Information security and privacy standards for SMEs

Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises

DECEMBER 2015

www.enisa.europa.eu

European Union Agency For Network And Information Security

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.

Authors

Clara Galan Manso (ENISA), **Evangelos Rekleitis** (ENISA),

Fotis Papazafeiropoulos (EY) and **Vasilios Maritsas** (EY).

ENISA was supported by **EY Greece** in this project under contract D-COD-15-C15.

Editor(s)

European Union Agency for Network and Information Security
For contacting the authors please use isdp@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

We would like to express our gratitude to the following individuals for participating in the interviews and/or external review process of the report (in no particular order):

Panagiotis Papagiannakopoulos (EY)**, Claus C. Houmann** (ImproveIT), **Aggeliki Tsoxou** (Ionian University), **Ian Glover** (CREST), **Raj Atwal** (KPMG UK), **Vasilis Tountopoulos** (ATC Innovation Lab), **Brian Honan** (BH Consulting), **Arthur Leijtens** (Bicore), **Scott Cadzow** (Cadzow Communications Consulting), **Jon Shamah** (EJ consultants), **Wouter van Gils** (EY) and **Steve Furnell** (Plymouth University).

Acknowledgement should also be given to ENISA colleagues who helped in this project, in particular: **Prokopios Drogkaris** and **Adrian Belmonte Martin**.

ISBN 978-92-9204-159-5, DOI 10.2824/829076

Table of Contents

Executive Summary

Context of this study

European SMEs are increasingly dependent on their information systems and networks to provide services to customers and meet their business objectives. The use of new technologies brings new opportunities for enhanced business performance and operations, but also introduces several information security and privacy risks. Addressing these risks plays a significant role in business success and development nowadays, as growing security threats[1] may potentially disrupt business continuity and cause monetary, reputational, as well as other types of losses to SMEs.

In parallel, new information security and privacy standards are being drafted and proposed to support organizations to integrate best practices into their procedures and mitigate risks. To this end, a wide and effective adoption of information security and privacy related standards by SMEs across Europe can be a beneficial factor for fostering their growth, competitiveness and innovation.

In this context, ENISA has carried out this project under its Work Program 2015[2], with the objective of providing a set of relevant recommendations regarding how to increase the adoption of information security and privacy standards in SMEs. These recommendations are targeted to EU and MS policy makers; standards developing organizations; and professional, industry and small businesses associations.

To reach relevant conclusions, an extensive analysis was conducted in order to investigate the status of security and privacy standard adoption in European SMEs, the main drivers that can motivate SMEs towards the adoption of these standards and, especially, the perceived existing barriers for SMEs in this area. The methodology of the study consisted in interviews with subject matter experts and analysis of available studies in the area. The report identifies as well existing information security and privacy standards that can be used by European SMEs, presenting a list of standards that could be considered for adoption by SMEs, along with descriptions of these standards.

Key findings

The analysis conducted for this study, based on the interviews with subject matter experts and review of available studies, shows that, despite rising concerns on information security risks, the level of SMEs information security and privacy standard adoption is relatively low. The main existing drivers and barriers that contribute to the limited uptake of information security and privacy standards in European SMEs have been identified to be the following:

I. Drivers

Mitigating information security risks

- ✓ Threats to information security and privacy, varying from inadvertent events to deliberate attacks, pose significant risks to any organization nowadays.
- ✓ Adoption of information security and privacy standards is an effective means to mitigate these risks.

Increasing consumer trust

[1] ENISA Threat Landscape 2014: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014

[2] ENISA Work Programme 2015: https://www.enisa.europa.eu/publications/programmes-reports/enisa-work-programme-2015

- ✓ Users are becoming more concerned when handling their data to businesses and trust is becoming a relevant decision factor.
- ✓ Adoption of standards indicates to customers that the organisation is committed to enforce security mechanisms for protecting their data.

Proactively demonstrating commitment towards regulatory compliance

- ✓ In many cases SMEs need to demonstrate compliance with information security and privacy requirements derived by national or EU legislation.
- ✓ Implementing, maintaining and enforcing internal policies through the use of standards as a supporting tool is an effective mean to proactively show a commitment with regulations.

Achieving competitive advantage

- ✓ Proof of compliance to an acknowledged standard provides reassurance both to providers and business customers.
- ✓ This constitutes a possible competitive advantage when dealing with corporate clients both from the private and public spheres.

II. Barriers

Barriers related to knowledge and engagement

- ✓ SMEs are in general not aware of the available standards that may assist them mitigate technology risks and there are limited single points of reference that SMEs can use.
- ✓ Standards implementation requires commitment of resources that otherwise an SME would allocate into more transparent business activities.
- ✓ Management does not yet perceive clearly how implementing these standards adds business value to their organisation and there is a prevailing perception that cyber-attacks are mainly threatening large enterprises.
- ✓ The design of standards is mainly driven from larger size organisations and thus many standards are not easily scalable for use by SMEs.

Barriers related to available capabilities and resources

- ✓ In SMEs that assume the ICT function internally, an employee is responsible for security along with his/her other ICT operational responsibilities, which leads to limited dedication for ICT security.
- ✓ Meanwhile, in SMEs where it is outsourced, the lack of internal knowledge hardens the negotiation with providers on security features or contracts.
- ✓ Implementation of information security and privacy standards can be demanding in terms of financial resources and getting the necessary budget can be a challenging task.
- ✓ Many SMEs do not have still a solid foundation of effective information security risk management.

Barriers related to shortage of standards in specific areas

- ✓ There are limited European or international standards designed to assist small organizations towards ensuring appropriate protection of personal data.

Barriers related to implementation aspects

- ✓ Many statements of the standards are challenging for SMEs in order to clearly identify the tasks and activities that must be conducted.
- ✓ There is a lack of adequate implementation guidelines with specific detailed steps on how to apply each information security and privacy requirement.
- ✓ Standards rely on processes that might not yet be implemented in a small organization and standard adoption will require the design or reengineering of internal core processes.

Recommendations

Based on the analysis from the findings on enabling factors and barriers to pursuing standard adoption, the study proposes the following key recommendations to improve the information security and privacy standardisation level in the European SME community:

Increasing knowledge and engagement

- ✓ EU public administrations should develop centralized catalogues with extended information of existing information security and privacy standards that are scalable for, and applicable by, SMEs.
- ✓ Public and private information security awareness organizations at all EU levels should create specific campaigns targeting SMEs on how information security and privacy standards can help them protect their core business assets and processes.
- ✓ Organizations developing information security standards should promote the participation in the development process of SMEs coming from a variety of sectors.

Driving adoption and compliance

- ✓ EU public administrations and/or industrial organizations should promote the development of certification schemes targeted at SMEs to boost information security and privacy standard adoption.
- ✓ EU public administrations should promote the establishment of voluntary reference standards that presume conformity with regulations in the area of information security and privacy.
- ✓ EU public administrations should assess enforcing standard compliance for contracts related to their information supply chain or to personal data handling.

Facilitating implementation

- ✓ Standard developing organizations should consider creating security and privacy standards targeting specifically SMEs which take into account their specific features and processes.
- ✓ Public and private information security organizations could support SMEs by developing easy to follow implementation guidelines focusing on the scoping and initial stages of implementation.
- ✓ Standards applicable by SMEs could incorporate maturity levels with different sets of requirements to facilitate a phased implementation.
- ✓ SMEs should be incited to deploy security by default configurations to facilitate later standard adoption, and software vendors can support SME by ensuring secure default configurations in products targeting small organizations.

Increasing capabilities

- ✓ SMEs should be encouraged to designate an Information Security Officer to ensure ownership of the information security and data protection functions.
- ✓ Member States should create professional training programs to provide foundation training for Information Security Officers.
- ✓ Public administrations at all EU levels should provide incentives to SMEs to adopt security and privacy standards.

Fostering cooperation

- ✓ International, European and national SDOs, as well as industry associations, should work together towards developing a harmonized plan to create information security and privacy standards specifically designed for SMEs.

1 Introduction

The European Commission defines micro, small and medium-sized enterprises as enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding 50 million euro, and/or an annual balance sheet total not exceeding 43 million euro[3]. SMEs comprise more than 99% of all European businesses. In the past five years, they have created around 85% of new jobs and provided two-thirds of the total private sector employment in the EU[4].

Small and Medium Enterprises (SMEs) have paramount importance for the innovation, growth and development of the economy, both at the European and national level and they are a priority focus sector for governments' economic policy. The prominence of their role and growth has been recognised by the European Institutions and the Member States through multiple policy actions aiming to promote SMEs' development, by helping them to tackle the obstacles and problems that obstruct their business development.

Nowadays, SMEs are increasingly dependent on their information systems and networks to provide services to customers and meet their business objectives. If micro enterprises are excluded, the vast majority of SMEs relies on some form of information system and many of them already have an online presence. Electronic communication networks, interconnected information systems and digital services are an essential part of an increasing number of SMEs[5].

In parallel with the growing ICT adoption by SMEs, emerging information security and privacy threats are becoming an increasing concern. Due to the constant and evolving threat landscape and the progressively developing corporate risk exposure, SMEs nowadays face significant information security risks that threaten their business[6]. SMEs need to implement formal information security processes, technical mechanisms and organisational measures. Without such safeguards, SMEs may be severely impacted by inadvertent threats or deliberate attacks on their information systems and networks, which could ultimately lead to negative business effects.

To support organizations in adopting best security practices, a significant number of information security and privacy standards have been developed and published during the last decade by international or European standard developing organisations, professional or expert associations (See Annex A for a comprehensive list of information security and privacy standards). These standards aim to assist organisations to effectively manage and strengthen their information security safeguards, and reduce risks in acceptable levels, all the while maintaining a competitive advantage in today's online world and ensuring protection of business assets.

There are many drivers for SMEs to pursue the adoption of an information security or privacy standard. Yet their level of standard adoption in this area is still low and their uptake is not largely perceived as a priority. The analysis conducted for this study, through interviews with subject matter experts and research on available studies, shows that there are several perceived barriers for SMEs to embrace standards in the security and privacy field, and that the low standard adoption rate can be improved by undertaking specific actions to overcome these barriers. One of the primary barriers is that there is a limited awareness in the

[3] EC. 2015. The new SME definition - User guide and model declaration. European Commission, Enterprise and Industry Publications: http://ec.europa.eu/research/bitlys/sme_definition.html

[4] Entrepreneurship and Small and medium-sized enterprises (SMEs). http://ec.europa.eu/growth/smes/index_en.htm

[5] Tim Mazzarol (2015) SMEs engagement with e-commerce, e-business and e-marketing, Small Enterprise Research, 22:1, 79-90. DOI: 10.1080/13215906.2015.1018400

[6] David R. Han, (2012) SME Cybersecurity and the Three Little Pigs. ISACA Journal Volume 6

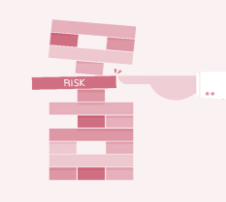
SME community of the potential business and economic value of standardisation in the information security and privacy field, as well as limited existing initiatives towards supporting the implementation of information security and privacy standards specifically targeting small and medium organizations.

