IS2ME

Information Security to the Medium Enterprise

A Method for Approaching and Implementing Information Security in Small and Medium Enterprises

Authors:
Samuel Linares (Samuel.Linares@gmail.com)
Ignacio Paredes (iparedes@gmail.com)

English Version Advisor:
Marga Menéndez-López (M.Menendez-Lopez@surrey.ac.uk)

IS2ME: Information Security to the Medium Enterprise

A Method for Approaching and Implementing Information Security in Small and Medium Enterprises

1 Introduction

The term SME (Small and Medium Enterprises) represents a broadly deployed type of company whose main feature is to have a reduced number of employees and moderate billings. The definition of what constitutes an SME varies depending on the country. For the purposes of this document they will be defined them as organizations of approximately 500 employees maximum. This, from a general point of view, includes more than 90% of all worldwide enterprises, and more than 99% of the enterprises within the European Union.

Security professionals, commonly involved in high level issues such as information security management and governance, standards, digital signature projects, PKI or log consolidation, among others, tend to suffer a loss of perspective on assuming a high level of knowledge, deployment and culture on security across organizations, when the truth among SMEs is quite different. Only a small number of companies possess a high level of information security deployment, whereas the great majority lacks important knowledge about security in general, as well as about associated organizational and technical measures. The reality is that this kind of organisation lacks maturity about information security.

Such organizations usually need an adequate organisational structure; in most cases, they lack a chief security officer, whose job is assumed by the IT manager (systems and/or communications). This fact, joined to little or no training on information security, leads to a very basic and insufficient deployment of security measures, which are mostly taken to solve ad hoc problems and needs in the organization.

The daily tasks do not allow the people involved to have an overview or to plan and manage information security adequately. This, in turn, leads to a lack of awareness at the top level management about these issues, and inevitably ends up in unacceptable levels of risk for the organization. Such is the case of security incidents or non compliance issues that have an undesirable impact on the business. It is then that information security professionals are needed in the organization, to solve those immediate problems and, in the medium and long term, to reduce the risk and deploy adequate security measures.

When such incidents occur, companies usually require a reduction of the existing risk, deployment of short-term critical security measures, and without doubt, the development of an action plan for the top level management and the security manager (in fact the IT manager) to identify the necessary resources, and how security can be integrated as an additional requirement in the business processes of the organization.

This complex challenge could be approached in a traditional fashion, following the typical methodologies and standards (mainly ISO 27001), and consequently starting the ISMS (Information

Security Management System) with its usual phases, whose description is not in the scope of this document, but will be outlined here as reference:

- Scope and policy definition of the ISMS
- Setting resources and responsibilities
- Asset Assessment
- Risk Management
- Risk Treatment (control selection)
- Statement of Applicability
- Deployment

The strict execution of these phases in SMEs tends to be quite complicated, due to lack of awareness at the top level management and to the absence of some minimal structure for information security. Security measures (controls) are deployed only when the project is well into its course (probably months after the beginning). As a result of this, one of the objectives of the company, the short term critical measures, is not achieved.

This approach, otherwise accepted as the long-term path to follow, is then not commonly accepted by companies looking for immediate results (*"we want security and we want it now"*).

Here arises the need for a methodology to scenarios like the one outlined earlier (again, bearing in mind that SMEs are 99% of the enterprises across the EU). This approach should provide a bridge between total non-compliance and a methodological deployment of security management according to a standard like ISO 27001.

This is the reason for presenting IS2ME (Information Security to the Medium Enterprise) as an approach and solution for the deployment of information security in organizations whose security model is not mature enough, but wish to undertake security deployment and its associated management system in an efficient, effective, and practical way. Such a method reduces risk in the short term while setting up a framework to achieve the required standards.

IS2ME also pursues an ambitious social objective: closing the gap between information security and medium (and small) enterprises. The process includes weaving information security in the organisational culture so that the general level of risk is reduced, resulting in an increase on the value, revenues and economic level of the majority of organizations that exist nowadays.

