



ENISA Deliverable:

Information Package for SMEs

**With examples of
Risk Assessment / Risk Management
for two SMEs**

(also available under www.enisa.europa.eu/rmra)

Conducted by the
Technical Department of ENISA
Section Risk Management
in cooperation with:

Mr. George Patsis
Obrela Security Industries (OSI)
www.obrela.com

February 2007

Legal Notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless it is stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of-the-art and it might be updated from time to time.

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

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

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic mechanical, photocopying, recording, or otherwise without the prior written permission of ENISA, or as expressly permitted by Law or under terms agreed with the appropriate rights organisations. Source must be acknowledged at all times. Enquiries for reproduction can be sent to the contact address quoted in this publication.

© European Network and information Security Agency (ENISA), 2007

Executive Summary

The present document comprises the second ENISA deliverable as mentioned in the ENISA 2006 Work Programme. Parts of the present material are based on the need communicated to ENISA for a simplified approach to risk assessment.

The aim of this document is to provide a simplified and comprehensive view of risk management/risk assessment for use within small and medium sized enterprises (SMEs). To achieve this goal, the present document has been structured in a modular way. It is made up of various parts each devoted to particular needs of stakeholders involved in the process of risk assessment and risk management.

The philosophy behind the generation of this material was to shield (non-expert) users from the complexity of risk management and risk assessment activities. In doing so, some complex security matters have been simplified to the minimum needed to achieve an acceptable security level.

There is no doubt that if a high level of security is needed the full complexity of security management must be taken into account including a plunge into the fine details of corresponding measures and technology. In this regard, the ideas and approach presented here are thought to cover an acceptable security level for small organisations with reduced security investments. More advanced forms of security (e.g. critical infrastructure components) would require a more thorough treatment that is beyond the scope of this document.

The present material has been generated by anticipating the whole range of skills of different stakeholders involved in risk assessment. The proposed risk assessment process is structured by means of a simplified four-phase assessment approach. We do not assume any advanced knowledge of security issues on the part of users of this material. Where this knowledge would be necessary, the present approach represents a "black box" offering a limited number of comprehensive choices.

Another criterion that has been taken into account is the cost effectiveness in all stages of risk assessment and risk management. The present material can help decision makers to decide which approach is most suitable to their organisation for the assessment of risks, based on cost and performance indicators. Furthermore, in the case where self assessment has been selected, this document provides the necessary tools to perform same, without requiring previous experience in this area.

The simplified risk assessment approach presented in this document is one example of good practice for assessing information risks. It is assumed that other similar approaches/good practices exist which could be used instead. In this way the present approach is neither an attempt to replace existing standards nor to redefine good practices. Rather, it is designed to give interested SMEs a tool which they could not easily find elsewhere.

The application of the ideas presented here has been demonstrated using examples. Two representative SME types have been chosen whose risks are assessed using the present assessment approach. These examples are presented within the framework of the proposed simplified risk assessment approach.

It is worth mentioning that this document is the first in a series of material that will be released by ENISA to generate awareness about risk management and risk assessment for SMEs. As such, it will be subject to further improvements, adaptations and expansions. ENISA activities that will follow in the future embrace the validation of this material via pilot projects in SMEs, evaluation/review through expert teams, dissemination via professional and/or training associations, etc. Final objective is to have a version of this document that can be used by SMEs "as is", that is, without further improvements/explanations/adaptations. For this reason, we refer to the present document as "beta version" meaning that additional improvements and adjustments will follow after various pilots, deployments and disseminations, leading thus in the middle term to the maturity of the presented material.

Contact details: ENISA Technical Department, Section Risk Management, Dr. L. Marinos, Senior Expert Risk Management, e-mail: RiskMngt@enisa.europa.eu

Contents

1. PURPOSE AND SCOPE	6
2. STRUCTURE OF THE DOCUMENT	7
3. GUIDANCE FOR THE DECISION MAKER	8
3.1 WHAT A DECISION MAKER HAS TO CONSIDER	8
3.2 WHAT A DECISION MAKER NEEDS TO KNOW	9
3.3 HOW TO PROCEED WITH INFORMATION SECURITY	10
3.3.1 <i>In-sourcing</i>	11
3.3.2 <i>Full outsourcing</i>	12
3.3.3 <i>Partial Outsourcing</i>	14
4. A SIMPLIFIED APPROACH: OVERVIEW	17
4.2 WORKING ASSUMPTIONS	18
4.3 A FOUR-PHASE APPROACH	19
4.3.1 <i>Phase 1 - Risk profile selection</i>	20
4.3.2 <i>Phase 2 - Critical Assets Identification</i>	21
4.3.3 <i>Phase 3 - Control Cards Selection</i>	23
Organizational Control Cards Selection	24
Asset-Based Control Cards Selection	24
4.3.4 <i>Phase 4 - Implementation and Management</i>	25
5. SELF ASSESSMENT GUIDELINES WITH TWO EXAMPLES	27
PHASE 2 - IDENTIFY CRITICAL ASSETS	31
<i>Step 1. Select your organization's five most critical assets.</i>	31
<i>Step 2. Record the Rationale for Selecting Each Critical Asset.</i>	32
<i>Step 3. Identify Critical Asset Security Requirements</i>	32
PHASE 3 - SELECT CONTROL CARDS	36
<i>Step 1. Select Organization Control Cards</i>	37
<i>Step 2. Select Asset Based Controls</i>	37
<i>Step 3. Document List of Selected Controls and Rationale</i>	37
PHASE 4 - IMPLEMENTATION AND MANAGEMENT	42
<i>Step 1. Gap Analysis</i>	42
<i>Step 2. Create Risk Mitigation Plans</i>	43
<i>Step 3. Implementation, Monitoring and Control</i>	43
ANNEX A. ORGANIZATIONAL CONTROL CARDS	49
ANNEX B. ASSET CONTROL CARDS	50
ANNEX C. ORGANIZATIONAL CONTROLS	64
ANNEX D. ASSET BASED CONTROLS	68
ANNEX E. SIMPLE ADVICE	73
REFERENCES	84

Table of Figures

Figure 1: Risk assessment activities in relation to information security risk management.....	10
Figure 2: The four phases underlying the proposed risk assessment approach.....	19
Figure 3: Phase 1 - Risk profile selection workflow	28
Figure 4: Phase 2 - Identification of Critical Assets Workflow.....	31
Figure 5: Phase 3 - Control Cards Selection Workflow	36
Figure 6: Phase 4 - Implementation and management workflow.....	42
Figure 7: Management vs. implementation outsourcing options	44

Table of Tables

Table 1: Risk Assessment Implementation Options	11
Table 2: Risk profile evaluation table.....	21
Table 3: Asset List	22
Table 4: Security Requirements Selection Table.....	23
Table 5: Controls used in the approach presented.....	24
Table 6: Organizational Control Cards	24
Table 7: Asset Control Cards	25
Table 8: An example of a control card for the asset application in a high risk profile.....	25
Table 9: Risk Profile evaluation table - Example A.....	29
Table 10: Organization Risk Profile - Example A.....	29
Table 11: Risk profile evaluation table- Example B	30
Table 12: Organization risk Profile - Example B.....	30
Table 13: Security requirements selection table - Example A	33
Table 14: Security requirements rationale.....	33
Table 15: Security requirements selection table - Example B	34
Table 16: Security requirements rationale.....	35
Table 17: Organizational controls selection - Example A.....	38
Table 18: Asset based controls selection - Example A	38
Table 19: CC-1A Asset based control card - Example A	39
Table 20: Selected controls table and rationale - Example A	39
Table 21: Organizational controls selection - Example B.....	40
Table 22: Asset based control card selection - Example B.....	40
Table 23: CC-2S Asset based control card - Example B	41
Table 24: Controls selection rationale - Example B	41
Table 25: Gap analysis list - Example A.....	46
Table 26: Action list - Example A.....	46
Table 27: Implementation plan - Example A	47
Table 28: Gap analysis list - Example B.....	47
Table 29: Action list - Example B.....	48
Table 30: Implementation plan - Example B	48

1. Purpose and Scope

Small and Medium Enterprises (SMEs) are a priority focus area for government economic policy and are considered to be of key importance to socio-economic growth in European Union. SMEs are usually born out of entrepreneurial passion and limited funding, with business systems that are often heterogeneous and independent. Moreover, tangible and intangible business assets of SMEs are rudimentarily defined, and the value of such assets is often only partially known. Typically this is the case with one of the most important assets, namely, information.

Much like any other business asset, information needs to be strategically managed and protected. Information security is the protection of information within a business, including the systems and hardware used to store, process and transmit this information. It is imperative that SME business leaders understand the value of information contained within their business systems and have a framework for assessing and implementing information security. Numerous internationally approved security frameworks and schemes may be implemented to safeguard an organisation against information loss and potential liability. Since these frameworks are complex, all embracing, and ultimately costly to implement, they are mostly adopted by large organisations.

Usually, due to the dynamic and ad hoc development of many SMEs, neither integration nor security issues are systematically addressed in the building-up phase. Thus, policies and frameworks for information security planning and disaster recovery are usually very rudimentary or even non-existent. It is often the case that the basic understanding of information security risk in SMEs does not extend much beyond viruses and anti-virus software. Inadvertent threats pose some of the highest information security risk to SMEs, and yet personnel training and awareness programmes are often neglected.

Survey results reveal that the level of information security awareness among SME leaders is as variable as the state of their information systems, technology and security. Although a minority of SMEs do embrace security frameworks such as ISO / IEC 27001 or the International equivalent ISO 17799, most SME executives have not heard of security standards and consider information security only as a technical intervention designed to address virus threats and data backups.

Far from blaming SME executives for not understanding the critical issue surrounding information security, research concludes that SME leadership needs to engage, understand and implement formal information security processes, including technical and organisational measures. Without such measures, their organisations may be severely impacted by inadvertent threats / deliberate attacks on their information systems which could ultimately lead to business failure.

Based on the contents of this information package SMEs will be able to perform risk assessments on their environments, select and apply suitable measures for performing and managing information security related risks. In this document we assist SMEs in defining such an effort, in deciding the way to initiate and perform it and, if they have sufficient resources, we provide guidelines for performing a self-assessment of information risks. For this purpose, we offer a simple risk assessment method that leads to a quick and encompassing identification and mitigation of information risks.

The assessment method presented in this document is based on a simplified model that has been generated for small organizations which share certain common characteristics. First, their organizational structures are relatively flat, and people from different organizational levels are accustomed to working with each other. Second, people are often required to multi-task, exposing staff members to the entire variety of processes and procedures used across the organization.

2. Structure of the document

In order to cover the needs of various SME types, we have chosen a modular structure for this document. Depending on the needs of a particular SME and the extent to which it seeks to cope with risk assessment, different portions of this document are going to be useful. For SMEs requiring an overview of risk management in order to define their future strategy, the generic part of this document will be useful (see Chapter 3. [Guidance for the Decision Maker](#) and Chapter 4. [A Simplified Approach: Overview](#)).

Should a SME decide to implement its risk management on its own, then the parts of this document containing the detailed description of the risk assessment method and the examples will be required (see Chapter 5. [Self Assessment Guidelines with two examples](#)). In the case of a self-assessment, the detailed material found in the annexes will be necessary in order to define the measures that have to be implemented in the organisation (see [Annex A. Organizational Control Cards](#), [Annex B. Asset Control Cards](#)). To give a better view of how this document can be used, we provide some cases of use based on the various possible roles of readers:

- **People with managerial background:** consider chapter three about decision makers. It explains the background of information security and the necessity of risk management. It draws possible options for the implementation of risk management and defines decision criteria. Interested managers might like to understand the structure of the risk assessment process proposed in this document as presented in chapter four.
- **Non-experienced members of a risk assessment team:** the members of a risk assessment team will need to understand the proposed simplified risk assessment approach, read its details and the examples presented (see Chapter 4. [A Simplified Approach: Overview](#)).
- **Expert members of a risk assessment team:** expert members of a risk assessment team will need to read the method and understand the details. They will also be in the position to cope with the material presented in the annexes and in particular with the choice of measures (also referred to as countermeasures, controls or security controls within this document). Alternatively, new measures may be assigned to existing assets or new assets may be added (see [Annex A. Organizational Control Cards](#), [Annex B. Asset Control Cards](#) and [Annex C. Organizational Controls](#)).

3. Guidance for the Decision Maker

3.1 What a decision maker has to consider

Today, the information created, processed, and used by an organization is one of its most valuable assets. The disclosure, compromise or unavailability of this asset can **severely impact** an organization, constitute a **breach of laws and regulations**, and negatively **affect its brand name**.

Adequate security of information and of information-processing systems is a fundamental management responsibility. Proprietors and decision makers must understand the current status of their information security program in order to make well-founded judgments and investments that appropriately mitigate risks to an acceptable level. Information risks might lead to critical situations when extrapolated to vital business and legal issues of the organisation. Thus, information risks may lead to more generic and more critical risk categories such as:

- **Legal / Compliance Risk** is the risk arising from violations of or non-conformance with laws, accounting rules, regulations, prescribed practices, or ethical standards. Legal or compliance risks can expose an organization to negative publicity, fines, criminal and civil money penalties, payment of damages, and the voiding of contracts. Theft of customer information such as credit card information, financial information, health information or other personal data can also raise potential risks from third party claims. **In recognition of information security as a rising concern and a multifaceted issue, and in order to protect civil rights and to ensure corporate liability, EU Governments and the European Union have established laws and regulations which require compliance by organizations regardless of size or industry. These regulations mandate companies to implement internal controls to safeguard against information risks. They also aim at improving risk management practices and procedures.**
- **Financial Stability Risks.** Lack of appropriate production infrastructure, management infrastructure, or staff to execute the entity's business strategy can cause failure to achieve stated goals and financial objectives in a well-managed and controlled environment. **The inappropriate management of information security can spill over to risks related to the financial stability of the organisation. Such risks, in turn, may leave the door open to fraud, money laundering, financial instability etc.**
- **Productivity Risk** is the risk of operational losses and **poor customer service delivery** as an effect of lack of adherence to basic processing procedures and controls. It usually refers to all cooperative production activities that contribute in some way to the overall delivery of a product or service. Productivity Risk is not confined to the use of technology; it can also be the result of organisational activities. The risk arising from inadequate or poorly controlled systems and software applications used to support the front office, risk management operations, accounting, or other units is captured in this risk family. Inadequate information security management may result in high productivity risks including high operating costs, operational failures, poor management decisions (price, liquidity, and credit risk exposures), and lack of **privacy and disruption of service to customers**.
- **Reputation and Customer Confidence.** Perhaps the most difficult and yet one of the most important risks to understand is the risk of damage to the organization's reputation, an intangible but important asset. Will customers give a company their credit card numbers once they read in the paper that a company's database of credit card numbers was hacked into? Will top employees remain at a company so damaged? And, what will be the reaction of the company's shareholders? What is the expected loss of future business revenue? What is the expected loss of market capitalization?

Many SME owners think they are not at risk because of the size of their business and information assets. Most think that large corporations with more assets are the only ones at risk. This is not true. First, sensitivity of information applies to the quality and not the quantity of information.

Secondly, SMEs do not have the resources or personnel to address security in a similarly intensive manner like large corporations do and are therefore more exposed. As a matter of fact, new technology allows small businesses to use many of the same information systems employed by large enterprises. In doing so small businesses expose themselves to many threats that were traditionally associated with large corporations. **In fact, 56 per cent of small businesses have experienced at least one security incident during the past year.** Unfortunately, a significant proportion of businesses that suffer a major computer failure never recover and the business itself fails. Therefore it is imperative to their continued success that SME proprietors and decision makers recognize these pitfalls and take steps to address information security issues.

Information-security-risk-mitigating measures (controls) should be commensurate with the risks faced by the information in question. However, the process to determine which security controls are appropriate and cost effective is quite often a complex and sometimes a subjective matter. **One of the prime functions for putting this process onto a more objective basis is permanent security risk assessment.**

3.2 What a decision maker needs to know

Information security is about identifying, mitigating and managing risks that are relevant for the information assets. Risk assessment is the first necessary step to understanding risks by carrying out a comprehensive risk **identification** and **evaluation** of an organization's information security risks. The output of such an activity is essential for managing business as the risks involved can influence significantly the confidentiality, integrity, and availability of information assets and **may be critical for maintaining a competitive edge, financial stability, legal compliance, and a strong commercial image.**

As such, risk assessment can help decision makers to:

- **Assess organizational practices and installed technology base;**
- **Enforce information protection based on potential impact on the organization;**
- **Focus security activities on what is important. Measures that are associated with acceptable risks can be abandoned;**
- **Ensure that implemented measures and expenditure are fully commensurate with the risks to which the organisation is exposed. In this way a balance between the costs of addressing a risk and the benefits derived from avoiding the negative impact can be maintained.**

During a risk assessment, an organization performs activities to (a) identify information security risks, (b) evaluate the risks to determine priorities and (c) define how to mitigate the risks (s. also Figure 1).

Information security risk assessment, though, is only the first step towards information security risk management, which is the ongoing process of identifying risks and implementing plans to address them. Figure 1 illustrates an information security risk management process and the "portion" of the risk management that a risk assessment constitutes.

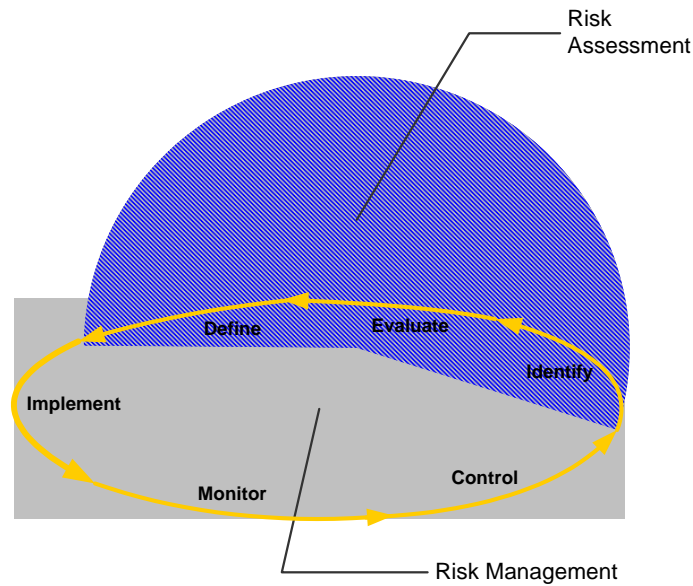


Figure 1: Risk assessment activities in relation to information security risk management

Clearly, risk assessment itself provides a direction for an organization's information security activities; it **does not necessarily lead to meaningful improvement unless an implementation of measures has taken place**. As in any other management discipline, implementing one part of the management life-cycle alone does not bring the desired effects. No evaluation, no matter how detailed or how expert, will improve the security posture unless the organization follows through with implementation. Besides risk assessment, effective risk management includes the **following steps**:

- **Plan** how to implement the protection strategy and risk mitigation plans from the evaluation by developing detailed action plans. This activity can include a detailed cost-benefit analysis of various strategies and actions.
- **Implement** the selected detailed action plans.
- **Monitor** the plans for progress and effectiveness. This activity includes monitoring any changes in risk levels.
- **Control** variations in plan execution by taking appropriate corrective actions.