Implementing information security and privacy standards is perceived as being challenging by SMEs. This might be partially caused by SMEs' specific needs and characteristics not having been largely taken into consideration during the standards development process, making many standards complex for SMEs with simple internal procedures. SMEs primarily use standards as guidance and the maturity and rigour levels are very likely to vary considerably from one organization to another.

Although SMEs have already taken some steps, there is still a long way towards a wide adoption of information security and privacy standards as a means to mitigate the risks introduced by the velocity and complexity of business and technology changes, and of cyber threats. SMEs should be encouraged to take bolder proactive steps in order to deal with and prevent information security and privacy threats and attacks. Prioritising their efforts towards adopting information security and privacy standards can enhance their visibility, add value and provide a competitive advantage to their organisation, which will enable them to achieve and maintain a robust security posture.

2 Drivers for pursuing information security and privacy standards

Mitigating information security risks



- ✓ Threats to information security and privacy, varying from inadvertent events to deliberate attacks, pose significant risks to any organization nowadays.
- ✓ Adoption of information security and privacy standards is an effective means to mitigate these risks.

The fast-growing and increasingly more complex cyber threat landscape poses a greater risk than ever to organisations, including small and medium organizations. Use of new technologies provides opportunities for enhanced business performance but also introduces potential security risks that must be mitigated. Threats to information security and privacy, varying from inadvertent events to deliberate attacks, pose significant risks to any organization nowadays. Without safeguards, SMEs may suffer severe impact on their information systems and networks, which can ultimately lead to negative business effects. Adoption of information security and privacy standards is an effective means to mitigate these risks.

Increasing consumer trust

- ✓ Users are becoming more concerned when handling their data to businesses and trust is becoming a relevant decision factor.
- ✓ Adoption of standards indicates to customers that the organisation is committed to enforce security mechanisms for protecting their data.

According to the Eurostat 2014 information security barometer[7], concerns among internet users on risks associated with online transactions are raising; especially mistrust on how their personal data are used and the security of online payments. Users are becoming more concerned when handing their data to businesses and trust is becoming a relevant decision factor that can give an advantage to well-prepared organizations. Increasing customers' confidence is emerging as a significant driver for adopting information security and privacy standards in enterprises. Adoption of standards indicates to customers that the organisation is committed to enforce security mechanisms for protecting their data and in this way it might create added value for an SME. Moreover, whenever personal data are involved, customer expectations are met, since they feel that their personal information is well protected, and as a result trust is generated.

Proactively demonstrating commitment towards regulatory compliance

- ✓ In many cases SMEs need to demonstrate compliance with information security and privacy requirements derived by national or EU legislation.
- ✓ Implementing, maintaining and enforcing internal policies through the use of standards as a supporting tool is an effective means to proactively show a commitment with regulations.

In many cases SMEs need to demonstrate compliance with information security and privacy requirements derived by national or European legislation, industry specific regulations and contractual obligations. Failure

[7] Special Eurobarometer 423 Cybersecurity Report (2015): http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf

to comply with these requirements may have negative impact and long-term consequences to the business of the SMEs. These consequences are very transparent to management and as a result they are committed and support efforts towards compliance. The specific compliance requirements are in many cases aligned with information security and privacy standards controls. Implementing, maintaining and enforcing internal policies through the use of standards as a supporting tool is an effective means to proactively show a commitment with regulations in the area of information security and privacy.

Achieving competitive advantage

- ✓ Proof of compliance to an acknowledged standard provides reassurance both to providers and business customers.
- ✓ This constitutes a possible competitive advantage when dealing with corporate clients both from the private and public spheres.

Finally, standards can offer a significant competitive edge to SMEs by facilitating the improvement of the products and services they offer. Proof of compliance to an acknowledged standard provides reassurance both to providers and business customers, adds credibility to the organization and increases confidence by demonstrating commitment to protecting the information assets handed to the SME by customers. When an SME adopts an information security standard, customers will likely have more assurance in establishing and maintaining business relationships with the organisation, and this can constitute a possible competitive advantage when dealing with corporate clients both from the private and public spheres.

3 Barriers to SME adoption of information security and privacy standards

3.1 Barriers related to knowledge and engagement

Knowledge of applicable standards

- ✓ SMEs are not in general aware of the available standards that may assist them mitigate technology risks
- ✓ There are limited single points of reference that SMEs can use.
- ✓ SMEs face difficulties with the identification of the standards that will meet their specific business objectives or those they should comply with due to sectorial requirements.

Several information security and privacy standards have been developed and published by international or European standards development organizations and by industry associations during the last years. There are limited single points of reference, at an EU or MS level, that SMEs can use in order to identify which standard is the most suitable for them and better covers their business needs and requirements. SMEs are not largely aware of the available standards that may assist them mitigate technology risks; the majority of SMEs are only familiar with a limited number of standards (e.g. the ISO/IEC 27000 series).

Moreover, security requirements are spread in numerous different standards and documents. SMEs face difficulties with the identification of the standards that will meet their specific business objectives and needs, or even those they should comply with due to sectorial requirements. Thus, SMEs must identify relevant standards, aggregate and correlate requirements in order to identify overlaps and inter-dependencies. This makes it complex for SMEs to determine which standards are suitable for them, taking into consideration all business, legal, regulatory and contractual requirements and obligations.

For example, SMEs that store, process or transmit cardholder and customer/personal data may not be aware of specific obligations, as defined by relevant standards (e.g. PCI Data Security Standard[8]). Although PCI DSS must be implemented by all entities that store, process or transmit cardholder data from major credit card companies, small merchants and service providers are not required to explicitly validate compliance. However in the event of a security breach, they may be subject to penalties if it is proved they were not compliant.

Management commitment

- ✓ Standards implementation requires commitment of resources that otherwise an SME would allocate into business activities with a more transparent return of investment.
- ✓ Management does not yet perceive clearly how implementing these standards adds business value to their organisation.

[8] Payment Card Industry Data Security Standard (PCI DSS): https://www.pcisecuritystandards.org/security_standards/

In today's economic environment, SMEs need to focus their efforts on staying competitive within their core operations, further expanding into other territories and markets, and surviving in the current dynamic business atmosphere. Achievement of growth (e.g. new markets, customers, products, higher revenue), innovation (e.g. use of new technologies to interact with customers in more efficient and effective ways) and corporate governance, in order to provide stakeholders with confidence, are usually the top priorities for European SMEs. Moreover, SMEs need to achieve growth with limited resources, which they need to allocate carefully by taking into account strict time and budget considerations.

Meanwhile, information security and privacy risks are transforming into a relevant issue in all organizations which require management's attention and commitment. Indeed, adoption of new technologies impacts every aspect of business function; it is therefore becoming increasingly visible that technology risks are threatening the core business processes and they must be effectively managed and mitigated.

Information security risks had historically been assigned as the sole responsibility of the IT department and were not considered a strategic business risk requiring an organisation-wide attention. But information security has in the last years been recognized to add a strategic value to the strategy pyramid of organizations, rather than as a necessary evil to protect the information assets from potential attackers and exposure risks.

However, many SMEs still choose to take a reactive approach, as opposed to a proactive approach (i.e. respond to a security incident after it has happened and not act in order to prevent it). Furthermore, adoption of information security and privacy standards requires commitment in terms of time and resources that otherwise an SME would allocate into business activities with more transparent return of investment. It is difficult for management to perceive clearly how implementing these standards adds business value and provides competitive advantage to their organisation.

By contrast, for SMEs operating in regulated environments it is easier to engage management, gain their attention and commitment, and acquire the necessary budget. Without this compliance driving force, experts perceive that there is not enough motivation for adopting information security and privacy standards; making it difficult for IT and/or security professionals to convince management in that particular direction.

Perceptions on cyber threats targeting SMEs

- ✓ There is a prevailing, but wrongful, perception that cyber-attacks are mainly threatening large enterprises.
- ✓ Recent reports indicate that every type of business, regardless of its size, is a potential target of a cyber-attack.

There is a concern among experts participating in the study about the prevailing perception that cyber-attacks are mainly threatening large enterprises and SMEs remain largely unaffected from these threats since they do not store, process or transfer information as critical as larger organizations. Indeed, according to a 2013 survey conducted among small business by the US National Small Bussiness Associaton[9], only 30% of small business were very concerned about being vulnerable to a cyber attack, while 60% were only somewhat concerned. Because of this misconception, many SMEs consider that information security standards are designed mainly for the large enterprises and they don't grasp the added value of adopting them.

However this is not the case; recent reports indicate that every type of business, regardless of its size, is a potential target of a cyber-attack. The UK Government Information Security Breaches Survey[10] indicates that,

[9] 2013 Small business technology survey, US National Small Bussiness Associaton, http://www.nsba.biz/wp-content/uploads/2013/09/Technology-Survey-2013.pdf

[10] HM Government (2015) 2015 Information Security Breaches Surveyhttp://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf

among the survey participants, 90% of large organizations suffered a security breach in 2015, with this figure standing at 74% for small organizations. Since large enterprises usually have a stronger security culture with robust security controls, less determined malicious attackers may be discouraged by the protection mechanisms that are in place, targeting instead SMEs, which offer less resistance.

Contribution in the development process

- ✓ The design of standards is mainly driven from larger size organisations and is oriented to cover their multiple processes.
- ✓ Many standards are not easily scalable for use by SMEs.
- ✓ Non-technological SMEs do not participate extensively in the standards development and review processes.

Non-technological SMEs do not participate extensively in the standards' development and review process, and thus their particular business needs and objectives are not largely taken into account. The design of standards is mainly driven from larger size organisations and is oriented to cover their multiple processes. As a direct consequence, standards assume that organisations have a thorough understanding of all technical and non-technical terms, as well as enough resources (both financial and non-financial), to implement the requirements. Hence, many standards are not instantiated for use by SMEs with simpler procedures in place.

Although standard developing organizations (SDOs) make an effort to engage SMEs in their activities, it is difficult for non-technological SMEs to participate, due to a combined lack of available resources and expertise. For example, although 25% of ETSI members are SMEs[11], most of them are related to the information technology sector, which means they have extensively more information security capabilities than the average SME. This leads to the average SMEs' characteristics, nature and capabilities not being largely taken into consideration during the development phase of standards.

3.2 Barriers related to available capabilities and resources

Cybersecurity capabilities

- ✓ In SMEs that assume the ICT function internally, an employee is responsible for information security along with his/her other ICT operational and time pressing responsibilities.
- ✓ In SMEs that outsource the ICT function, the lack of internal knowledge in information security complicates the negotiation with providers on custom security features or contracts.
- ✓ Various multidisciplinary security roles are usually required to manage these standards, and this goes beyond the capacity and expertise of SMEs.

