, 2004

[M33] Criminal Code, January 1, 2006

Spain

[M34] Instrucción 1/2000, de 1 de diciembre, de la Agencia Española de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos (B.O.E. núm. 301, de 16 de diciembre), FREE

Instruction governing the international data transfers.
http://www.boe.es/boe/dias/2000/12/16/pdfs/A44253-44257.pdf

[M35] Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, FREE
Exclusive regulation of the telecommunications sector.
http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2003-20253
Act 32/2003, November 3rd, Telecommunications Act
https://www.agpd.es/portalwebAGPD/english_resources/regulations/common/pdfs/Ley_32-2003_LGT.pdf (Partial translation into English)

[M36] Ley 59/2003, de 19 de diciembre, de Firma Electrónica, FREE
Incorporation of new safety technologies for electronic communications in the activity of enterprises, citizens and government.
http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2003-23399

[M37] Royal Decree 3/2010, of January 8th, which regulates the National Security Framework within the e-government scope
http://www.csae.map.es/csi/pdf/ENS_SECURITY_ENGLISH_final.pdf
http://www.epractice.eu/en/cases/ens

[M38] Real Decreto 899/2009, de 22 de mayo, por el que se aprueba la carta de derechos del usuario de los servicios de comunicaciones electrónicas
http://www.boe.es/boe/dias/2009/05/30/pdfs/BOE-A-2009-8961.pdf

[M39] Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios
http://www.boe.es/boe/dias/2005/04/29/pdfs/A14545-14588.pdf

[M40] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones
http://www.boe.es/boe/dias/2007/10/19/pdfs/A42517-42523.pdf

[M41] Real Decreto 903/1997, de 16 de junio, por el que se regula el acceso, mediante redes de telecomunicaciones, al servicio de atención de llamadas de urgencia a través del número telefónico 112
http://www.boe.es/boe/dias/1997/06/27/pdfs/A19953-19955.pdf

[M42] Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información
http://www.boe.es/boe/dias/2007/12/29/pdfs/A53701-53719.pdf

[M43] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico http://www.boe.es/boe/dias/2002/07/12/pdfs/A25388-25403.pdf
Act 34/2007, December 28th, Services of the I.S. and Electronic Commerce https://www.agpd.es/portalwebAGPD/english_resources/regulations/common/pdfs/Ley_34-2002_LSSI_ingles.pdf (Partial translation into English version)

[M44] Capitulo V Orden ITC/912/2006, de 29 de marzo, por la que se regulan las condiciones relativas a la calidad de servicio en la prestación de los servicios de comunicaciones electrónicas
http://www.boe.es/boe/dias/2006/03/31/pdfs/A12469-12484.pdf

Switzerland

[M45] Directives on IT Security in the Federal Administration (available in German, French and Italian), FREE
Directives regulating the following areas of IT security in the Federal Administration: organisation, security practices and network security.
http://www.isb.admin.ch/themen/sicherheit/00150/00836/index.html?lang=en

United Kingdom

[M46] UK NICC minimum standard
http://www.niccstandards.org.uk/files/current/ND1643%20%20Minimum%20Security%20Standards%20v1%201%201.pdf?type=pdf

[M47] UK CESG standard on standard level of assurance
http://www.cesg.gov.uk/products_services/csscs/index.shtml

United States

[M48] COMPUTER SECURITY ACT OF 1987, FREE
The Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use.
http://csrc.nist.gov/groups/SMA/ispab/documents/csa_87.txt

[M49] Federal Information Security Management Act of 2002 (FISMA), FREE
Act (Title III of the E-Government Act of 2002) providing a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.
http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

NIST: FIPS Publications, http://csrc.nist.gov/publications/PubsFIPS.html

[M50] FIPS 200: Minimum Security Requirements for Federal Information and Information Systems
Publication specifying minimum security requirements for information and information systems supporting the executive agencies of the federal government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements.
FIPS-200-final-march.pdf

[M51] DOE M 205.1-4, National Security System Manual
Manual composing of two chapters that provide direction for the characterization of information, risk management, and security controls to be implemented for National

Security Systems and the responsibilities for managing cyber security.
https://www.directives.doe.gov/directives/current-directives/205.1-DManual-4/at_download/file