3.3 How to proceed with information security

Part of the responsibility of SME managers is to provide for the security of their business environment. According to most applicable legal requirements, liability for breaches of security lies with them. Just as they must provide a safe and secure physical environment, they must also make sure that information is protected. Given the fact, however, that computers are not "fix and forget" devices, the protection of information is a permanent concern.

Decision makers can initiate risk assessment on their environment and trigger the introduction of suitable measures to face unacceptable risks. This is the precondition for the management of information security. In performing this, a variety of approaches may be followed concerning the staffing of such an effort (also known as a "make-or-buy" decision). We differentiate between three approaches:

- **In-sourcing of risk assessment:** the risk assessment and the identification of necessary measures is performed by internal staff. The assessment is based on a risk assessment approach that has been selected by the organisation (e.g. a good practice, a known standard, etc.). This will help the organisation to master the assessment approach for recurring executions.

- **Full outsourcing of risk assessment:** according to this approach, the entire risk assessment is performed by an external contractor. The assessment is based on a risk assessment approach that is chosen by the external contractor. The contractor can also undertake recurring future assessments. No know-how transfer to internal personnel is foreseen for the entire life cycle of the risk assessment/risk management of the SME.
- **Partial outsourcing of risk assessment:** this approach assumes that the initial risk assessment is performed by an external company. The assessment will be based on a risk assessment approach that is known to the SME. Hence, further risk assessments can be performed by internal personnel. The initial assessment performed by the outsourcer serves as know-how transfer to the SME's internal personnel.

The present document provides SMEs with all relevant material required for the make-or-buy decision. Furthermore, we deliver all necessary information to help SMEs perform a self-assessment. The proposed risk assessment approach can be used in in-sourcing and partial outsourcing decisions as a guideline for the initial and future risk assessments (s. chapters 4. [A Simplified Approach: Overview](#) and 5. [Self Assessment Guidelines with two examples](#)).

When compared to all other approaches, every approach to risk assessment is associated with advantages and disadvantages. Table 1 gives a first impression of the facts related to a make-or-buy decision in respect to a risk-assessment effort. The following paragraphs contain a detailed discussion on the parameters and factors that should be considered when selecting a risk management approach for an SME.

Risk Assessment Implementation Options	Implementation Parameters and Factors				
	In-house Expertise required	Dependency to third Parties	Internal Resources Required	Assessment Objectivity	Third Party effort ¹
In sourcing	Yes	Low	1-5 People	Low	-
Full outsourcing	No	High	1 Person (for Project Management)	High	10-40 Days
Partial outsourcing	Yes	Low	1-2 People	Medium	5-10 Days

Table 1: Risk Assessment Implementation Options



In the following sections we describe each possible option for the performance of risk assessment/risk management. A questionnaire will help decision makers to determine whether this option is good for a given type of an SME.

3.3.1 In-sourcing

In-sourcing can offer many **advantages such as the development of internal organization know-how and competence in risk assessment and risk management. Moreover, depending on consulting prices in the security market, this approach may result in reduced expenses.**

¹ For the figures of the effort we assume a SME up to 100 people.

This is a particularly attractive option for organizations with a simple structure, a successful track record in implementing internally similar activities (i.e. ISO9001), and adequate capacity and skills. The following set of questions can be used to help determine whether in-sourcing risk assessment is the right decision for an organization:

Questions for the decision	Answer	
		
	YES	No
Is your organization small? Does it have a flat or simple hierarchical structure?		
Do you have internal know-how in IT Systems and Networks?		
Does your organization have qualified and available human resources?		
Do your business activities have a low dependency on IT systems and are they uninvolved in storing or processing customer data of a sensitive nature and has your organization been involved in similar activities, i.e. quality improvement processes?		
Can you find a group of three to five people who have a broad and deep understanding of the organization and also possess most of the following skills? <ul style="list-style-type: none"> <input type="checkbox"/> problem-solving ability <input type="checkbox"/> analytical ability <input type="checkbox"/> ability to work in a team <input type="checkbox"/> leadership skills <input type="checkbox"/> Ability to understand the firm's business processes and the underlying infrastructure of the organization <input type="checkbox"/> ability to spend a few days working on this method 		
Do you have a relatively simple information technology infrastructure that is well-understood by at least one individual in your organization?		

The more “yes” answers have been given to these questions, the greater is the likelihood that a self-assessment of risk is the right choice for an SME.



Using the proposed risk assessment approach and best practices (see. Chapter 4. [A Simplified Approach: Overview](#) and 5. [Self Assessment Guidelines with two examples](#)) decision makers will be able to initiate risk assessments with an efficient approach for identifying and managing their information security risks, enabling them to continuously improve their security posture.

3.3.2 Full outsourcing

Via a full outsourcing a SME fully transfers the risk assessment and risk management to an external contractor. This may include initial as well as repeated assessments and management activities that will cover the entire risk management life-cycle (e.g. implementation and maintenance of measures). The contractor applies his own risk assessment/risk management approach. In this way, the contractor does not perform any know-how transfer to the client. At this point it should be noted that outsourcing of assessment and management activities does not release the SME management from its responsibility for (information) security.

Depending on the structure, strategy, available resources and market situation, outsourcing **can offer definite advantages**. Deciding to outsource information risk assessment allows the SME to focus on core business strategies, while letting peripheral activities be performed by an outside expert specialized in information security.

The following questions can be used to help determine whether fully outsourcing risk assessment is the right decision for an organization:

Questions for the decision	Answer	
		
	YES	No
Do you deem it necessary to retain an increased focus on core competencies and strategic business processes?		
Would you find it hard to make available two to five people who have a broad and deep understanding of the organization and also possess most of the following skills? <ul style="list-style-type: none"> o Ability to understand the business processes and the underlying infrastructure of the organization o problem-solving ability o analytical ability o ability to work in a team o leadership skills o ability to spend a few days working on this method 		
Do you have a highly complex and a relatively large IT infrastructure ?		
Does your business and service offerings include financial transactions ?		
Do you operate a business which is highly subject to strict EU or Domestic Legal and Regulatory constraints and/or mandates ?		
Do you have a relatively simple information technology infrastructure which is well-understood by at least one individual in your organization ?		

Again, the more “yes” answers appear for an organisation, the better outsourcing is suited to its needs.

To outsource risk assessment activities to a third party requires **a vendor selection process including a due-diligence and vendor’s overall valuation, as well as the assessment of the vendor’s competency in information security (see also Annex E. Simple advice, Third Parties, Service Providers)**.

If made, a service level agreement should constitute the primary base for cooperation and should define key elements such as the professional certification of the vendor’s security engineers, confidentiality and non-disclosure, timeframe, resource allocation, cost and the methodology to be employed.

When a Service Level Agreement (SLA) is to be made the following questions should be considered (i.e. as a sort of checklist for the contents of an SLA):

- **Are liability issues covered?** What will happen for example if during the assessment major business activities are halted or disturbed due to vendor’s incompetence to perform an assessment of the underlying IT and Network infrastructure?

- **Are responsibilities clearly identified** with the SLA? Who will be responsible for doing what? What is the Organization’s involvement in terms of resources?
- **Is the scope of the work clearly documented?** What will the vendor include in the scope of the work? It is highly recommended that the scope of the work includes the complete range of business activities and the underlying infrastructure. In any other case it is possible that the output can be inadequate or even misleading.
- **How are the legal requirements to be met**, e.g. data protection legislation?
- What arrangements will be in place to enable that all parties involved in the outsourcing, including subcontractors, are aware of their security responsibilities?
- How are the **integrity and confidentiality of the organization’s business assets to be maintained and tested?**
- **What physical and logical controls will be used to restrict and limit the access to the organization’s sensitive business information to authorized users?**
- **How is the availability of services to be maintained in the event of a disaster?**
- **Is the right to audit the vendor’s security and information protection measures included in terms and conditions?**
- Are the vendor’s **minimum resources, competency and Professional Certification** clearly stated?
- Are the content, frequency and structure of reporting clearly defined?



Clearly, organizations can order vendors to perform an assessment based on the risk management approach methodology proposed herein (see Chapter 5. [Self Assessment Guidelines with two examples](#)). As long as the SME understands the contents of the proposed approach, this will allow them to better control the activities of the contractor.

3.3.3 Partial Outsourcing

A mixed source solution **can combine the benefits from both in-sourcing and outsourcing**. In a mixed source solution the organization actively participates in a self-assessment process by using a third party as a facilitator. Moreover, the assessment is based on a risk assessment model that is understood by the client, for example the risk assessment approach presented herein (s. chapter 4. [A Simplified Approach: Overview](#)). This is a necessary **precondition in order to achieve a know-how transfer** between contractor and client.

In this scenario the SME develops the internal ability to perform some important security tasks when and where appropriate. Clear benefits can arise from the fact that the organization can regulate and manage future contractor costs and significantly contribute to the expertise provided by a third, specialized party.

The following set of questions can be used to help determine whether a risk assessment should be partially outsourced:

Questions for the decision	Answer	
	 YES	 No
Do you deem it necessary to retain an increased focus on core competencies and strategic business processes but also improve internal information security awareness and competency in information security matters?		
Is it likely you can make available one to two people in your organisation who have a broad and deep understanding of the		

organization and also possess most of the following skills?		
<input type="checkbox"/> Ability to understand the business processes and the underlying infrastructure of the organization		
<input type="checkbox"/> problem-solving ability		
<input type="checkbox"/> analytical ability		
<input type="checkbox"/> ability to work in a team		
<input type="checkbox"/> leadership skills		
<input type="checkbox"/> ability to spend a few days working on this method		
<input type="checkbox"/> they are going to be on a longer term employment		
Do you have a complex and a relatively large IT infrastructure but a relatively simple business model?		
Do your business and service offerings include financial transactions?		
Do you operate a business that is highly subject to strict EU or Domestic Legal and Regulatory constraints and/or mandates?		

As in the previous implementation approaches, the more questions that have been answered with “yes” the better is the SME suited for this risk assessment implementation approach.

The decision to partially outsource a risk assessment requires a Service Level Agreement (SLA) as the primary base for cooperation with the contractor. Key elements of an SLA include the professional certification of the vendor’s security engineers, confidentiality, timeframe, resource allocation, cost and the methodology to be employed. Again, organizations can order vendors to perform an assessment based on the ENISA methodology proposed herein (Use Chapter 4. [A Simplified Approach: Overview](#)).

The following questions should be at a minimum addressed within an SLA for outsourcing information security risk assessment:

- Does the contractor agree to use a predefined risk assessment approach that is also known to the client (e.g. the proposed risk assessment approach)?
- Are **liability** issues covered? What will happen for example if during the assessment major business activities are halted or disturbed due to vendor’s incompetence to perform an assessment of the underlying IT and Network infrastructure?
- Are **responsibilities** clearly identified by the SLA? Who will be responsible for doing what? What is the Organization’s involvement in terms of resources?
- Is the **scope** of the work clearly documented? What will the vendor include in the scope of the work? It is highly recommended that the scope of work includes the complete range of business activities and the underlying infrastructure. In any other case it is possible that the output can be inadequate or even misleading.
- How are the **legal requirements** to be met, e.g. data protection legislation?
- What arrangements will be in place to enable that all parties involved in the outsourcing, including subcontractors, are aware of their security responsibilities?
- How are the **integrity and confidentiality of the organization’s business assets** to be maintained and tested?
- What **physical and logical controls** will be used to restrict and limit access to the organization’s sensitive business information to authorized users?
- How is the **availability of services to be maintained in the event of a disaster?**

- Is **the right to audit the vendor's** security and information protection measures included in terms and conditions?
- Are **vendor's minimum resources, competency and Professional Certification** clearly stated?
- Are the content, frequency and structure of reporting clearly defined?

4. A Simplified Approach: Overview

The present chapter presents the contents of a simplified risk assessment and risk management approach that can be used by SMEs for self assessment including within outsourcing projects, as indicated in Chapter 3.

Most existing approaches to the assessment and management of security risks generally focus on the needs of large organizations. A simple approach designed for small organizations does not exist today, at least not in the form of publicly available guidelines. Some consulting firms have developed good practices for that purpose, but they use them within customer projects. Other approaches, although claiming to be appropriate for SMEs are still too complex for self assessments (e.g. OCTAVE). On the other hand, as already discussed most SMEs cannot afford the cost of fully outsourcing this function to external parties.

Our intent is to provide those organizations with a simple, efficient and inexpensive approach to identifying and managing their information security risks. **The resulting simplified approach provides small organizations with a means to perform self-assessments. It is based on OCTAVE² principles, attributes, and outputs and is tailored to typical SME environments and needs. In fact this approach is also compatible with other existing standards, like for example ISO 13335-2.**

For an organization looking to understand its information security needs, the present approach is a risk-profiling-based self-assessment and planning technique for security. Unlike typical technology-focused assessments which are targeted at technological risk only, this method targets context and inherent risks and focuses on strategic, practice-related issues.

The main advantage of the present approach is that it can provide an acceptable security level with a low assessment and management effort. This is due to the following aspects that enhance practicability:

- The risk profile of the organisation can be easily identified
- The typical assets for small organisations are given
- The protection of the assets by means of measures (controls) is predefined by means of control cards

These advantages can lead to a low cost self-assessment by teams with low expertise in security. If done carefully, an acceptable level of security will result.

The proposed assessment approach can be applied by non-experts. During an assessment, the assessment team will not have to cope with various aspects of threats to vulnerable assets. Rather, a predefined protection level according to the asset type and the level of security required is suggested.

The work done for development of the risk model underlying this approach is based on the following assumptions/elements:

- **The assessment of inherent risks** - The environment can often define the risk context (inherent risk) within which a business operates. For example a small organization engaged in baking has a significantly lower risk context than a small organization engaged in providing health care or business intelligence services. Regardless of the security measures, infrastructure and revenues the two businesses are operating in a totally different risk environment which has to be seriously considered before an information security strategy is defined and security controls are selected.
- **The variation in the threat scenarios (profiles) found in the SMEs.** In the SME context, despite the naturally expected dispersion in terms of inherent risks, we have noticed that threats are rather typical and most often, when grouped together, can form generic threat

² Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University. OCTAVE was developed at the CERT Coordination Centre (CERT/CC). Established in 1988, it is the oldest computer security response team in existence.

profiles applicable to the vast number of SMEs. In this regard, our work is focused on modelling threats by means of generic threat profiles. The developed risk profiles help reflect the inherent risk level of an organisation. Measures were subsequently identified and grouped in order to cover threats for the respective risk profiles.

The **proposed approach is self-directed**, meaning that people from an organization assume responsibility for assessing the risks, selecting controls and thus setting the organization's security strategy. This technique leverages people's knowledge of their organization's security-related practices and processes to **(a) capture the current state of security practice within the organization, (b) identify risks to the most critical assets, (c) prioritize areas of improvement and set the security strategy for the organization**. In doing this, one will cover the entire life-cycle of risk assessment and risk management.

When applying the proposed approach, a small team of people from the operational (or business) units and the information technology (IT) department work together to address the security needs of the organization, balancing thus two key aspects for security, namely organizational measures and asset-based measures.

Organizations are strongly encouraged to apply the guidelines and best practices included in this approach only as short term plan to meet the objective toof quickly and effectively protecting crucial and critical components of their business. The contents of this approach cover significant risks to which SMEs are usually exposed. However the proposed approach is not a permanent replacement for complete and thorough risk assessment of critical assets. We strongly recommend such "deep dives" to better assess risks especially if complex components are used for highly valuable assets.

The objectives behind the introduction of this risk assessment and risk management approach are to:

- **Improve existing European Information Security Thresholds.** The approach can be used as a catalyst to accelerate SME efforts towards information security risk management by addressing high risks. Furthermore, by targeting typical threat scenarios it will ultimately improve existing European information security thresholds.
- Fulfil business requirements, context, and constraints typically found in SMEs environments by **avoiding specialized terminology and eliminating highly demanding tasks** incorporated in almost every existing, wide-spread professional methodology and industry standard (i.e. asset evaluation, business impact analysis, identification of security requirements etc.).
- **Use a self-directed approach** tailored to the means, resources and expertise typically found in an SME environment.
- **Focus on critical assets and highest risks.** The method was developed as a simple and easy guide for identifying and protecting assets judged to be most critical to the organization.
- Develop a **measure-independent** risk assessment and management method. For the purpose of producing a first practical and realistic output, OCTAVE controls have been used. However the method can use virtually any standard controls available today (ISO, BS7799, NIST, BSI).

4.2 Working assumptions

In addition to the above mentioned objectives, some considerations/assumptions have been made for the development of this guide and the risk assessment approach it presents:

- In many cases the SME may be unfamiliar with computer security and in consequence may benefit from access to awareness, training and guidance material.
- The establishment of a security guidance framework through SME trade bodies and associations will help promote understanding of security issues by those with little background in information security.

- SMEs are a priority focus area of EU economic policy and are considered to be of key importance to socio-economic growth in the European Union.
- SMEs are usually born out of entrepreneurial passion and limited funding, with business systems that are often 'patched together' and thus are heterogeneous and independent.
- Policies and frameworks for information security planning and disaster recovery are usually non-existent. Moreover, a basic understanding of information security risk in SMEs does not extend much beyond viruses and anti-virus software.
- Most SME business managers barely understand highly technical and complex scientific terminology related to information security.
- Small sized companies are usually working within a framework where the data-processing environment is standardized but is important for the business. They use packages like off-the-shelf products, consisting in part or entirely of a "black-box" (with all potential risks associated) and are connected to the Internet, where a lot of IT security threats lurk.
- Inadvertent threats pose some of the highest information security risk to SMEs and yet personnel training and awareness programmes are often neglected. Even if the staff of SMEs has special knowledge of information systems, they might not possess special know-how on IT security matters. An aggravating factor is that companies generally cannot afford to invest enough resources in risk assessment and risk management.

