Summary of National Reports on IS

Document Details:	
Reference	**CISO SME**
WP/Activity	WP 2 - Reports on IS
Author(s)	IDEC
Character	National Reports & Summary
Date	10.01.2014

Lifelong Learning Programme

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of Content

PART 1 – Summary of National Reports

PART II – The National Reports

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

PART 1 – Summary of National Reports

1) Aim of the Report

Information and eventually knowledge are vital capital for each company and most important for the capacity to compete. Therefore especially the security of information and knowledge should be of general concern to each company. Further more, as companies and organisations store not only company related but also personal related information the legislator shares interests in questions of information security and data protection. Due to structure and organisation, bigger companies are generally better organised in managing necessary processes. Smaller companies on the contrary quite often show a lack of necessary competences.

Against this background the aim of this report is to provide an overview of the demands and needs small and medium sized enterprises (SME) are facing while implementing Information Security Management.

In this regard, an overview of national rules and regulations concerning Information Security relevant for SME will be given. Next qualification offers covering this topic will be identified and their suitability for SME will be estimated. Further more the current situation of SME e. g. regarding their general structure, implementation of Information Security Management, qualification needs of responsible persons will be described. Against this background a possible profile of an "Information Security Officer in SME" will be drafted.

Definition of Terms

As the terms Information Security, Computer Security and Information Assurance are frequently incorrectly used interchangeably the definition of the terms Information Security and Information Security Management used within this report will be clarified here. Furthermore the term Small and Medium Sized Enterprises will be used in accordance to the EU definition:

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms. (Reference: http://en.wikipedia.org/wiki/Information_security, 04.11.2011)

An information security management system (ISMS) is a set of policies concerned with information security management or IT related risks. The idioms arose primarily out of ISO 27001.

The governing principle behind an ISMS is that an organization should design, implement and maintain a coherent set of policies, processes and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk. (Reference: http://en.wikipedia.org/wiki/Information_security_management_system, 04.11.2011)

Lifelong Learning Programme

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Small and Medium Sized Enterprises

Enterprises qualify as micro, small and medium-sized enterprises (SMEs) if they fulfil the criteria laid down in Recommendation 2003/361/EC which are summarized in the table below. In addition to the staff headcount ceiling, an enterprise qualifies as an SME if it meets either the turnover ceiling or the balance sheet ceiling, but not necessarily both.

Enterprise category	Headcount	Turnover	or	Balance sheet total
medium-sized	< 250	≤ € 50 million		≤ € 43 million
small	< 50	≤ € 10 million		≤ € 10 million
micro	< 10	≤ € 2 million		≤ € 2 million

(Reference: http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/index_en.htm, 08.11.2011)

Lifelong Learning Programme

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2) Resume of the National Reports

An overview of the national reports demonstrates that the vast majority of enterprises are SMEs. It is generally accepted that SMEs are the driving force for development and innovation in all economies. However, all partners have concluded that there is a lack of safety awareness and safety measures regarding Information Security, especially in SMEs.

Poland

A study shows that over 77% of polish organizations are aware of high-value information and its security is considered as top priority. All kinds of security systems and information management systems are gaining popularity. Polish entrepreneurs are aware of the importance of information security however the training offers are not adapted to the needs of SMEs and what they can find on the training market is either very detailed and not relevant for SMEs or too expensive and time consuming. There are no information security e-learning courses for entrepreneurs in Poland.

Spain

The main objective of CISO IN SMEs should be awareness of the information security both of SMEs and the public institutions of the EU. Nowadays there is a strong dependence on Information Technology and as a result, a strong demand to keep the information data stored or processed safe.

Austria

Surveys on information security in small enterprises show that a request for comprehensive information on information security is desired and would certainly be welcomed by small businesses. According to a study on information security in small and medium-sized enterprises a big problem factor for the lack of implementation of safety measures was the lack of safety awareness.

Italy

The analysis conducted shows that a profound change is underway. New opportunities, unfortunately, are seen only by a very small part of the Italian economy and businesses. The result is that actors of the production system resorting to information security, is still patchy and mainly undertaken by large companies and an objectively modest number as regards SMEs.

Lifelong Learning Programme

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Bulgaria

A major characteristic of the SME sector in Bulgaria is the overwhelming number of micro enterprises and of small enterprises. As opposed to large companies, the small enterprises have insufficient capacity to manage various technical, organizational and economic problems, because of the lack of resources to employ experts in strategic planning, marketing, trading policy or simply access details to computer systems.

Greece

According to a research of the Federation of enterprises there will be an increased demand in Information Security Officer for the next 10 years. Another research demonstrates that sometimes security measures are not effective while everyone recognizes that an adoption of an effective information security strategy will have to be a priority. The research shows that security is another "victim" of the economic crisis, especially in Greece.