[M52] DOE M 205.1-8 Cyber Security Incident Management Manual
Manual establishing minimum requirements for a structured cyber security incident detection and management process for detecting, identifying, categorizing, containing, reporting, and mitigating cyber security incidents involving DOE information and information systems operated by DOE or by contractors on behalf of the Department.
https://www.directives.doe.gov/directives/current-directives/205.1-DManual-8/at_download/file

[M53] US NRIC standards
http://www.nric.org/pubs/

International standards

Risk management

[I1] ISO 31000:2009 Risk management - Principles and guidelines
ISO 31000:2009 provides principles and generic guidelines on risk management.
http://www.iso.org/iso/catalogue_detail.htm?csnumber=43170

[I2] BS 31100:2008 - Risk management. Code of practice
Key standard for risk management, providing an understanding on how to develop, implement and maintain effective risk management within your business. Using BS 31100 effectively can help you increase your company's effectiveness.
http://shop.bsigroup.com/ProductDetail/?pid=000000000030191339

[I3] ITU-T X.1055: Risk management and risk profile guidelines for telecommunication organisations
Recommendation identifying processes and techniques to reduce information security risk. These processes and techniques can be used to assess telecommunications security requirements and risks, and to help to select, implement and update appropriate controls to maintain the required security level. Many specific methodologies have been developed to address risk management. Recommendation ITU-T X.1055 provides the criteria for assessing and selecting appropriate methodologies for a telecommunication organisation. However, it does not propose any specific risk management methodology.
http://www.itu.int/rec/T-REC-X.1055-200811-I

[I4] ISO/IEC 13335-1:2004 - Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management

[I5] ISO/IEC 13335-3:1998 - Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security

[I6] AS/NZS 4360:2004 - Risk Management

Business continuity management

[I7] ISO 22301 PENDING (Business Continuity management)
Societal security -- Preparedness and continuity management systems -- Requirements
http://www.iso.org/iso/catalogue_detail.htm?csnumber=50038

[I8] BCI GPG 2010 (Business Continuity Global best practice)
http://www.thebcicertificate.org/bci_gpg.html

[I9] ASIS Business Continuity Management: Preparedness, Crisis Management, and Disaster Recovery.
http://www.bcm-institute.org/bcmi10/

[I10] British Standards Institute (BSI) BS25999 BS 25999 - Business Continuity
Publication divided in two parts. Part 1 provides code of Practice best practice recommendations for BCM. Part 2 provides, the requirements for a Business Continuity Management System (BCMS) based on BCM best practice.
http://www.bsigroup.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes/BS-25999/

[I11] Availability and Robustness of Electronics Communications Infrastructures - "The ARECI Study"

Disaster recovery

[I12] ISO 24762:2008 Guidelines for ICT and disaster recovery services
Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services
http://www.iso.org/iso/catalogue_detail?csnumber=41532

[I13] ITIL 2008 SCM: Disaster Recovery Self-Assessment
Set of concepts and practices for Information Technology Services Management (ITSM), Information Technology (IT) development and IT operations. ITIL gives detailed descriptions of a number of important IT practices and provides comprehensive checklists, tasks and procedures that any IT organisation can tailor to its needs. ITIL is published in a series of books, each of which covers an IT management topic.
http://www.itil-officialsite.com/

Incident management

[I14] ISO PAS 22399: 2007 Societal security - Guideline for incident preparedness and operational continuity management
Standard providing general guidance for an organisation — private, governmental, and nongovernmental organisations — to develop its own specific performance criteria for incident preparedness and operational continuity, and design an appropriate management system. It provides a basis for understanding, developing, and implementing continuity of operations and services within an organisation and to provide confidence in business, community, customer, first responder, and organisational interactions. It also enables the organisation to measure its resilience in a consistent and recognized manner.
http://www.iso.org/iso/catalogue_detail.htm?csnumber=50295

[I15] ITIL Incident management
The Information Technology Infrastructure Library (ITIL) is a set of concepts and practices for Information Technology Services Management (ITSM), Information Technology (IT) development and IT operations. ITIL gives detailed descriptions of a number of important IT practices and provides comprehensive checklists, tasks and procedures that any IT organisation can tailor to its needs. ITIL is published in a series of books, each of which covers an IT management topic.
http://www.itil-officialsite.com/