While SMEs rely increasingly on ICT systems to support their business processes, their size only justifies the employment of a small number of dedicated individuals for ICT functions, if any at all. Some SMEs decide to internalize the ICT services while others opt to outsource them. Regardless of the ICT management model selected, the ultimate responsibility over protecting corporate and client information contained in information systems remains within the SME.

[11] European Telecommunications Standards Institute: http://www.etsi.org/index.php/membership

If the ICT function is assumed internally, usually an employee is responsible for information security along with other ICT related responsibilities. These individuals are already in charge of governance, design, implementation and monitoring the whole ICT infrastructure; thus it comes as an added effort for them to manage the organisation's security aspects. It is understandable that the top priority for these employees is to maintain the availability of information systems and networks that support the business operations, hence security processes are somehow overlooked.

When SMEs decide to outsource ICT services to specialized companies, they also face difficulties, as the lack of internal knowledge in information security complicates the negotiation with providers on custom security features or contracts. SMEs typically acquire standardised, off-the-shelf, services and products under fixed, boilerplate, contracts and SLAs. Moreover, SMEs in many cases are not largely aware of specific security products and solutions that could assist them secure their data and business information.

Limited access to information security capabilities can constitute one of the most critical vulnerabilities for an SME, exposing the organisation to several risks. This absence of capabilities might manifest itself, for example, in difficulties in the interpretation of the technical focused aspects of standards. Standards in many cases contain fairly general statements that actually require a degree of specialised knowledge to translate into a specific context. Even in the case of outsourced services, understanding of information security requirements is necessary to draft and enforce appropriate contract clauses with suppliers.

Finally, one of the first actions required to adopt information security and privacy standards is to allocate information security roles and responsibilities to specific employees. Indeed, various multidisciplinary security roles are usually required to manage these standards, and this usually goes beyond the human resource capacity of the average SME.

Budget and resources

- ✓ Implementation of information security and privacy standards can be demanding in terms of financial resources and getting the necessary budget from management can be a challenging task.
- ✓ In many cases SMEs need to seek the assistance of an experienced consultant in order to support them, which adds financial costs to the process.

The lack of budget for information security seems to be one of the largest impediments for adopting standards. Implementation of information security and privacy standards can be demanding in terms of financial resources and getting the necessary budget from management can be a very a challenging task, especially if compliance with these standards may not be perceived to be on the top priorities for small businesses managers.

In the last years, the change of the allocated budget for information security has been relatively positive, with studies such as the EY Global Information Security Survey[12] finding that around 50% of organizations planned to increase their information security budget in 2015. However, the year-on-year increase of information security budgets is more visible in large organisations, and less pronounced in SMEs. For example, the UK Government Information Security Breaches Survey[13] found that while 42% of UK large businesses planned to increase their information security budget in 2015, this figure is reduced to 7% in the case of small businesses.

[12] EY Global Information Security Survey 2014: https://webforms.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf

[13] HM Government (2015) 2015 Information Security Breaches Surveyhttp://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf

In many cases SMEs seek assistance of an experienced consultant in order to support them on the design and implementation phases of standards. Active guidance from external consultants may also be required during the first steps of the operation of a new information security model in order to ensure future compliance. Additionally, organisations usually need to acquire technical and software solutions in order to comply with the technical requirements of the standards. Finally, there is a shortage of knowledge in SMEs regarding relevant products, scalable to their size, which can help them meet the security and privacy requirements of the standards, while meeting their business needs.

There are some additional costs that, albeit small compared to the previously mentioned activities, cannot be overlooked. First, the existence of fees that some SDOs request to provide access to the standard's documentation. In some cases, the small budget required for purchasing a standard is not easily accepted by management. Moreover, implementation of a standard might be followed by certification from a third-party assessor (which needs to be renewed periodically); thus introducing additional costs that need to fit in the overall business strategy of the company.

Finally, implementation of standards is also time-consuming. Limited staff to assist with the deployment, as well as maintenance of compliance, makes the whole adoption process a lengthy task. Consequently, SMEs may allocate resources into business activities with a more transparent return of investment.

Risk management

- ✓ Many SMEs do not have still a solid foundation of effective information security risk management, and there are limited available risk management frameworks scalable to small organizations.
- ✓ The risk environment of the organization must be known in order to determine the applicable standards.

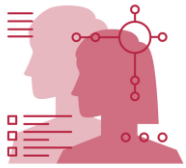
A primary objective of any SME is to achieve growth, however, this must be performed, as within any organization, inside appropriate risk and control boundaries. With information security being an emerging field, small organizations may not apply the same degree of rigorousness to assess the information security risks as they would for financial, legal, regulatory or operational risks. Furthermore, many SMEs operate in sectors where there is no strong culture of risk management to build upon. Due to these factors, many small and medium enterprises do not still have a solid foundation of effective information security risk management.

SMEs are slowly, but gradually, becoming aware of the potential impact of disrupted business services due to technology incidents, as well as how risk management can protect them from threats and vulnerabilities applicable to their information assets. According to the UK Government 2015 Information Security Breaches Survey[15], only 49% of SMEs participating in the survey had conducted a security risk assessment in the previous year.

Prior to selecting and implementing any specific standard, SMEs, as any organization, must identify the existing information security and privacy risks they are exposed to. Indeed, standard adoption can be a helpful tool to develop a structured approach to mitigate risks, however the risk environment of the organization must be known in order to determine the best applicable standards. There are, however, limited available risk management frameworks and implementations guidelines scalable to small organizations that can enable and support them in this area.

3.3 Barriers related to shortage of standards in specific areas

Specific privacy standards



- ✓ In the last years, there has been a shift in the perception for enterprises on the importance of protecting personal data.
- ✓ There are limited European or international standards designed to assist small organizations towards ensuring appropriate protection of personal data.

In the past, SMEs were not largely aware of the risks posed to their customers' data, resulting from the lack of privacy preserving controls. However, in the last years, there has been a shift in the perception of the importance of protecting personal data. The 2015 UK Government Information Security Breaches Survey[14] found that the single, largest driver for information security expenditure in enterprises is protecting customer information, followed by protecting the organization reputation; with these two factors together accounting for more than half of the responses.

This would support the notion that SMEs consider privacy protection as a competitive advantage that will mitigate business risks and enhance customers' trust. But there is still some work to be done in order to make SMEs fully conscious on the risks and the value of protecting customers' data for their business.

Another important aspect to consider when discussing the relevance of privacy protection in SMEs are the EU and Member States personal data protection legal frameworks. The regulatory requirements have become more mature over the years, even addressing specific industry sectors, and European SMEs need to be compliant with their national personal data protection laws. The Proposed General Data Protection Regulation[15], will further develop the privacy protection legal framework in the EU, introducing a harmonised approach across EU Member States.

Yet, the ongoing issue for organizations is that they do not have enough guidance on which specific controls they should implement in order to be compliant with personal data protection laws. Even in regulated industry sectors, enterprises find it sometimes challenging to translate into concrete measures the specific privacy requirements they must comply with. This problem becomes more pressing for SMEs, as they have limited ICT governance.

Regulations focus on the objective and standards can support them by providing guidance on the means to achieve it. However, only a limited number of standards with regards to privacy have been developed and published, and no specific implementation guidelines have been further analysed and developed in depth, compared to the situation for information security controls. Aside from the ISO/IEC 29100:2011 [34] and the CEN CWA 16113:2010 [44], which provide a general privacy framework, there are limited European or international standards designed to assist organisations all types of organizations, especially small ones, towards ensuring appropriate protection of personal data.

[14] HM Government (2015) 2015 Information Security Breaches Survey.
http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf

[15] Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/legalcontent/en/TXT/?uri=CELEX:52012PC0011

3.4 Barriers related to implementation aspects

Standards' complexity

- ✓ Many statements of the standards are challenging for SMEs in order to clearly identify the tasks and activities that must be conducted.
- ✓ SMEs do not fully realize the rationale behind many security and privacy requirements.
- ✓ SMEs are largely unaware of the flexibility that standards provide with regards to the implementation and monitoring of controls.

One relevant barrier to information security and privacy standards adoption in SMEs is that these standards have been generally documented in a way that makes it difficult for non-technological SMEs to comprehend. Standards tend to be framed in terms that are most directly applicable to large scale and enterprise organisations. There is a concern among experts that the language used contains terms that are too complex for small organizations and this is hardening the early stages of the adoption process.

There is a perception that, in general, SMEs do not fully realize the rationale behind many security and privacy requirements, either related or unrelated to technology. Indeed, if technology aspects are excluded, the information security and privacy organizational processes, as dictated by standards, are considered by experts quite elaborate and challenging by SMEs, depicting complex business processes that do not map the SMEs environment.

Furthermore, SMEs are generally unaware of the flexibility that standards provide with regards to the implementation and monitoring of controls. Current standards do not clearly depict the flexibility offered, resulting sometimes in misinterpretations. SMEs seem to be failing in appropriately tailoring the standards based on their business needs and the applicable legal, regulatory and contractual requirements.

Guidance on scope

- ✓ SMEs generally interpret differently what activities must be performed in order to achieve compliance.
- ✓ There is a lack of adequate implementation guidelines with specific detailed steps on how to apply each information security and privacy requirement.

Another critical factor that hardens the adoption process and is highly associated with the complexity of standards is that SMEs quite often tend to interpret standards in very different ways based on their own perspective and understanding. In fact, typically there is more than one interpretation for each information security and privacy requirement in standards, but not all interpretations are equally suitable for every organization. It is not uncommon for SMEs to interpret differently what activities must be performed in order to achieve compliance.

Consequently, a challenge for SMEs is not just to know what they need to do, but also how they must do it, with regard to their business context. Experts believe SMEs face difficulties to understand how standards operate in detail and how standards can be further customized and combined in order to meet their specific business needs.

Besides, there is a lack of adequate implementation guidelines with specific detailed steps on how to apply each information security and privacy requirement (i.e. translating it to specific technological and organizational controls). As a result, experts interviewed stated that SMEs many times either do more than they can afford or of what is needed in order to achieve compliance and may end up either under protecting, or overprotecting their information assets and allocating more resources than required.

Organisational and procedural controls

- ✓ Organizations are still more familiar with technical aspects of information security, rather than organisational and procedural ones.
- ✓ Standards rely on processes that might not yet be implemented in a small organization
- ✓ Standard adoption will require the design or reengineering of internal core processes.

Aside from the deployment of technical controls, conformity to information security standards also calls for organizational and procedural changes that will complement the required controls. In the past, information security was regarded more as a technical issue and as such many organizations are still more familiar with technical aspects rather than organisational and procedural ones. Most SMEs have usually implemented, at least, the basic infrastructure and software components required for protecting their business assets (i.e. firewalls, anti-virus protection mechanisms etc.).

But nowadays there is a clear consensus that information security transcends technology and also involves organizational and procedural aspects. Indeed, most security and data breaches are caused by human errors, misconfiguration and/or failure of information systems and network components (according to IBM's recent Security Services 2014 Cyber Security Intelligence Index report[16], 95% of security incidents involve human error as a contributing factor).

As such, SMEs do not require only guidelines for deploying security products and technical controls. They also need support to design, implement and maintain clear, structured, effective and realistic organisational and procedural mechanisms to ensure adequate levels of conformity with information security standards.

Furthermore, the complete set of processes covered in some standards is not scalable to small organizations, and these standards rely on processes that might not yet be implemented, or being conducted in an informal way, in a small organization (e.g. asset management, capacity management, etc.). Thus, standard adoption will require the design or reengineering of internal core processes. There is an associated effort to all organizational changes, which may introduce additional management overhead in order to tailor the implementation. A small organization may need additional guidance on how to make these changes, communicate them and put them into practice.

There is an associated effort to all organizational changes, and a small organization may need additional guidance on how to make these changes, communicate them and put them into practice. There is an associated effort to all organizational changes, and a small organization may need additional guidance on how to make these changes, communicate them and put them into practice.

[16] IBM (2015) Security Services 2014 Cyber Security Intelligence Index.
http://www.ibm.com/developerworks/library/se-cyberindex2014/se-cyberindex2014-pdf.pdf

4 Recommendations for increasing the level of adoption of standards

Based on the interviews with experts and the available existing research - conducted to assess the level of standards adoption in SMEs and the main existing barriers to adopt standards - the study proposes a series of recommendations in order to facilitate the adoption process of information security and privacy standards by small and medium businesses. The following sections elaborate on specific measures on how SMEs could be effectively and efficiently supported to cope with the perceived barriers to the standards' adoption process.

The proposed recommendations have been grouped in five domains:

- Increasing knowledge and engagement: Making SMEs more familiar with the standards that they can apply, as well as of the benefits they can obtain by implementing them.
- Driving adoption and compliance: Providing mechanisms to foster standard adoption by SMEs through certification and regulatory compliance.
- Facilitating implementation: Making standards more easily deployable by SMEs by adapting to their specific characteristics.
- Increasing capabilities: Increasing cybersecurity capabilities in SMEs in order to make them ready for standard adoption.
- Fostering cooperation: Creating a common strategy among stakeholders towards a global strategy for improving information security and privacy standardization for SMEs.

Recommendations are targeted at EU and MS public administrations; international or European SDOs; professional, industry and small business associations, and future interested parties; such as insurance companies. They identify areas where standards can be further improved and develop adequate strategies and instruments that could be introduced to support SMEs in the adoption of standards in these fields.

Increasing knowledge and engagement	✓ Developing information security and privacy standards catalogues ✓ Raising general awareness on the benefits of adopting standards ✓ Increasing SME participation in the development and review process
Driving adoption and compliance	✓ Defining certification schemes ✓ Promoting regulatory compliance through standard adoption
Facilitating implementation	✓ Creating standards specifically targeting SMEs ✓ Developing implementation guidelines ✓ Implementing a phased approach during the adoption process ✓ Promoting security and privacy by design
Increasing capabilities	✓ Creating ownership of the information security function ✓ Providing support for standard adoption
Fostering cooperation	✓ Promoting international, European and national collaboration

Table 1 Recommendations to increase the level information security and privacy adoption in SMEs

4.1 Increasing knowledge and engagement

Developing information security and privacy standards catalogues

- ✓ EU Institutions and Member States should develop centralized catalogues with extended information of existing information security and privacy standards that are scalable for, and applicable by, SMEs.
- ✓ Standards catalogues should include information on existing certification schemes and auditing processes for each identified standard.

As a prerequisite to increase adoption, SMEs should be well informed about the published information security and privacy standards along with all the relevant details and accompanying information (e.g. how to reach them, what are the primary benefits and objectives, what are the specific implementation requirements etc.). SMEs should be able to reach the appropriate level of knowledge of existing standards and to perform an analysis and conclude on the standards that are most relevant to them.

To facilitate this process for SMEs, the development of centralised catalogues/inventories of all published information security and privacy standards that are scalable for, and applicable by, SMEs would be very beneficial. These catalogues, at an EU or Member State level, would serve as a point of reference with the objective to assist SMEs to identify standards and clearly describe compliance requirements, facilitating the early steps of the adoption process.

The catalogues should be comprehensive, including all relevant available standards at international, European or industry level that are scalable for SMEs, and explicative, featuring a high level description of the specific security and privacy requirements that must be implemented to comply with the specific standards. In addition, the inventories should depict areas of overlaps and dependencies between the several standards in order for the SMEs to identify how standards are complementary and interconnected.

Moreover, an added value to catalogues would be to include information about the certification and auditing process that can be undertaken to prove compliance with the each specific standard (e.g. more accessible information about accredited organisations that provide certification services, how to find them, what services they provide, etc.).

Raising general awareness on the benefits of adopting standards

- ✓ Public and private information security awareness organizations at all EU levels should create specific campaigns targeting SMEs on how information security and privacy standards can help them protect their core businesses.
- ✓ All stakeholders in the information security domain should collaborate to find effective ways to reach SMEs, especially at the management level.

General awareness, and specific engagement at the management level of SMEs, should be further enhanced in order to ensure the successful buy-in of the standards adoption process. SMEs should have access to substantiated information both on (a) the risks and the potential impact as a result of security incidents (e.g. negative affect of consumers' trust, damage of reputation, loss of revenue, financial penalties, loss of competitive advantage etc.) and (b) the benefits and the business value of standards for their organisation. Only that way SMEs will integrate the real value of adopting an information security and privacy standard for their business. The security and privacy culture must be enforced with a top down approach within the organisation.

Public administrations in Member States, International or European SDOs, professional, industry and small business associations, such as National Chambers of Commerce, can assist in that particular direction by planning, organising and delivering appropriate awareness initiatives and campaigns with regards to benefits

of information security and privacy standards, targeting directly SMEs. The main objective of the initiatives should be to strengthen the confidence of SMEs to take up implementation of standards and make them aware of the real business value and benefits. These activities should have defined clear vision and objectives, effective communication plans and measurable metrics in order to assess effectiveness of the program. Moreover, campaigns should be conducted over an extended amount of time, on a regular basis and focus primarily on the executive level of SMEs.

Fulfilment of the awareness gap is a real challenge. The SME universe is large, heterogeneous and not always easy to approach through a single channel. Awareness and engagement cannot be resolved by one single entity, it must be an industry-wide collaboration. As such, more interaction and collaboration among the aforementioned organisations, and especially among the small business and sectorial associations, is considered as prerequisite in order to ensure the success of the campaigns.

Increasing SME participation in the development and review process

- ✓ Standards development organizations publishing information security standards should promote the participation in the development process of SMEs from a variety of sectors.
- ✓ Small businesses associations should be engaged as an effective broker to include SMEs needs in the standard development process.

Although SMEs are currently actively involved in the standard development process in European SDO's (for example, a quarter of ETSI members are SMEs[17]), their representation is mostly comprised of SMEs in the ICT sector. Information technology SMEs constitute a particular case among SMEs, as they are much more aware of the importance of information security and how it relates to their business needs.

In order to have a broader view of the SME specific environment, SMEs from other sectors should be incentivized to have a more active role in the design and development phases of the standards. A possible method to increase involvement is to encourage SMEs to participate in the standards' review process to provide their feedback and comments, bringing that way together key stakeholders from SME sectors around EU, to reach a common and unified approach.

Finally, as individual SMEs may be difficult to engage directly, due to their limited resources, a viable alternative would be to promote the involvement of small businesses associations, which are well aware of the specificities of SMEs, in these activities. This way there will be an alignment between the particular business needs of the SMEs and the objectives of the standards.

4.2 Driving adoption and compliance

Defining certification schemes

- ✓ EU governments and information security organizations should promote the development of certification schemes targeted for SMEs to boost information security and privacy standard adoption.
- ✓ SMEs certification schemes should incorporate maturity ratings and different levels of certification.

[17] ETSI SMEs portal: http://www.etsi.org/about/who-we-are/smes

An effective method to recognize efforts in adoption of information security and privacy standards in SMEs would be the development of third party certification schemes for SMEs, with assessment and certification activities performed by accredited external certification bodies. The schemes should incorporate the requirements of the SME specific standard(s) and provide different levels of assessment and certification based on the phases of the adoption process that characterizes each standard. Moreover, the introduction of maturity ratings in the certification scheme could further assist organizations to identify the exact compliance level they like to achieve, drive adoption of next certification levels and provide to their customers and other stakeholders confidence and transparency on the organization's information security management.

Such certification schemes could follow the European common framework for accreditation under EC Regulation 765/2008[18], applied already in the ISO 27001 certification scheme[19], or could be based on an industry led framework, such as the Cloud Security Alliance STAR certification[20] for security assurance in the cloud. These schemes could evolve to a competitive differentiator for SMEs and drive rapid adoption of the standard within the next years. Finally, it is important that the total cost of certification process should be affordable to SMEs.

Some steps in this direction have already been taken at a Member State level. For example, the Cyber Essentials Scheme[21], developed by the UK Department for Business, Innovation and Skills, is a framework targeted at SMEs. The document *"Cyber Essential Scheme: Requirements for basic technical protection from cyber-attacks"*[22] provides a set of technology focused requirements, using a simplified language, that can be applied by small organizations, focusing on five domains (boundary firewalls and internet gateways, secure configuration, access control, malware protection and patch management). The scheme offers two levels or certification, cyber essentials and cyber essentials plus, which support the phased approach as a mean to facilitate compliance.

Promoting regulatory compliance through standard adoption

- ✓ EU public administrations should promote the establishment of voluntary reference standards that presume conformity with regulations in the area of information security and privacy.
- ✓ EU public administrations should assess enforcing standard compliance for contracts related to their information supply chain or to personal data handling.

In order to foster adoption, SMEs covering specific criteria (e.g. operating in specific markets, providing certain information products and services, storing, processing or transferring customer personal information)

---

[18] 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 (Text with EEA relevance). http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:l33248

[19] ISO 27001 information security management standard. http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[20] Cloud Security Alliance STAR certification. https://cloudsecurityalliance.org/star/

[21] Cyber Essentials Scheme. https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

[22] Cyber Essentials Scheme - Requirements for basic technical protection from cyber-attacks. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf

could be driven to voluntary comply and be certified against specific information security and privacy standards, as a method to proactively demonstrate regulatory compliance. This would create, as a secondary effect, confidence to customers, key stakeholders and other interested parties that their information assets and the information that the SMEs manage on their behalf is adequately protected.

An approach to drive this adoption would be to promote the establishment of voluntary reference standards. Adoption of reference standards is not compulsory for organizations, but compliance is presumed when conformity with the reference standard is met. This model poses benefits for all interested stakeholders. From a regulator point of view, it provides flexibility with regards to setting technical requirements that might be too detailed or dynamic to fit in the regulatory lifecycle. Furthermore, it facilitates achieving harmonization in the market and facilitates compliance. From the perspective of the organization adopting the standard, it greatly helps to increase customer confidence by demonstrating proactive compliance with the existing regulatory framework. An example of this approach can be observed in Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market[23].

The proposed EU General Data Protection Regulation[24], foresees as well the possibility of establishing voluntary certification mechanisms to help data subjects to quickly assess the level of data protection of relevant products and services. Although the details regarding how this certification scheme will be implemented and which standards will be used to assess compliance are not yet determined, this provision is expected to foster adoption of personal data protection standards by EU organizations. Indeed, proving compliance will be advantageous for an organization because of the growing concern among European users of how their personal data are handled, and furthermore because of the reputation for the European data protection regulatory framework to be one of the strictest and most advanced globally.

Another possible model to drive adoption is by enforcing compliance for certain contracts with the public administration, as is the case for the UK Cyber Essentials Scheme. The UK Government (through its *"Procurement Policy Notice on the use of Cyber Essentials Scheme certification"*[25]) encourages achieving this certification for Central Government contracts that involve handling of personal data and provision of certain IT products and services. Although a Cyber Essentials certification is not compulsory for organizations, providers will need to prove by a third party assessment that they meet the information security requirements set in the scheme, making conformance with the scheme the most effective way to prove compliance.

[23] Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market.

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[24] Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52012PC0011

[25] UK Cyber Essentials Scheme Procurement Policy.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/368247/Cyber_Essentials_Scheme_draft_PPN_28_10.pdf

4.3 Facilitating implementation

Creating standards specifically targeting SMEs

- ✓ Standards developing organizations should consider creating security and privacy standards targeting specifically SMEs.
- ✓ Security awareness organizations should develop recommendations on security practices that can be easily applied by SMEs.
- ✓ A further step in the development of standards for SMEs should be to take into account specific requirements for different business sectors.

A critical recommendation to facilitate the adoption process is to design and develop specific standards that meet the needs and capabilities of SMEs. These standards should be oriented and be applicable to SMEs through the incorporation of their specific requirements; thus imposing lower financial and non-financial adoption costs. Standards that are specifically developed for SMEs are generally expected to have a greater adoption rate by the SME community.

The scheme of the existing standards should be reengineered in order to ensure that the proposed process can be mapped to those of an average SME. Critical areas of existing standards, where more in depth explanation is required, should be identified and further elaborated. Specifications from existing standards should be analysed and modified appropriately in order to be applicable to the organisation of the SME community. Security requirements on these standards could be more straightforward and structured (e.g. like SANS top 20 critical security controls[26]). Furthermore, the new standards should take into consideration the organisational structure and characteristics of SMEs (e.g. most of the actions and activities are conducted by a limited number of human resources).

Finally, since the SME sector is encompassed by various organisations with many specificities, different business needs and priorities, as well as various legal, regulatory and contractual security and privacy requirements (e.g. size, industry), a further step in this direction could be taken by classifying SMEs and developing standards targeted for each specific category to accommodate diversity.

Generalised security and privacy profiles (e.g. business needs, size, industry, etc.) could be defined to enable SMEs to roughly match themselves to a profile in order to get an indication of the security requirements that they should implement. Since the SME sector is composed by diverse entities, organisations could be classified and assigned to one or several specific profiles.

Developing implementation guidelines

- ✓ Standards development and information security awareness organizations should develop easy to follow implementation guidelines.
- ✓ Business associations should consider creating programs to enhance information security capabilities with advice for SMEs on how to implement standards.
- ✓ Guidelines should focus on the initial stages of implementation, especially on customised scoping.

Current information security and privacy standards are perceived as complex for SMEs to implement, especially for small enterprises, and additional external guidance would be beneficial. A helpful support action would be the development, by International or European SDOs, or professional and industry

[26] SANS top 20 critical security controls. https://www.sans.org/critical-security-controls/

associations, of clear, structured and easy to use implementation guidelines and best practices handbooks with realistic and concrete examples using simple terms and easily translatable language.

The main objective of these documents would be to enable SME personnel with general ICT knowledge and skills to understand the specific activities and tasks that must be conducted in order to achieve compliance with each security and privacy requirement of the standards. It is essential that these sources provide reliable, up-to-date and detailed information to guide SMEs to implement the requirements step by step. Moreover, implementation guidelines should also encompass information with regards to exact security processes and procedures that must be in place to ensure adequate security safeguards (e.g. awareness, log monitoring, vulnerability management etc.). These guidelines should contemplate both internalized and outsourced ICT services models, providing advice to increase governance of ICT security in outsourced models.

Special emphasis and attention should be given to the initial scoping and planning phases of the adoption process. Although most standards are flexible, usually SMEs face some difficulties to appropriately customise the standards based on their business needs and the applicable legal, regulatory and contractual requirements. As such, further guidance should also be provided on how to identify the exact range of the scope during the implementation of the standards as well as how to get the most out of the flexibility that standards provide. SMEs should be assisted in the customisation and interpretation of the standards to the point that they are economically, technically and financially relevant to their business.

Small Businesses Associations are well positioned to provide SMEs with advice and assistance towards adopting and implementation standards. With this objective, stakeholders in information security area, such as governments and information security industry entities, should support small business associations in the development of more information security and privacy capabilities and expertise.

As an example, the French national information security agency (ANSSI) in partnership with the general confederation of small and medium enterprises (Confédération Générale du patronat des Petites et Moyennes Entreprises - CGMP), has published a reference guide of 12 good information security practices (Guide des bonnes pratiques de l'informatique[27]). The guide is written in easy to understand language and includes examples and clear implementation guidelines.

Implementing a phased approach during the adoption process

- ✓ SMEs should perform an information security risk assessment before engaging in the adoption of specific security and privacy standards.
- ✓ Standards applicable by SMEs should incorporate maturity levels with different sets of requirements to facilitate a phased implementation.

Recommending the implementation of a phased approach during the implementation of information securityand privacy standards can facilitate adoption. As an initial step, it is critical for SMEs to perform a risk analysis and assessment process prior to engaging in the adoption of any standard. Only upon completion of risk assessment activities and determination of the organisation's risk environment, SMEs should be in the position to develop their own security strategy, define the exact scope of standardisation and conclude on the most suitable and appropriate standards that should be implemented in order to effective mitigate identified risks.

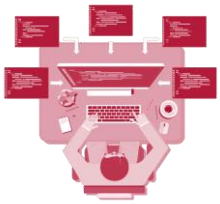
A phased approached could be enforced by incorporating a maturity rating scale in the standards. Standards could have specific maturity levels defined for each profile. Each maturity level would have certain security

[27] Guide CGPME: les bonnes pratiques de l'informatique. http://www.ssi.gouv.fr/guide/guide-des-bonnes-pratiques-de-linformatique/

and privacy requirements (ranging from the easiest to the most difficult as the level increases) that should be implemented in order to reach the specific level, be certified and advance to the next one. The first level should only cover basic controls and quick wins that are easy for SMEs to implement and, therefore, comply with in order to add a layer of protection to their information assets.

As the maturity level increase the safeguards would become more advanced, sophisticated and hence difficult to implement and maintain compliance with. The maturity rating scale would assist SMEs to comprehend their current maturity level in terms of information security and privacy capabilities, address gaps with the standards and develop a roadmap to reach desired levels. Finally, in order for SMEs to be able to monitor deployment effectiveness and efficiency, identify gaps and encourage controls improvement, specific metrics should also be defined for each maturity level.

Promoting security and privacy by design



- ✓ SMEs should be encouraged to implement security by default configurations to facilitate later standard adoption.
- ✓ Software vendors should implement security and privacy default configurations in products targeting small organizations.

One of the key factors for facilitating the adoption process of standards is to focus on the information security and privacy from the beginning of an information system design model. SMEs can adopt the security by design approach as they setup, configure and implement their corporate infrastructures, information systems and networks. Specific guidelines should be developed indicating and accommodating the means by which secure architecture can be taken into consideration during the early stages of an SME establishment.

Overall, integrating information security and privacy principles and controls in the early stages of implementation can create efficiencies and make compliance with standards much easier in the future phases. As such, organisations across the SME sector will be able to achieve a consistent and common security maturity level through the implementation of basic security and privacy safeguards that adequately protect corporate and customers' information assets, prevent a large percentage of cyber-attacks and overall lower information security and privacy risks.

To support SMEs, software vendors should be encouraged to provide products targeted to small organizations that offer appropriate default security configurations, facilitating the installation and maintenance process for staff with general information knowledge. Although most software products available nowadays in the market come with the possibility to establish granularity in the security features that can be configured, interfaces and options may be difficult to understand for non-specialized staff. For SMEs that outsource their ICT services, clear guidelines on security aspects to consider of contracting third party services would be very helpful.

In the case of privacy, further steps should be taken by software vendors to provide systems that ensure that customer information is protected with a sufficient level of granularity. Privacy controls, aligned with European regulations, are still not fully translatable in all available software products targeting small organizations.

4.4 Increasing capabilities

Creating ownership of the information security function

- ✓ SMEs should be encouraged to designate an Information Security Officer to ensure ownership of the information security and data protection functions.
- ✓ Member States should create professional training programs to provide foundation training for Information Security Officers.

SMEs should be encouraged to assign a specific role to a resource that will carry out the security responsibilities required to protect the critical business information assets, emphasising more on the organisational and procedural aspects of information security and privacy. Even if this resource has only part time dedication, and regardless on whether the ICT services are assumed internally or externally, the allocation of responsibility to a specific employee of the organization is an effective way to ensure ownership of the information security functions.

The information security officer should be responsible of designing and implementing a strategy that is aligned with corporate goals and objectives. He/she should also be responsible for managing all security-related interactions within the organisation, as well as those external to the organisation, such as providers of ICT services. As information security officer, he/she must also ensure that appropriate procedural, technical and physical security controls are in place, directly or through appropriate contracts and SLAs. Finally, he/she should have adequate information security skills and expertise to comprehend and enact the guidance that standards require.

Member States should promote the creation of professional training programs on information security and privacy principles for employees that will take up this role in small organizations. Taking into consideration that these individuals do not necessarily have extensive technical or legal foundation on the area, and their dedication will be on a part time basis, these programs should be designed for security and data protection officers to understand the risks, principles and rationale behind the existing and proposed security measures.

Providing support for standards adoption

- ✓ Public administrations at all EU levels should provide incentives to SMEs to adopt security and privacy standards.
- ✓ Public and private organizations in the area of professional training should develop programs to enhance information security skills of SME staff.

SMEs could be assisted in order to overcome the obstacle of financial cost in implementing standards and achieving certifications. Economic incentives can be provided with programs directly managed by public administrations at the EU and member state level and/or through professional, industry and small business associations at a national level. These incentives may include, but not limited to:

- Reduced cost/free direct access to standards for SMEs.
- Funding (e.g. credits, grants, subsidies or tax incentives) associated to standard adoption and third party certification.
- Affordable access for SMEs to professional training on information security standard implementation.

Among the above, it is critical to provide incentives for training SME personnel on information security and privacy in order to further develop their skills and therefore the overall cybersecurity capacity of the organization. These initiatives may include well organised seminars, trainings, hands-on labs, workshops that are delivered by several different delivery methods such as live or virtual, classroom-style, guided study, etc.

4.5 Fostering cooperation

Promoting international, European and national collaboration

✓ International, European and national SDOs, as well as industry associations, should work together towards developing a harmonized plan to create information security and privacy standards specifically designed for SMEs.

Strong, clear and flexible international cooperation and collaboration between extended communities of cyber security stakeholders is required in order to drive and foster adoption of standardization for the SME sector. This entails efforts at the national, European and international level. European and international SDOs should work together with SME professional and industry associations in order to develop an effective and concrete plan as well as a harmonized approach towards creating and driving adoption of standards specifically designed for SMEs.

A European wide approach in this field to ensure harmonization can be positive for the advancement of the Digital Single Market[28]. European SMEs should be able to adopt European information and privacy standards that are easily recognized throughout Europe by their potential customers. Furthermore, standards that prove compliance with European regulations, especially in the area of data protection, can be perceived by EU costumers a proactive way to enhance their trust. Additionally, further emphasis should be given to engage business, professional and industry associations in this cooperation for standardization, to ensure that the exchange of relevant information on topics related to information security and privacy standardization takes into consideration the specific needs of the SME community.

[28] European Comission 10 priorities: Digital Single Market: http://ec.europa.eu/priorities/digital-single-market/

Annex A: Existing information Security and Privacy Standards for SMEs

In order to understand the availability of information security and privacy standards that can be applied by SMEs, the study gathered and analysed information regarding existing standards in these areas. For this purpose, a desk research was conducted in order to identify what specific published standards are related to information security and privacy and can be adopted by SMEs. The main sources for research were:

- International or European SDOs, professional associations, industry associations etc.
- Specific standards targeting SMEs.
- Standards for codes of practices, for securing business processes, for procuring secure products, for regulatory compliance etc.

The outcome of the research is the following list of well-known information security and privacy standards that are categorised in terms of:

- The context of each standard (i.e. risk management, privacy, business continuity etc.).
- The industry each standard refers to (i.e. health, financial services etc.).

Further information about the description of each specific standards can be found in Annex B.

Information Security

The following section contains a list of cross industry standards related to the information security domain in general, aiming to provide adequate protection of information and information assets from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction and ensure preservation of confidentiality, integrity, and availability.

ISO/IEC 27001:2013 Information security management systems – Requirements	[7]
ISO/IEC 27002:2013 Code of practice for information security controls	[8]
ISO/IEC 27003:2010 Information security management system implementation guidance	[9]
ISO/IEC 27004:2009 Information security management – Measurement	[10]
ISO/IEC 27013:2012 Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	[12]
ISO/IEC 27014:2013 Governance of information security	[13]
ISO/IEC TR 27016:2014 Information security management - Organisational economics	[15]
ISO/IEC 27032:2012 Guidelines for information security	[19]
ISO/IEC 27033-1:2009 Network security - Part 1: Overview and concepts	[20]
ISO/IEC 27033-2:2012 Network security - Part 2: Guidelines for the design and implementation of network security	[21]

ISO/IEC 27033-3:2010 Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues	[22]
ISO/IEC 27033-4:2014 Network security - Part 4: Securing communications between networks using security gateways	[23]
ISO/IEC 27033-5:2013 Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)	[24]
ISO/IEC 27034-1:2011 Application security - Part 1: Overview and concepts	[25]
ISO/IEC 27039:2015 Selection, deployment and operations of intrusion detection systems (IDPS)	[31]
ISO/IEC 27040:2015 Storage security	[32]
CSA Cloud Controls Matrix	[38]
BSI PAS 555:2013 Cyber security risk. Governance and management. Specification	[39]
PCI Data Security Standard	[42]
ISF The Standard of Good Practice for Information Security	[43]
UK Gov. Security policy framework	[45]
UK Gov. Cyber essentials scheme	[46]
ETSI GS ISI 001 Part 1: A full set of operational indicators for organisations to use to benchmark their security posture	[48]
ETSI TR 103 305 Critical Security Controls for Effective Cyber Defence	[49]
BSI 100-1 Information Security Management Systems (ISMS)	[50]
BSI 100-2: IT-Grundschutz Methodology	[51]

Risk Management

The following section contains a list of cross industry standards related to the risk management domain, aiming to assist organisations to enhance the effectiveness of their risk management efforts towards measuring, managing and mitigating uncertainties and risks that could negatively compromise their business.

ISO/TR 31004:2013 Risk management - Guidance for the implementation of ISO 31000	[2]
ISO/IEC 27005:2011 Information security risk management	[11]
ISO/IEC 31000 Risk management - Risk assessment techniques	[36]
IEC 31010:2009 Risk management - Risk assessment techniques	[37]

BSI BIP 0076 Information security risk management. Handbook for ISO/IEC 27001	[41]
BSI 100-3: Risk Analysis based on IT-Grundschutz	[52]

Business Continuity Management

The following section contains a list of cross industry standards related to the business continuity management domain, aiming to protect organisations against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise and ensure continuity of critical business functions and processes.

ISO 22301:2012 Business continuity management systems – Requirements	[3]
ISO 22313:2012 Business continuity management systems – Guidance	[5]
ISO/IEC 27031:2011 Guidelines for information and communication technology readiness for business continuity	[18]
100-4: Business Continuity Management	[53]

Data Protection and Privacy

The following section contains a list of cross industry standards related to the data protection and privacy domain, aiming to the adequate protection and privacy of information during their entire lifecycle.

ISO/IEC 27018:2014 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	[16]
ISO/IEC 29100:2011 Privacy framework	[34]
ISO/IEC 29101:2013 Privacy architecture framework	[35]
BSI BS 10012:2009 Data protection. Specification for a personal information management system	[40]
CEN CWA 16113:2010 Personal Data Protection Good Practices	[44]

Incident Management

The following section contains a list of cross industry standards related to the incident management domain, aiming to assist organisations towards detecting, evaluating and managing security incidents and minimising business damage and loss.

ISO/PAS 22399:2007 Societal security - Guideline for incident preparedness and operational continuity management	[6]
ISO/IEC 27035:2011 Information security incident management	[26]
ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence	[30]

Third Party Management

The following section contains a list of cross industry standards for the third party management domain, aiming to assist organisations towards defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships.

ISO/IEC 27036-1:2014 Information security for supplier relationships - Part 1: Overview and concepts	[27]
ISO/IEC 27036-2:2014 Information security for supplier relationships - Part 2: Requirements	[28]
ISO/IEC 27036-3:2013 Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security	[29]

Industry specific standards

The following section contains a list of industry specific standards:

ISO/TR 13569:2005 - Financial services - Information security guidelines [Financial Services]	[1]
ISO/IEC TR 27015:2012 - Information security management guidelines for financial services [Financial Services]	[14]
ISO/IEC TR 27019:2013 - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry [Energy]	[17]
ISO 27799:2008 - Information security management in health using ISO/IEC 27002 [Healthcare]	[33]
ISO 22307:2008 Financial services - Privacy impact assessment [Financial Services]	[4]

Annex B: Description of information security and privacy standards

Information Security

Cross Industry

DOCUMENT ID	7
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 27001:2013 Information security management systems - Requirements
Description	SO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organisations, regardless of type, size or nature.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

DOCUMENT ID	8
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 27002:2013 Code of practice for information security controls
Description	ISO/IEC 27002:2013 gives guidelines for organisational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organisation's information security risk environment(s).
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533

DOCUMENT ID	9
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 27003:2010 Information security management system implementation guidance
Description	ISO/IEC 27003:2010 focuses on the critical aspects needed for successful design and implementation of an Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2005. It describes the process of ISMS specification and design from inception to the production of implementation plans. It describes the process of obtaining management approval to implement an ISMS, defines a project to implement an ISMS (referred to in ISO/IEC 27003:2010 as the ISMS project), and provides guidance on how to plan the ISMS project, resulting in a final ISMS project implementation plan.

Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42105

DOCUMENT ID	10
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 27004:2009 Information security management – Measurement
Description	ISO/IEC 27004:2009 provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an implemented information security management system (ISMS) and controls or groups of controls, as specified in ISO/IEC 27001.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42106

DOCUMENT ID	12
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 27013:2012 Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
Description	ISO/IEC 27013:2012 provides guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43753

DOCUMENT ID	13
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 27014:2013 Governance of information security
Description	ISO/IEC 27014:2013 provides guidance on concepts and principles for the governance of information security, by which organisations can evaluate, direct, monitor and communicate the information security related activities within the organisation.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43754

DOCUMENT ID	15
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC TR 27016:2014 Information security management - Organisational economics
Description	ISO/IEC TR 27016:2014 provides guidelines on how an organisation can make decisions to protect information and understand the economic consequences of these decisions in the context of competing requirements for resources. ISO/IEC TR 27016:2014 is applicable to all types and sizes of organisations and provides information to enable economic decisions in information security management by top management who have responsibility for information security decisions.
Document Type	Technical Report
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43756

DOCUMENT ID	19
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 27032:2012 Guidelines for information security
Description	ISO/IEC 27032:2012 provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular: information security, network security, internet security, and critical information infrastructure protection (CIIP).
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44375

DOCUMENT ID	20
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 27033-1:2009 Network security - Part 1: Overview and concepts
Description	ISO/IEC 27033-1:2009 provides an overview of network security and related definitions. It defines and describes the concepts associated with, and provides management guidance on, network security.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51580

DOCUMENT ID	21
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 27033-2:2012 Network security - Part 2: Guidelines for the design and implementation of network security
Description	ISO/IEC 27033-2:2012 gives guidelines for organisations to plan, design, implement and document network security.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51581

DOCUMENT ID	22
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 27033-3:2010 Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues
Description	ISO/IEC 27033-3:2010 describes the threats, design techniques and control issues associated with reference network scenarios. For each scenario, it provides detailed guidance on the security threats and the security design techniques and controls required to mitigate the associated risks. Where relevant, it includes references to ISO/IEC 27033-4 to ISO/IEC 27033-6 to avoid duplicating the content of those documents.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51582

DOCUMENT ID	23
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 27033-4:2014 Network security -- Part 4: Securing communications between networks using security gateways
Description	ISO/IEC 27033-4:2014 gives guidance for securing communications between networks using security gateways (firewall, application firewall, Intrusion Protection System etc.) in accordance with a documented information security policy of the security gateways.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51583