4.3 A four-phase approach

The proposed risk assessment approach uses **four phases** to examine organizational and technology security issues, thus assembling a comprehensive holistic picture of information security needs. The four phases for the Method are depicted in Figure 2.

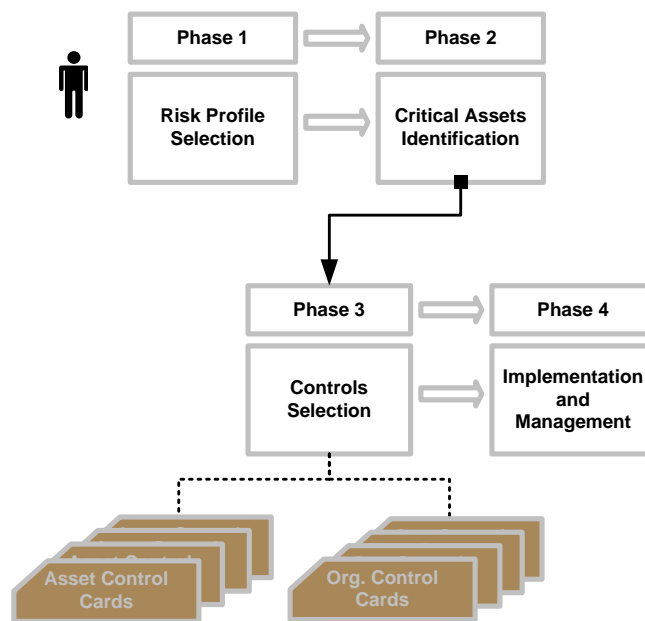


Figure 2: The four phases underlying the proposed risk assessment approach

The risk assessment approach is driven by two key aspects: **(1) the business risk profile and (2) identification of critical assets.**

Risk assessment is led by a small, interdisciplinary assessment team (three to five people, SME staff, external staff or mixed according to implementation type as mentioned in chapter 3.3 [How to proceed with information security](#)) who gather and analyze information and produce mitigation plans based on the organization's security risks. To conduct the risk assessment effectively, the team must

have broad knowledge of the organization’s businesses (also referred to as business processes) and its IT- infrastructure.

As a starting point the SME analysis team **will use the risk profile evaluation table to identify the business risk profile**. The next step is the **identification of organization’s critical assets** and the relevant **security requirements** in terms of confidentiality, integrity and availability.

Controls (control cards) are subsequently selected. The selection process is radically simplified by the use of standard control cards. Teams conclude the controls selection process **simply by “pulling out” risk-associated control cards**, both for the organization and the identified critical assets, created for every risk profile level, asset category and security requirement (confidentiality, integrity, availability).

Control cards contain controls from the catalogue of practices used in OCTAVE. This decision has been made because these controls are fairly simple and more easily understood by non-security-experts. Alternatively, other security controls can be used. This might be necessary in the case that an SME already possesses a security policy based on another standard (e.g. ISO 17799).

In the final step the SME analysis team is occupied with the prioritizing of assets according to their criticality and business effect and the protection plan.

The following paragraphs describe the risk assessment phases in greater detail.

4.3.1 Phase 1 - Risk profile selection

During this phase the assessment teams evaluate their business risk profile by using a predefined set of **qualitative criteria**. By using the risk profile evaluation table (Table 2) assessment teams are in a position to identify their risk context. The risk context is derived from the business and the external environment of an organisation and can be divided into **four risk areas: Legal and Regulatory, Reputation and Customer Confidence, Productivity, and Financial Stability**.

Risk Areas	High	Medium	Low
Legal and Regulatory	The organization handles customer information of a sensitive and personal nature including medical records and critical personal data as defined by the EU Data Protection Law.	The organization handles customer information of a personal but not sensitive nature as defined by the EU Data Protection Law.	The organization does not handle personal data other than those of the people employed by the organization.
Productivity	The organization employs more than 100 employees who have a daily need to access business applications and services.	The organization employs more than 50 employees who have a daily need to access business applications and services.	The organization employs less than 10 employees who have a daily need to access business applications and services.
Financial Stability	Yearly revenues of the organization exceed 25M Euros or/and financial transactions with third parties or customers are taking place as part of the business as usual process.	Yearly revenues of the organization do not exceed 25 M. Euros.	Yearly revenues of the organization do not exceed 5M euros.
Reputation and Loss of Customer Confidence	Unavailability or Service Quality directly impact the businesses of the organization or/and more than 70% of customer base have online access to business products and services.	Unavailability or Service Quality can indirectly impact the businesses of the organization and/or less than 5% of customer base have online access to business products and services.	Unavailability or Service Quality cannot directly or indirectly impact the businesses of the organization or result in loss of revenues.

Table 2: Risk profile evaluation table

Each area is classified in three classes: High, Medium and Low. These classes express quantitative criteria for the organisation in question with regard to the risk area and help identify a risk level. The team evaluates risks identified for every area in order to produce the **organization risk profile**.

As a rule of thumb the highest risk identified in a risk class defines the overall business risk profile. A high risk carried in the financial risk class marks a high risk profile. Equally, a medium risk leads to a medium risk profile and low risks to low risk profiles. For example a low risk carried in the reputation and confidence, in legal and regulatory compliance and productivity but a high risk in financial stability risk class concludes to a high organization risk profile.

Risk profiling should be considered as a very important decision which subsequently leads to the risk-related selection of assets and their protection via control cards.

4.3.2 Phase 2 - Critical Assets Identification

During this phase, the assessment team selects critical assets based on relative importance to the organization and defines security requirements for each critical asset.

Typically, an organization's management knows what its **key assets** are and can use their limited resources to focus on protecting those key assets. The assessment team determines what is important to the organization (e.g. information-related assets) and selects those assets that are most important to the organization, also referred to as **critical assets**.

The following table defines categories of assets and types that are considered during the critical asset selection. Attention is given to assets that are used to help the organization perform its businesses. It should be noted that asset types may be composed of other asset types. For instance components of an application might be servers, workstations, routers, network segments etc.

It should be noted that the following list is representative of most small businesses and is not exhaustive. Upon request (e.g. in future versions of this document) additional assets can be introduced. Further, it is possible, that an asset type might use other assets for its operations. For example, an application might use as components a server, few workstations, a storage device and a network segment. It has to be noted, that in addition to the protection of an asset, all of each components have to be also appropriately protected.

Asset Category	Description	Asset (types)
Systems	Information systems that process and store information. Systems are a combination of information, software, and hardware assets. Any host, client, server, or network can be considered a system. Critical systems are those identified as essential for the continuous provision of the business service and product offerings, those that store critical business information (customer or business proprietary) or these that are exposed to the outside world for business functions or services.	<ul style="list-style-type: none"> Server Laptop Workstation Archiving and Backup Storage
Network	Devices important to the organization's networks. Routers, switches, and modems are all examples of this class of component. Wireless components/devices, such as cell phones and wireless access points that staff members use to access information (for example, email). Typically, critical networks are those that are used to support essential critical applications or systems or those that are shared with third party and usually un-trusted networks.	<ul style="list-style-type: none"> Routers Cabling Gateways Wireless Access Points Network Segment (e.g. cabling and equipment between two computers) Other (SAT, Laser)
People	People in the organization, including their skills, training, knowledge, and experience. Critical people are those that play a key role in production or operational processes.	<ul style="list-style-type: none"> Business and Human Resources Management Operations and Technology

		Research and Development
		Sales and Marketing
		Contractors and Third Parties
Applications	Critical Applications. Applications that are key to or part of the product and service offerings. Disruption of critical applications typically results in severe hindering or even congestion of the dependent processes.	Financial Control
		Customer Care
		Logistics
		E-commerce
		ERP

Table 3: Asset List

It is essential during the identification to consider the views of the top level management (or business owner). Top level participation in the analysis ensures that the business value of the business information assets is properly identified.

Next, an evaluation of security requirements for the most important assets is necessary. The security requirements outline the qualities of an asset that are important to protect. The following are the security requirements examined during the assessment process:

- confidentiality – the need to keep proprietary, sensitive, or personal information private and inaccessible to anyone who is not authorized to access it
- integrity – the authenticity, accuracy, and completeness of an asset
- availability – the property of an asset to be available at the time of its use

Assessment teams should use the requirements selection criteria as provided in table 4 in order to identify the most important security requirements for the different asset categories. Asset security requirements will be used later during the selection of asset control cards. The selection of security requirements has been developed as a simple and practical guide to identify the security properties of the critical assets selected previously. The requirements highlight the importance of the asset and are an indicator of the protection level that is needed (e.g. through the use of appropriate controls).

The following table will help assessment teams to identify the security requirements for the different asset categories mentioned above.

Asset Category	Confidentiality	Integrity	Availability
Systems	A system with confidentiality requirements often handles information with corporate proprietary information (R&D), customer base information, sensitive customer information of medical or personal nature.	Systems with integrity requirements typically handle transactions of financial nature, procurement of goods or e-commerce.	Availability requirements are encountered in systems that are critical to daily business operations and where downtime usually incurs costs and overheads in terms of resource allocation.
Network	A network with confidentiality requirements typically covers communications and information exchange over insecure and untrusted environments.	Network integrity requirements are typically necessary when transactions that take place over public and shared metropolitan network or telecommunication providers.	Availability requirements are especially necessary when the network is used as part of customer care, or service and product offerings.
People	Confidentiality requirements are typically encountered when people handle organizational proprietary and confidential information that when disclosed can damage the organization's brand name and customer base.	Integrity requirements when people are concerned address shared secrets like cryptographic keys or passwords. Possession of such knowledge introduces human factor threats that should be addressed with respective controls.	Availability requirements for people assets are especially important when these people are critical resources for the continuous operations of the service or product offerings.

Applications	Applications with confidentiality requirements often handle information with corporate proprietary information (R&D), customer base information, sensitive customer information of medical or personal nature.	Applications with integrity requirements typically handle transactions of financial nature, procurement of good or e-commerce.	Availability requirements are met in applications that are critical to the business daily operations and where downtime usually incurs costs and overheads in terms of resource allocation.
---------------------	--	--	---

Table 4: Security Requirements Selection Table

As an output of this process assessment teams should have a table of critical assets classified by asset categories and a list of corresponding security requirements, together with justification or supporting information considered during the evaluation.

The output will then be used as input by phase 3 - Control Cards Selection, as indicated in the next chapter.

4.3.3 Phase 3 - Control Cards Selection

During Phase 3 the assessment team selects appropriate controls based on the risk profile selected for every risk category and the list of identified critical assets (including their requirements). Controls are separated in two Categories –organizational controls and the asset-based control.

The entire organisation is assumed to be one single asset that must be protected. Organizational security controls are typically broad and apply to the asset organization in a horizontal manner. On the contrary, asset-based controls are targeted at the implementation of the protection required by assets (e.g., enforcing the availability of a critical network component).

Controls are further grouped in control cards. Two types of control cards are available for selection by the teams that carry the assessment of a SME:

- Controls cards that contain controls applicable to the organization horizontally and are concerned with practices and management procedures and
- Control cards that are applicable to critical assets and are asset-category-specific. Control cards are essentially pre-selected – grouped controls according to risk profiles and the asset security requirements.

Table 5 lists the categories of controls, their structure and their name as they are considered in this approach. As already mentioned, these controls have been adopted from OCTAVE. The decision to use these controls was based on their simplicity. Other controls may be used instead (e.g. ISO 17799, IT-Grundschutz, etc.). A more detailed description can be found in.

Controls Category	Control No.	Name of the control
Organizational	SP1	Security Awareness and Training
	SP2	Security Strategy
	SP3	Security Management
	SP4	Security Policies and Regulations
	SP5	Collaborative Security Management
	SP6	Contingency Planning/Disaster Recovery
Asset Based	OP1.1	Physical Security Plans and Procedures
	OP1.2	Physical Access Control
	OP1.3	Monitoring and Auditing Physical Security
	OP2.1	System and Network Management
	OP2.2	System Administration Tools
	OP2.3	Monitoring and Auditing IT Security

	OP2.4	Authentication and Authorization
	OP2.5	Vulnerability Management
	OP2.6	Encryption
	OP2.7	Security Architecture and Design
	OP3.1	Incident Management
	OP3.2	General Staff Practices

Table 5: Controls used in the approach presented

Accordingly, phase 3 of the proposed assessment approach consists of two separate but equally important steps:

- Step A, Selection of Organizational Controls
- Step B, Selection of Asset-Based Controls

During these steps, controls are assigned to the organisation (as a single important asset) and to the identified critical assets as indicated below.

Organizational Control Cards Selection

The selection of the organisational control cards is performed in a fairly straightforward manner: organization controls are available for every risk profile (defined in the risk profiling matrix). The following table assigns organisational controls to the risk profiles as mentioned in [chapter 4.3.1 Phase 1 - Risk profile selection](#). Controls listed below are recommended in order to mitigate respective organisational risks. A detailed description of the controls is included in [Annex C. Organizational Controls](#).

Risk Areas	High	Medium	Low
Legal and Regulatory	(SP1)	(SP1)	SP1.1
	(SP4)	(SP4)	
Productivity	(SP3)	(SP4)	SP4.1
	(SP4)		
	(SP6)	(SP6)	
	(SP5)		
Financial Loss	(SP2)	(SP4)	SP4.1
	(SP1)		
	(SP4)		
Reputation and Loss of Customer Confidence	(SP1)	(SP4)	SP4.1
	(SP5)	(SP1)	

Table 6: Organizational Control Cards

Asset-Based Control Cards Selection

Based on the risk profile and the asset security requirements SME assessment teams can use asset control cards table (s. table 7) to identify the controls appropriate for the protection of critical assets.

Asset Control Cards			
Asset	High Risk Cards	Medium Risk Cards	Low Risk Cards
Application	CC-1A	CC-2A	CC-3A
System	CC-1S	CC-2S	CC-3S
Network	CC-1N	CC-2N	CC-3N
People	CC-1P	CC-2P	CC-3P

Table 7: Asset Control Cards

Asset control cards are essentially grouped in three categories, corresponding to organization risk profile, asset category and security requirement. For example assessment teams facing a high risk organization profile will have different security requirements than medium or low risk profiles. Each control card involves a number of asset controls (see Annex B. Asset Control Cards) to address the complete range of risks and security requirements as needed in the particular profile and dictated by the selected security requirements. A more detailed description of the controls included in the control cards can be found in Annex D, Asset based Controls.

For the sake of this presentation, we add at this point the control card CC-1A. As indicated in the table, this card is appropriate for the protection of an application in a high risk scenario (high risk profile).

Asset Based Control Card ID		CC-1A								
Risk Profile	High									
Asset Category	Application									
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality		2.1.3			2.4.2	2.5.1	2.6.1			
Integrity		2.1.4			2.4.2	2.5.1	2.6.1			
Availability		2.1.6								

Table 8: An example of a control card for the asset application in a high risk profile

Assessment teams, using the previously identified security requirements and the control card can subsequently identify more specific controls (e.g. the controls for availability, confidentiality or integrity). It has to be noted that in cases where more than one requirement is selected, the controls that apply to the asset are the sum of the controls for each requirement.

4.3.4 Phase 4 – Implementation and Management

During Phase 4 and based on the assessed information, the assessment team creates mitigation plans to address the risks to the critical assets.

Once (1) organization risk profile, (2) critical assets and (3) control cards have been identified, the assessment team plans the implementation of the selected controls. It is anticipated that due to limited resources SMEs will be unable to implement all identified controls for all critical assets in one shot. In this regard, prioritization is a key element of successful risk mitigation efforts.

An implementation plan defines how an organization intends to raise or maintain the existing level of security. Its objective is to provide a direction for future information security efforts rather than to find an immediate solution to every security vulnerability and concern.

Bellow some criteria for prioritizing actions for implementing identified control cards can be found. Not all of them are applicable in all companies. However, this can serve as a generic guide:

- **Strategic alignment with organization goals:** Does this asset directly support documented organization and/or divisional work plan goals? What goals and/or work plan objectives will be supported and how?
- **Continuous improvement efforts:** Does this asset support a division's continuous improvement asset effort? What is the continuous improvement asset? How does this asset support continuous improvement goals?
- **Legal or Regulatory mandates:** If an asset is necessary to meet regulatory requirements, this will be reflected in setting priorities
- **System-wide benefits:** System-wide benefits include improved customer service for several customer groups. A higher priority will be given to customer groups that are considered critical, but the larger the customer group affected the greater the benefit.
- **Cost/Time Savings:** Estimates of cost and/or time savings include staff time, customer time savings, revenue generation, and direct budget/cost reductions.
- **Risk Reduction:** As result of a project, information and/or services will prevent lost revenues and/or non-compliance with policies, legal, and audit requirements.

The next step is the planning process, which indicates and monitors the exact time plan of security tools and procedures implementation.

A key question in almost every implementation is of whether internal resources are adequate or competent to fulfil the implementation plan. In other words a decision either to in-source or outsource the related implementation and management work might be necessary.

5. Self Assessment Guidelines with two examples

In this chapter, a more detailed breakdown of the four phases will be presented in logical steps. This is to help SMEs (1) identify the risk profile of their organization, (2) identify the critical assets that need to be secured, (3) select controls and solutions for improved security and finally (4) develop plans for improvement. However, actions and solutions that may be applied to SME's are not solely and limited to the ones provided here.

Again, organizations are strongly encouraged to perform the guidelines and best practices included in this method only as short term plan and towards a goal of quickly and effectively protecting crucial and critical components of their business. However, the process does not replace a complete and thorough risk assessment approach, which is strongly recommended as the basis for a long term risk management strategy.

Before attempting to use the method, SMEs need to understand the following three unique aspects of this method:

- A small interdisciplinary analysis team of three to five people leads the risk assessment process. Collectively, analysis team members must have broad insight into the organization's business and security processes, sufficient to conduct all of the RA activities. For this reason, the method does not require formal data-gathering workshops to kick-off the evaluation.
- The method includes a limited exploration of the computing infrastructure. Since small organizations frequently outsource their IT services and functions, they typically have not developed organizational capabilities for running and interpreting the results of vulnerability evaluation tools. However, the lack of an organizational capability for running such tools does not preclude an organization from establishing a protection strategy.
- Rather than using vulnerability data to refine its view of its current security practices, an organization conducting an evaluation examines the processes employed to securely configure and maintain its computing infrastructure.

The document is structured with phases and steps as the building blocks. Two examples are provided for every phase. The examples use the following company scenarios:

- **Company in Example A.** In example A we consider the special case of a medium sized online medical care service providing on-line medical support for doctors that need to have advise for their patients and information regarding recent advances in medicine. As such the database supporting the application stores critical and confidential data of a personal nature. The company employs 100 people and has three departments, the medical and medicine support department, the medical science department and the management department which includes activities concerning the human resources and financial control.
- **Company in Example B.** The company in example B is a small sized law firm. In this case, IT-systems are widely used to store information about the cases, to exchange emails and to prepare and process the needed documents. The company employs five lawyers and one secretary.

Figures (workflow diagrams) for every phase are also supplied; implementation hints for every step are provided in the dotted boxes for each of the forthcoming phase descriptions.

Phase 1 – Select Risk Profile

The analysis team considers business risk aspects of information protection that can (a) directly or indirectly affect or damage reputation and customer confidence, (b) result in legal and regulatory non-compliance, (c) create financial loss and (d) decrease productivity. AIt then selects an appropriate risk level for each risk area using the risk profile evaluation table. The specified areas are the following: Legal and Regulatory, Productivity, Financial Stability, Reputation and Loss of Customer Confidence. As shown in figure 3, the phase involves two steps.

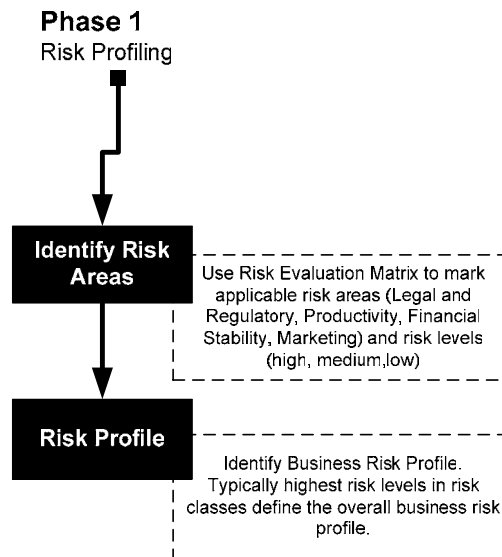


Figure 3: Phase 1 - Risk profile selection workflow

To identify the current or potential risk level, analysis team members should highlight the risk area and read the description in each column. Risk areas that are closer to their business profile are chosen. The process is followed for every risk area. At the end there should be a MATRIX highlighting the applicable risk level in each risk area.

Example A. (High Risk Profile)

In example A the team uses the **Risk Profile Evaluation Table** to identify the risk context of the company. As such the team identifies a high risk level (marked with red colour) in the legal and regulatory area since the business handles information of a sensitive and personal nature. At the same time it finds a high risk level in productivity since it employees 100 people, a medium risk level (marked with orange) in financial stability and a low risk level (marked with blue) in reputation and loss of customer confidence as shown in the following risk profile evaluation table.

Risk Areas	High	Medium	Low
Legal and Regulatory	Business handles customer information of a sensitive and personal nature including medical records and critical personal data as defined by the	Business handles customer information of a personal but not sensitive nature as defined by the EU Data Protection Law.	Business Does not handle personal data other than those of the people employed by the organization

	EU Data Protection Law.		
Productivity	The business employs more than 100 employees who have a daily need to access business applications and services.	The business employs more than 50 employees who have a daily need to access business applications and services.	The business employs less than 10 employees who have a daily need to access business applications and services.
Financial Stability	Yearly revenues are of excess of 25 M. Euros or/ and financial transactions with third parties or customers are taking place as part of the business as usual process	Yearly revenue do not exceed 25 M. Euros	Yearly revenue do not exceed 5 M. Euros
Reputation and Loss of Customer Confidence	Unavailability or Service Quality directly impact Business Profile or/and more than 70% of customer base have online access to business products and services	Unavailability or Service Quality can indirectly impact Business Profile and/or less than 5% of customer base have online access to business products and services	Unavailability or Service Quality cannot directly or indirectly impact Business Profile or result in loss of revenue

Table 9: Risk Profile evaluation table - Example A

Next the Business Risk Profile is calculated. Risk areas signify the overall business risk context. **It is recommended that the risk profile should equal the highest level identified in the subordinate risk areas in the risk matrix.**

The table below illustrates the identified risk levels in the predefined risk areas and shows where the organization should focus its efforts to apply appropriate security controls. The table can be used to set up priorities as well. High risk levels indicate an urgent need for improvement while low risk levels highlight actions that should be taken into consideration for future improvement.

Risk Areas	Risk Level	Risk Profile
Legal and Regulatory	High	High
Productivity	High	
Financial Stability	Medium	
Reputation and Loss of Customer Confidence	Low	

Table 10: Organization Risk Profile - Example A

Example B. (Medium Risk Profile)

In example B the team uses the **Risk Profile Evaluation Table** to identify the risk context of the company. The analysis team proceeds by identifying a low risk (marked with blue colour) level in the legal and regulatory area since the company does not handle personal data other than those of the people employed by the organization, a low risk level in productivity (marked with blue), a low risk level (marked with blue) in financial stability and a medium risk level (marked with orange) in reputation and loss of customer confidence, as shown in the following risk profile evaluation table.

	High	Medium	Low
--	------	--------	-----

Risk Areas			
Legal and Regulatory	Business handles customer information of sensitive and personal nature including medical records and critical personal data as defined by the EU Data Protection Law.	Business handles customer information of personal but not sensitive nature as defined by the EU Data Protection Law.	Business Does not handle personal data other than those of the people employed by the organization
Productivity	The business employs more than 100 employees who have a daily need to access business applications and services.	The business employs more than 50 employees who have a daily need to access business applications and services.	The business employs less than 10 employees who have a daily need to access business applications and services.
Financial Stability	Yearly revenues are of excess of 25 M. Euros or/ and financial transactions with third parties or customers are taking place as part of the business as usual process	Yearly revenue do not exceed 25 M. Euros	Yearly revenue do not exceed 5 M. Euros
Reputation and Loss of Customer Confidence	Unavailability or Service Quality directly impact Business Profile or/ and more than 70% of customer base have online access to business products and services	Unavailability or Service Quality can indirectly impact Business Profile and/or less than 5% of customer base have online access to business products and services	Unavailability or Service Quality cannot directly or indirectly impact Business Profile or result in loss of revenue

Table 11: Risk profile evaluation table- Example B

Next, the Business Risk Profile is calculated. Risk areas signify the overall business risk context. **It is recommended that the risk profile should equal the highest level identified in the subordinate risk areas in the risk matrix.**

The table below illustrates the identified risk levels in the predefined risk areas and shows where the organization should focus its efforts to apply appropriate security controls. The table can be used to set up priorities as well. High risk levels indicate an urgent need for improvement while low risk levels can be considered as a security note that must be taken into consideration for future improvement.

Risk Areas	Risk Level	Risk Profile
Legal and Regulatory	Low	Medium
Productivity	Low	
Financial Stability	Low	
Reputation and Loss of Customer Confidence	Medium	

Table 12: Organization risk Profile – Example B

Phase 2 - Identify Critical Assets

Phase 2 requires decisions that shape the remainder of the evaluation—selecting the organization's critical assets. Depending upon the size of the organization, the number of information assets identified during this phase could easily exceed a hundred. To make the analysis manageable, SMEs need to narrow the focus of the evaluation by selecting the few assets that are most critical to achieving the mission and meeting the business objectives of the organization. These are the only assets that will be analyzed during later activities. As depicted in figure 4 the phase involves three steps.

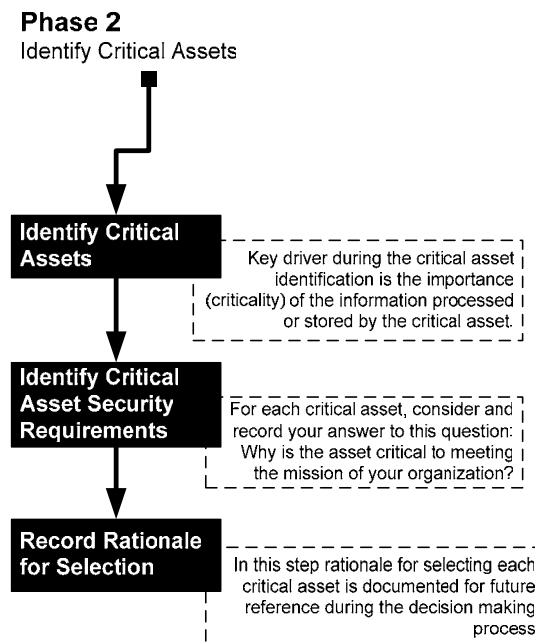


Figure 4: Phase 2 - Identification of Critical Assets Workflow

Step 1. Select your organization's five most critical assets

When critical assets are selected, teams are not limited to choosing only five. Five assets are normally enough to enable organizations to develop a good set of mitigation plans during phase 4. However, analysis team members must use their judgement whether to use more or fewer than five. During the selection process of critical assets, team members should consider which assets will result in a large adverse impact on the organization in one of the following scenarios:

- **Disclosure** of information to unauthorized people
- **Modification** of information without authorization
- **Loss or destruction** of the asset
- **Interrupted access** to the asset or to the information stored

In cases where the critical assets are difficult to identify, teams should consider the Business functions/ areas inside the organization. These could be different projects, work groups (groups of people with different job description) or even separate organizational departments (HR Department, Accounts Department, Marketing Department, Sales Department etc.). These assets should then be listed by level of importance to the business process. After defining the areas that need to be secured, or reorganising the organization's assets, the next step is to list all assets according to their impact on the business process. A more feasible way to do this is to group the assets by organizational department or function.

A key driver during the critical asset identification is the importance (criticality) of the information processed or stored by the critical asset. By performing the decomposition analysis, team members can easily identify where and how critical information is stored or used.

Step 2. Record the Rationale for selecting each Critical Asset

While selecting critical assets in step 1, a number of issues related to these assets are discussed. In this step the rationale for selecting each critical asset is documented for future reference during the decision making process. In addition, understanding why an asset is critical can better enable the definition of the security requirements during the next step. For each critical asset, the following questions should be considered and answers recorded:

- Why is the asset critical to meeting the mission of the organization?
- Who controls it?
- Who is responsible for it?
- Who uses it?
- How is it used?

These questions focus on how assets are used and why they are important. If answers to all of these questions are not provided, people in the organization who can provide the answers must be located and included in the analysis team. The information that is generated by answering these questions will be useful later in this process. In this regard, information gathered here must be carefully recorded.

Step 3. Identify Critical Asset security requirements

In general, when describing a security requirement for an asset, one needs to understand what aspect of the asset is important. For information assets, security requirements will focus on the confidentiality, integrity, and availability of the information.

Security requirements can vary for different categories of assets within an SME, but careful selection of requirements is critical for the controls selection task that follows. In other words, high availability requirements impose high availability controls etc.

Analysis teams use the **requirements selection criteria** as provided in order to identify most important security requirements. **Asset security requirements will be used later during the asset control card selection.** The security requirements evaluation criteria have been developed as a simple and practical guide for evaluating the security requirements in terms of confidentiality, integrity and availability of the critical assets selected. The evaluation highlights the importance of the asset security attributes and indicates the appropriate controls for their protection.

As an output, the analysis teams should have **a table listing critical assets along with a short description of their importance for the accomplishment of the business mission, its basic elements, and the security requirements.**

For all three steps discussed above, the tables of section 4.3.2 can be used to identify relevant assets and their requirements (see Table 3 and Table 4).

Example A. (Risk Profile: High, Critical Asset: Application - Phase 2.)

[Step 1] In example A, the most critical asset is identified to be the Web Application providing on-line support to the clients – the doctors. This application is essential to the business as it represents the most important element of the service offerings, and therefore it is selected as the most critical asset.

[Step 2] In the next step the team members document the elements that constitute the asset and the rationale for their selection. In this way they eventually identify the Database that stores client information, the network segment that supports connectivity with internal and external networks, the web server and the firewalls as core components of the asset.

[Step 3] Next, security requirements are identified. By using the following table (Table 13), teams recognize the boxes that fit their requirements. In example A, the team selects the database to have confidentiality requirements since the data stored concern the company's clients, they select the network to have availability and confidentiality requirements since the network transmits information that must remain intact and secret for completing transactions or queries.

Assets	Confidentiality	Integrity	Availability
Systems	A system with Confidentiality Requirements often handles information with Corporate Proprietary Information (R&D), Customer Base Information, Sensitive Customer Information of a Medical or Personal Nature	System with Integrity Requirements typically handle transactions of a financial nature, procurement of good or e-commerce	Availability Requirements are met in systems that are critical to the business daily operations and where downtime usually incurs costs and overheads in terms of resource allocation
Network	A network with Confidentiality requirements typically covers communications and information exchange over insecure and un-trusted environments	Network Integrity Requirements are typically necessary when transactions take place over public and shared metropolitan networks or telecommunication providers	Availability requirements are especially necessary when the network is used as part of the customer care or service and product offerings
People	Confidentiality requirements are typically encountered when people handle organizational proprietary and confidential information which when disclosed can damage the Organization's brand name and customer base	Integrity requirements when people are concerned address shared secrets like cryptographic keys or passwords. The knowledge of this to people introduces human factor threats that should be addressed with respective controls	Availability requirements for people assets are especially important when these people are critical resources for the continuous operations of the service or product offerings.
Applications	Applications with Confidentiality Requirements often handle information with Corporate Proprietary Information (R&D), Customer Base Information, Sensitive Customer Information of Medical or Personal Nature	Applications with Integrity Requirements typically concern transactions of financial nature, procurement of goods or e-commerce	Availability Requirements are met in Applications that are critical to daily business operations and where downtime usually incurs costs and overheads in terms of resource allocation

Table 13: Security requirements selection table – Example A

As an output the analysis teams documents a table listing critical assets along with the rationale for selection, its basic elements, and the security requirements for the services provided. The table below is the output of example A for Phase 1 (see Table 14).

Critical Asset	Asset Category	Components	Security Requirements	Rationale For Selection
E-commerce Application	Application	Database	Confidentiality Integrity Availability	The application is essential for the business as it represents the most important element of the service offering.
		Firewall		
		Network Segment		
		Server		

Table 14: Security requirements rationale

Example B. (Risk Profile: Medium, Critical Asset: System- Phase 2.)

[Step 1] In example B, the most critical asset is identified as Workstations used for performing daily activities including customer correspondence, client information regarding cases, and basic accounting information regarding invoicing and accounts receivable.

[Step 2] In the next step the team members document the elements that constitute the asset and the rationale for their selection. Hence they identify four workstations, the internal network and the file server.

[Step 3] Next, security requirements are identified. By using the following table teams recognize the boxes that fit their requirements. In example B, the team selects the workstations with availability requirements as those that are used for daily business activities and therefore must remain operational.

Critical Assets	Confidentiality	Integrity	Availability
Systems	A system with Confidentiality Requirements often handles information with Corporate Proprietary Information (R&D), Customer Base Information, Sensitive Customer Information of a Medical or Personal Nature	System with Integrity Requirements typically handle transactions of a financial nature, procurement of goods or e-commerce	Availability Requirements are met in systems that are critical to daily business operations and where downtime usually incurs costs and overhead in terms of resource allocation
Network	A network with Confidentiality requirements typically covers communications and information exchange over insecure and un-trusted environments	Network Integrity Requirements are typically necessary when transactions take place over public and shared metropolitan networks or telecommunication providers	Availability requirements are especially necessary when the network is used as part of the customer care or service and product offerings
People	Confidentiality requirements are typically addressed when people handle organizational proprietary and confidential information which when disclosed can damage the Organization's brand name and customer base	Integrity requirements when people are concerned address shared secrets like cryptographic keys or passwords. The knowledge of this to people introduce human factor threats that should be addressed with respective controls	Availability requirements for people assets are especially important when these people are critical resources for the continuous operations of the service or product offerings.
Applications	Applications with Confidentiality Requirements often handle information with Corporate Proprietary Information (R&D), Customer Base Information, Sensitive Customer Information of Medical or Personal Nature	Applications with Integrity Requirements typically handle transactions of a financial nature, procurement of goods or e-commerce	Availability Requirements are met in Applications that are critical to the business daily operations and where downtime usually incurs costs and overhead in terms of resource allocation

Table 15: Security requirements selection table – Example B

As an output the analysis teams documents a table listing critical assets along with the rationale for selection, its basic elements, and the security requirements for the services provided. The table below is the output of example B of step 3 (Table 16).

Critical Asset	Asset Type	Components	Security Requirements	Rationale For Selection
Workstations	System	4 Workstations Network Seament Server	Availability	Workstation are important for performing daily activities including customer correspondence, client information regarding cases, and basic accounting information regarding invoicing and accounts receivable

Table 16: Security requirements rationale

Phase 3 – Select Control Cards

During Phase 3 the analysis team members are in a position to “pull out” the control cards associated with the already defined (in phase 1) applicable risk areas and the list of identified critical assets. As depicted in figure 5 the phase involves three steps.

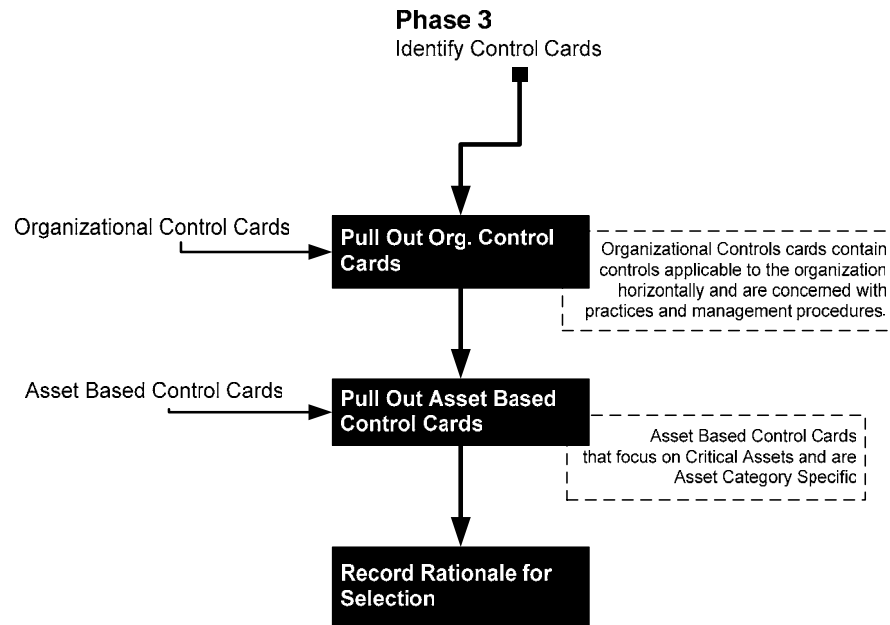


Figure 5: Phase 3 – Control Cards Selection Workflow

Control cards contain controls from the catalogue of practices used in the OCTAVE approach. The catalogue of practices comprises a collection of good strategic and operational security practices. An organization that is conducting an information security risk evaluation measures itself against this catalogue of practices. The catalogue is used as a measure of what the organization is currently doing well with respect to security (its current security practices) and what it is not doing well (its organizational vulnerabilities).

The catalogue of practices is deliberately divided into **two types of controls: Organizational Controls and Asset Based Controls:**

- **Organizational controls** focus on organizational issues at the policy level and provide good general management practices. Organizational Controls include issues that are business-related as well as those that require organization-wide planning and participation.
- **Asset Based Controls** practices focus on technology-related concerns. They include issues related to how people use, interact with, and protect technology.

The catalogue of practices is a general catalogue; it is not specific to any domain, organization, or set of regulations. It can be modified to suit a particular domain's standard of due care or set of regulations (e.g., the medical community and HIPPA security regulations). It can also be extended to add organization-specific standards, or it can be modified to reflect the terminology of a specific domain. **Furthermore, it can be replaced with any compatible standard controls list.**

Controls are further grouped into Control Cards separated in two Categories / Control Areas: the organizational control areas and the asset based control areas. Two types of control cards are available for selection by the teams that carry out the analysis of an SME:

- **Organizational Controls cards** that contain controls applicable to the organization horizontally and are concerned with practices and management procedures. Organizational

security control cards are typically broad and are intended to mitigate typical information risks associated with the organizational profile.

- **Asset Based Control Cards** that focus on Critical Assets and are Asset-Category-Specific. Control cards are essentially pre-selected – grouped controls according to the risk profiles and the asset security requirements. As mentioned above, the major groups of organization assets are: Information, System/ Network, People, and Applications. Asset-based control cards are created to focus on day-to-day tasks and they target asset-specific risks.

A detailed description of the organizational controls can be found in [Annex C. Organizational Controls](#).

Step 1. Select Organization Control Cards

During this step, analysis teams select organizational control cards for the risk areas identified during phase 1 (Risk Profiling) and thereby define the direction for information security efforts in the organization. However, practical considerations will prevent SMEs from immediately implementing all of the initiatives after the evaluation. Organizations will likely have limited funds and staff members available to implement the protection strategy. After the evaluation, the analysis team prioritizes the activities in the protection strategy and then focuses on implementing the highest-priority activities.

Organization Controls are available for every risk profile as defined in the Risk Profiling Matrix.

Step 2. Select Asset Based Controls

Based on the risk profile and the asset security requirements SME analysis teams can use Asset Control Cards Table (see [Annex B. Asset Control Cards](#)) to identify the appropriate asset controls. Asset-Based Control cards are essential controls grouped into three categories, according to organization risk profile, asset category and security requirement. For example, analysis teams with a high risk organization profile will have different risks and security requirements as opposed to medium or low risk profiles. Equally, controls cards will include more controls to address a higher range of risks and security requirements.

Step 3. Document List of Selected Controls and Rationale

While pulling out control cards of critical assets in step 2, you will discuss a lot of issues related to these controls. In this step you document your rationale for selecting each control card and the necessary actions for implementation. In addition, by understanding control cards, you will be better able to define action plans during the next step. For each control card, consider and record your answer to this question: What is required in terms of resources and changes to implement the selected controls? Discuss the operational aspects of each control. Consider the following questions for each one.

- Who should implement it?
- Who should be responsible for it?
- Who should benefit from it?
- How should it be implemented?

These questions focus on how controls should be used and why they are important. If you can't answer all of these questions, you may need to ask people in your organization who can answer them. The information that you identify by answering these questions will be useful in phase 4 when you build mitigation plans. Make sure that you record this information.

Example A. (Risk Profile: High, Critical Asset: Application)

[Step 1] In step 1, analysis teams using the **Risk Profile Evaluation Table and the organizational controls table (Table 17)** select organizational control cards for the risk areas identified during phase 1 (Risk Profiling), thereby defining the direction for information security efforts in the organization.

In example A the organizational controls for a high Legal and Regulatory risk level introduce security practices (controls) that are dictated by **SP1 and SP4** organizational controls. In the same way, a high risk in productivity risk class imposes a need for countermeasures and practices implied by **SP3, SP4, SP5 and SP6** organizational controls. For Medium risk level in Financial Stability, SP4 is dictated, and for Low risk level of Reputation and Loss Customer Confidence, SP4.1 (section included in controls of SP4).

Risk Areas	High	Medium	Low
Legal and Regulatory	(SP1)	(SP1)	SP1.1
	(SP4)	(SP4)	
Productivity	(SP3)	(SP4)	SP4.1
	(SP4)		
	(SP6)	(SP6)	
	(SP5)		
Financial Loss	(SP2)	(SP4)	SP4.1
	(SP1)		
	(SP4)		
Reputation and Loss of Customer Confidence	(SP1)	(SP4)	SP4.1
	(SP5)	(SP1)	

Table 17: Organizational controls selection – Example A

[Step 2] In step 2 analysis team selects asset-based control card(s) using the asset-based control cards table. In example A given the high risk profile of the organization identified in phase 1 and the critical asset type identified in step 2, they select card 1 for high risk profile applications, namely card CC-1A.

Control Cards Table			
Critical Assets	High Risk Cards	Medium Risk Cards	Low Risk Cards
Application	CC-1A	CC-2A	CC-3A
System	CC-1S	CC-2S	CC-3S
Network	CC-1N	CC-2N	CC-3N
People	CC-1P	CC-2P	CC-3P

Table 18: Asset based controls selection – Example A

The card selected in example A (see Annex B. Asset Control Cards) displays the necessary controls for an Application running at an organization with a risk profile. The team identifies the controls that address the security requirements identified in phase 3. In this example confidentiality and availability requirements are used. The following asset controls **2.1.3, 2.1.6, 2.4.2, 2.5.1, and 2.6.1** are selected.

Asset Based Control Card ID	CC-1A
Risk Profile	High

Asset Category		Application								
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and	Incident Management	General Staff Practices
Confidentiality		2.1.3			2.4.2	2.5.1	2.6.1			
Integrity		2.1.4			2.4.2	2.5.1	2.6.1			
Availability		2.1.6								

Table 19: CC-1A Asset based control card – Example A

[Step 3] In Step 3 analysis teams are occupied with data gathering and analysis of the output produced in Steps 1 and 2. Documenting the output of previous steps, both the selected asset-based controls and the organizational controls are then listed in the table below.

Asset	Control	Rationale For Selection
Asset Based Controls	2.1.3	System and Network Management controls are essential for maintaining the availability and confidentiality of the asset under consideration.
	2.1.6	
	2.1.4	Integrity of the application is important because medical information has to be accurate.
	2.4.2	Authentication and Authorization for either internal and external users or third parties can ensure controlled access to the asset under consideration.
	2.5.1	Vulnerability Management including regular vulnerability assessment and the necessary remediation activities is essential in order to evaluate security measures and systems.
	2.6.1	Confidential information has to be protected during transport and storage.
Organizational Controls	SP1	Security Awareness and Training
	SP3	Security Management
	SP4	Security Policy
	SP5	Collaborative Management
	SP6	Disaster Recovery

Table 20: Selected controls table and rationale – Example A

Example B. (Risk Profile: Medium, Critical Asset: System)

In step 1, analysis teams using the **organizational controls table** (Table 21) select organizational control cards for the risk areas identified during phase 1 (Step 1 - **Risk Profile Evaluation Table**), defining the direction for information security efforts in the organization.

For **example B**, the dictated organizational control for a Low Legal and Regulatory risk level is SP1.1 while for a Low risk level of Productivity and Financial Stability is SP4.1. Medium risk level of Reputation and Loss of Customer Confidence dictates the use of SP1 and SP4 organisational controls.

Table 21 summarizes the mapping controls for previously mentioned Example B.

Risk Areas	High	Medium	Low
Legal and Regulatory	(SP1)	(SP1)	SP1.1
	(SP4)	(SP4)	
Productivity	(SP3)	(SP4)	SP4.1
	(SP4)		
	(SP6)	(SP6)	
	(SP5)		
Financial Loss	(SP2)	(SP4)	SP4.1
	(SP1)		
	(SP4)		
Reputation and Loss of Customer Confidence	(SP1)	(SP4)	SP4.1
	(SP5)	(SP1)	

Table 21: Organizational controls selection – Example B

[Step 2] In step 2 analysis team selects asset-based control card(s) using the asset-based control cards table. In example B given the medium risk profile of the organization identified in phase 1 (Step1) and the critical asset type identified in step 2, they select card 2 for medium risk profile systems, namely card CC-2S.

Control Cards Table			
Critical Assets	High Risk Cards	Medium Risk Cards	Low Risk Cards
Application	CC-1A	CC-2A	CC-3A
System	CC-1S	CC-2S	CC-3S
Network	CC-1N	CC-2N	CC-3N
People	CC-1P	CC-2P	CC-3P

Table 22: Asset based control card selection – Example B

The card selected in example B (see [Annex B. Asset Control Cards](#)) displays the necessary controls for system assets at an organization with a medium profile. The team identifies the controls that address the security requirements identified in phase 3. Following Example B output from Phase 2 (step3), availability requirements are used to identify appropriate controls from the control card **CC-2S**. Hence the asset controls **2.1.7, 2.1.6** are selected.

Asset Based Control Card ID		CC-2S								
Risk Profile		Medium								
Asset Category		System								
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality		2.1.6 2.1.7			2.4.1					
Integrity		2.1.9			2.4.1					
Availability		2.1.6 2.1.7								

Table 23: CC-2S Asset based control card – Example B

[Step 3] In Step 3 analysis teams are occupied with data gathering and analysis of the output produced in Steps 1 and 2. Documenting the output of previous steps, both the selected asset-based controls and the organizational controls are then listed in table below.

Asset	Control	Rationale For Selection
Asset Based Controls	2.1.6	System and Network Management controls are essential for maintaining the availability and confidentiality of the asset under consideration.
	2.1.7	
Organizational Controls	SP1	Security Awareness and Training
	SP4	Security Policy
	SP1.1	Included in SP1
	SP4.1	Included in SP4

Table 24: Controls selection rationale – Example B

Phase 4 – Implementation and Management

During Phase 4 the analysis team identifies actions and recommends an action list, setting forth the direction for security improvement. Essential for the successful implementation is the establishment of Senior Management (Decision Makers) sponsorship for the ongoing security improvement.

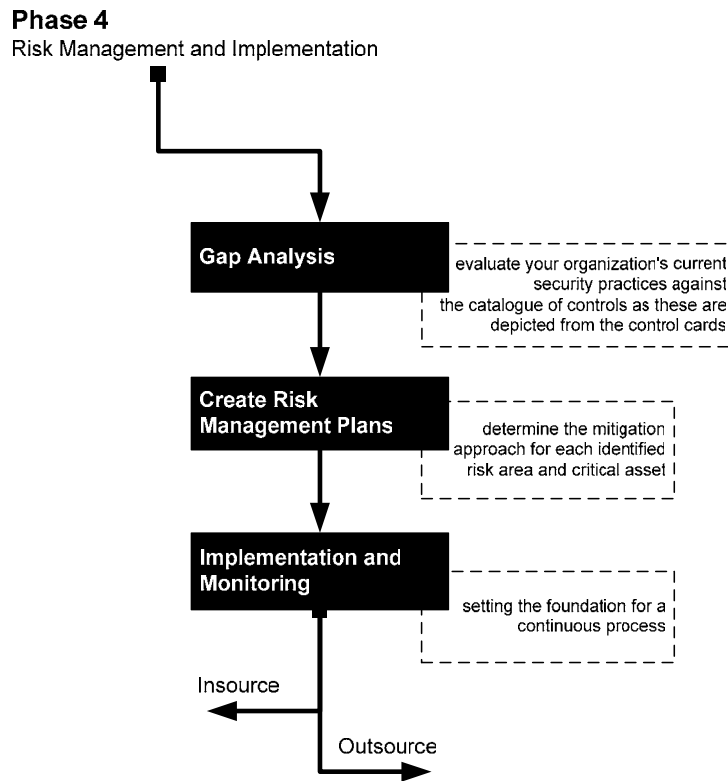


Figure 6: Phase 4 – Implementation and management workflow

Step 1. Gap Analysis

Gap analysis is essential in order to improve how an organization handles information security, and establish the current state of security, that is, what is currently done well and where improvement is needed.

In this step, analysis teams are occupied with the evaluation of the organization's current security practices against the controls as these are depicted from the control cards. Analysis teams read carefully selected control cards and elicit detailed information about the organization's current security policies, procedures, and practices, thus providing a starting point for improvement.

During the Gap Analysis process teams use the control cards as the "requirements" and assess the gaps between these and current security practices both at an organizational and critical asset level. Analysis teams should carefully document output in two distinct plans – **(1) one for the organizational improvement** and **(2) one for the asset protection**.

The output from this process can form the basis for the planning activity that follows next. It is separated into two categories: **(a) Organizational Controls**, where the analysis teams should identify what they do and don't do and define actions for improvement at an organizational level and **(b) Asset Based controls** where analysis teams assess existing protection measures for the identified critical assets.

Step 2. Create Risk Mitigation Plans

In this step analysis team members have already identified critical assets, their organization risk profile, the security requirements and have further selected appropriate controls and are about to determine the mitigation approach for each identified risk area and critical asset.

By taking these initial steps toward improvement, organizations can start to build the momentum needed to implement its protection strategy.

The output of this activity is the risk mitigation plan, which **leads to a series of steps** that an organization can take to raise or maintain its existing level of security. Its objective is to provide a direction for future information security efforts rather than to find an immediate solution to every security vulnerability and concern. Since a mitigation plan provides organizational direction with respect to information security activities, we suggest structuring it around the selected (phase 3) control cards (organizational and critical-asset-based).

Step 3. Implementation, Monitoring and Control

One of the principles of the risk assessment method is setting the foundation for a continuous process. This principle addresses the need to implement the results of an information security risk evaluation, providing the basis for security improvement. **If an organization fails to implement the results of an evaluation, it will also fail to improve its security posture.**

One of the most difficult tasks in any improvement activity is maintaining the momentum generated during an evaluation. However, practical considerations will prevent most organizations from immediately implementing all of the initiatives after the evaluation. SMEs will likely have limited funds and staff members available to implement the protection strategy.

In **this step analysis teams prioritize the activities and then focus on implementing the highest-priority activities.**

Three distinct options are provided:

- **Risks accepting.** When a risk is accepted, no action to reduce the risks is taken and the consequences should the risk materialize are accepted.
- **Risks mitigating.** When a risk is mitigated, actions designed to counter the threat and thereby reduce the risk are identified and enforced.

Now that specific action items have been identified, analysis team members need to assign responsibility for completing them as well as set a completion date. Answers -- for each action item -- to the following questions must be reordered:

- Who will be **responsible** for each action item?
- What can management do **to facilitate** the completion of this action item?
- How much will it **cost**?
- **How long** will it take?
- **Can we do it ourselves?**
- **Do we need external assistance?**

NOTE:

The last two questions are critical **to whether an organization can handle implementation** of the **necessary controls internally**. The answers to these are equally important and very hard to establish since both (outsource or in-source) have benefits and disadvantages.

Outsourcing is the **"make or buy" decision applied to the resource in question**. If it is done right, outsourcing can offer definite advantages. The main objectives for outsourcing are, besides support functions, cost-cutting, downsizing, and a desire to focus on the business (core competence). The lack of IT competence in the organization can also be a reason for IT outsourcing. As IT is getting

more important, companies frequently confront a wide disparity between the capabilities and skills necessary to realize the potential of information technology and the reality of their own in-house technology expertise.

There are however several options that should be considered and which combine core organization competencies and external or third party support (partial or full outsourcing). As deduced from figure 7, management and implementation can both be outsourced. **Service offerings typically found in vendors can be summarized as follows:**

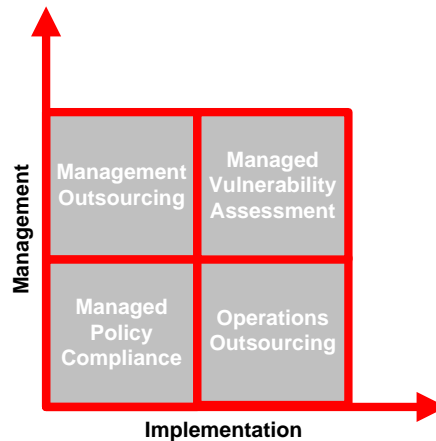


Figure 7: Management vs. implementation outsourcing options

- **Management Outsourcing.** In management outsourcing vendors provide management services in information security. In other words **a security officer is allocated by the vendor** to manage your security program. Charges are typically calculated on a quarterly fee basis depending on the size and the complexity of the organization, the necessary skills and the culture.
- **Managed Policy Compliance.** In managed-policy-compliance-type agreements, expert security advisors **perform regularly scheduled audits** to ensure continued compliance with your established information security policy and controls and to identify any non-conformance. As an output of this regular process you receive a detailed report on the overall status of systems, areas of non-compliance, and guidance on how to return these systems to compliance. Trend reporting and analysis that helps you determine whether your security posture is improving or not, and why, is typically also included.
- **Managed Vulnerability Assessments.** Under these forms of service level agreements, **vendors provide a unique set of Vulnerability Assessment Services** that can be customized to target all organization's possible information entry points - the Internet, internal networks, applications, remote access, and wireless implementations. Based on business drivers, technical assets, and threat factors, vendors help clients determine the appropriate interval for recurring assessments and the optimal degree of probing depth and breadth.
- **Managed Operations Support.** Ongoing security operations support services provide resources to the client organizations in order to cover their **internal security operations** on a daily basis. Vendors typically offer different and modular levels of support from simple consulting/coaching for implementing security solutions and policies to engineering and technical implementation of security infrastructure. Ongoing security operations typically include tasks like server hardening, security configuration changes, application security patching, etc.
- **Emergency and Incident Response.** Emergency and Incident Response Services ensure support with expert engineers on your premises for emergency or crisis situations. Incident

Management and Response Services enable client organizations to **respond quickly and confidently to computer-related security incidents** - including system compromise, virus infection and denial of service attacks - helping you minimize downtime and lost revenue.