[I16] ISO 27035 security incident management (PENDING)
http://www.iso.org/iso/catalogue_detail.htm?csnumber=44379

[I17] ITU-T E.409: Incident organisation and security incident handling
Recommendation providing an overview and framework that gives guidance for planning an organisation to detect and handle security-related incidents. It is generic in nature and does not identify or address requirements for specific networks. A ITU-T E.409 attempts to standardize incident detection and reporting terminology and also to classify incidents according to their severit. ITU-T E.409 also defines an incident handling structure and sets out procedures for detecting, classifying, assessing, handling and following up incidents.
http://www.itu.int/rec/T-REC-E.409-200405-I/en

[I18] ITU-T X.1056, Security incident management guidelines for telecommunications organisations
Recommendation building on the guidance provided in Rec. ITU-T E.409. Telecommunication organisations need to have processes in place both to handle incidents and to prevent them re-occurring. Five high-level incident management processes are described in Rec. ITU-T X.1056 along with the relationship to the security management. In addition, Rec. ITU-T X.1056 identifies a range of reactive, proactive, and security quality management services that a security incident management team can provide.
http://www.itu.int/rec/T-REC-X.1056-200901-I

[I19] RFC 2350 (06/1998), Expectations for Computer Security Incident Response

[I20] Handbook for Computer Security Incident Response Teams (CSIRTs)

System/other security

[I21] ITU-T X.800, the open systems security architecture.
Recommendation defining the security-related architectural elements that can be applied according to the circumstances for which protection is required. ITU-T X.800 provides a general description of security services and the related mechanisms that may be used to provide the services. It also defines, in terms of the seven-layer Open Systems Interconnection (OSI) Basic Reference Model, the most appropriate location (i.e. the layer) at which the security services should be implemented.
http://www.itu.int/rec/T-REC-X.800-199103-I/e

[I22] ISO/IEC 27000:2009 - Information technology - Security techniques - Information security management systems - Overview and vocabulary

[I23] ISO/IEC 27001:2005 - Information technology - Security techniques - Information security management systems - Requirements

[I24] ISO/IEC 27002:2005 - Information technology - Security techniques - Code of practice for information security management

[I25] ISO/IEC 27005:2008 Information technology - Security techniques - Information security risk management

[I26] ISO/IEC 27011:2008 - Information technology - Security techniques - Information security management guidelines for telecommunications organisations based on ISO/IEC 27002

[I27] COBIT
Set of best practices (framework) for information technology (IT) management, created by ISACA and the IT Governance Institute (ITGI) in 1996. COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices, to assist them in maximizing the benefits derived through the use of information technology, and developing appropriate IT governance and control in a company.
http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

[I28] PCI DSS 1.2
https://www.pcisecuritystandards.org/security_standards/index.php

[I29] ITU-T X.1051: Information security management guidelines for telecommunications organisations
Recommendation establishing guidelines and general principles for initiating, implementing, maintaining and improving information security management in telecommunications organisations and provides an implementation baseline for information security management to ensure the confidentiality, integrity and availability of telecommunications facilities and services.
http://www.itu.int/rec/T-REC-X.1051

[I30] ITU-T Recommendation X.200 (07/1994), Information technology - Open Systems Interconnection - Basic Reference Model: The basic model

[I31] ITU-T Recommendation X.805 (10/2003), Security architecture for systems providing end-to-end communications

[I32] ITU-T Recommendation X.1121 (04/2004), Telecommunication security Framework of security technologies for mobile end-to-end data communications

[I33] ITU-T X.800-X.849 series - Supplement 2 (09/2007) - Supplement on security baseline for network operators

[I34] ISF Standard of Good Practice (SoGP)
Standard addressing information security from a business perspective, providing a practical basis for assessing an organisation's information security arrangements.
http://www.isfsecuritystandard.com/SOGP07/index.htm

Annex 2: Rationale for the selection of standards and good practices

This annex explains the rationale behind the shortlist of standards and good practices (see Section 2), by looking at a number of different categories of standards and good practices.