2 Objectives

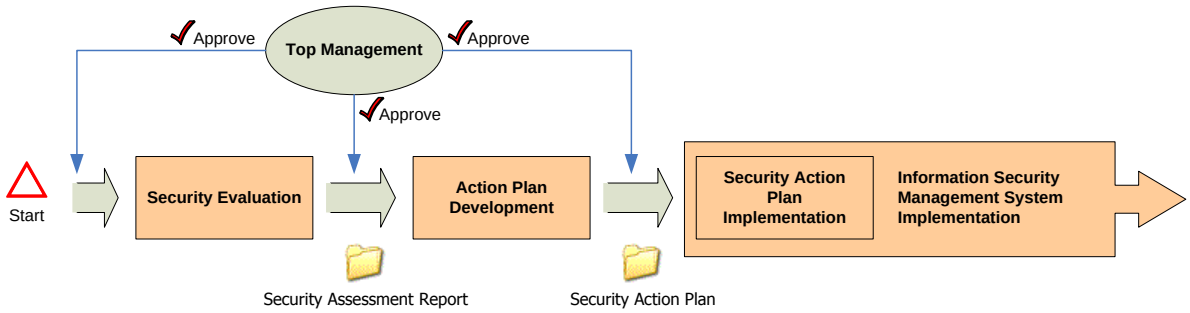
The main objective of the IS2ME method is the rapid reduction of the information security risk taken by the organization. Within this framework, technical and organisational measures will be implemented in stages as part of a defined project. Its final aims are twofold: binding security to the usual operations of the organization, just as any other requirement of the business processes, while obtaining, simultaneously, short term results that identify the current state of security, the tasks needed to increase it and the action plan for its implementation.

Besides, a prerequisite for the development of these steps is compliance to applicable standards. The objective of IS2ME is not to develop a new standard of information security management, but to approach SMEs towards their standard targets. In order to do this, clearly defined steps that are easily assessed and provide immediate benefits and results on the improvement of security levels establish the grounds for a more detailed development. It is then when Information Security Management Systems may be implemented according to existing normative, if desired.

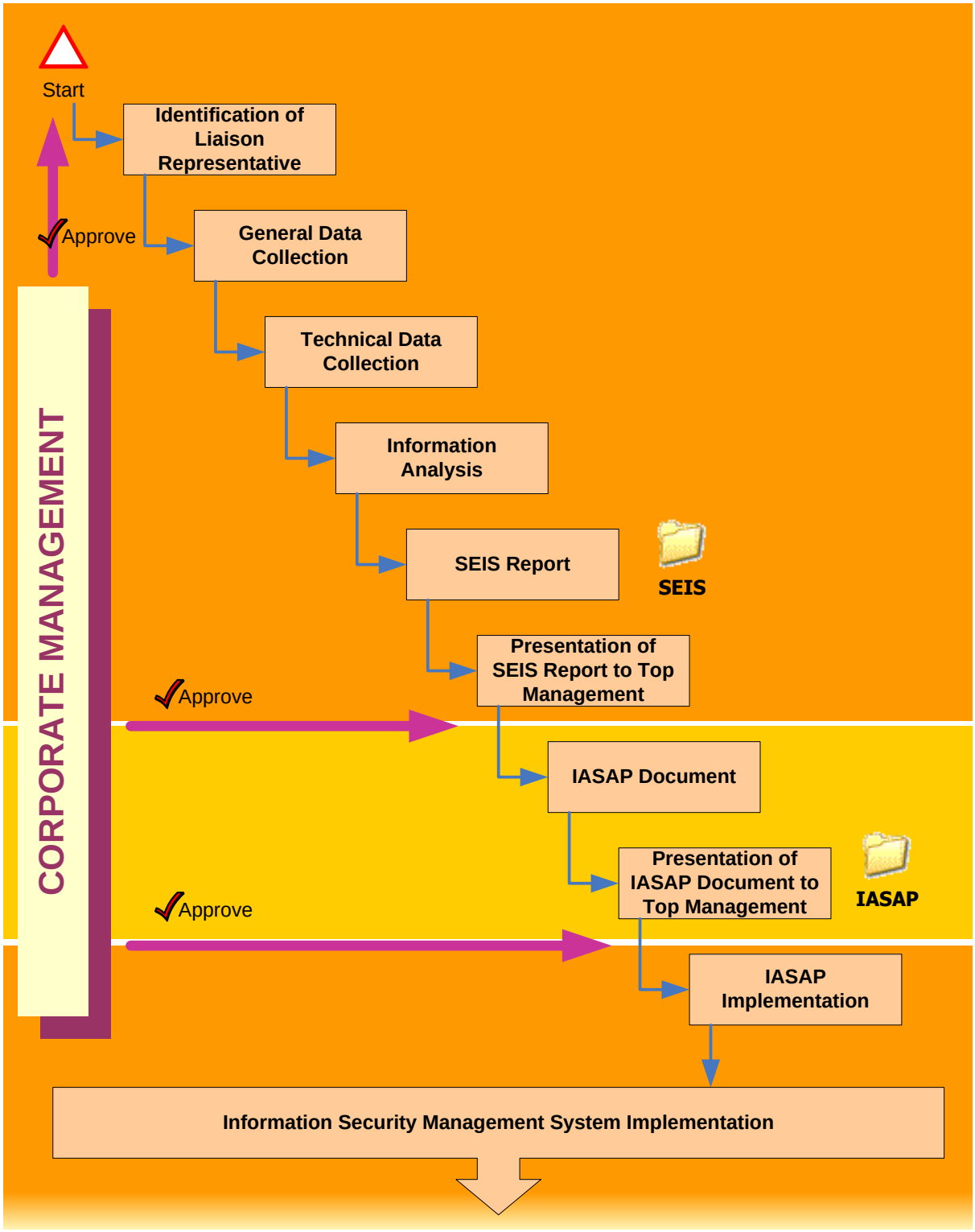
In order to achieve these objectives, security needs to be considered not only at an abstract and general level, but also in detailed technical and organizational measures. Organizational issues such us organization structure, existing roles, defined responsibilities or information flow will be studied, as well as technical issues such as services topology and architecture, networks, systems and communications, existing security devices or vulnerability assessments.