The security requirements of organizations that outsource the management and control of all or some of its information systems, networks and/or desk top environments should be addressed in service level agreements between the parties (SLA). At the very least, the following issues (controls) should be addressed by any SLA for outsourcing Information Security Management and Operations:

- A. Level of outsourcing and liability issues
- B. Compliance monitoring
- C. Management responsibilities
- D. Scope of work
- E. How legal requirements are to be met, e.g. data protection legislation
- F. What arrangements will be in place to ensure that all parties involved in the outsourcing, including subcontractors, are aware of their security responsibilities
- G. How the integrity and confidentiality of the organization’s business assets are to be maintained and tested
- H. What physical and logical controls will be used to restrict and limit the access to the organization’s sensitive business information to authorized users
- I. How the availability of services is to be maintained in the event of a disaster
- J. The right of audit
- K. Resources competency and Professional Certification
- L. Reporting Content, Frequency and Structure

Example A. (Risk Profile: High, Critical Asset: Application)

[Step 1] In this step analysis teams are occupied with the evaluation of the organization's current security practices compared to controls described on control cards. Analysis teams carefully read controls that apply to their profile (as depicted from the selected control cards - Phase 3, Step 3) and elicit detailed information about the organization's current security policies, procedures, and practices, thus providing a starting point for improvement.

The following Table is refers to Example A:

Asset	Control	Are we currently following the controls included in the control cards?
Asset Based Controls	2.1.3	No
	2.1.4	Partially
	2.1.6	No
	2.4.2	Partially
	2.5.1	No
	2.6.1	No
Organizational Controls	SP1	No
	SP3	No
	SP4	Yes
	SP5	No
	SP6	Partially

Table 25: Gap analysis list – Example A

[Step 2] In step 2 analysis teams read the controls (Annex A, B, C, D) and decide on the necessary actions.

Asset	Control	Action
Asset-Based Controls	2.1.3	The team decides to protect sensitive information by secure storage such as defined chains of custody, backups stored off-site, removable storage media, discard process for sensitive information or its storage media.
	2.1.4	The team decides to protect sensitive information by regularly verifying the integrity of the installed software base for the application.
	2.1.6	The team decides to develop a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.
	2.4.2	The teams decides to establish documented information-use policies and procedures for individual and group access to (A) establish the rules for granting the appropriate level of access, (B) establish an initial right of access, (C) modify the right of access, (D) terminate the right of access, and (F) periodically review and verify the rights of access.
	2.5.1	The team decides to select vulnerability evaluation tools, checklists, and scripts, keeping up to date with known vulnerability types and attack methods, reviewing sources of information on vulnerability announcements, security alerts, and notices, identifying infrastructure components to be evaluated, scheduling of vulnerability evaluations, interpreting and responding to the results, maintaining secure storage and disposition of vulnerability data.
	2.6.1	The team decides NOT to implement encryption of the transmitted data. Stored data are protected against confidentiality by means of an access control system.
	Organizational Controls	SP1
SP3		Security Management Function to be established. A security officer will be assigned.
SP4		The team also decides to develop a Generic Security Policy defining information ownership and responsibilities.
SP5		Collaborative Management procedures that concern the third party responsible for the maintenance of the application are decided.
SP6		Disaster Recovery Plan to be implemented and tested regularly.

Table 26: Action list – Example A

[Step 3] In step 3 for example A. analysis teams prioritize the activities and then focus on implementing the highest-priority activities. They decide high priority actions to be implemented within the next quarter, medium priority actions for the next six months and low priority ones to be implemented before the end of the coming year.

Now that you have identified specific action items for the action list, you need to assign responsibility for completing them as well as a completion date. Answer the following question for each action item on your list and record the results:

- Who will be responsible for each action item?
- By what date does the action item need to be addressed?
- What can management do to facilitate the completion of this action item?
- How much will it cost?
- How long will it take?
- Can we do it ourselves?
- Do we need external assistance?

The output of their plan is summarized in the table below:

Asset	Control	Responsible	External Assistance Required	Milestone	Priority
Asset Based Controls	2.1.3	Employee A	No	Mm / dd	High
	2.1.4	Employee A	Yes		Medium
	2.1.6	Employee A	Yes		High
	2.4.2	Employee A	Yes		Medium
	2.5.1	Employee A	No		Low
	2.6.1	Employee A	No		Medium
Organizational Controls	SP1	Employee B	No		Low
	SP3	Employee B	No		Medium
	SP4	Employee B	Yes		Medium
	SP5,	Employee B	No		High
	SP6	Employee B	No		High

Table 27: Implementation plan – Example A

Example B. (Risk Profile: Medium, Critical Asset: System)

[Step 1] In this step analysis teams are occupied with the evaluation of the organization's current security practices compared to controls described on control cards. Analysis teams carefully read controls that apply to their profile (as depicted from the selected control cards - Phase 3, Step 3), and elicit detailed information about organization's current security policies, procedures, and practices, thus providing a starting point for improvement.

The following Table refers to Example B:

Asset	Control	Are we currently following the controls included in the control cards?
Asset-Based Controls	2.1.6	No
	2.1.7	Yes
Organizational Controls	SP1	Partiallv
	SP4	Yes
	SP1.1	No
	SP4.1	Yes

Table 28: Gap analysis list – Example B

[Step 2] In step 2 analysis teams read the controls (Appendix A, B, C, D) and decide on the necessary actions.

Asset	Control	Actions
Asset-Based Controls	2.1.6	The team decides to develop a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.
	2.1.7	The team decides to inform and educate all staff in order to understand and be able to carry out their responsibilities under the backup plans.
Organizational Controls	SP1	The team decides to launch a basic awareness campaign by educating all lawyers about the risks involved in using email, internet etc.
	SP4	The team also decides to develop a Generic Security Policy defining information ownership and responsibilities.
	SP1.1	Included in SP1.
	SP4.1	Included in SP4.

Table 29: Action list – Example B

[Step 3] In step 3 of example B, analysis teams prioritize the activities and then focus on implementing the highest-priority activities. They decide high priority actions to be implemented within the next quarter, medium priority actions for the next six months and low priority ones to be implemented before the end of the coming year.

Now that you have identified specific action items for the action list, you need to assign responsibility for completing them as well as a completion date. Answer the following question for each action item on your list and record the results:

- Who will be responsible for each action item?
- By what date does the action item need to be addressed?
- What can management do to facilitate the completion of this action item?
- How much will it cost?
- How long will it take?
- Can we do it ourselves?
- Do we need external assistance?

The output of their plan is summarized in the table below:

Asset	Control	Responsible	External Assistance Required	Milestone	Priority
Asset Based Controls	2.1.6	Employee A	No	Mm/dd	High
	2.1.7	Employee A	No		High
Organizational Controls	SP1	Employee A	No		Medium
	SP4	Employee A	No		Low
	SP1.1	Employee A	No		Low
	SP4.1	Employee A	No		High

Table 30: Implementation plan – Example B

Annex A. Organizational Control Cards

Security Awareness and Training (SP1)

SP1 Security Awareness and Training Control Card includes controls that require staff members to understand their security roles and responsibilities. Security awareness, training, and periodic reminders should be provided for all personnel. Staff understanding and roles should be clearly documented and conformance should be periodically verified.

Security Strategy (SP2)

SP2 Security Strategy Control Card includes controls that require the organization's business strategies to routinely incorporate security considerations. Equally, security strategies and policies must take into consideration the organization's business strategies and goals.

Security strategies, goals, and objectives should be documented and are routinely reviewed, updated, and communicated to the organization.

Security Management (SP3)

SP3 Security Management Control Card includes controls that require a security management process to be implemented and enforced. The process must continuously assess the required levels of information security and define appropriate and cost/risk balanced controls that should be applied and documented.

Security Policies and Regulations (SP4)

SP4 The Control Card requires an organization to have a comprehensive set of documented, current information security policies that are periodically reviewed and updated.

Collaborative Security Management (SP5)

SP5 Collaborative Security Management Control Cards includes security controls that enforce documented, monitored, and enforced procedures for protecting the organization's information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners).

Contingency Planning/Disaster Recovery (SP6)

SP6 Continuity Planning/Disaster Recovery Control Cards incorporates security controls in order to assure continuous business operations in case of a disaster or unavailability of the information. Key elements of the control card are:

- business continuity or emergency operation plans,
- disaster recovery plan(s) and
- contingency plan(s) for responding to emergencies.

Annex B. Asset Control Cards³

Asset Based Control Card ID						CC-1A				
Risk Profile						High				
Asset Category						Application				
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality		2.1.3			2.4.2	2.5.1	2.6.1			
Integrity		2.1.4			2.4.2	2.5.1	2.6.1			
Availability		2.1.6								

Application-based confidentiality controls for a high risk organizational profile typically address security requirements on an application, system, network and people level to safeguard critical information lifecycle. Controls are selected mainly to address information assets from disclosure to unauthorized entities whether external or internal to the environment.

Essential Controls for the protection of confidentiality in critical assets are the following:

OP2.4.2 Control requires documented information-use policies and procedures for individual and group access to (A) establish the rules for granting the appropriate level of access, (B) establish an initial right of access, (C) modify the right of access, (D) terminate the right of access, and (F) periodically review and verify the rights of access.

OP2.5.1 Control requires that there is a documented set of procedures for managing vulnerabilities, including selecting vulnerability evaluation tools, checklists, and scripts, keeping up to date with known vulnerability types and attack methods, reviewing sources of information on vulnerability announcements, security alerts, and notices, identifying infrastructure components to be evaluated, scheduling of vulnerability evaluations, interpreting and responding to the results, maintaining secure storage and disposition of vulnerability data.

OP2.1.3 Control requires that sensitive information is protected by secure storage such as defined chains of custody, backups stored off site, removable storage media, discard process for sensitive information or its storage media.

OP2.1.4 Control requires that the integrity of installed software is regularly verified.

OP2.1.6 Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission including data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, and encryption for all Internet-based transmission.

³ The assignment of controls to the asset control cards throughout this annex has been performed in a way that a good degree of protection can be achieved. In case of assets with very high security requirements, additional controls might be considered. Nevertheless, by using these assets control cards a good average protection can be achieved which seems to be appropriate for the majority of SMEs. In the middle term, ENISA plans to validate the assumptions made herein by means of pilot projects.

Asset Based Control Card ID						CC-1S				
Risk Profile						High				
Asset Category						System				
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality		2.1.3 2.1.4 2.1.5 2.1.9			2.4.1 2.4.6		2.6.1			
Integrity		2.1.4 2.1.5 2.1.8 2.1.9 2.1.10			2.4.1 2.4.3 2.4.6			2.7.1 2.7.2		
Availability		2.1.6 2.1.7 2.1.9			2.4.6					

A high risk profile implies threats that occur in system unavailability leading to unavailability of business service. Systems are unable to host business applications or may cause loss of critical information. Threat source can be the instability of the system due to mechanical malfunction or improper installation and use.

System based confidentiality controls for high risk organizational profiles involve methods that ensure proper configuration and functionality of the system. System based integrity controls for a high risk organizational profile typically address security requirements on an application, system, network and people level to ensure stability of the system and critical information integrity. Constant Availability of the system is a requirement for business continuity. Controls are selected to address mainly information assets from disclosure to unauthorized entities either external or internal to the environment.

Essential Controls for the safeguard of integrity in critical assets are the following:

OP2.1.3 Control requires that sensitive information is protected by secure storage, such as defined chains of custody, backups stored off site, removable storage media and discard process for sensitive information or its storage media.

OP2.1.4 Control requires that the integrity of installed software is regularly verified.

OP2.1.5 Control requires that all systems are up to date with respect to revisions, patches, and recommendations in security advisories.

OP2.1.6 Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP 2.1.7 Control requires that all staff understand and are able to carry out their responsibilities under the backup plans.

OP2.1.8 Control requires that changes to IT hardware and software are planned, controlled, and documented.

OP2.1.9 Control requires that IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. Unique user identification is required for all information system users, including third-party users. Default accounts and default passwords have been removed from systems.

OP2.1.10 Control requires that only necessary services are running on systems – all unnecessary services have been removed.

OP2.2.1 Control requires that new security tools, procedures, and mechanisms are routinely reviewed for applicability in meeting the organization's security strategies.

OP2.2.2 Control requires that tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced. Examples are: data integrity checkers, cryptographic tools, vulnerability scanners, password quality-checking tools, virus scanners, process management tools, intrusion detection systems, secure remote administrations, network service tools, traffic analyzers, incident response tools, forensic tools for data analysis.

OP2.3.1 Control requires that system and network monitoring and auditing tools are routinely used by the organization. Activity is monitored by the IT staff, System and network activity is logged/recorded, Logs are reviewed on a regular basis, Unusual activity is dealt with according to the appropriate policy or procedure, Tools are periodically reviewed and updated.

OP2.4.1 Control requires that appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, system utilities, program source code, sensitive systems, specific applications and services, network connections within the organization, network connections from outside the organization.

OP2.4.3 Control requires that access control methods/mechanisms restrict access to resources according to the access rights determined by policies and procedures.

OP2.4.6 Control requires that authentication mechanisms are used to protect availability, integrity, and confidentiality of sensitive information. Examples are the digital signatures and biometrics.

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission, including: Data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, encryption for all Internet-based transmission.

OP2.7.1 Control requires that System architecture and design for new and revised systems include considerations for security strategies, policies, and procedures, history of security compromises and results of security risk assessments.

OP2.7.2 Control requires that the organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.

Asset Based Control Card ID						CC-1N				
Risk Profile						High				
Asset Category						Network				
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality					2.4.6	2.5.3	2.6.1			
Integrity	1.1.4	2.1.1 2.1.10			2.4.1 2.4.3 2.4.4 2.4.6	2.5.3		2.7.2		
Availability	1.1.4				2.4.6					

A high risk profile implies threats that occur in network vulnerabilities that can lead to external attacks or internal unauthorised access to certain network areas of high interest or risk.

Lack of Network security has an immediate and direct effect in applications running and information flow.

Network-based confidentiality controls for a high risk organizational profile should protect critical and internal information from potential loss or misuse. Furthermore, information stored in network must be available and easily accessed and separated according to criticality level.

Essential Controls for the safeguard of confidentiality, integrity and availability in a network are the following:

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission including data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, encryption for all Internet-based transmission.

OP2.4.6 Control requires that authentication mechanisms are used to protect availability, integrity, and confidentiality of sensitive information. Examples are digital signatures and biometrics.

OP2.7.2 Control requires that the organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.

OP2.1.1 Control requires that there are documented security plan(s) for safeguarding the systems and networks.

OP2.4.1 Control requires that appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, system utilities, program source code, sensitive systems, specific applications and services, network connections within the organization, network connections from outside the organization.

OP2.4.3 Control requires that access control methods/mechanisms restrict access to resources according to the access rights determined by policies and procedures.

OP2.1.10 Control requires that only necessary services are running on systems – all unnecessary services have been removed.

OP 2.5.3 Control requires that technology vulnerability assessments are performed on a periodic basis, and vulnerabilities are addressed when they are identified.

OP1.1.4 Control requires that there are documented policies and procedures for managing visitors, including sign in, escort, access logs, reception and hosting.

OP2.4.6 Control requires that authentication mechanisms are used to protect availability, integrity, and confidentiality of sensitive information. Examples are digital signatures and biometrics.

Asset Based Control Card ID						CC-1P				
Risk Profile						High				
Asset Category						People				
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality										3.2.1 3.2.2 3.2.3
Integrity	1.1.4 1.3.2									3.2.1 3.2.2 3.2.3
Availability										

A high risk profile implies threats that occur in management of people and in human resources in general. The level of staff commitment on using the appropriate security controls on network resources determines level of protection that can be achieved.

The manipulation of information and the reuse of older records with high value for the organization is a critical aspect. Internal or confidential information from staff should be treated respectfully. Monitoring of staff policies on such procedures ensures the confidentiality, integrity and availability of information.

Essential Controls for securing the confidentiality, integrity and availability of information in combination with a critical asset like people are the following:

OP3.2.1 Control requires that staff members follow good security practice: securing information for which they are responsible; not divulging sensitive information to others (resistance to social engineering); having adequate ability to use information technology hardware and software; using good password practices; understanding and following security policies and regulations; recognizing and reporting incidents.

OP3.2.2 Control requires that all staff at all levels of responsibility implement their assigned roles and responsibility for information security.

OP3.2.3 Control requires that there are documented procedures for authorizing and overseeing those who work with sensitive information or who work in locations where such information is stored. This includes employees, contractors, partners, collaborators, and personnel from third-party organizations, systems maintenance personnel, or facilities maintenance personnel.

OP1.1.4 Control requires there are documented policies and procedures for managing visitors, including signing in, escort, access logs, reception and hosting.

OP1.3.2 Control requires that an individual's or group's actions -- with respect to all physically controlled media -- can be accounted for.

Asset Based Control Card ID						CC-2A				
Risk Profile						Medium				
Asset Category						Application				
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality					2.4.2		2.6.1			
Integrity					2.4.2					
Availability		2.1.6 2.1.7								

A medium risk profile implies storage and processing of internal or moderate-value proprietary information that would typically incur a generic threat profile involving external malicious entities intending to violate or compromise specific and moderate-value information confidentiality. Application-based confidentiality controls for a medium risk organizational profile typically address security requirements on an application, system, network and people level to safeguard critical information life-cycle. Application-based integrity controls for a medium risk organizational profile define the level of accuracy of information of an application while availability refers to the level of accessibility.

Essential Controls for the protection of confidentiality, integrity and availability in applications are the following:

OP2.4.2 Control requires that there are documented information-use policies and procedures for individual and group access to establish the rules for granting the appropriate level of access, establish an initial right of access, modify the right of access, terminate the right of access and periodically review and verify the rights of access.

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission including data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, encryption for all Internet-based transmission.

OP2.1.6 Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP2.1.7 Control requires all staff understand and is able to carry out their responsibilities under the backup plans.

Asset Based Control Card ID						CC-2S				
Risk Profile						Medium				
Asset Category						System				
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality		2.1.6 2.1.7			2.4.1					
Integrity		2.1.9			2.4.1					
Availability		2.1.6 2.1.7								

A medium risk profile implies moderate level threats that occur in system instabilities leading to unavailability of business service for a short period of time. Systems are unable to support applications or functions properly.

System based controls for medium risk organizational profiles involve methods that ensure proper configuration and functionality of the system for appropriate access.

Essential Control for the protection of confidentiality, integrity and availability in systems is the following:

OP2.4.1 Control requires that appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, system utilities, program source code, sensitive systems, specific applications and services, network connections within the organization, network connections from outside the organization.

OP2.1.6 Control requires that there is a documented data backup plan which is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP2.1.7 Control requires that all staff understand and is able to carry out their responsibilities under the backup plans.

OP2.1.9 Control requires that IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. Unique user identification is required for all information system users, including third-party users. Default accounts and default passwords have been removed from systems.