DOCUMENT ID	24
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 27033-5:2013 Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
Description	ISO/IEC 27033-5:2013 gives guidelines for the selection, implementation, and monitoring of the technical controls necessary to provide network security using Virtual Private Network (VPN) connections to interconnect networks and connect remote users to networks.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51584

DOCUMENT ID	25
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 27034-1:2011 Application security - Part 1: Overview and concepts
Description	ISO/IEC 27034 provides guidance to assist organisations in integrating security into the processes used for managing their applications. ISO/IEC 27034-1:2011 presents an overview of application security. It introduces definitions, concepts, principles and processes involved in application security. ISO/IEC 27034 is applicable to in-house developed applications, applications acquired from third parties, and where the development or the operation of the application is outsourced.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44378

DOCUMENT ID	31
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 27039:2015 Selection, deployment and operations of intrusion detection systems (IDPS)
Description	ISO/IEC 27039:2015 provides guidelines to assist organisations in preparing to deploy intrusion detection and prevention systems (IDPS). In particular, it addresses the selection, deployment, and operations of IDPS. It also provides background information from which these guidelines are derived.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56889

DOCUMENT ID	32
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 27040:2015 Storage security
Description	ISO/IEC 27040:2015 provides detailed technical guidance on how organisations can define an appropriate level of risk mitigation by employing a well-proven and consistent approach to the planning, design, documentation, and implementation of data storage security. Storage security applies to the protection (security) of information where it is stored and to the security of the information being transferred across the communication links associated with storage. Storage security includes the security of devices and media, the security of management activities related to the devices and media, the security of applications and services, and security relevant to end-users during the lifetime of devices and media and after end of use.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44404

DOCUMENT ID	38
Issuing Organisation	Cloud Security Alliance
Document Name	Cloud Controls Matrix
Description	The CSA CCM provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains.
Document Type	Security Controls Framework
URL Link	https://cloudsecurityalliance.org/research/ccm/

DOCUMENT ID	39
Issuing Organisation	British Standards Institute
Document Name	PAS 555:2013 Cyber security risk. Governance and management. Specification
Description	This PAS details a framework for the governance and management of cyber security risk. The requirements of this PAS (publicly available specification) define the outcomes of effective cyber security and include technical, physical, cultural and behavioural measures, alongside effective leadership and governance. It is designed to be scalable and so is suitable for businesses of all sizes.
Document Type	Publicly Available Specifications
URL Link	http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030261972

DOCUMENT ID	42
Issuing Organisation	PCI Security Council
Document Name	Data Security Standard
Description	The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information. PCI DSS provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents.
Document Type	Standard
URL Link	https://www.pcisecuritystandards.org/security_standards/index.php

DOCUMENT ID	43
Issuing Organisation	Information Security Forum
Document Name	The Standard of Good Practice for Information Security
Description	The standard covers the complete spectrum of information security arrangements that need to be made to keep the business risks associated with information systems within acceptable limits, and presents good practice.
Document Type	Standard
URL Link	https://www.securityforum.org/tools/sogp/

DOCUMENT ID	45
Issuing Organisation	UK Government
Document Name	Security policy framework
Description	The security policy framework describes the standards, best-practice guidelines and approaches that are required to protect UK government assets.
Document Type	Framework
URL Link	https://www.gov.uk/government/publications/security-policy-framework

DOCUMENT ID	46
Issuing Organisation	UK Government
Document Name	Cyber essentials scheme
Description	The government has worked with the Information Assurance for Small and Medium Enterprises (IASME) consortium and the Information Security Forum (ISF) to develop Cyber Essentials, a set of basic technical controls for organisations to use. The Cyber Essentials Requirements document sets out the necessary technical controls. From 1 October 2014, government requires all suppliers bidding for certain sensitive and personal information handling contracts to be certified against the Cyber Essentials scheme.

Document Type	Standard
URL Link	https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

DOCUMENT ID	47
Issuing Organisation	European Telecommunications Standards Institute
Document Name	ETSI GS ISI 001 Part 1: A full set of operational indicators for organisations to use to benchmark their security posture
Description	This document provides a full set of information security indicators (based on already existing results and hands-on user experience), covering both security incidents and vulnerabilities. These one become nonconformities when they violate organisation's security policy. The present document is meant to aid CISOs and IT security managers in their effort to evaluate and benchmark accurately their organisation's security posture.
Document Type	Standard
URL Link	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=37802

DOCUMENT ID	48
Issuing Organisation	European Telecommunications Standards Institute
Document Name	ETSI GS ISI 001 Part 2: Guide to select operational indicators based on the full set given in part 1
Description	This document provides a full set of information security indicators (based on already existing results and hands-on user experience), covering both security incidents and vulnerabilities. These one become nonconformities when they violate organisation's security policy. The present document is meant to aid CISOs and IT security managers in their effort to evaluate and benchmark accurately their organisation's security posture.
Document Type	Standard
URL Link	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=39405

DOCUMENT ID	49
Issuing Organisation	European Telecommunications Standards Institute
Document Name	ETSI TR 103 305 Critical Security Controls for Effective Cyber Defence
Description	This Technical Report describes a specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of cyber-attacks developed and maintained by the Council of Cybersecurity. The measures reflect the combined knowledge of actual attacks and effective defences.
Document Type	Technical report
URL Link	http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?WKI_ID=45868

DOCUMENT ID	50
Issuing Organisation	Federal Office for Information Security (BSI)
Document Name	100-1 Information Security Management Systems (ISMS)
Description	BSI Standard 100-1 defines the general requirements for an ISMS. It is completely compatible with ISO Standard 27001 and moreover takes the recommendations in ISO Standards of the ISO 2700x family into consideration. It provides readers with easily understood and systematic instructions, regardless of which methods they wish to use to implement the requirements.
Document Type	Standard
URL Link	https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html

DOCUMENT ID	51
Issuing Organisation	Federal Office for Information Security (BSI)
Document Name	100-2: IT-Grundschutz Methodology
Description	The IT-Grundschutz Methodology progressively describes (step by step) how information security management can be set up and operated in practice. The tasks of information security management and setting up a security organisation are important subjects in this context.
Document Type	Standard
URL Link	https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html

Financial Services

DOCUMENT ID	1
Issuing Organisation	International Organisation for Standardisation
Document Name	ISO/TR 13569:2005 Financial services - Information security guidelines
Description	ISO TR 13569:2005 provides guidelines on the development of an information security programme for institutions in the financial services industry. It includes discussion of the policies, organisation and the structural, legal and regulatory components of such a programme. Considerations for the selection and implementation of security controls, and the elements required to manage information security risk within a modern financial services institution are discussed. Recommendations are given that are based on consideration of the institutions' business environment, practices and procedures. Included in this guidance is a discussion of legal and regulatory compliance issues, which should be considered in the design and implementation of the programme.
Document Type	Technical Report
URL Link	http://www.iso.org/iso/catalogue_detail.htm?csnumber=37245

DOCUMENT ID	14
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC TR 27015:2012 Information security management guidelines for financial services
Description	ISO/IEC TR 27015:2012 provides information security guidance complementing and in addition to information security controls defined in ISO/IEC 27002:2005 for initiating, implementing, maintaining, and improving information security within organisations providing financial services.
Document Type	Technical Report
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43755

Energy

DOCUMENT ID	17
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC TR 27019:2013 Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
Description	ISO/IEC TR 27019:2013 provides guiding principles based on ISO/IEC 27002 for information security management applied to process control systems as used in the energy utility industry. Its aim is to extend the ISO/IEC 27000 set of standards to the domain of process control systems and automation technology, thus allowing the energy utility industry to implement a standardized information security management system (ISMS) in accordance with ISO/IEC 27001 that extends from the business to the process control level.
Document Type	Technical Report
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43759

Healthcare

DOCUMENT ID	33
Issuing Organisation	International Organisation for Standardisation
Document Name	ISO 27799:2008 Information security management in health using ISO/IEC 27002
Description	ISO 27799:2008 defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002 and is a companion to that standard. ISO 27799:2008 specifies a set of detailed controls for managing health information security and provides health information security best practice guidelines. By implementing this International Standard, healthcare organisations and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organisation's circumstances and that will maintain the confidentiality, integrity and availability of personal health information.
Document Type	Standard
URL Link	http://www.iso.org/iso/catalogue_detail?csnumber=41298

Risk Management

Cross Industry

DOCUMENT ID	2
Issuing Organisation	International Organisation for Standardisation
Document Name	ISO/TR 31004:2013 Risk management - Guidance for the implementation of ISO 31000
Description	ISO/TR 31004:2013 provides guidance for organisations on managing risk effectively by implementing ISO 31000:2009.
Document Type	Technical Report
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56610

DOCUMENT ID	11
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 27005:2011 Information security risk management
Description	ISO/IEC 27005:2011 provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56742

DOCUMENT ID	36
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 31000 Risk management - Risk assessment techniques
Description	ISO 31000:2009 provides principles and generic guidelines on risk management. ISO 31000:2009 can be used by any public, private or community enterprise, association, group or individual. Therefore, ISO 31000:2009 is not specific to any industry or sector.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43170

DOCUMENT ID	37
Issuing Organisation	International Electrotechnical Commission
Document Name	IEC 31010:2009 Risk management - Risk assessment techniques
Description	IEC 31010:2009 is a dual logo IEC/ISO (single prefix IEC), supporting standard for ISO 31000 and provides guidance on selection and application of systematic techniques for risk assessment.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51073

DOCUMENT ID	41
Issuing Organisation	British Standards Institute
Document Name	BIP 0076 Information security risk management. Handbook for ISO/IEC 27001
Description	Handbook for the use and application of ISO/IEC 27005. It provides specific guidance and advice to support the implementation of requirements defined in ISO/IEC 27001 that relate to risk management processes and associated activities.
Document Type	Handbook
URL Link	http://shop.bsigroup.com/ProductDetail/?pid=000000000030172860

DOCUMENT ID	52
Issuing Organisation	Federal Office for Information Security (BSI)
Document Name	100-3: Risk Analysis based on IT-Grundschutz
Description	The IT-Grundschutz Catalogues of the BSI contain standard security safeguards required in the organisational, personnel, infrastructure and technical areas that are generally appropriate for normal security requirements and to protect typical information domains.
Document Type	Standard
URL Link	https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html

Business Continuity Management

Cross Industry

DOCUMENT ID	3
Issuing Organisation	International Organisation for Standardisation
Document Name	ISO 22301:2012 Business continuity management systems - Requirements
Description	ISO 22301:2012 specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50038

DOCUMENT ID	5
Issuing Organisation	International Organisation for Standardisation
Document Name	ISO 22313:2012 Business continuity management systems - Guidance
Description	ISO 22313:2012 for business continuity management systems provides guidance based on good international practice for planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving a documented management system that enables organisations to prepare for, respond to and recover from disruptive incidents when they arise.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50050