3 The Method

IS2ME starts by evaluating the security of the organization by collecting information through interviews with staff, field tests and technical analyses. This information is then compiled in a report that states the level of implementation of the different security measures. A proposal for an action plan is produced from it. After the approval of the plan by top management, it is developed and implemented, establishing a basis for complying with and deploying the Information Security Management System according to ISO 27001.



IS2ME follows a holistic and extremely practical oriented approach which allows the user a simple and immediate application, just by following a sequence of well defined phases. They are showed in the next graphic and will be described in the following sections.


Start
Identification of Liaison Representative
Approve
General Data Collection
Technical Data Collection
Information Analysis
SEIS Report
SEIS
Presentation of SEIS Report to Top Management
Approve
IASAP Document
Presentation of IASAP Document to Top Management
IASAP
Approve
IASAP Implementation
CORPORATE MANAGEMENT
Information Security Management System Implementation

3.1 Identification of Liaison Representative

Objective: To identify valid speakers in the organization and to plan their availability during subsequent tasks.

The data collection phase has great significance to the development of the method, since this information will be the source of the analysis and of subsequent tasks that will form the base of the action plan. For that reason, the organization's involvement and collaboration will be very important during this phase to obtain the information needed.

The organization will usually appoint a person (or several if necessary) who will liaise between the evaluators and the organization. In this way, the representative will redirect questions from the evaluators to the corresponding persons inside the organization. It is central for the success of the programme that the organization foresees his/her availability during the data collection phase.

Additionally, the evaluation team may need direct access to systems or devices within the organization to carry out security and configuration checks, tasks clearly identified in advance. This access should be provided by the organization under their standard requirements: supervised by company staff, with an operations log, or any other similar mechanism that keeps information integrity during the work. The evaluation team will also sign a confidentiality and non disclosure agreement that will act as a warranty about the proper use of the collected data. On the other side, the organization should provide written authorization for those tasks.

3.2 General Data Collection

Objective: To obtain information related to information security, including technical, organizational and compliance information, through interviews, documentation and other general methods.

Following on the earlier section, special attention should be paid to achieving this objective, since this is one of the key phases in IS2ME (considering that the collected information will be the source for the analysis and action plan).

During this phase there will be substantial interaction between the organization and the data collection team. Members of the team will visit the company premises. The face to face meeting with the company contact will facilitate the data collection for both sides. Therefore, an appropriate work space should be provided, as well as availability of the company representative.

Previous to the work team visit, a questionnaire is sent for the company representative to fill in and return. The questionnaire includes technical and organizational questions regarding the scope of the work. This way the data collection team can focus its efforts during their visit, maximizing results and minimizing the length of this phase.

The baseline information to obtain in this phase includes:

- Technical Aspects
    - Network and services architecture and topology.
    - Public and internal services. Access medium (Internet, VPNs, etc.)
    - Existing security devices and functional description (firewalls, IDSs, IPSs, Centralized/Distributed antivirus systems, proxies, etc.)
    - Interconnection points to other networks, description of existing DMZs, security levels.

- Identified points of failure, devices, servers, etc. High availability mechanisms, emergency procedures, etc.
- Network addressing plans (public and private) and related procedures (address allocation, requesting, etc.)
- Network- and services-related documentation and procedures.
- Network management methods. Description and related procedures.