Asset Based Control Card ID		CC-2N								
Risk Profile		Medium								
Asset Category		Network								
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management (OP2.5)	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality							2.6.1			
Integrity					2.4.3					
Availability		2.1.5								

A medium risk profile implies threats that occur in network vulnerabilities due to wrong or poorly-implemented network architecture that can lead to external attacks or internal unauthorised access to certain network areas of moderate interest and of medium organization value.

Lack of Network security has immediate and direct effect on applications running and information flow. The risk is considered medium when the system does not permit access to critical components that could directly affect organization reputation or financial health.

Essential Controls for the safeguard of confidentiality, integrity and availability in a network is the following:

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission including data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, encryption for all Internet-based transmission.

OP2.4.3 Control requires that access control methods/mechanisms restrict access to resources according to the access rights determined by policies and procedures.

OP2.1.5 Control requires that all systems are up to date with respect to revisions, patches, and recommendations in security advisories.

Asset Based Control Card ID										CC-2P
Risk Profile										Medium
Asset Category										People
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management (OP2.5)	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality										3.2.1 3.2.2
Integrity										3.2.1 3.2.2
Availability	1.1.4									

A medium risk profile implies threats that occur in management of human resources of medium size enterprises when current security practices could lead to business problems of moderate impact.

Incidents from improper use of passwords or access rights can lead to information leakage. A medium level of confidentiality of information determines the risk level or the money loss for the organization.

Monitoring of staff policies on such procedures ensures the confidentiality, integrity and availability of information.

Essential Controls for securing the confidentiality, integrity and availability of information in combination with a critical asset like people are the following:

OP3.2.1 Control requires that staff members follow good security practice: securing information for which they are responsible; not divulging sensitive information to others (resistance to social engineering); having adequate ability to use information technology hardware and software; using good password practices; understanding and following security policies and regulations; recognizing and reporting incidents.

OP3.2.2 Control requires that all staff at all levels of responsibility implement their assigned roles and responsibility for information security.

OP1.1.4 Control requires there are documented policies and procedures for managing visitors, including signing in, escort, access logs, reception and hosting.

Asset Based Control Card ID						CC-3A				
Risk Profile						Low				
Asset Category						Application				
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management (OP2.5)	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality					2.4.2					
Integrity										
Availability										

A low risk profile implies storage and processing of public or internal information but with no critical level of importance that would entail more than a minimal loss of money. Organization reputation is not at stake. However, controls that would prevent even that kind of information leakage and that can secure the information life-cycle should be applied.

Furthermore, even if there is no confidentiality impact, information integrity and availability to every authorized user must be secured.

An essential control for confidentiality in the application asset is the following:

OP2.4.2 Control requires that there are documented information-use policies and procedures for individual and group access to establish the rules for granting the appropriate level of access, establish an initial right of access, modify the right of access, terminate the right of access and periodically review and verify the rights of access.

Asset Based Control Card ID		CC-3S								
Risk Profile		Low								
Asset Category		System								
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management (OP2.5)	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality		2.1.9			2.4.1					
Integrity					2.4.1					
Availability		2.1.6								

A low risk profile implies minimum level threats that entail potential system instabilities leading to unavailability of business service for a short period of time.

System based controls for minimum risk organizational profiles involve methods that ensure proper configuration and functionality of the system for appropriate access.

Impact of system unavailability does not affect organization reputation as information is neither private nor critical to the organization.

Unavailability of system does not affect quality of service or product.

Essential Control for the protection of confidentiality and availability in systems are the following:

OP2.4.1 Control requires that appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, system utilities, program source code, sensitive systems, specific applications and services, network connections within the organization, network connections from outside the organization.

OP2.1.6 Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP2.1.9 Control requires that IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. Unique user identification is required for all information system users, including third-party users. Default accounts and default passwords have been removed from systems.

Asset Based Control Card ID							CC-3N			
Risk Profile							Low			
Asset Category							Network			
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management (OP2.5)	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality							2.6.1			
Integrity										
Availability										

A low risk profile implies threats that occur in minor network vulnerabilities or unavailability of information due to wrong or poorly-implemented network architecture. The impact however could be considered insignificant since information is not of great interest nor highly confidential for the organization. Therefore potential financial loss for the organization is small.

Nevertheless, security controls that address encrypted transferred information are recommended.

Essential Controls for the safeguard of confidentiality in a network is the following:

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information while in storage and during transmission including data encryption during transmission, data encryption when writing to disk, use of public key infrastructure, virtual private network technology, encryption for all Internet-based transmission.

Asset Based Control Card ID		CC-3P								
Risk Profile		Low								
Asset Category		People								
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management (OP2.5)	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality										
Integrity										
Availability	1.1.4									

A low risk profile implies potential threats with low impact on management of human resources when current security practices could lead to business problems but with a minimum risk for the organization.

Criticality of information is not of a high level. Thus, impact in financial terms is low and money loss can be considered as insignificant.

However, monitoring of staff policies even on such procedures further ensures the confidentiality, integrity and availability of information.

Essential Control for securing the confidentiality, integrity and availability of information in combination with people is the following:

OP1.1.4 Control requires that there are documented policies and procedures for managing visitors, including signing in, escort, access logs, reception and hosting.

Annex C. Organizational Controls

Security Awareness and Training (SP1)	
SP1.1	Staff members understand their security roles and responsibilities. This is documented and verified.
SP1.2	There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified.
SP1.3	<p>Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified. Training includes these topics:</p> <ul style="list-style-type: none"> · security strategies, goals, and objectives · security regulations, polices, and procedures · policies and procedures for working with third parties · contingency and disaster recovery plans · physical security requirements · users' perspective on <ul style="list-style-type: none"> - system and network management - system administration tools - monitoring and auditing for physical and information technology security - authentication and authorization - vulnerability management - encryption - architecture and design · incident management · general staff practices <ul style="list-style-type: none"> - enforcement, sanctions, and disciplinary actions for security violations - how to properly access sensitive information or work in areas where sensitive information is accessible · termination policies and procedures relative to security

Security Strategy (SP2)	
SP2.1	The organization's business strategies routinely incorporate security considerations.
SP2.2	Security strategies and policies take into consideration the organization's business strategies and goals.
SP2.3	Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization.

Security Management (SP3)	
SP3.1	Management allocates sufficient funds and resources to information security activities.
SP3.2	Security roles and responsibilities are defined for all staff in the organization.
SP3.3	The organization's hiring and termination practices for staff take information security issues into account.
SP3.4	The required levels of information security and how they are applied to individuals and groups are documented and enforced.
SP3.5	The organization manages information security risks, including
	· assessing risks to information security both periodically and in response to major changes in technology, internal/external threats, or the organization's systems and operations
	· taking steps to mitigate risks to an acceptable level
	· maintaining an acceptable level of risk
SP3.6	Management receives and acts upon routine reports summarizing the results of
	· review of system logs
	· review of audit trails
	· technology vulnerability assessments
	· security incidents and the responses to them
	· risk assessments
	· physical security reviews
· security improvement plans and recommendations	

Security Policies and Regulations (SP4)	
SP4.1	<p>The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. These policies address key security topic areas, including</p> <ul style="list-style-type: none"> · security strategy and management · security risk management · physical security · system and network management · system administration tools · monitoring and auditing · authentication and authorization · vulnerability management · encryption · security architecture and design · incident management · staff security practices · applicable laws and regulations · awareness and training · collaborative information security · contingency planning and disaster recovery
SP4.2	<p>There is a documented process for management of security policies, including</p> <ul style="list-style-type: none"> · creation · administration (including periodic reviews and updates) · communication
SP4.3	<p>The organization has a documented process for periodic evaluation (technical and non-technical) of compliance with information security policies, applicable laws and regulations, and insurance requirements.</p>
SP4.4	<p>The organization has a documented process to ensure compliance with information security policies, applicable laws and regulations, and insurance requirements.</p>
SP4.5	<p>The organization uniformly enforces its security policies.</p>
SP4.6	<p>Testing and revision of security policies and procedures is restricted to authorized personnel.</p>

Collaborative Security Management (SP5)	
SP5.1	The organization has documented, monitored, and enforced procedures for protecting its information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners).
SP5.2	The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements.
SP5.3	The organization documents, monitors, and enforces protection strategies for information belonging to external organizations that is accessed from its own infrastructure components or is used by its own personnel.
SP5.4	The organization provides and verifies awareness and training on applicable external organizations' security policies and procedures for personnel who are involved with those external organizations.
SP5.5	There are documented procedures for terminated external personnel specifying appropriate security measures for ending their access. These procedures are communicated and coordinated with the external organization.

Contingency Planning/Disaster Recovery (SP6)	
SP6.1	An analysis of operations, applications, and data criticality has been performed.
SP6.2	The organization has documented
	· business continuity or emergency operation plans
	· disaster recovery plan(s)
	· contingency plan(s) for responding to emergencies
SP6.3	The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls.
SP6.4	The contingency, disaster recovery, and business continuity plans are periodically reviewed, tested, and revised.
SP6.5	All staff are
	· aware of the contingency, disaster recovery, and business continuity plans
	· understand and are able to carry out their responsibilities

Annex D. Asset Based Controls

Physical Security (OP1)	
Physical Security Plans and Procedures (OP1.1)	
OP1.1.1	There are documented facility security plan(s) for safeguarding the premises, buildings, and any restricted areas.
OP1.1.2	These plans are periodically reviewed, tested, and updated.
OP1.1.3	Physical security procedures and mechanisms are routinely tested and revised.
OP1.1.4	There are documented policies and procedures for managing visitors, including
	· sign in
	· escort
	· access logs
OP1.1.5	There are documented policies and procedures for physical control of hardware and software, including
	· workstations, laptops, modems, wireless components, and all other components used to access information
	· access, storage, and retrieval of data backups
	· storage of sensitive information on physical and electronic media
	· disposal of sensitive information or the media on which it is stored
	· reuse and recycling of paper and electronic media
Physical Access Control (OP1.2)	
OP1.2.1	There are documented policies and procedures for individual and group access covering
	· the rules for granting the appropriate level of physical access
	· the rules for setting an initial right of access
	· modifying the right of access
	· terminating the right of access
OP1.2.2	There are documented policies, procedures, and mechanisms for controlling physical access to defined entities. This includes
	· work areas
	· hardware (computers, communication devices, etc.) and software media
OP1.2.3	There are documented procedures for verifying access authorization prior to granting physical access.
OP1.2.4	Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access.
Monitoring and Auditing Physical Security (OP1.3)	
OP1.3.1	Maintenance records are kept to document the repairs and modifications of a facility's physical components.
OP1.3.2	An individual's or group's actions, with respect to all physically controlled media, can be accounted for.
OP1.3.3	Audit and monitoring records are routinely examined for anomalies, and corrective action is taken as needed.

Information Technology Security (OP2)	
System and Network Management (OP2.1)	
OP2.1.1	There are documented security plan(s) for safeguarding the systems and networks.
OP2.1.2	Security plan(s) are periodically reviewed, tested, and updated.
OP2.1.3	Sensitive information is protected by secure storage, such as
	· defined chains of custody
	· backups stored off site
	· removable storage media
OP2.1.4	The integrity of installed software is regularly verified.
OP2.1.5	All systems are up to date with respect to revisions, patches, and recommendations in security advisories.
OP2.1.6	There is a documented data backup plan that
	· is routinely updated
	· is periodically tested
	· calls for regularly scheduled backups of both software and data
OP2.1.7	All staff understands and is able to carry out their responsibilities under the backup plans.
OP2.1.8	Changes to IT hardware and software are planned, controlled, and documented.
OP2.1.9	IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges.
	· Unique user identification is required for all information system users, including third-party users.
OP2.1.10	Only necessary services are running on systems – all unnecessary services have been removed.
System Administration Tools (OP2.2)	
OP2.2.1	New security tools, procedures, and mechanisms are routinely reviewed for applicability in meeting the organization's security strategies.
OP2.2.2	Tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced. Examples are
	· data integrity checkers
	· cryptographic tools
	· vulnerability scanners
	· password quality-checking tools
	· virus scanners
	· process management tools
	· intrusion detection systems
	· secure remote administrations
	· network service tools
	· traffic analyzers
	· incident response tools
· forensic tools for data analysis	

Monitoring and Auditing IT Security (OP2.3)	
OP2.3.1	System and network monitoring and auditing tools are routinely used by the organization.
	· Activity is monitored by the IT staff.
	· System and network activity is logged/recorded.
	· Logs are reviewed on a regular basis.
	· Unusual activity is dealt with according to the appropriate policy or procedure.
OP2.3.2	Firewall and other security components are periodically audited for compliance with policy.
Authentication and Authorization (OP2.4)	
OP2.4.1	Appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to
	· information
	· systems utilities
	· program source code
	· sensitive systems
	· specific applications and services
	· network connections within the organization
OP2.4.2	There are documented information-use policies and procedures for individual and group access to
	· establish the rules for granting the appropriate level of access
	· establish an initial right of access
	· modify the right of access
	· terminate the right of access
OP2.4.3	Access control methods/mechanisms restrict access to resources according to the access rights determined by policies and procedures.
OP2.4.4	Access control methods/mechanisms are periodically reviewed and verified.
OP2.4.5	Methods or mechanisms are provided to ensure that sensitive information has not been accessed, altered, or destroyed in an unauthorized manner.
OP2.4.6	Authentication mechanisms are used to protect availability, integrity, and confidentiality of sensitive information. Examples are
	· digital signatures · biometrics
Vulnerability Management (OP2.5)	
OP2.5.1	There is a documented set of procedures for managing vulnerabilities, including
	· selecting vulnerability evaluation tools, checklists, and scripts
	· keeping up to date with known vulnerability types and attack methods
	· reviewing sources of information on vulnerability announcements, security alerts, and notices
	· identifying infrastructure components to be evaluated
	· scheduling of vulnerability evaluations

	<ul style="list-style-type: none"> interpreting and responding to the results maintaining secure storage and disposition of vulnerability data 	
OP2.5.2	Vulnerability management procedures are followed and are periodically reviewed and updated.	
OP2.5.3	Technology vulnerability assessments are performed on a periodic basis, and vulnerabilities are addressed when they are identified.	
Encryption (OP2.6)		
	Appropriate security controls are used to protect sensitive information while in storage and during transmission, including	
OP2.6.1	<ul style="list-style-type: none"> data encryption during transmission data encryption when writing to disk use of public key infrastructure virtual private network technology encryption for all Internet-based transmission 	
	OP2.6.2	Encrypted protocols are used when remotely managing systems, routers, and firewalls.
	OP2.6.3	Encryption controls and protocols are routinely reviewed, verified, and revised.
	Security Architecture and Design (OP2.7)	
		System architecture and design for new and revised systems include considerations for
OP2.7.1	<ul style="list-style-type: none"> security strategies, policies, and procedures history of security compromises results of security risk assessments 	
	OP2.7.2	The organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.

Staff Security (OP3)		
Incident Management (OP3.1)		
	Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations, including	
OP3.1.1	<ul style="list-style-type: none"> network-based incidents physical access incidents social engineering incidents 	
	OP3.1.2	Incident management procedures are periodically tested, verified, and updated.
	OP3.1.3	There are documented policies and procedures for working with law enforcement agencies.
General Staff Practices (OP3.2)		
	Staff members follow good security practice, such as	
OP3.2.1	<ul style="list-style-type: none"> securing information for which they are responsible not divulging sensitive information to others (resistance to social engineering) having adequate ability to use information technology hardware and software using good password practices understanding and following security policies and regulations recognizing and reporting incidents 	

OP3.2.2	All staff at all levels of responsibility implements their assigned roles and responsibility for information security.
	There are documented procedures for authorizing and overseeing those who work with sensitive information or who work in locations where the information resides. This includes
OP3.2.3	<ul style="list-style-type: none"> · employees
	<ul style="list-style-type: none"> · contractors, partners, collaborators, and personnel from third-party organizations
	<ul style="list-style-type: none"> · systems maintenance personnel
	<ul style="list-style-type: none"> · facilities maintenance personnel

Annex E. Simple advice⁴

IMPORTANT SECURITY TIPS FOR SMALL AND MEDIUM-SIZED ENTERPRISES

The following constitute the essentials of defence for your company

- Carrying out basic screening checks on all your employees and contractors (e.g. based on references or recommendations)
- Knowing and documenting the valuable assets of your organisation
- Having short, efficient and clearly documented security policies and procedures
- Carrying out basic security awareness training with your employees
- Implementing patches for software vulnerabilities automatically or as soon as possible, after checking their functionality
- Knowing who is accessing your systems and why
- Using strong passwords and changing them regularly
- Making sure that you are implementing anti-virus functions for all your computer and mobile devices and that your anti-virus system is updated automatically
- Use different anti-virus products for your server and your client computers
- Using a content filtering system to guard against spam, phishing, malicious and forbidden content
- Using firewall, especially if you have broadband internet access
- Using an "all-in-one" network defence system with a small network

Passwords

These are the door keys to your electronic information. Anybody can read information that is not password-protected. If you choose weak passwords, it is quite possible for somebody to guess them or to de-cipher them. Here are some tips for strong passwords.

- Open the dictionary at a random page and select a long word (say 4 syllables). Use this word but insert the page number in the middle of it. For example if <multifarious> is on page 345 of your dictionary, your password is <multi345furious>. (If you forget the password, you should be able to remember which page you selected.)
- Choose a "pass phrase" that means something to you. For example» my zebra is called Spot and is 9 years old". This can be turned in to a password <mzicS&i9yo>. This is a very strong password because it uses letters, numbers and special characters. Breaking this will be extremely difficult.

⁴ The purpose of the material presented in this annex is to give simple guidance to users on basic security matters. This material has been compiled from the sources [1], [6] and [10] mentioned in the bibliography.

Must-do's with passwords are:

- use at least 8 characters in the password
- Make sure you change passwords regularly, e.g. every month.
- If an employee leaves, change their old password immediately.
- use one password for one application - never use the same password for everything.

On the other hand, there are some things you must never do with passwords.

These include:

- Never, ever write down a password!
- never use your name, your partner's name, the kids names, the car registration, birthdays or anything else about you or your family that is widely known or can easily be worked out with a bit of "social engineering"
- never use special codes that apply to you, e.g. your phone number, your NI number, the licence number of the software, all of which could be worked out by someone
- never use all the same numbers or letters, e.g. <11111111>, in a password and never use the password <password> because that's the first one a hacker will try
- never share your password with others
- never use a default password provided with a piece of software - change it
- Never use any "Remember Password" functions on a computer because passwords stored in this way are easily recoverable with little skill needed.