Lifelong Learning Programme

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3) National Rules & Regulations Concerning Information Security in SME

Each partner was asked to give an overview of the national regulations and the legal framework regarding Information Security in small and medium-sized enterprises (SMEs). Many legal acts are established by European Union Directives in accordance with each country's needs. From the comparison of the national reports, we conclude that different national regulations and legal acts apply depending on the situation in each country separately.

Poland

In Poland there are legal acts concerning the Protection of Personal Data and the Protection of Certain Services Provided by Electronic Means. These acts implement Directives of the European Union while there is a National Development Strategy with a main goal the Network and Information Security as part of the information society strategy.

Spain

The main Spanish law dealing with data protection is the Ley Orgánica 15/1999 as well as the Ley 34/2002, on society services information and electronic commerce (LSSICE). In Spain also exists the international standard UNE ISO/IEC 27001 which is configurated as a standard about auditing aspects of Information Security in organizations.

Austria

The Austrian Data Protection Act provides no obligation to nominate a Data Protection Commissioner. However, the creation of enterprise data protection is explicitly welcomed in the Data Protection Act. According to Data Protection 2000, everyone – from customers to suppliers- has the right to have his personal data kept confidential. As far as the quality thinking of SMEs is concerned, an internationally recognised standard, the ISO 9001, has been established a long time ago while recently a standard for information security management, the ISO 27001, has been also established.

Italy

In Italy the protection of confidential data is not optional. In businesses, the Legal Representative is obliged to take all necessary measures to ensure a suitable level of security in line with the value of the data even in the case of companies that are not subject to

Lifelong Learning Programme

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

notifying the privacy guarantor (art. 37 D. Law 196/03). Besides this, the Privacy Code (Decree Law no. 28/05/2012 n. 69) imposes strict security measures to control anyone who comes in contact with 'personal' or 'sensitive' data on natural or legal persons, to ensure that data is not used improperly or unduly disclosed.

Bulgaria

In 2007 laws on personal data protection and electronic management were edited in order to adapt to recent situation. There is mainly the national ordinance concerning information security and the Directive 2006/24/EC of the European Parliament on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or public communications networks.

Greece

In Greece different laws are in force related to the Privacy of Communications and the Protection of Individuals with regard to the Processing of Personal Data. The Hellenic Data Protection Authority enforced the Law 2774/1999 on the Protection of Personal Data in Telecommunications as well as the Law 3115/2003 that establishes the Hellenic Authority for the Information and Communication Security and Privacy in order to protect the secrecy of mailing, the free correspondence or communication in any possible way as well as the security of networks and information.

Lifelong Learning Programme

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

4) Vocational and Continuing Education and Training

The protection of essential data is a key issue for every modern business. The main objective of the project is to verify the knowledge on Information Security (IS) available on SMEs. The project is aimed to develop training curricula for tutors, to develop the e-learning platform, tools and online assessment for tutors, to prepare and implement of pilot using VCC (Vocational Competence Certificate) system.

4.1) Overview of Existing Training Offers in the Field of Information Security

The partners were asked to describe and analyze the qualifications covering Information Security and the services available on the national market. A detailed description of availability of the qualifications and the prerequisites concerning the programs could be found in the complete National Reports.

Poland

The only one standard of certification in terms of Information Security recognised on the polish market is ISO/IEC 27001:2005 while just a few training companies offer the trainings for ISO 27001 Auditors. There is lack of the trainings concerning information security, management of information, cyber safety for SMEs in Poland. There are more offers of postgraduate studies for Information Security Managers.

Spain

For Spain a variety of courses could be identified covering IT Service Management, Data Protection, protection on the Internet, while there is only one course covering the Basics of Information Security for SMEs.

Austria

As in Austria the corresponding job description of a data protection officer does not exist, mainly three courses in information security available with certification could be identified. For instance, there is the Information Security Manager, the Information Auditor and a formation to be a Data Protection Officer. Basics for the Information Security can be also found in 1-day seminars.

Italy

In Italy there are different types of training provided on Information Security. It is worth mentioning the CEFRIEL as well as in training within the IT industry. Another important body that provides training on Information Security is ISACA – Information Systems Audit and Control Association.

Lifelong Learning Programme

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Bulgaria

In Bulgaria a variety of trainings is available covering the topics: fundamentals of security management, secure coding design practices, quality testing, network security, protocols, encryption/decryption, digital forensics, daily tasks in management of Microsoft Forefront family of products for Gateway, SharePoint, exchange servers.

Greece

For Greece two postgraduate courses could be identified concerning Information Security and Computer Forensics as well as Science in Information Technology. In addition, there is a program for certified information security manager.

4.2) Overview of Existing Information Services Regarding Information Security

The existing services concerning the Information Security is inconsequent. Besides the courses mentioned above, there are also some freely accessible internet sites that provide information especially for Information security.

Poland

For Poland six main providers could be identified referring to public and private institutions. A variety of topics is covered including security threats, security bulletins, the protection of Personal Data, the internal security of the Republic of Poland and its citizens as well as postal and telecommunications.