- Organizational and Compliance aspects.
  - Definition of the organization, areas or departments included affected (functions, responsibilities, etc.).
  - Organizational structure of the organization within the scope of the work. Links with other areas, departments or organizations. Existing roles, flows, managers, etc.
  - List and description of policies, procedures, guidelines or regulations in the company (ISO9001, security policies, communication policies, resources policies, etc.)
  - List and description of other existing security policies or documents.
  - List and description of current compliance regarding information technologies.

3.3 Technical Data Collection

Objective: To obtain information through different technical and empirical methods in order to obtain representative samples of systems and devices across the organization.

The information collected in the previous phase will be analysed to identify the systems in need of attention. A set of technical tests will then gauge their actual level of technical security, detecting existing and potential security problems that may affect the integrity, operation or performance of the systems in the organization.

Following is a list with the points to be covered during the technical collection of information.

3.3.1 List and Characterization of data

The information collected during the General Data Collection phase will highlight the systems, devices and applications in need of attention. An exhaustive description of each element is essential as they will be the basis of the technical analysis and results evaluation.

The minimum information that should be collected is listed next (but could be extended to other information that the data collection team may consider of interest):

Systems Characterization

- System (name, type, vendor)
- Location
- Person(s) in charge
- Software versions (OS, applications)
- State of patches and updates

Applications Characterization

- Application (name, version, vendor)
- Associated subsystems (systems the application runs in)
- Links with other applications
- Person(s) in charge
- State of patches and updates

3.3.2 Traffic Analysis

Traffic analysis determines the type of traffic through the organisation networks and detects possible failure points or bottlenecks in these networks.

For an optimal result of the analysis, key measure points across the network should be identified. Typically these points include:

- Segment interconnection
- Critical applications/server segments
- User segments
- Other points of interest

Each measure should be taken for a period of time so an appropriate amount of traffic is captured for later analysis. The measure time will depend on the amount of traffic the network handles per unit of time. In some networks a measure held for several minutes is enough, while in others it is necessary to take the measure for a whole day or even longer periods.

Time patterns of network use also need to be considered in order to select appropriate times to capture traffic. For instance, the capture of traffic will be different in an office network and in the network of a factory open 24 hours a day.

Captures will be taken with no filters (using a suitable protocol analyser), stored on disk in order to be replayed and analysed in the laboratory. The information can then be used in reports and statistics of use.

3.3.3 Systems and Applications Vulnerability Assessment

The aim of the applications and systems vulnerability assessment is to detect weak security points. Weak points are programming or configuration errors in applications and in the operating system whose vulnerability may potentially be exploited by attackers. Therefore, it is important to identify those weak points in order to eliminate them or avoid its exploitation.

Not every system has the same importance for the organization. For this reason, and also because the vulnerability assessment is time-consuming, it needs to be selective. Typical objectives of this analysis are malfunctioning systems that have an important impact in the key processes of the organization (i.e. main servers) or those whose visibility makes them more exposed to a possible attack (i.e. servers with public access from the Internet). The selection of such systems is a responsibility of the organization, with support from the assessing team.

3.3.3.1 Remote Analysis

Special attention will be paid to vulnerabilities that may be exploited remotely and therefore do not require physical presence for that, as they will pose a bigger risk. These vulnerabilities are usually linked to application ports waiting for remote connections. Therefore, the first step in the vulnerability assessment is to identify the ports in the systems that can be accessed remotely, using, for instance, port scanning.

The aim of port scanning is to find out which ports (normally TCP or UDP[1]) are listening in a given system, and therefore are able to receive remote connections. This information is of the utmost importance, since most of the application vulnerabilities are related to handling of remote connections. The basic technique to find out the state of a port is to attempt connecting to it and to analyse the result. Typically, there are three different states for a port:

- Open: The port is listening and ready to receive connections.
- Closed: The port is not listening.
- Filtered: There is a device (usually a firewall) that does not allow connections to the port.

There are different scanning techniques, most of them oriented to avoid detection controls in the target systems. This type of techniques may not be relevant in our case because we should have written authorisation from top management to execute the actions related to remote analysis, so there is no need to use stealth techniques except perhaps in cases where intrusion detection systems are present and could make void the test results.

Once defined the scope of the systems to be analysed, we can select its depth. That is, we decide which set of ports are going to be scanned. Obviously, a complete analysis should check the state of every TCP and UDP port. However, in some cases it could take more time than it is available, or else we have the certainty that a given device is listening in just some ports. Only then it is possible to reduce the set of ports to analyse, which will decrease the complexity and time of the scan.

Scanning the ports will provide accurate information about available ports in each system that accept remote connections. Each one of these ports is linked to a service, and consequently to an application. The next step is to find out those applications and, if possible, their versions.

Knowing the exact software installed in a system is one of the first tasks that a potential attacker will carry out, because with this information it is possible to find out the existing vulnerabilities in the remote access applications, and therefore to execute exploitation methods. The result of the execution of an exploit usually puts the system at jeopardy in the form of illegal access to data or even their destruction.

Software identification from the ports in listening state can be made using the answers (banners) that the service gives after an incoming connection. Nevertheless, since it is convenient to modify this information in order to confuse potential attackers, another way has to be found to carry out the applications identification. There are multiple tools, most of them open source, that can automate the identification of applications linked to listening ports. These tools not only recognise the banners, but also analyse the answers to certain inputs and identify, with a variable degree of accuracy, the application and version running in the system, based on differences in the implementation of the protocol among applications.

This process (scanning + identification) is the usual way a possible attacker would work, so it is important to carry it out in order to know what kind of information could be obtained by this means. However, from the point of view of security analysis, and with the aim of being certain about the accuracy of the results obtained, the identification of applications and its versions should also be carried out by traditional means such as local analysis of the systems in question.

At this point, a possible attacker could query some of the multiple online services about applications, its vulnerabilities and the exploits of a given version. Therefore, the team's job is to find out the patches or appropriate upgrades to solve the security problems of the application. In the event that there are no patches or upgrades or these cannot be deployed, alternatives to decrease the level of risk or exposure of the applications are searched.

[1] This document only refers to IP communications networks, since they make the great majority of existing networks in this kind of organizations. If the analysed organization network is supported by another protocol, the associated tasks should be similarly run, but with the particular features of that protocol.

Nowadays, the communication networks where the analysed systems are located are not plain. It is common the existence of different segments, separated by different devices and with different access policies. For that reason, the vulnerability assessment will produce different results depending on the place where it is launched from. Taking this into account, the validity of the results is assured if the analysis is executed from every possible location that could be taken by a potential attacker, thus obtaining different profiles of visibility (and of course of risk exposure) of the analysed system.

The analysis is typically executed from the following locations:

- **Internet:** only the public services of the organization are reached from the Internet. This analysis will determine that these and only these services are publicly accessible.
- **DMZ:** in the event that several DMZ segments are present in the organization, the analysis is executed from every DMZ towards the internal servers of the organization. The reason for doing this is that DMZs are a typical entry point for attackers once they have exposed a public server, so the analysis reveals the degree of visibility that internal servers have for an attacker that has already jeopardized some of the systems of the organization.
- **Same Segment:** scans from the same network segment where internal servers are show, without physical access to the system, both the services that the system has running and those ones that are running but are not being used due to bad administration practices or default installations.
- **Internal Network:** since an important amount of security incidents originates from inside the organization, it is necessary to know which services are accessible (and therefore a possible source of vulnerability) from the internal users' networks.

3.3.3.2 Local Analysis

Although it is not usually available to potential attackers, the local analysis allows us to obtain an accurate knowledge about the state of security in the system by characterizing it exhaustively.

At least, the following information should be collected:

Name
Person(s) in charge
Type of system
File systems
Memory usage
Patches and updates
Software and applications installed
Listening ports and active connections
Service Banners
Services
Boot scripts
Processes in execution
Users and passwords
Network configuration
Periodic tasks

Additionally, depending on the operating system of the analysed system, it may be necessary to collect more data, in which case an expert in that area will identify them. In Unix systems, for instance, data like tcp wrappers, suid and sgid files, NFS services or RPCs should be collected.

3.3.4 Configuration Review

During the technical collection of information, configuration files of key elements in the network are also reviewed. In many cases, due to the high number of devices in the network, it is not possible to carry out an exhaustive review. It is then necessary to select, in accordance with the organization representative, the key devices whose configuration will be reviewed.

This configuration review requires the participation of experts in the devices analysed, in order to identify configuration failures, more efficient configurations or alternatives that may improve the security and efficiency of the device.

A typical review includes, at least, network devices (routers, switches, bridges, etc.), security devices (firewalls, IDS/IPS, Authentication Servers), applications (web, FTP, mail servers, etc.) and any other device that may be a source of vulnerabilities and therefore of an increased risk level in the organization.

3.3.5 External Visibility

There is a large amount of information about organizations which is available to the public from the Internet. This information may become a key part in the design of an attack plan against the organization, because it can reveal interesting technical and organizational details that may facilitate the job of potential attackers.

Hence the importance for the organization to be conscious about the existence of this information, especially in the following aspects:

3.3.5.1 Public Addressing

Using whois services from regional registrars of the Internet (i.e. RIPE in Europe, ARIN in North America) reveals the public addressing ranges allocated to an organization, as well as postal and e-mail addresses, telephone numbers and names of contact persons inside the organization.

The organization needs have an accurate knowledge of this information in order to be sure that the data are correct and can not reveal sensitive information.

3.3.5.2 Domain Names and DNS

Every domain name belonging to the organization needs to be collected, since information about technical, administrative and billing contacts can be obtained through the domain registrar.

For each domain belonging to the organization DNS queries are made paying special attention to:

- Name Servers (NS)
- Mail Exchangers (MX)
- Known names (e.g. www, ftp)

These names correspond to servers that can be attacked, so they need to be carefully hardened against possible attacks.

3.3.5.3 Documentation Filtering

A wrong configuration in the corporate web servers may disclose internal information through the Internet. Today's web crawlers (i.e. Google) allow the user to execute sophisticate queries -for example restricted to a given domain and file type. It is always surprising the amount of information that can be obtained by this means. This type of queries need then to be executed as part of the technical data collection, to determine whether the organization is vulnerable to this kind of attacks and to identify its root cause.

3.3.6 Other Technical Analyses

Depending on the technical features of the organization's infrastructure, it may be necessary to execute extra tests to collect additional information. These tests should be coordinated by the evaluation team and experts on the system or application under test.

3.4 Data Analysis

Objective: To study and analyse the information collected in the previous phases according to best practices, standards, methodologies, knowledge and experience of the evaluation team.

The general and technical information collected in the previous sections is now systematically analysed to reveal possible deficiencies of information security in products, network design, accesses to information, processes and other aspects. The tools to carry out the analysis encompass codes of good practice, methodologies, standards (like ISO 27001), laws, regulations, as well as existing knowledge bases about the different systems or products analysed, and of course the expertise and knowledge of the evaluation team in charge of the project.

This expertise and knowledge of the evaluation team is a critical asset. The team's task is to identify vulnerabilities, concept failures, and weaknesses in technical designs and processes within the organization, which requires extensive knowledge and experience in the fields under analysis.

This analysis is the previous step to the State of Enterprise Information Security Report (SEIS Report). As can be seen in the next point, it develops all the findings and recommendations product of the analysis.

3.5 SEIS Report Development (State of Enterprise Information Security)

Objective: To produce a report about the state of information security within the organization. This report is a snapshot of the current state of the organization in terms of deployment of technical and organizational measures regarding information security.

The findings discovered during the analysis of the data collected in the previous phases are fed into the SEIS (*State of Enterprise Information Security)* report. The objective of the report is twofold: first, to provide a global and detailed overview of the state of the organization regarding information security. The second objective, not less important, is to indicate the improvable aspects on information security, and to propose corrective actions, prioritized according to their importance for the organization.

The SEIS report comprises the following sections:

3.5.1 Description of Current State

This section describes the findings of the analysis of all the data collected previously, as well as the current state of communication networks and information systems within the organization. A possible structure for this section is described next:

- Topology: description of network topologies within the organization. Collection of physical and logical diagrams.
- Systems: inventory and characterization of public and private services within the organization.
- Physical Security: description of deployed physical security measures in the organization's premises.
- Logical Security: description of logical security measures deployed for protection of the security systems within the organization.
- Management and Operations: list of policies and procedures about management of information systems within the organization.

3.5.2 Analysis and Technical Recommendations

Each one of the subsections of the previous section, and following the same structure, includes a review of the existing implications for information security, and recommendations to solve the problems that have been found.

3.5.3 Conclusions and Action Proposals

In this section, the recommended actions from the last section are prioritised using a scale based on the critical level of their application. This critical level is assigned according to the amount of risk that the non application of that action will cause to the organisation. The calculation of risk is not always objective (i.e. monetary loss); in many cases it depends on other considerations specific to the organization.

Special attention should be paid to actions marked as extremely urgent, because they imply a high and immediate level of risk that cannot be taken by the organization. Every recommended action is given a proposed time frame for its execution. An example of classification levels is proposed next:

- Critical: immediate deployment
- High: deployment finished in three months
- Medium: deployment finished from three to six months
- Low: deployment finished from six to twelve months

3.5.4 Security Measures and Recommended Controls

Additionally, a series of applicable measures and security controls is proposed, following recommendations from current good practice guides. IS2ME does not require the use of a specific methodology, yet its philosophy and objectives are in line with the ISO 27001 framework.

At this point it is recommended to identify and describe all the security measures and applicable controls proposed by the methodology that is going to be used. This way, this section of the report serves as reference for its subsequent implementation. In this IASAP phase every control is then further developed.

3.5.5 Executive Summary

In this section of the report, the executive summary lists the main results, such as risks run by the organisation due to the current deployment of information security measures. The language used is clear and avoids technical terms.

Special attention should be paid to this section, because it is probably the most visible across the organization, and therefore the one that may influence management support to both compliance with the proposed security measures and the gradual introduction of information security to the organisation's culture.

3.6 Presentation of the SEIS Report to Top Management

Objective: To present the State of Enterprise Information Security report to top-level management. This presentation is a milestone in the process of incorporating security to the organisation's business culture.

The SEIS report as documented evidence of the technical and general collection of information seeks a twofold objective: on one hand, to summarise the technical and organisational state of information security in the company in a concise and clear document. This documentation can be used as reference material in proposals for future projects -probably after hiding confidential information.

On the other hand, and even more important, the report serves as a reference (specially the executive summary) to top management to support their decisions about decreasing risk and therefore increasing the value of the organisation.

On this note, a presentation to top management transmits the key messages from the report in clear business and financial risks terms, avoiding technical terms where possible, for the audience to understand the significance of the messages.

The presentation may use the following structure:

- Brief introduction about information security.
- Description and rationale of the work undertaken
- Current state of the organization
- Examples of findings, problems and/or existing vulnerabilities
- Recommendations
- Immediate actions required
- Conclusions
- Round of questions

The level of risk taken by the organization needs to be emphasised in both the initial part of the presentation (current state) and the final one (conclusions). For instance, clear and concise statements like the following can be used: "The level of risk is High and unacceptable in an organization of this size and visibility" or "The organisational structure needs to improve and there is an insufficient level of technical and organizational measures".

The length of the presentation depends on the size of the organization, the nature of the information to be presented and other factors, such as availability of management staff, etc. In any case, it is recommended to take between 1 and 2 hours. At the end of the presentation, some time is set aside for a round of questions, or to elaborate some aspects of the presentation in more detail at the audience's request.

The presentation should result in approval of the SEIS report by top management and their support and explicit commitment to the continuation of the project, that is, the development of the IASAP (Information Assurance and Security Action Plan) document.

3.7 IASAP Document (Information Assurance and Security Action Plan Document)

Objective: To produce the Information Assurance and Security Action Plan document; this serves as foundation for the deployment of recommended actions and development of the security plans.

Approval of the SEIS report from top management explicitly entails agreement to then develop the IASAP document (Information Assurance and Security Action Plan), tackling each one of the actions proposed in the SEIS report in detail.

Information is one of the most important assets for the organisation. Like other resources, it has great value and therefore needs to be properly protected. The objective of information security is to protect it from a wide range of threats, in order to guarantee the continuity of the organization's activities, minimize information damage and maximise the return on investments and opportunities. This is done following the principles of confidentiality (guaranteeing that information should be accessible only by authorized personnel), integrity (protecting the accuracy and total amount of information, and its processing mechanisms) and availability (ensuring information, and associate resources, access to authorised users whenever they need it).

The security of information is the result of the implementation of adequate controls and security measures that encompass policies, procedures, practices, organizational structures and software functions, among others. The design or development of many information systems does not consider adequate security requirements. In compensation for the limitations of technical security measures, there is a need for adequate procedures and management supported by every employee of the organisation and even suppliers, users and/or customers, in some cases.

It is essential for the organization to identify its security requirements through an evaluation of the risks. It also needs to identify the legal, normative, statutory and contractual requirements as well as the objectives and requirements of information processing needed to support its operations.

Once identified the security requirements, the security measures and actions selected in the SEIS report are developed in detail in the IASAP document. This document includes required resources for the planning, implementation and economic assessment of those actions to reduce risk to an acceptable level,.

The IASAP document is actually the organization's Information Security Action Plan. It includes an integral plan of the deployment of identified actions so deadlines and milestones can be established to achieve different objectives: organizational, departmental, and even personal. For each of the actions, at least the following information is needed:

- Technical (and organizational where required) development of the action in detail.
- Detailed planning of each action, including time frames and deployment plan (short, medium or long term)
- Identification of required human resources, stating whether they are internal or external.
- Economic assessment where possible (in both internal actions and actions carried out by external contractors)
- Suppliers quotes in tasks where external support is needed.