DOCUMENT ID	18
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 27031:2011 Guidelines for information and communication technology readiness for business continuity
Description	ISO/IEC 27031:2011 describes the concepts and principles of information and communication technology (information) readiness for business continuity, and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organisation's information readiness to ensure business continuity.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44374

DOCUMENT ID	53
Issuing Organisation	Federal Office for Information Security (BSI)
Document Name	100-4: Business Continuity Management
Description	The BSI Standard 100-4 points out a systematic way to develop, establish and maintain an agency-wide or company-wide internal business continuity management system.
Document Type	Standard
URL Link	https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html

Data Protection and Privacy

Cross Industry

DOCUMENT ID	16
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 27018:2014 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
Description	ISO/IEC 27018:2014 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61498

DOCUMENT ID	34
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 29100:2011 Privacy framework
Description	ISO/IEC 29100:2011 provides a privacy framework which specifies a common privacy terminology; defines the actors and their roles in processing personally identifiable information (PII); describes privacy safeguarding considerations; and provides references to known privacy principles for information technology.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45123

DOCUMENT ID	35
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 29101:2013 Privacy architecture framework
Description	ISO/IEC 29101:2013 defines a privacy architecture framework that specifies concerns for information and communication technology (information) systems that process personally identifiable information (PII); lists components for the implementation of such systems; and provides architectural views contextualizing these components.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45124

DOCUMENT ID	40
Issuing Organisation	British Standards Institute
Document Name	BS 10012:2009 Data protection. Specification for a personal information management system
Description	This standards provides a framework for maintaining and improving compliance with data protection legislation and good practice. It has been developed to help businesses to establish and maintain a best practice personal information management system that complies with the Data Protection Act 1998.
Document Type	Standard
URL Link	http://shop.bsigroup.com/ProductDetail/?pid=000000000030175849

DOCUMENT ID	44
Issuing Organisation	European Committee for Standardisation
Document Name	CWA 16113:2010 Personal Data Protection Good Practices
Description	This document is targeted for use by Small to Medium size Enterprises (SMEs) in the European Union. It defines a set of voluntary good practices for Operational Protection Measures and appropriate use of Privacy Enhancing Technologies to help businesses and data managers comply with Directive 95/46/EC.
Document Type	CEN Workshop Agreement
URL Link	http://standards.cen.eu/dyn/www/f?p=204:110:0::::FSP_PROJECT,FSP_ORG_ID:34912,413610&cs=1D2E7CD2D46C13C8EEB03F18D1EEAF2B4

Financial Services

DOCUMENT ID	4
Issuing Organisation	International Organisation for Standardisation
Document Name	ISO 22307:2008 Financial services - Privacy impact assessment
Description	ISO 22307:2008 recognizes that a privacy impact assessment (PIA) is an important financial services and banking management tool to be used within an organisation, or by “contracted” third parties, to identify and mitigate privacy issues and risks associated with processing consumer data using automated, networked information systems.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=40897

Incident Management

Cross Industry

DOCUMENT ID	6
Issuing Organisation	International Organisation for Standardisation
Document Name	ISO/PAS 22399:2007
Description	ISO/PAS 22399:2007 provides 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.
Document Type	Publicly Available Specification
URL Link	http://www.iso.org/iso/catalogue_detail?csnumber=50295

DOCUMENT ID	26
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 27035:2011 Information security incident management
Description	ISO/IEC 27035:2011 provides a structured and planned approach to: detect, report and assess information security incidents; respond to and manage information security incidents; detect, assess and manage information security vulnerabilities; and continuously improve information security and incident management as a result of managing information security incidents and vulnerabilities.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44379

DOCUMENT ID	30
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence
Description	ISO/IEC 27037:2012 provides guidelines for specific activities in the handling of digital evidence, which are identification, collection, acquisition and preservation of potential digital evidence that can be of evidential value. It provides guidance to individuals with respect to common situations encountered throughout the digital evidence handling process and assists organisations in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44381

Third Party Management

Cross Industry

DOCUMENT ID	27
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 27036-1:2014 Information security for supplier relationships - Part 1: Overview and concepts
Description	ISO/IEC 27036-1:2014 is an introductory part of ISO/IEC 27036. It provides an overview of the guidance intended to assist organisations in securing their information and information systems within the context of supplier relationships. It also introduces concepts that are described in detail in the other parts of ISO/IEC 27036. ISO/IEC 27036-1:2014 addresses perspectives of both acquirers and suppliers.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=59648

DOCUMENT ID	28
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 27036-2:2014 Information security for supplier relationships - Part 2: Requirements
Description	ISO/IEC 27036-2:2014 specifies fundamental information security requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships.
Document Type	Technical Report
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=59680

DOCUMENT ID	29
Issuing Organisation	International Organisation for Standardisation and International Electrotechnical Commission
Document Name	ISO/IEC 27036-3:2013 Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security
Description	ISO/IEC 27036-3:2013 provides product and service acquirers and suppliers in the information and communication technology (information) supply chain with guidance on: gaining visibility into and managing the information security risks caused by physically dispersed and multi-layered information supply chains; responding to risks stemming from the global information supply chain to information products and services that can have an information security impact on the organisations using these products and services; integrating information security processes and practices into the system and software lifecycle processes while supporting information security controls.
Document Type	Standard
URL Link	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=59688

Annex C: List of Standards Issuing Organisations

The following table lists the standards issuing organisations that were identified during the study.

ORGANIZATION NUMBER	ISSUING ORGANISATION
1	International Organisation for Standardisation (ISO)
2	International Electrotechnical Commission (IEC)
3	International Organisation for Standardisation and International Electrotechnical Commission (ISO/IEC)
4	British Standards Institute (BSI UK)
5	European Committee for Standardisation (CEN)
6	Cloud Security Alliance (CSA)
7	Information Systems Audit & Control Association (ISACA)
8	PCI Security Council (PCI SSC)
9	Information Security Forum (ISF)
10	European Telecommunications Standards Institute (ETSI)
11	Federal Office for Information Security of Germany (BSI Germany)

Annex D: Interviews methodology and content

D.1. Methodology

Two questionnaires were developed which specifically targeted SMEs and organisations involved in the information security and/or standardisation areas. The objective of the questionnaires was to identify and assess the following areas of information security and privacy standards:

- Level of adoption of security and privacy standards
- Perceived obstacles for their adoption
- Enabler factors for the standardisation
- Areas where standardization would be useful
- Strategies that could be introduced to support SMEs in the adoption of security standards.

Following the development of the questionnaires, the potential target audience was identified and concluded on a shortlist of organisations that represented the most relevant participants for the study. The final target audience had a balanced mixture of organisations involved in the following activities:

- International and European standard developing organizations
- Professional and industry associations developing or promoting the use of standards in SMEs, at a European and Member State level
- Small businesses associations, at a European and Member State level
- Existing large initiatives aimed at promoting information security in SMEs, arising from the public or private sector
- SMEs operating at a European and Member State level.

Selected stakeholders of the target audience participated and answered the questionnaire. Follow-up interviews were conducted with identified stakeholders and experts in order to further discuss, elaborate on details and deep dive into the subject. The survey was conducted in the period of June to August 2015.

D.2. Questionnaire for SMEs

Note: *The specific questionnaire was adaptive based on the selection of the participating*.

1. Does your organisation have an information security and/or data protection policy? [*Yes/No*]
2. Are you planning to implement an information security and/or data protection policy within the next two years? [*Yes/No*]
3. What are the main reasons behind this decision? [*Lack of business need, Lack of specialised staff, Implementation is too costly, Other*]
4. Are you planning to adopt an information security and/or privacy standard in order to implement your policy(s)? [*Yes/No*]
5. Please select the security domain(s) the standard(s) your organization is using refer to: [*Risk Management, Data Protection and Privacy, Business Continuity Management, Incident Management, Third Party Management, Other*]
6. Please select which general information security standard: [*List with the general information security standards*]
7. Please select which risk management standard: [*List with the risk management standards*]
8. Please select which data protection and privacy standard: [*List with the data protection and privacy standards*]
9. Please select which business continuity management standard: [*List with the business continuity management standards*]

10. Please select which incident management standard: [*List with the incident management standards*]
11. Please select which third party management standard: [*List with the third party management standards*]
12. What are the main drivers for your organization for implementing an information security and privacy standard(s)? [*Regulatory compliance, Contractual obligations, Business need, Information security need, Reputation / Differentiation from competitors, Protecting clients' information, Other*]
13. In which aspects do you think the standard(s) add(s) business value to your organization? [*Stakeholders confidence, Organizational data security and governance, Conforming to legal obligations, Conforming to contractual obligations, Competitive advantage, Reducing security incidents costs, Other*]
14. Have you followed / are you following a standard(s) to implement any of your information security policies? [*Yes, No*]
15. Have you ever tried to adopt an information security and/ or privacy standard? [*Yes, No]*
16. *What are the main reasons behind this decision? [Implementation of standards is too costly, Lack of business need, Lack of specialized staff to do implementation, Existing standards are too complex for my business, Other*]
17. What were the main difficulties and obstacles that your organisation faced during the standard's adoption process? [*free text*]
18. How long did on average the adoption process last / is lasting so far? [*Less than 6 months, More than 6 months and less than 1 year, More than 1 year*]
19. Did you / Are you using utilise external assistance? If yes, to what extent? [*Yes, mostly external, Yes, mixed resources, No*]
20. What are the lessons learned from the whole adoption process? [*free text*]
21. In which ways do you think can the standard(s) or the adoption process be further improved in order to assist your organisation? [Reducing the complexity of the standard requirements, Providing further and clearer implementation guidance, Developing standards targeted specifically for SMEs, Introducing economic incentives for SMEs by public institutions to adopt standards, Other]
22. What are the main reasons behind this decision? [Existing standards are too complex for my business, Implementation would be too costly, Lack of specialized staff to do implementation, Other]

D.3. Questionnaire content for organizations

1. Based on your knowledge, how would estimate the level of use of information security and privacy standards by SMEs? [free text]
2. In which security domains do you think it is more appropriate for SMEs to have available standards to adopt? [General Information Security, Risk Management, Data Protection and Privacy, Business Continuity Management, Incident Management, Third Party Management, Other]
3. Do you think existing information security and privacy standards are adequate for SMEs? What elements do you believe harden the adoption process? [free text]
4. Which do you think are the main difficulties and obstacles that SMEs face to adopt standards in these fields? [free text]
5. How do you think standards in these fields, as well as their adoption process, could be further improved to increase their adoption rate by SMEs? [free text]
6. What other initiatives and strategies do you think could be undertaken in order to further support SMEs in adopting standards? [free text]

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 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

TP-02-15-977-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-159-5
DOI: 10.2824/829076