Spain

In Spain S21SEC is one of the main providers regarding Information Security. Services are designed to ensure compliance with legislation, regulations and safety standards that apply to organizations based on their activity.

Austria

In Austria there are freely accessible Internet sites that provide information specifically for SMEs on information security, as well as fee-based services. Experts in information security provide consulting and analysis of the existing security system and assist companies in planning and implementing security measures.

Italy

In Italy the 'Search Security' is one of the sites that offer free support and advice for the world of ICT security. Research conducted on the site shows how several consumer products companies, designed for information security, have created special products designed for the needs of SMEs.

Lifelong Learning Programme

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Bulgaria

For Bulgaria six main providers could be identified that offer services regarding Information Security.

Greece

In Greece there are two main providers with free access that protect the individual's rights and supervise telecommunications and postal market.

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

5) Description of Target Group

After a brief description of the existing services regarding information technology, the partners were asked to describe the persons working in SMEs that should be trained and qualified in order to ensure the data and information protection.

5.1) SME (in general)

Poland

In Poland the vast majority of companies (99.8%) are small and medium that operate primarily in services and trade (76%), and less often in construction (13.4%) and manufacturing (10.6%). A majority, 92.1% of all businesses in the SME sector are natural persons conducting economic activity. According to Central Office of Statistics the company operating in Poland generates nearly three-quarters of Polish GDP (71.8% in 2011). In the structure of the contribution to the GDP SMEs generate 47.3% of GDP, including the smallest companies – 29.6%.

Spain

SMEs in Spain are often family businesses. The majority of them are operating in the service sector, followed by commerce. It is worth mentioning that the business with zero employees constitutes 52% of companies. There are numerous reasons that lead companies to consider the management of Information Security, as a regulatory requirement in order to increase competitiveness and profitability.

Austria

Based on a study presented by the Austrian Security Forum (ASF), we came to the conclusion that data protection and data security in Austria are one of the important functions of the internal IT departments. In 2010 99.6% of Austrian companies were SMEs. They achieved approximately 60% of all revenues and approximately 57% of the gross value added of market-oriented economy. More than one third of all businesses involve companies with only one employee while family- businesses dominate the Austrian economy.

Italy

From surveys conducted by ISTAT (year 2009) on the classification of SMEs in Italy, Italian companies in the main have up to 9 members of staff. Micro enterprises constitute 94.7% of the overall national entrepreneurial network, with 96.6% working in service activities and 82.1% in industry in the strict sense of the word. One of the critical issues for Italian micro-enterprises is the close relationship between the business and family dimension. Finally, most companies are aware of the importance of information security, but the level of 'maturity' of solutions used is still very heterogeneous.

Bulgaria

SMEs are the backbone of the Bulgarian economy. According to the last data provided by the Bulgarian Small and Medium Enterprises Promotion Agency (BSMEPA), in 2010, there were 353588 enterprises in the non-financial sector of Bulgarian economy and their number slightly decreased on a year ago.

Lifelong Learning Programme

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Greece

The SME sector in Greece is more dependent on micro enterprises than in other European countries. In Greece, 98% of businesses are small, having less than 10 employees. The majority of companies engage in the wholesale and retail trade by carrying 43% of the total turnover.

5.2) Persons to be trained (in particular)

As mentioned above, partners were asked to identify persons working in SMEs who should be trained and qualified in the sector of Information Technology.

Poland

In Poland electronic means are essential in order to perform daily work and to run a business. Owners of the micro, small and medium enterprises are in the focus of this project as they are responsible for the data protection in their companies.

Spain

As far as Spanish SMEs are concerned, the target group should be the director/ owner, the head of the information technologies, the personal data protection officer, the sales management as well as all the employees.

Austria

In Austria decisions regarding IT security are in 80% of the company made by the management or at least they are made by their inclusion. Especially in small companies the directors are responsible for all matters, including the security issue. The target group is not focused on IT professionals, but to people across a variety of jobs, which have basic IT skills.

Italy

Based on a study, there is a major need for protection from computers risks in businesses and especially in SMEs. In Italian SMEs, the target group suitable for a complete training in IT security should be the enterprise managers.

Bulgaria

The target group is IT security, owners of micro and SMEs, employees with basic IT skills, Managing Directors, IT Managers as well as Sales Managers.

Greece

Information security is important for the boss and every employee of an organization or a SME. Besides this, the owner of a SME should also be trained in order to ensure that all information is secure.

Lifelong Learning Programme

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

6) Resume

Based on the results of the national reports, common training needs regarding Information Security can be summarised as follows:

Prerequisites of Target Group

- Basic IT knowledge
- No formal qualification in IS or data protection
- Imperative for every business activity

To be considered Surrounding Conditions

- In most countries there are no e-learning courses regarding Information Security
- Lack of time and money

Central Training Topics

- Overview and understanding of national regulations regarding IS
- Principles of Information Security Management
- Understanding the importance of the security of information especially in SMEs

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

PART 2 – The National Reports

This project has been funded with support from the European Commission.This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.