The actions to include in the IASAP document depend on the security measures already deployed by the organization and the degree of penetration of information security within the organizational culture. Some of the usual tasks include:

- Improvement of organizational structures (creation of a security committee, allocation of responsibilities).
- Possible outsourcing of some IT functions.
- Development and distribution of security policies and associated procedures.
- Improvements in systems and the data centre.
- Improvements in the security of network devices (wireless networks, WAN, LAN).
- Vulnerability assessment.
- Development of business continuity process.
- Risk analysis.
- Development of IT contingency plan.
- Training plan.
- Others.

In some cases it is necessary to seek the support of external experts on specific areas, or supplier quotes to calculate the human and economic resources of some of the required actions.

3.8 Presentation of the IASAP Document to Top Management

Objective: To present the Information Assurance and Security Action Plan to Top Management for their approval, and so establishing a foundation for its deployment.

The completed IASAP document is then presented to top management. This presentation is planned in advance, during the presentation of the SEIS report, thus ensuring continuity in the execution of the project.

Approval of the IASAP document by top management is yet another milestone in their commitment to integrate information security in all its processes. It means approval to start the Information Security Action Plan, according to corresponding features, planning and estimation of human and economic resources.

At this point, top management has all the necessary information to properly evaluate the efforts required in the organization to achieve their objectives of reducing risk and improving security levels. They can assess the convenience of the tasks and time frames proposed in the IASAP document, and adjust or modify them as required according to additional considerations, in some cases only known by top level management (global business strategies, existing synergies, etc.).

As in the presentation of the SEIS report, it is necessary to take into account that the audience may not have technical knowledge on security. For that reason, the key messages need to be presented adequately, following the same recommendations of the section “Presentation of the SEIS report to Top Management”.

The following is an example of a possible structure of the presentation, which can be used as reference:

- Introduction: origins of the IASAP document and its process.
- Justified description of short, medium and long terms, and rationale for the inclusion of tasks in these time frames.
- Short Term: Detailed description of each task to be completed in this deadline, including deadlines for: deployment, resources (stating if they are internal and/or external), suppliers’

quotes (where needed), tasks and economic assessment. (For example, tasks that should be executed in under six months).
- Medium Term: Detailed description of each task to be executed as stated in the previous point. (6 to 12 months)
- Long Term: Detailed description of each task to be executed as stated in the previous point. (more than 12 months[2])
- Time planning proposal: Proposal with real dates for the fulfilment of objectives stated in the IASAP document (i.e. a Gantt chart).

In addition to improvements on security, the IASAP document can be used as a framework for a policy of compliance to objectives at different levels in the organization, from departmental to personal/role ones.

3.9 IASAP Implementation

Objective: To develop and implement the Information Assurance and Security Action Plan.

Once the IASAP document has been presented to and accepted by management, the tasks outlined in the Information Assurance and Security Action Plan can be executed. Although the staff involved in the different phases of the IS2ME method do not necessarily have to be the ones to execute these tasks, it is nevertheless convenient that they monitor and coordinate them in order to ensure that the objectives are met and the controls are correctly deployed. The correct implementation of the proposed tasks is a key step towards compliance and implantation of an ISO 27001 Information Security Management System. It is then when information security management can be approached in a conventional way.

A Coordination Project Plan is needed for the execution of the IASAP. This plan includes:

- **Acquisition/Allocation of necessary resources:** These resources identified in the IASAP plan are earmarked for the tasks to be executed. Their availability within the deadlines needs to be guaranteed, as well as the possibility that some of them are allocated to simultaneous tasks.
- **Monitoring:** Monitoring ensures correct execution of the tasks outlined in the action plan within the deadlines. Staff in charge of monitoring coordinates the teams working in systems with common interfaces, in order to avoid interferences in the actions deployed.
- **Review Meetings:** Periodical review meetings are scheduled as well as update meetings with management to report the development of the different tasks.

4 Conclusions

Lately the corporate world has become aware of the need to incorporate security into the organizations. This task is hard and nontrivial, but fortunately there are methodologies that facilitate this process. However, most of the times, these methodologies take for granted that organizations have an information security section, the necessary resources and experience on this field, which is not the case in most organizations.

The authors believe that IS2ME fills a gap in the implementation of security in small and medium enterprises. Unlike traditional methodologies, IS2ME delivers immediate results with a reasonable use of resources. These results mean an immediate reduction of the risk faced by the organization, the solution of a large amount of organizational and technical problems, and a solid foundation of security measures for a full implementation of an Information Security Management System.

[2] The time frame of these deadlines is indicative and fit the purposes of most organizations. Adequate terms must be defined and aligned according to the set objectives and the business strategy of the organization.