Risk Management under NIS Directive

Author: Liliana Apetri

The Role of Risk Management

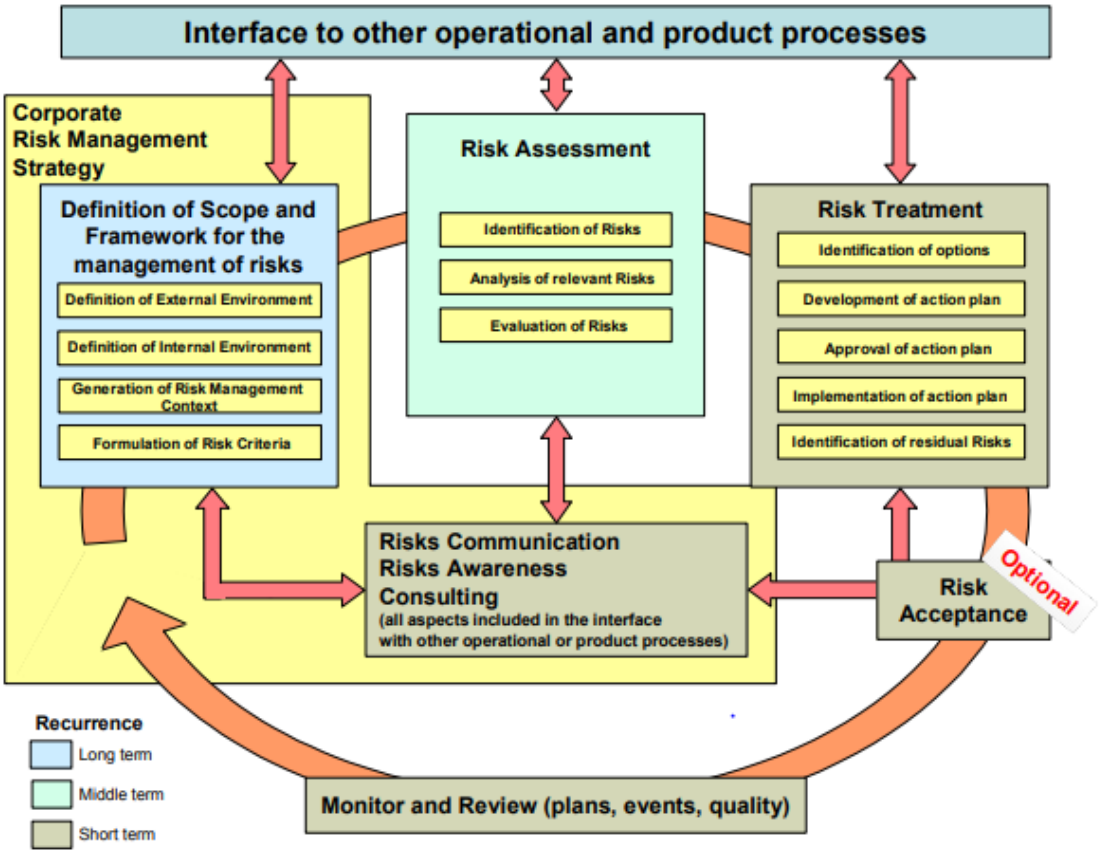
Risk management is the process of identifying, quantifying, and managing the risks that an organization faces; it is a process aimed to obtain efficient balance between realizing opportunities for gains and minimizing vulnerabilities and losses. As an integral part of management practices and an essential element of good governance, risk management needs to be recurrent seeking to support organizational improvement, performance and decision making.

Enisa's point of view related to Risk Management (including example for SMB-small and medium business)

ENISA contributes to Risk Management by collecting, analysing, and classifying information on emerging and current risks and the evolving threat environment.

The ENISA Risk Management/Risk Assessment (RM/RA) Framework is basically an overview of relevant content found in corresponding literature about Risk Management.

The figure below shows a schematic overview of the framework as it has been published by ENISA. The various (sub-) processes of the Risk Management Framework may be performed in isolation or performed as a whole. In case that all the processes are performed, the orange, thick arrows represent a cycle which depicts a control flow through the Risk Management processes. The process *Definition of Scope and Framework* is the ideal starting point for this control flow. The process aims at the establishment of global parameters for the performance of Risk Management within an organization. For this purpose, it takes internal and external aspects into account. Subsequently, a process describing activities which deal with the identification, analysis and evaluation of risks is executed (*Risk Assessment*). This process is succeeded by *Risk Treatment*, which selects and implements measures to modify risk. *Risk Acceptance* aims at deciding which risks are accepted by the responsible management of the organization. *Monitor and Review* describes a continuously ongoing process for monitoring the success of the Risk Management implementation and delivering valuable input to any recursion of the (re)definition of the corporate Risk Management. Also included in the framework is a *Risk Communication* process, which aims at exchanging information about risk to and from all stakeholders. In addition to the above processes the interfaces to operational processes are indicated but not elaborated.



Source: ENISA Project Report Demonstrators of RM/RA in Business Processes Integration of Risk Management with Operational IT Processes

Risk management components

The first component of risk management addresses how organizations frame risk or establish a risk context—that is, describing the environment in which risk-based decisions are made. The purpose of the risk framing component is to produce a risk management strategy that addresses how organizations intend to assess risk, respond to risk, and monitor risk—making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions. The risk management strategy establishes a foundation for managing risk and delineates the boundaries for risk-based decisions within organizations. The second component of risk management addresses how organizations assess risk within the context of the organizational risk frame. The purpose of the risk assessment component is to identify: (i) threats to organizations (i.e., operations, assets, or individuals) or threats directed through organizations against other organizations; (ii) vulnerabilities internal and external to organizations; (iii) the harm (i.e., adverse impact) that may occur given the

potential for threats exploiting vulnerabilities; and (iv) the likelihood that harm will occur. The result is a determination of risk (i.e., typically a function of the degree of harm and likelihood of harm occurring). The third component of risk management addresses how organizations respond to risk once that risk is determined based on the results of a risk assessment. The purpose of the risk response component is to provide a consistent, organization-wide response to risk in accordance with the organizational risk frame by: (i) developing alternative courses of action for responding to risk; (ii) evaluating the alternative courses of action; (iii) determining appropriate courses of action consistent with organizational risk tolerance; and (iv) implementing risk responses based on selected courses of action. The fourth component of risk management addresses how organizations monitor risk over time. The purpose of the risk monitoring component is to: (i) determine the ongoing effectiveness of risk responses (consistent with the organizational risk frame); (ii) identify risk-impacting changes to organizational information systems and the environments in which the systems operate; and (iii) verify that planned risk responses are implemented and information security requirements derived from and traceable to organizational missions/business functions, federal legislation, directives, regulations, policies, standards, and guidelines are satisfied.

Below is presented a representative SMB type within the framework of simplified risk assessment approach for 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.

Phase 1 – Select Risk Profile

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. It 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.

Below is presented the matrix highlighting the applicable risk level in each risk area.

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 EU Data Protection Law.**	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
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**

Source: ENISA Information Package for SMBs with examples of Risk Assessment / Risk Management for SMB

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	

Source: ENISA Information Package for SMBs with examples of Risk Assessment / Risk Management for SMB

Phase 2 - Identify Critical Assets

During this phase, the assessment team selects critical assets based on relative importance to 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.

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

Below are presented in detail the steps to be followed in this phase:

Step 1. Select your organization's most critical assets

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). These assets should then be listed by level of importance to the business process. After defining the areas that need to be secured, or reorganizing the organization's assets, the next step is to list all assets according to their impact on the business process. 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

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 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 SMB, but careful selection of requirements is critical for the controls selection task that follows. In other words, high availability requirements impose high availability controls.

Analysis teams use the **requirements selection criteria** as provided 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**.

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

[Step 1] In our example 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, teams recognize the boxes that fit their requirements. In our example 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**

Source: ENISA Information Package for SMBs with examples of Risk Assessment / Risk Management for SMB

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 our example.

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

Source: ENISA Information Package for SMBs with examples of Risk Assessment / Risk Management for SMB

Phase 3 – Select Control Cards

During Phase 3 the analysis team members can "pull out" the control cards associated with the already defined (in phase 1) applicable risk areas and the list of identified critical assets. This phase involves three steps.

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 SMBs from immediately implementing all 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 SMB analysis teams can use Asset Control Cards Table 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, it will be identified a need to discuss a lot of issues related to these controls. In this step it should be documented the rationale for selecting each control card and the necessary actions for implementation. In addition, by understanding control cards, it will be better able to define action plans during the next step. For each control card, consider and record the 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?

The information that is identified by answering these questions will be useful in phase 4 when you build mitigation plans. This information should be recorded.

Step 1 for our company

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

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)	

Source: ENISA Information Package for SMBs with examples of Risk Assessment / Risk Management for SMB

[Step 2] In step 2 analysis team selects asset-based control card(s) using the asset-based control cards table. In our example 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

Source: ENISA Information Package for SMBs with examples of Risk Assessment / Risk Management for SMB

The card selected in our example 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								

Source: ENISA Information Package for SMBs with examples of Risk Assessment / Risk Management for SMB

[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

Source: ENISA Information Package for SMBs with examples of Risk Assessment / Risk Management for SMB

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.

Step 1. Gap Analysis

Gap analysis is essential to improve how an organization handles information security, and establish the current state of security, respectively, 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. A mitigation plan provides organizational direction with respect to information security activities.

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 the initiatives after the evaluation. SMBs 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?**

For our example

[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.

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

Source: ENISA Information Package for SMBs with examples of Risk Assessment / Risk Management for SMB

[Step 2] In step 2 analysis teams read the controls 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**	The team decides to launch a basic awareness campaign by providing educating all lawyers about the risks involved in using email, internet etc.
	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.

Source: ENISA Information Package for SMBs with examples of Risk Assessment / Risk Management for SMB

[Step 3] In step 3 for example 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?

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

Source: ENISA Information Package for SMBs with examples of Risk Assessment / Risk Management for SMB

Security measures related to Governance and risk management

Responsibilities under NIS Directive related to Governance and Risk management are related to establishing and maintaining an appropriate governance and risk management framework, to identify and address risks for the communications networks and services.

	Security measures	Evidence
1	a) Set a high level security policy addressing the security of networks and services. b) Make key personnel aware of the security policy.	i. List of main risks described at a high level, including the underlying threat(s) and their potential impact on the security of networks and services ii. Key personnel know the main risks (interview).
2	c) Set detailed information security policies for critical assets and business processes d) Set up a risk management methodology and/or tools based on industry standards. e) Ensure that key personnel use the risk management methodology and tools. f) Review the risk assessments following changes or incidents. g) Ensure residual risks are accepted by management.	iii. Documented risk management methodology and/or tools. iv. Guidance for personnel on assessing risks. v. List of risks and evidence of updates/reviews. vi. Review comments or change logs for risk assessments. vii. Management approval of residual risks.
3	h) Review the risk management methodology and/or tools, periodically, taking into account changes and past incidents.	viii. Information security policies are up to date and approved by senior management. ix. Logs of policy exceptions, approved by the relevant roles. x. Documentation of review process, taking into account changes and past incidents.

Source: ENISA GUIDELINE ON SECURITY MEASURES UNDER THE EECC

Below are described important security tips for small and medium sized enterprises:

- 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 organization
- 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

Third parties

Third parties are quite often engaged in various business activities concerning a SMB.

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 SMBs 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 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.

Source: This article was made based on the following materials: Enisa -Technical guidelines for the implementation of minimum security measures for DSPs-enisa, Enisa ENISA RM/RA Framework, Project Report Demonstrators of RM/RA in Business Processes Integration of Risk Management with Operational IT Processes, Enisa article GUIDELINE ON SECURITY MEASURES UNDER THE EECC, Guide for Conducting Risk Assessments, *ENISA* Information Package for SMBs With examples of Risk Assessment / Risk Management for SMB.