In short, treat your password with care. Choose a strong one, change it regularly and take good care of it.

Virus, Worms and Trojans

Purist will say these are all different but from a business perspective you can treat them as the same. The critical point is that all of them can and do cause damage to computers and the information stored on them. However, it is really simple to avoid them. Use anti-virus software. Any anti-virus software will do because they all work in more or less the same way and do the same sort of job. The most important thing is simply to use one.

What most people don't appreciate is that anti-virus software must be kept up to date. This means daily - yes, daily - updates because the people who write this software release new versions every day.

If you don't install the software and keep it up-to-date, you are 100% guaranteed to catch a virus sooner or later.

Whatever antivirus software you use, you should install it to check any new data automatically. This way, if you get new data on a floppy disk, a CD or over the Internet, it will be checked for viruses before they can do any damage.

A golden rule is that any virus infected files or data should be destroyed. Some anti virus software will claim to disinfect files but this is never guaranteed. The safest bet is to destroy the file with the virus. If it is email, destroy it without opening it every time!

Spam

You may think this is just a nuisance but unfortunately it has its dangers as well. Spam can be:

- a front for fraud
- poisonous chain email
- contain hidden code which will alter your computer settings (e.g. direct you to a porn site)
- Contain hidden code which turns your computer into a spam relay (i.e. a large quantity of spam is sent from your computer all round the world) thereby sending all your customers' addresses all around the world and with a new copy of the span/worm/Trojan attached to it!

In the case of hidden code, this will most likely fall in to the 'Trojan' category and may will be picked up by your anti-virus software. However, there are some rules that you need to follow with spam email and if you do you will minimise any risks.

- If the email is obviously of no value, nor of any relevance to you or your business, is semi-literate, etc. just delete it without opening it.
- Never respond to spam email. Your email address has been picked up in some way and the spammers do not know whether you actually exist.
- If you reply, you will be confirming your existence and you will get much more of the same.
- Don't click on any "click here to remove your name from our mailing list" button on the email. It's normally a trick. You will not be removed you will just be confirming you exist.
- Don't give out your email address except to people you can trust.
- This is very difficult when running a business because you will want your email address to be widely available. Consider having two email addresses; one publicly available and one for personal use which is carefully controlled.
- If an Internet site asks for your email address, do a quick risk assessment. Is it a legitimate organisation that has an established reputation? Is it somebody you have never heard of before and doesn't quote a physical business address on their web site? Remember that crooks pose as legitimate businesses.
- Internet sites that promise to remove you from spam email lists generally do not do so. Never use them.

Spam blocking is a possibility. Specialist blocking software is available but may be too expensive for small businesses. It is probably worthwhile asking your Internet Service Provide (ISP) if they can - for a small extra fee - provide spam blocking using their own facilities. However, a word of caution here: Spam blocking is as much an art as a science. You can easily block legitimate email if the anti-spam criteria are set too high.

N.B. If you get an email which directly threatens your business in any way, e.g. threats of blackmail, get in touch with the Police in your area and do so immediately. You will be referred quickly to a team which is trained to handle electronic threats. This very likely will not happen to you, but just in case ...

Spyware

These are small programs that are inserted in to the computer system to covertly gather information about the user/business without them being aware. Mostly this is for

advertising purposes but it can also gather information about e-mail addresses and even passwords and credit card details.

Recently there have been official warnings about spyware being used to gather commercially sensitive information, e.g. contract details.

Spyware is not a good idea and the careful user tries to restrict it or remove it completely. There are two good packages available from the Internet and which will remove spyware. They are both free for personal use but businesses are expected to buy them. They are:

- Lavasoft's <Ad-aware>
- Spybot

It is recommended that you download both these packages and run them at least once a week. You will be surprised at what they find. (And don't forget, they need to be kept up-to-date as well!)

Firewalls

These take their name from the physical barriers constructed in buildings to prevent the spread of fire. In computer terms, a firewall is something that acts as a barrier to prevent unauthorised access to/from a private computer system. Think of it as a sort of security door and burglar alarm for computers. It helps to mitigate all those intentional threats outlined earlier. A firewall is now considered essential if you have one or more computers connected to the Internet.

The firewall is either a piece of software or it might be a hardware item. To protect large computer systems, it might be a combination of software and hardware.

The main point is that a firewall will check all data coming into and even out of the computer to make sure it is legitimate. To put it in a nutshell: a firewall is your best defence against the hacker. To take a real life case, a firewall could stop your computer being taken over by a third party and set up as a spam email relay. It's worth remembering that when you connect your computer to the Internet, you are opening 65,536 "doors" - or technically "ports" - through which data can enter your computer. What you really want to do is have the necessary ports open only for you to send or receive data and remain closed the rest of the time.

This is a very complex area of computing and this is not the place to expound on its principles and practices, which are the subject of doctoral theses. Fortunately, software firewalls are now inexpensive, simple to operate, and readily available.

If you have one computer, buy a software firewall. It is easy to install. You just accept its default settings. If you have two or more computers connected to the Internet, a hardware firewall might be a better investment and can be installed between all of your computers and the cable that goes out to the Internet. Hardware firewalls are more complex, and it is preferable to have an expert install and configure it. A professional will make sure your firewall is not so secure that you can't actually connect to the Internet.

(Businesses with one or two computers could buy combined firewall and anti-virus software in one package. This has economic and technical advantages for the small business.)

Patches

Patches are little known but are very important and are linked to viruses and hacking. All software has problems and defects. In most cases, the defects are so minor that they can be ignored and will probably not have any impact on the business. Some defects are too important to ignore.

All software producers provide patches - i.e. software updates designed to remove problems from their software. If you have a single computer that is not connected to anything else (like another computer, the Internet, etc) you probably don't need to worry about patches as long as your computer is working perfectly.

The issues below primarily concern your computer's operating system. This is the basic program that runs at the heart of the computer. You will probably use some version of Microsoft Windows, possibly Apple OSX or maybe Unix/Linux. All of these operating systems need patching from time to time. But many applications also need occasional patching. Internet browsers and email packages frequently need patching and it is not unknown for common accounting packages to need a patch.

If you don't keep your software patching up-to-date, you risk the software failing or, in the case of the browser or email software, of letting in malicious software that will corrupt your computer, or malicious users that will take over your computer.

Most software manufacturers provide a notification service via email to tell their customers when new patches are issued. They normally grade these notices from critical down to can be done at any time. If you get a warning of a critical patch and it affects a piece of software that your business relies on, you are advised to get it installed as soon as possible. Your business continuity may depend on it. Also check the software supplier's web site for news of updates.

These days most software manufacturers offer automatic updates via the Internet.

Backup

Backing up is the process of taking a copy of the electronic data, such as a copy of the accounts files. Why bother? Because electronic data is very easy to lose, mislay, or destroy. If you lose the only copy of your electronic accounts, how will you run your business tomorrow?

A formal and efficient back up regime will avoid many of the natural or unintended threats outlined earlier. You can copy essential data to:

- tape (an older method but still worth considering because you can keep reusing them)
- a duplicate disk drive (preferably a removable one)
- a CD (c.700 Mb) or a DVD (c.4.3 Gb)

You should consider making multiple backups of critical data using three generations of media. For example, keeping the last three week's "end of week" data on a rolling cycle so that you always have three week's (or generations) of back ups just in case you need to recreate the system. A proper back up regime for a business (even a sole trader) would be:

- end of each day - back up all files that have changed that day
- end of each week - back up all applications (accounts, correspondence, etc)
- end of each month - back up the operating system as well

If you have to rebuild the computer after a catastrophic failure, you will use the last "end of month" back up to recreate the operating system. Then restore the last "end of week" application back up.

Finally, restore each "end of day" back up taken after the last "end of week". That way, you will have rebuilt the complete system. If any of the backups cannot be read (a surprisingly common occurrence regardless of the backup medium), you can revert to the previous one of the three copies and start from there. If this happens, you are unlikely to restore every last one of your data files. Inevitably something will be missing and on the failed media. This is nonetheless preferable to losing all your precious data.

This type of backup regime has been used since computers were invented and has proved to be reliable over time. More complicated backup regimes can be used where data changes rapidly or has very high value. Be prepared to change if your business risks change.

Keep your backups safe. They are just as valuable as your original data and also subject to the same IA Principles. Don't leave them where they can be stolen or damaged.. And don't leave them on top of the computer. If that blow up / burns down, what will happen to your security backups? Ideally, keep your backups in a totally different building than your computer. If the office burns down, you don't want the same fate to happen to your backups!

One major problem with backups occurs when the owner forgets to label them properly with the date and the subject. Then when the back up is needed in a hurry

One option if you have a large number of back ups on different media is to buy a "fire proof safe". Such a safe can be kept on-site but you should be aware that after a very hot fire it might be 2/3 days before the safe is cool enough to be opened.

Information and Identity Theft

This is one of the fastest growing crimes both in the UK and in other developed nations. There has been a lot of publicity about it but one important point does not get mentioned. Information and ID theft can affect businesses as well as individuals.

For a business it is vital that old information is disposed of securely. This includes paper and electronic copies. It is not unknown for small businesses with their own Internet sites to have the site hijacked by somebody who has stolen old letter headed stationery and found signatures of directors. This is used to forge letters to the Internet name registration agencies to get the web site re-registered to a new physical address. A fraudulent business is then set up and business loans taken out.

Individuals can also have their ID's stolen with fraudulent intent. While you will not be liable for a clear fraud perpetrated by others, the problem after an ID theft is recovering credibility with banks and other financial organisations and especially with credit reference agencies.

Some things not to do:

- Never give personal information over the Internet, via email, over the phone or by letter to anybody unless you are already certain you can trust them.
- Remember that banks never ever ask customers to confirm their passwords or access codes via email so don't provide this information.

- Don't throw away confidential business or personal papers without shredding them first and ideally use a shredder that cuts twice (across and diagonally).
- Electronic or magnetic material no longer required must be physically damaged to such an extent that it cannot be re-used.
- If you have unused business bank accounts or credit lines with old suppliers, close them down because they could be exploited with fraudulent intent.

In any event you will be hacking your bank statements and other financial documents line by line as soon as you get them. Any odd payments or debits must be investigated immediately. Your bank won't mind your raising queries. They are as anxious as you to limit fraud. Another point is to periodically check your personal or business credit records for any of the following unexpected items:

- enquires about your credit rating from firms you have never dealt with,
- derogatory comments about your rating,
- notifications of a change of address or
- references to Court judgements, etc

Wireless Networks

Wireless networks (WiFi for short) are very attractive for small businesses. They are inexpensive to install, easy to configure, provide flexibility and alleviate difficult and expensive data cabling. Unfortunately, it is also very easy to build a WiFi network that allows anybody and everybody to read your confidential business data.

The big risk is that anybody within wireless range could use your WiFi network. They could use your Internet connection for free, listen to your data traffic, e.g. emails, passwords, access data files on your computers or even sniff out your Internet banking details. An insecure WiFi network presents a large risk of industrial espionage.

Setting up a WiFi network in your business needs careful planning and will probably require expert help. This note cannot be a complete guide to setting up a network. The important point here is that a WiFi network can and must be set up securely so that only you and your staff can use it and access/share data. Here are some essential tips.

First, unfortunately, some important technical notes. All WiFi must conform to the IEEE 802.11 standard. There are several subsets of this standard. The important ones for you are 802.11 G and 802.11N. 'G' is here now but 'N' is a little further away. For business purposes, go for 'G' now, although there are what are called "pre N" kits on sale now but they may not be fully compliant with the final 'N' standard. 'N' offers much faster transmission speeds and potentially better security. Do not be tempted by the now out-of-date 'A' or 'B' variant as they are slower and less secure.

Don't rely on manufacturer's statement of performance. You will generally get half the transmission speed over half the distance unless you operate under laboratory conditions. Building construction can have a clear effect on WiFi performance with stone buildings experiencing the most problems.

What you will need:

- A wireless router which transmits and received the data signals broadcast throughout the office. More elaborate ones can be tuned so that the signal is limited to cover just your building.
- A broadband connection, if you don't already have one.
- A wireless adapter for each computer. Most modern laptops have these built in now but desk top computers will need a separate one. A wireless adapter that plugs directly in to a USB port is recommended.

Where the business has a central file server already installed with an established Internet connection, a router will be directly attached to the file server. Small offices can buy the router with a built-in broadband modem. More elaborate "black boxes" can be purchased which combine the router with a firewall for added protection. A good tip is to buy all your WiFi kit from one manufacturer. Don't mix and match because if it doesn't work, all the suppliers will blame each other. And, of course, don't buy an unknown brand.

These technical notes are essential for safety:

- All data transmissions must be encrypted. Do not use WEP encryption. Use WPA or WPA2 instead.
- Use Pre-Shared Keys (PSK) to create a form of password between your computers and the router. It is recommended to use a long one.
-
- Create a unique name for your WiFi network through the Service Set Identifiers (SSID). Create a secure name which is made up.
- Configure your WiFi router so that your SSID is not broadcast.
- Never use the manufacturer's default SSID name.
- Register your office computers' MAC addresses with the router and create a rule that only registered MAC addresses can talk to it.
- Make sure your server and other computers' operating systems support WiFi before you buy the kit!

If all this sounds a bit difficult, don't try DIY. Ask an expert to install your WiFi network. Don't forget, your data is probably your most important asset and it needs protecting with a secure WiFi. After all, you don't want to turn your network into a public access point.

Third Parties

Third parties are quite often engaged in various business activities concerning a SME. Typical engagements include consulting in business management and marketing as well as IT support for critical systems. Most often these parties are given access to confidential corporate information or access to systems and network infrastructure for maintenance purposes. It is essential that businesses ensure the confidentiality of this information both contractually but also through a proper access control management process. As a minimum SMEs should consider the following controls when dealing with third parties:

- Sign a Non-Disclosure and Confidentiality Agreement.
- Provide access to information on a need-to-know basis meaning that third parties should be given access only to information that is absolutely necessary to perform their work.
- Access to IT Support third parties should NOT be given on a permanent basis unless explicitly required and necessary. Access should be immediately terminated after necessary activities are ended. Audit trails

should be printed and reviewed in order to verify that activities that took place were limited to legitimate maintenance operations.

- Request from your third party the privilege to audit its security protection measures especially in cases where corporate proprietary and confidential information is processed in their premises.

Service Providers

Service providers are typically ISPs, ASPs and Telecommunication Providers. Before selecting a service provider, the responsible persons should inform themselves about the regulations laid down by the prospective provider, for example, whether upper limits have been set for the bandwidth, whether e-mail is filtered and, if so, according to what rules.

Providers typically store user data for invoicing purposes (name, address, user-ID, bank account) as well as connection data and transmitted contents (over a period of time which varies from one provider to another).

Users should ask their providers for how long which items of their data remain stored. When selecting a provider, it should be taken into account that EU providers must comply with data privacy regulations applying to the processing of this information.

Through the use of encryption, users can prevent providers from being able to read the contents of the transferred data.

Additional controls:

- According to which criteria has the provider been selected?
- Which security measures does the provider implement?
- According to which criteria is e-mail filtered by the provider (Mail Providers)? Is staff available around the clock to deal with technical problems, and how competent are they?
- How well is the provider prepared for the failure of one or more of its IT systems (contingency planning, data backup concept)?
- What level of availability can the provider guarantee (maximum downtime)? Does the provider regularly check that the connections to customers remain stable and if they are not are appropriate steps taken?
- What does the provider do to ensure the security of its IT systems and that of its customers?

An information security policy and security guidelines should be a matter of course with every provider. It should be possible for external users to inspect the security guidelines. The staff of the provider should be made aware of IT security aspects and be under obligation to observe the security guidelines; they should also be given regular training (not only in security matters).

Data Protection and Privacy

Apart from the people you employ, what do you consider to be a key business asset of your organisation that is unseen, mostly undervalued, can be misused in the wrong hands, and lost instantaneously?

The most probable answer is Information. Good information security practice enables the correct business information to be viewed and processed by the right people, at the time when they need it. Now legislation requires you to ensure that information held on people is safeguarded adequately.

The 1998 Data Protection Act came into force on 1 March 2000. It pertains to personal data, i.e. information about living identifiable individuals or 'data subjects'.

The requirements of the Act can be summarized as follows:

- Assessment of risk of information of a personal and sensitive nature
- Identification of necessary controls to protect data and privacy
- Development and Implementation of an information security policy

References

1. The fraud advisory Panel – Cyber crime what every SME should know about
2. Jack A. Jones, CISSP, CISM, CIS - An Introduction to Factor Analysis of Information Risk (FAIR) - A framework for understanding, analyzing, and measuring information risk
3. ENISA - Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs)
4. ENISA - Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools
5. ISO 27001
6. DTI – Directors Guide for Information Security
7. Oxford Integrated Systems - Security in an Uncertain World SME's and a Level Playing Field
8. COMMISSION OF THE EUROPEAN COMMUNITIES - DIRECTORATE GENERAL - B6: Security of Telecommunications and Information Systems -Information Technology Security Evaluation Manual (ITSEM) Version 1.0
9. UK Department of Trade and Industry, Information Technology Security Evaluation Criteria (ITSEC)
10. Leeds Council - Information Assurance Guide and Questionnaire for Small & Medium Sized Businesses (SMEs)
11. Russell Morgan - Information Security for Small Businesses
12. Network and Information Security Report – ICTSB / NISSG
13. COMMISSION RECOMMENDATION of 3 April 1996 concerning the definition of small and medium-sized enterprises
14. The OCTAVE (SM) Method Implementation Guide Version 2.0
15. Charles A. Shoniregun, Impacts and Risk Assessment of Technology for Internet Security – Enabled Information Small-Medium Enterprises
16. Official Journal of the European Union (20.5.2003)
17. Risk Management among SMEs Executive report of discovery research by Alpa A. Viridi (November 2005) Institute of Chartered Accountants in England and Wales
18. Reputation: Risk of risks (An Economist Intelligence Unit white paper) December 2005
19. Risk management service for SMEs (Newsletter) International Accounting Bulletin: 3, May 24, 2006. ISSN: 0265-0223, Lafferty Publications Ltd
20. Information Security Guide for Small businesses (Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), INFOSEC of the office of Government Chief Information Officer (OGCIO) and the Technology Crime Division HK Police force of the HKSAR Government.)
21. <http://sme.cordis.lu/home/index.cfm> (SME TechWeb)
22. http://europa.eu.int/information_society/policy/ecomm/info_centre/documentation/legislation/index_en.htm#top (Europe's Information Society – Thematic Portal)