International standards

In the desktop research phase the following international standards/frameworks were identified and considered:

- **British Standards Institution (BSI) standards related to security**
  BSI has many good standards for the scope of this work. The Guide to Business Continuity Management (BS 25999) [I10] was chosen since it offers a good solid package on Continuity management. Other BSI standard topics are more or less covered in other standards/frameworks that are included in the mapping. The selection of BS 25999 was also supported by the survey and interviews.
- **Internet Engineering Task Force (IETF) standards (RFCs) related to security**
  IETF standards are excluded from the mapping, as they are too technical, too detailed and highly specific to certain area. They also were rarely mentioned in the survey and interviews.
- **ETSI-standards related to security**
  ETSI standards are excluded from the mapping as they are too technical, too detailed and highly specific to certain area. They also were rarely mentioned in the survey and interviews.
- **ISO-standards related to security**
  Several ISO standards ([I12], [I23], [I24], [I25] and [I26]) were included in the mapping. These standards are widely known and adopted. The selection of those standards was also supported by the survey and interviews.
- **PCI Security Standards Council and other payment & banking standards**
  PCI DSS 1.2 was chosen for the mapping as it is widely known and used within the payment industry. Other banking and payment standards are adequately represented by PCI DSS [24]. The selection of PCI DSS was also supported by the survey and interviews.
- **The Office of Government Commerce (OGC)**
  OGC has the ITIL framework and it was chosen to the mapping. Other OGC publications were not chosen due to the fact that OGC is already represented by ITIL. In addition ITIL covers a lot of different topics [13]. The selection of OGC/ITIL was also supported by the survey and interviews.
- **ISACA**
  ISACA has several different publications on security and the CobiT framework is the most widely know and used. It offers a good high level view to IT. CobiT framework was thus chosen for the mapping. Other ISACA publications were not chosen due to the fact that ISACA was already represented by CobiT [27]. The selection of CobiT was also supported by the survey and interviews.
- **Information Security Forum (ISF)**
  ISF publishes the Standard of Good Practice, which is documented and updated collection of good practices in information security. This was included in the mapping [34]. Forum has also a tool to cross-reference several different standards.

- **National fire protection Association (NFPA)**
  NFPA publishes fire and building safety standards and thus were scoped out.
- **Institute of Internal Auditors (IIA)**
  These focus mainly on auditing and thus are not the primary focus of this work. These were excluded from the mapping.
- **International Social Security Association (ISSA)**
  ISSA is focused on Social security and thus is out of the scope of this work and there are better general standards for network/organisation security, which are more widely accepted.
- **ITU-T Recommendations related to telecommunication security**
  There are a lot of these standards/recommendations and some of them were included in the mapping. Our opinion is that those standards/recommendations that were included in the mapping reflect the best of the original scope of this work. Excluded standards were too technical and too tied to a specific area [7], [8], [9] and [10].

Risk management (excluded)

Reasoning: *These documents are excluded as they cover risk management in general and are not sufficiently security oriented.*

Business continuity management (partially excluded)

Reasoning: *Pending documents such as I7 are excluded. From this category, the BS 25999 standard is included, as it is a de facto standard for business continuity, and covers the topic in sufficient detail.*

Disaster recovery (partially excluded)

Reasoning: *From this category, document I12 is included. From ITIL, it was decided that Service Support and Security Management should be included – disaster recovery does not belong to this group.*

Incident management (partially excluded)

Reasoning: *From this topic, the ITU- T X.1056 document is included, as it is seen most appropriate for the target sector. ITU- T standards were not often mentioned in the survey and interviews.*

System/other security (partially excluded)

Reasoning: *From the ITU-T series, it was decided to include documents X.1051, X.1056, X.800 and X.805. Also the ISO 27000 series is included, specifically ISO/IEC 27001/27002 standards. CobiT is included as well, as it is widely recognized, as well as the Standard of Good Practice from ISF. PCI DSS is an industry de facto standard, enforced by the payment industry and is included.*

Other standards

Many EU countries have regulations for telecommunications with at least one paragraph on security. It was decided to exclude all national laws to reduce the number of standards. Most of those requirements are also either very common or very detailed and hence not suitable for this purpose. Standards and good practices from this category that were excluded or included to the mapping are the following:

- Australian good practices G1-G3. *These documents are excluded from the standard mapping and comparison phase, as we found little evidence of their use outside of the Asia and Pacific region.*
- Austrian good practice G4. *This document is excluded from the standard mapping and comparison phase, as the same topics are covered sufficiently by the ISO 27001/27002 standards and BSI Grundschutz Catalogues.*
- Canadian standards and regulation M1-M6. *The SIDM Policy instruments and Ontario standards are excluded, as there is little evidence that they are in use outside Canada.*
- Danish standards and regulation M7-M14. *These documents are excluded from the standards mapping and comparison phase, as they can be considered as national laws.*
- Finnish good practices G6-G8 and standards and regulation M15-M18. *VAHTI documents (G6-G8) are excluded from the standard mapping and comparison phase, as there are no official translations to English and translating them was not in the scope of this project. KATAKRI (G5) is meant to replace VAHTI 2/2010 and an unofficial translation is available, thus that document is included. The standards and regulation documents are excluded as they are either covered sufficiently in other documents or cover a very narrow and specific topic.*
- German good practice G9. *The IT-Grundschutz-Kataloge (G10) is included as it covers a wide range of topics and gives detailed controls. For the purpose of this project, the English translation "IT Baseline Protection Manual Germany" from 2000 is used. The BSI Standard 100-4 (G9) is excluded, as the business continuity topics are covered in sufficient detail in other included documents.*
- Greek standards and regulation M19-M24. *These documents are excluded from the standards mapping and comparison phase, as they can be considered as national laws.*
- Italian good practices G11-G14 and standards and regulation M25. *These documents are excluded from the standards mapping and comparison phase, as they either cover very small and specific areas or are even too high level such as the application guidelines of Common Criteria. The standard and regulation document is excluded from the standards mapping and comparison phase, as no official English translation was available.*
- Dutch good practices G15-G16 and standard and regulation M26. *These documents are excluded from the standards mapping and comparison phase, as they were not available for review during the project. The standard and regulation document was excluded from the standards mapping and comparison phase, as it can be considered as a national law.*
- Romanian standard and regulation M27. *This document is excluded, as it covers quite a narrow and specific topic.*
- Slovakian good practices G17-G21 and standards and regulation M28-M33. *These documents are excluded from the standards mapping and comparison phase, as they can either be seen as national laws (G20-G21) or otherwise too country-specific. The standards and regulation*

documents are excluded from the standards mapping and comparison phase, as they can be considered as national laws.

- Spanish good practices G22-G24 and standards and regulations M34-M44. *These documents are excluded from the standards mapping and comparison phase, as they either cover very small and specific areas or describe methodologies and frameworks, not controls. The standards and regulation documents were excluded, mainly because this work concentrated on the standards and good practices that help implementing the necessary controls required by the law, not on the law itself.*
- Swedish good practice G25. *This document is excluded as it covers risk analysis, risk management and business continuity on a very high level (the document is only four pages long) and thus does not offer anything new when compared to the other documents.*
- Swiss standards and regulations M45. *These documents are excluded, as there is little evidence that they are in use outside Switzerland.*
- British good practices G26-G27 and standard and regulation M47. *The CPNI telecoms resilience document is excluded as the provided links do not work and it appears as though the document has been removed from the site. The CPNI BGP filtering guidelines document was excluded as it covers a specific product/technology and is thus outside the scope of this project. From the standards and regulation, the UK NICC minimum standard is included, as it fits nicely into the project scope. The UK CESG standard was excluded as the documentation available does not provide a clear list of controls/baseline that should be utilized.*
- US good practices G28, G31-G32 and standards and regulation M48-M49,M51-M53. *From the NIST SP 800 series, documents SP 800-34 [G29] and SP 800-61[G30] are included. SP 800-12 [G28] is excluded as it is already an old document and other documents cover the same topics. The COSO ERM document[G31] is excluded as it is considered a more generic enterprise risk management guideline and not security specific. The US NSTACs reports [G32] are excluded as they do not provide clear security controls/baseline that could be utilized. From the standards and regulation, the Computer security act and FISMA are excluded, as this work concentrated on the standards and good practices that help implementing the necessary controls required by the law, not on the law itself. The FIPS 200 document is included as FIPS is widely recognized and the document in question provides a good security baseline for computer systems. The DOE standards are not included, as there is little evidence that they are in use outside US. The same applies for the NRIC standards.*

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu