www.irhsr.org

INTERNATIONAL REVIEW OF HUMANITIES AND SCIENTIFIC RESEARCH
By International Scientific Indexing
ISSN (Online) : 2519-5336

PREPARING THE ORGANIZATION FOR THE SUCCESSFUL IMPLEMENTATION OF THE INFORMATION SECURITY MANAGEMENT SYSTEM

Nader Iranpour
Information Security Consultant & Researcher niranpour@gmail.com

Abstract

Many organizations face a lot of challenges in implementing the Information Security Management System (ISMS), which results in a halt to project execution, or delays and imposition of unforeseen costs. Even the vast majority of those who eventually implement the system and even had got the ISO27001 certification do not have the right security level. The purpose of this research is to identify athe main causes of these challenges and the lack of real security and to define indicators for measuring the readiness of the organization for the successful implementation of ISMS. In fact, by identifying the main reasons for not achieving the goals of Information Security in different organizations, the challenges of organizations in the implementation of this system are identified and after recognizing these challenges, the success key factors for implementation of ISMS will be derived and finally a model for assessing the readiness level will be developed. Thus, the overall structure of this research will be determining the definition of Information Security objectives, identifying challenges and key drivers for successful implementation of ISMS & developing a model to assess & prepare the organization for the successful implementation of ISMS. To fulfill the objectives of this study, some questionnaires were designed which were completed by brain storming and focus groups. For this logic, two panels was needed and their members selected through inertial sampling. The findings of this research are the reasons for the failure to implement ISMS and achieving its goals in different organizations. It is a step that needs to be taken to reduce the challenges and increase the organization's readiness for successful implementation of this system.

Every organization is formed based on its vision and mission which can be translated to its goals. For achieving its goals, required to provide some products or services. To be able to provide its products or services, should define some processes and to be able to run these processes needs different type of assets. However these assets should work together as a whole system and customize according to processes.

So I believe for successful implementation of an information security solution, the Process, People, and Technology model should be changed to Process, Asset, and Configuration model

Keywords: *Information Security objectives, Challenges for implementing Information Security Management System, Key Success Factors for implementing Information Security Management System, Organizational readiness for Information Security Management System implementation*

-

Introduction

In today's world which economy is globalized and threats for organizations are changing every day, the corporate partnerships are internationalized, and online business is conducted; information security plays a role more than a business enabler. Despite the continuous emerging of a variety of standards, tools and new technologies, organizations still face a lot of challenges to meet the upcoming security requirements, economic conditions and risk management. One of the main reasons for not fully implementing ISMS is the lack of readiness of organizations to accept this system. Most of senior executives do not have a proper understanding of the intangible concept of Information Security and the role of Information Security is not clearly defined in the organization, and even in some organizations, Information Security is still seen as a cost. In such organizations, financial management does not consider the cost of providing Information Security as unnecessary, and operational managers consider any activity in the field of Information Security contrary to the interests of the organization. In fact, the definition of security differs from the viewpoint of managers of different units according to their job descriptions. For a finance manager, security is equivalent to reducing financial risks and losses, while for the sales manager, security is preventing the intrusion of anything with the sales plan and the realization of its goals. The legal department sees it as complying with the rules, and the board member thinks that security is doing the right thing by the staff. In many organizations, Information Security is the responsibility of a single entity, and other departments of the organization do not have much to do with this, or there is no connection between the objectives of Information Security and the organization's goals. In order to resolve these issues, the objectives of Information Security in the organization must be defined in a transparent and measurable manner, and the structure and culture in the organization should be institutionalized that supports the security of information and by which each person understands his role in achieving the objectives of Information Security. The lack of indicators for assessing the level of security of information and effectiveness of the cost of its implementing is a serious challenge in determining the effectiveness and, consequently, a desirable implementation of the system.

Statistics in developing countries show that most of the information systems projects are facing a complete or partial failure, or if they are successful in implementing they don’t have the required continuity. A complete failure means failure to complete, and partial implementation failure means failure to achieve the goals. The purpose of this study is to provide a model for preparing organizations to implement ISMS successfully. Obviously, the first step in this area is to identify the problems and challenges of implementation. The most important and most practical study in the field of problems of implementation information based systems is done by Hinks (2002). Hinks has studied this issue in developing countries and has categorized them into seven major categories, known as ITPOMSO. These seven categories are Information, Technology, Process, Goals, Management and Structure, Manpower and Skills, and Other resources, especially financial ones. In the area of identifying the challenges of ISMS implementation, especially in Iranian organizations, a number of research has been carried out, most notably a joint research conducted by the Information Technology Organization in collaboration with Sharif Industrial University and a number of companies implementing and/or operating the ISMS with my partnership. In this research the challenges were identified and categorized as follows:

- Lack of prioritizing security in organization’s goals and ignoring it in the organization’s strategy
- Project-centric look at the ISMS implementation
- Lack of requirement for full implementation of ISMS
- Unwilling to third part audit

- Failure to provide personnel training
- Having this thought that implementation of ISMS will make possible all the impossible in the field of security
- Lack of adequate budget for complete implementation
- Failure to determine who is responsible for deploying the system in the organization
- Lack of specialists in the field of Information Security
- Lack of identification of individuals dedicated to the implementation of ISMS
- Lack of cooperation and coordination between involved units in the organization
- Tool-orientation vision versus goal-oriented vision and focusing on methods rather than results
- Inappropriate organization of the project
- Inappropriate definition of the domain of the project
- Inappropriate estimate of time and cost of the project
- Reducing ISMS concept to Network Security project
- Contractor misconceptions about the organization's implementation goals
- Immaturity of Information Technology in the organization

In another research conducted by Sayed Hossein Siadat and Niaz Saghafi, challenges for the implementation of the Information Security Management System, is classified as follows:

- Defining the project
  - Organizational maturity
  - Drafting of the goals of Information Security
  - The accurate recognition of security requirements and their mapping with the results of ISMS implementation
  - Determination the domain to be deployed
  - Understanding that security is not cost
- Senior Management
  - A sufficient knowledge of the Information Security Management System
  - Allocation of resources
  - The desire and necessary co-operation
  - Choosing competent people and supporting them at all stages of deployment
- Consultant selection
  - Documentation of expectations, needs and services requested
  - Accurate understanding of the performance of consulting firms
  - Co-operation with the consultant
- Responsibilities and duties
  - Selecting individuals and delegate tasks
  - Definition of responsibilities
  - Training and awareness
- Executive issues
  - Allocation of resources
  - Insurance services
  - Conclusion SLA
  - Holding meetings

Other issues mentioned as a challenge in this research are:

- Non-commitment of top management of the organization to Information Security
- Lack of familiarity of personnel with the mission of the organization

- Non-commitment of personnel to improve the organization's position
- Failure to provide an overview of the ISMS project and its implementation requirements to the personnel of the organization
- Denial of Information Security and ISMS as one of the main factors in promoting the organization in a competitive environment
- Lack of ongoing awareness-raising in the area of Information Security
- Sophisticated and rigorous design of Information Security Management System

Amirhoushang Tajfar, Mohammad Mahmoudi Meymand, Fatemeh Reza Soltani and Pouria Reza Soltani in their article "Ranking barriers to implement Information Security Management System and assessing readiness of Exploration Management Co." in Journal of Information Technology Management, Vol. 6, No. 4, Winter 2014, on pages 551- 556, the main reasons for failing to implement ISMS are as shown in Figure 1.

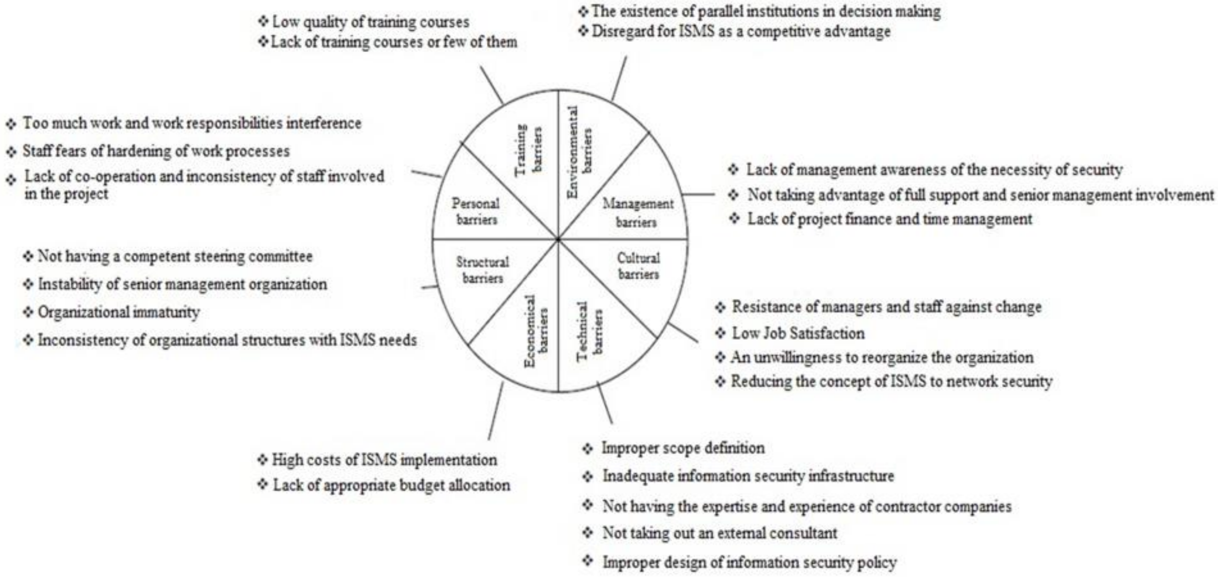
❖ Low quality of training courses
❖ Lack of training courses or few of them
❖ The existence of parallel institutions in decision making
❖ Disregard for ISMS as a competitive advantage
❖ Too much work and work responsibilities interference
❖ Staff fears of hardening of work processes
❖ Lack of co-operation and inconsistency of staff involved in the project
Training barriers
Environmental barriers
Personal barriers
Management barriers
❖ Lack of management awareness of the necessity of security
❖ Not taking advantage of full support and senior management involvement
❖ Lack of project finance and time management
Structural barriers
Cultural barriers
❖ Not having a competent steering committee
❖ Instability of senior management organization
❖ Organizational immaturity
❖ Inconsistency of organizational structures with ISMS needs
Economical barriers
Technical barriers
❖ Resistance of managers and staff against change
❖ Low Job Satisfaction
❖ An unwillingness to reorganize the organization
❖ Reducing the concept of ISMS to network security
❖ High costs of ISMS implementation
❖ Lack of appropriate budget allocation
❖ Improper scope definition
❖ Inadequate information security infrastructure
❖ Not having the expertise and experience of contractor companies
❖ Not taking out an external consultant
❖ Improper design of information security policy

Figure 1. Barriers to Implementation of Information Security Management System and Investigating Readiness of Exploration Management Co.

Also, in an article on the modern banking site http://modernbanking.ir on 22/7/1392 entitled "Challenges to Implementing Information Security Management System", the following points are noted:

- Management problems such as instability of senior and middle managers
- Staff problems such as lack of awareness, lack of experts, user resistance to change, and lack of effective communication.
- Organizational problems such as organizational immaturity, organizational change, lack of appropriate consultant, lack of trust in Information Security in the organization, lack of appropriate funding
- Technical problems such as the lack of appropriate development model with the view of Information Technology
- Tender problems such as mismatching the needs of the employer and suggestions provided by the executives

Research method

In this research, library studies, articles and websites that are valid and relevant are used to gather information in all areas of the study. The data gathering tool was questionnaires. After verifying its validity and reliability, it was distributed and collected among experts. Initially, the goals of the organizations are identified by the implementation of the Information Security Management System and their indicators in defining the desired level of security. To do this, a specific questionnaire is designed. Subsequently, using another questionnaire, the challenges faced by executives and employers in implementation of ISMS, are identified. The questions of this questionnaire are based on the summing up of the challenges presented in the introduction part of this paper as well as through the risk analysis of existing implementation methodologies. After completing the list of challenges, the next step is to identify the Critical Success Factors (CSF) of ISMS implementing. In order to complete the aforementioned questionnaires, the brain storming and creation of focus groups has been used and for this purpose, two panels has been predicted and panel members have been selected through inaccurate sampling. Members are not likely to be selected in this sampling, and therefore do not represent a specific community. In this case, the members are selected in order to apply their knowledge in a specific problem based on the criteria that originated from the nature of the subject and the research questions. One of the methods used in this field is targeted or judgmental sampling. The people who were nominated for Panel 1 had one of the following specifications:

- Being the project manager of one of the companies which have NAMA certification in the field of ISMS implementation with experience of management of at least three ISMS projects implementation.
- Being the Information Security project manager in one of the organizations that fully implemented the Information Security Management System.

The nominees appeared in Panel 2 to be the organizational security manager of companies whose organization has one of the following specifications:

- Being implementing the Information Security Management System.
- Already implemented Information Security Management System.

In order to identify members of Panel 1, I used the list of NAMA licensed companies and also organizations in different industries which has already implemented ISMS in their organizations. For the members of this panel, the challenges questionnaire was sent and, in order to complete the list of challenges, they were asked to insert any other challenges they have faced and not mentioned in the list. Obviously, the first step for the proper implementation of the Information Security Management System in each organization is to determine the goals and define the optimal security level for that organization. In order to investigate this in target organizations, the questionnaire with the title of the objectives, along with its supplementary forms, was made available to Panel 2 members. In this questionnaire, four questions have been asked, and its purpose is to assess the quality of defining goals and optimal security level in this organizations. In the next stage, based on the analysis of the results of the implementation challenges, the critical success factors in the implementation of the Information Security Management System were obtained. As mentioned, the statistical community of this research is some of the experts and managers of Iranian organizations who, due to security considerations, cannot refer to their names or industries, and the main tool of this research is the questionnaire and its completion through the Delphi method. Delphi's validity and reliability control is not easy (Chase and Bryan, 1998, quoted by Mortezania, 1391). Although Delphi users have confirmed the correctness of the technique (Oakley and Pawski, 2004), they criticized the validity of this technique. However, if the members participating in the research are representative of the group or field of knowledge, content validity is guaranteed (Trop & Lewiston, 2005). The Kendall Coordination coefficient is a measure to determine the degree of coordination and agreement between several rank categories related to an object or person. In fact, with the application of this scale, the correlation between the ranks K can be found. Such a scale is particularly useful in studies of narrative between judges. The Kendall Coordination coefficient shows that individuals who have arranged a few categories based on their importance essentially apply similar criteria for judging the importance of each of the categories and agree in this respect. The value of this scale, in coordination with the full agreement, is equal to one, and in the absence of full coordination, the zero is equal. Schmitt provides two statistical measures for deciding whether to stop with Delphi's continuation. The first criterion is a strong consensus between members of the panel, which is determined by the amount of Kendall coordination coefficient. In the absence of such a consensus, the persistence of this coefficient or its negligible growth over the consecutive period indicates that there has been no increase in the agreement of the members and the polling process should be stopped.

Findings

By analyzing the information obtained from the questionnaires, it was found that in the vast majority of the organizations of the target population:

- The goals of Information Security implementation according to the organization's business goals, have not been defined and documented.
- No significant upstream and downstream requirements have been identified in determining the goals of Information Security.
- Information Security measurable objectives and indicators for measuring them are not defined.

Based on the results of the evaluation, the main challenges that cause the lack of successful implementation of ISMS in different organizations are identified and classified as follows:

Information:

- Required information or individuals are not available for obtaining information.
- The list of products and/or services of organization is not provided.
- The processes of the organization have not been documented and the process map has not been prepared.
- Relationship between processes and goals is not defined.
- Organization’s stakeholders are not identified.
- There is no information or documentation about the organization's information security requirements or obligations that have been communicated or contracted in the upstream mandates, or the relevant audiences have not been identified for obtaining information.
- There is no information or documentation about training courses provided by staff, or the relevant audience has not been identified for obtaining information.
- There is no information or documentation on the types of information assets, including the documentation and types of electronic media containing information, or the relevant audience has not been identified for obtaining information.
- There is no information or documentation on human assets including personnel, contractors, suppliers, consultants and customers of the organization and its various units, or the relevant audiences have not been identified for obtaining information.
- Information or documentation on infrastructure services including emergency power system, ventilation system, various notification and disaster management systems, telephone system, WAN connections, Internet communications, monitoring systems, traffic control system, physical network connections including all relevant communications and communication environments, The logical layout of the network including the definition of areas, virtual networks (VLANs), the protocols used, or the relevant audience are not specified for obtaining information.

- Information or documentation on hardware assets, including network and communication equipment, security equipment, servers, including hardware specifications and services provided by them, workstations including hardware specifications and usage, data storage equipment, office equipment types or the relevant audience are not specified for obtaining information.
- Information or documentation on software assets, including applications, databases, operating systems used, and other software, usable protocols, or the relevant audience are not specified for obtaining information.
- There is no information or documentation about intangible assets such as passwords or the relevant contacts are not specified for obtaining information.

Culture and organizational maturity

- There is no background and organizational culture about information security.
- Senior management does not have adequate knowledge of the information security management system and is not aware of the need to implement information security.
- Managers and personnel consider ISMS deployment to be a regular and regular process.
- There is no common understanding of environment between the IT and other business units.
- IT values are not accepted by other units of the organization.
- Projects in the organization are not prioritized.
- None of the information security standards or related standards have been implemented in the organization.
- IT personnel do not understand the duties of personnel of other units of the organization.
- Personnel of other units of the organization do not understand the duties of IT personnel.
- Information technology has not played an important role in the development, growth, and usefulness of business.
- IT staff do not know the organization's business and do not speak the business language.
- Information technology does not play a role in designing a business strategy.
- Other entities do not play a role in the design of IT strategy.
- Risks and rewards are not shared among the various organizational units.
- Participatory programs in the organization are not effective.
- IT budget is not targeted.
- The amount of information technology participation has been low in terms of quality, production, and profitability of the business.
- Personnel are not familiar with the mission of the organization.
- Personnel resist change.

Process:

- A reasonable estimate of the time and cost of the project is not made.
- The scope of the projects is not set properly.
- Choosing the contractor is not done properly.
- The methodology and method for implementing information security and standards used do not support the organization's security objectives.
- The professional courses are not held or are of low quality.
- There is no co-ordination between the various components of the organization in implementing projects.
- Before the project starts, training is not provided to the personnel of the organization.
- The necessary training is not provided to project executive units.

- How to determine and allocate the budget of each project is not appropriate for the project's implementation goals.
- Knowledge management and internal and inter-organizational knowledge management structures have not been developed.
- Rules for communication between IT and other units of the organization have not been established.
- An internal and external environment analysis has not been performed and the risks are not specified.
- The service request process from the IT department has not been documented.
- The process of requesting services or information from other units of the organization by the IT department has not been documented.
- Organizational learning is not normal at the organization level.
- Performance and success rate of projects are not evaluated.
- The project management process is not improved on the basis of experience gained in previous projects.
- Skills do not increase through in-service training, job rotation, and job change.
- IT personnel are not properly recruited.

Goals and strategy:

- The organization's vision, mission, and strategy are not documented.
- The goals and objectives of the organization are not documented.
- The information security management system has not been seen as one of the main factors in promoting an organization in a competitive environment in the outlook.
- The implementation of the security management system has not been documented in the goals and strategy.
- The full implementation of the information security management system is not considered.
- Third-party auditing is not considered.
- Looking at the implementation of the ISMS as project-oriented.
- No measurable targeting of information security has been done.
- Implementation of the information security management system has not been a priority.

Management:

- The top management of the organization is volatile and varied.
- Senior management does not cooperate with the CIOs.
- Managing investment in IT is not done properly.
- The unit or units responsible for establishing the information security management system are not specified.
- The contacts and the executive team have not been identified for the implementation of the information security management system based on the methodology and selective standards.
- Individuals are not qualified to implement or support the selected system at all stages of deployment.
- The necessary authority is not delegated to the responsible project components.
- The various responsibilities of people are not defined or communicated to them.
- Managing an overview of the information security project and the need to implement it for the personnel of the organization.
- The necessary support from the top management of the organization is not implemented to implement information security.

- The board does not attend the meetings of the security committee and does not interact with the security team.
- No action is required to co-ordinate between the units involved in the project.
- There are a lot of changes in the technology used or the organizational structure or location of the organization occurs during the implementation of the project.
- There are parallel institutions in decision making.
- There is no co-operation and coordination between the involved units.
- Senior management has not taken any action regarding awareness of the importance of information security.
- There are no proper steps to justify the contacts and the executive team to implement the system properly.

Organizational Structure, Manpower and Skills:

- Information technology does not have an adequate organizational structure.
- Information technology in the organizational structure is not well-positioned.
- Information security structure is not formed in the organization.
- Persons assigned to the implementation of the information security management system in the organization are not or have not been obliged to cooperate with this project.
- There is not enough staffing expertise in the field of information security in the organization.
- The meetings of the Information Security Committee have not been organized regularly and have not been effective.
- Job satisfaction is low.
- Employees are more afraid of working processes.
- IT staff do not have the skills needed to be effective.
- Exit IT staff is high.
- Satisfaction of users with the services and responsiveness of IT experts is low.

Discussion & Conclusion

This section is presented in three parts, which are determining the steps required to prepare the organization, defining the objectives of information security and developing a model for assessing the level of readiness.

Determine the steps required to prepare the organization

Some organizational problems in the successful implementation of the information security management system are related to the stage of project definition and selection of consultant. Major problems in this stage are as follows:

- No targeting and designation of project success factors and how to measure them
- Lack of a process-centric look into the Information Security Management System
- Unwillingness to fully implement the Information Security Management System
- Unwillingness to third party audit
- Improper estimation of time and cost of the project
- Inappropriate definition of the project domain
- Inappropriate contractor selection factors
- Use of undesirable methodology due to security goals
- Failure to identify and justify the project team and contacts and their tasks

Therefore, it is necessary to do the followings to solve above mentioned problems:

- Determine the security objectives before starting the project
- Having a process-centric look at the implementation of the Information Security Management System
- Full implementation of Information Security Management System
- Perform third party audit
- Estimate the correct time and cost required for a complete implementation and achieving security objectives
- Establish balance between the information security budget and implementation goals
- Properly define the scope and boundaries of the project based on security goals
- Do not limit the concept of information security to network security
- Identify the appropriate indicators for contractor selection
- Sufficiently justify the contractor about the organization's goals in implementing ISMS
- Have purposefulness and attention to results
- Choose a methodology to implement information security appropriately and in line with the desired goals
- Assess potential challenges faced with the implementing the information security system based on the requirements of the chosen methodology and selected standards.
- Take actions to resolve the addressed potential challenges of implementation
- Identify contacts and executive team in charge of implementing the Information Security Management System based on the chosen methodology and selective standards.
- Determine the responsibilities of different organization’s units in charge of implementing the Information Security Management System
- Identify the required documentation or individuals in the organization for providing information to the contractor
- Take the necessary steps to justify the contacts and executive team in order to properly implement the ISMS

Also, based on the findings of the previous section, the steps required to prepare the organization are as follows:

- Make any necessary changes to the technology used or the organizational structure or location of the organization before starting the project and ensure there is no fundamental change in organization and its structures during project
- Justify senior management about the need to implement ISMS and prioritize it in goals and strategy of the organization
- Justify senior management about his obligations in implementing ISMS and the need for full support
- Have senior management force executives to implement ISMS based on organizational priorities
- Provide personnel of all levels with initial training courses before starting the project
- Have senior management inform all personnel about the importance of ISMS implementation
- Promote information security culture of the organization
- Build information security structures into the organization
- Train necessary specialists in the field of information security
- Determine the unit or units responsible for deploying ISMS
- Establish cooperation and coordination among involved units
- Familiarize personnel of business units with the environment and tasks of the IT department
- Familiarize IT personnel with the environment and responsibilities of other business units

- Develop and document the process of requesting services from the IT department
- Develop and document the process of requesting services or information from other units of the organization
- Develop knowledge management structures and create interpersonal learning
- Establish rules for effective communication between the IT department and other units of the organization
- Familiarize other units of the organization with the values of the IT department
- Modify the organizational structure of information technology in accordance with the description and volume of tasks
- Promote the status of information technology in an organizational structure
- Hold Information Security Committee meetings effectively on a regular basis
- Have the board attend in some meetings of the Security Committee and interact with the security group
- Prioritize organization projects
- Improve the project management process based on the experience gained in previous projects
- Identify indicators and evaluate performance and success rate of projects
- Allocate Separate and reasonable budget to information security management
- Enhance the role of IT in the development, growth, and business benefits
- Increase the amount of information technology participation in production quality
- Enhance the role of IT in designing business strategy
- Increase the role of other organizations in designing IT strategies
- Improve IT staff competencies for higher effectiveness
- Create synergies between IT staff and business
- Unify the values of information technology and organization
- Share risks and rewards between different organizational units
- Improve the effectiveness of participatory programs in the organization
- Improve investment management in information technology
- Increasing staff skills through in-service training and job rotation and job change
- Improve the IT personnel recruitment process
- Apply strategies to maintain IT personnel
- Improve user satisfaction with the services and accountability of IT experts
- Improve the quality of existing information technologies and systems and software
- Implement Information Technology Standards
- Integrate various IT architectures
- Improve the level of flexibility and transparency of IT infrastructure.
- Improve management of new technologies
- Document the vision, mission and strategy of the organization
- Analyze the internal and external environment and determine the risks of each
- Document goals of the organization and its various units
- Document objectives of the organization and the its various units
- Document the organizational structure of the entire organization and its various units
- Document tasks of personnel of different organizational units
- Document business services and/or products offered by organizations and its various units
- Document organization processes and process mapping
- Define the relationship between the organization's processes and goals
- Define the relationship between goals of the organization and the objectives of the units

- Document various stakeholders of the organization
- Document requirements and obligations in the field of information security that are communicated to the upstream authorities or contracted
- Document personnel training records
- Identify and document various types of assets, including, but not limited to, documents, electronic media containing information, personnel, contractors, suppliers and consultants, customers of the organization and its various units, emergency power system, ventilation system, various notification systems and disaster prevention, system Telecommunication, WAN connections, Internet communications, monitoring system, traffic control system, network equipment and communications, security equipment, servers including hardware specifications and services provided by them, workstations including hardware and user specifications, information storage equipment, Office hardware, applications and other software, racks and layout of equipment within them, protocols used, users and their levels of access to various information and assets, infrastructure services and their identification, network addressing scheme, physical connections of the network, including all communications and communication environments. The corresponding logic scheme of the network includes area definition, virtual network (VLAN), protocols used, and intangible assets.

Hence, in order to resolve the preparation challenges and project definition issues, the following supportive and management processes needed to be executed before ISMS implementation:

- Knowledge management
- Create strategic vision including:
  - Defining goals and business strategies
  - Setting the goals of information security
  - Analyzing internal and external environment
- Education and awareness include:
  - Holding training courses for personnel
  - Implementation of awareness programs and culture
- Establishing information security structures
- Increasing the level of information technology maturity
- Process management
- Project management
- Documentation management
- Documentation of assets
- Archive management
- Services management
- Preparation for implementation of information security management including:
  - Scope definition
  - Estimating time and cost in line with the goals set
  - Identification of contractor selection criteria
  - Executive team and their duties determination and justification

Determine the objectives of information security

Determining the objectives and definition of optimal security level in a measurable manner is necessary for all organization and without that, it is impossible to assess the information security level and measure the effectiveness of the implementation of the information security management system, and the lack of this item is obvious in all organization studied in this research. Therefore, the first step in preparing the organization in order to ensure optimal security, is to determine the objectives of information security comprehensively (Detmar Straub and Richard Welke, 1998; Johnston and Hale, 2007) And a desirable security plan should fit in with the goals, resources and environment of the organization (Straub and Welke, 1998; Siponen, 2000). In a study done by Qingxiong Ma, Allen C. Johnston, and J. Michael Pearson, the goals and actions taken by 354 managers from different organizations and the relationship between goals and actions have been analyzed. As a result of this research, the four main goals of most of organizations are Integrity, Confidentiality, Availability and Accountability and accountability towards it, have been the key goals of the information security of most organizations, confidentiality has had the most relation with security actions done. However, in most references and standards, the three main objectives of the information security management system are to preserve confidentiality, integrity and availability of information. After defining the goals of information security, they should be turned into measurable objectives. As stated, the main security goal of all organizations is to reduce information security incidents that will be achieved by maintaining confidentiality, integrity and availability of information. It is important to set indicators for this purpose, both measurable and relevant to the organization's business goals. Given the correlation between the occurrence of information security incidents and the degree of risk, the risk number can be a good indicator for this. It is clear that the higher the risk to the assets of an organization, the more the incidence of security incidents, and of course the number of security incidents has direct relation with the number of asset’s vulnerabilities. Therefore, realizing the goals of information security depends on addressing the weaknesses and vulnerabilities of different assets and, in principle, organizations can use the four main strategies for this purpose:

- Risk management through vulnerabilities identification like penetration testing
- Risk management through hardening based on recommendations from product manufacturers like Cisco ISE
- Information security processes implementation like ISM3
- Information security controls implementation like ISO27001

Therefore, the goals of information security in each organization should be addressed by the business goals. Occurrence of information security incidents will reduce the security objectives achievement and the degree of risk facing to organization is directly related to the incidence of events and number of vulnerabilities of the organization determines the degree of risk to the organization and finally with using the four strategies mentioned above can reduce vulnerabilities and realize business goals. In Figure 2, the relationship between business goals and security is shown.

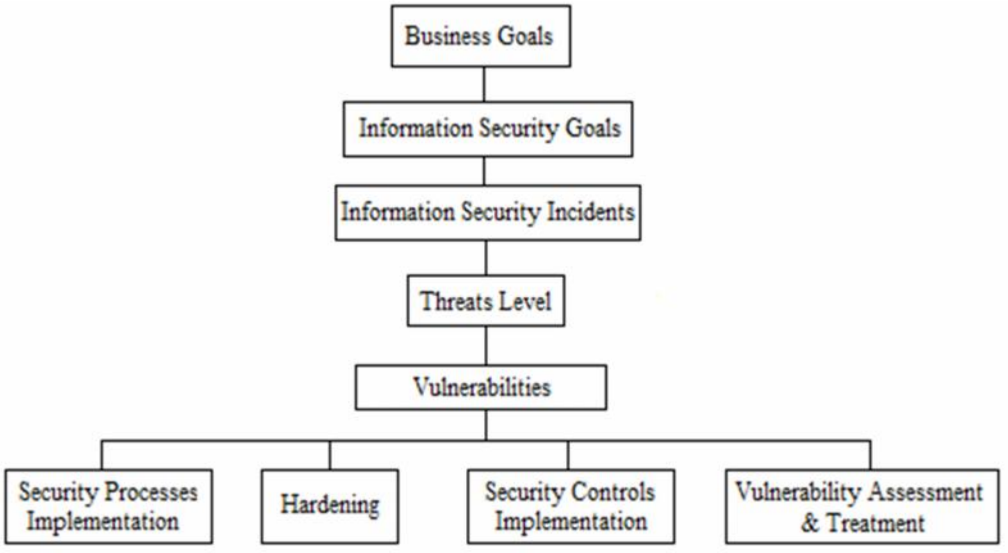
Business Goals
Information Security Goals
Information Security Incidents
Threats Level
Vulnerabilities
Security Processes Implementation
Hardening
Security Controls Implementation
Vulnerability Assessment & Treatment

Figure 2. Relation between business goals and security

Different business organizations are divided into two main categories of manufacturing and service. These organizations provide products or services to fulfill their business goals and require processes to deliver these products or services. The implementation of these processes requires the availability of assets of various types of hardware, software, human, physical, etc., and always the events recognize the desirable performance of these assets and, consequently, the implementation of processes and the realization of commercial goals.

In the event of applying controls or security processes or managing hazards, it can reduce the incidence of these incidents and make it possible to achieve business goals. On the other hand, these three indicators can be used to define the purposes of information security. In fact, the business objectives and organization's information security goals are based on the three indicators of the level of information security controls, the level of information security processes and the level of hazards that can be defined and interconnected. Figure 3 shows the relationship between business goals and the objectives of information security.

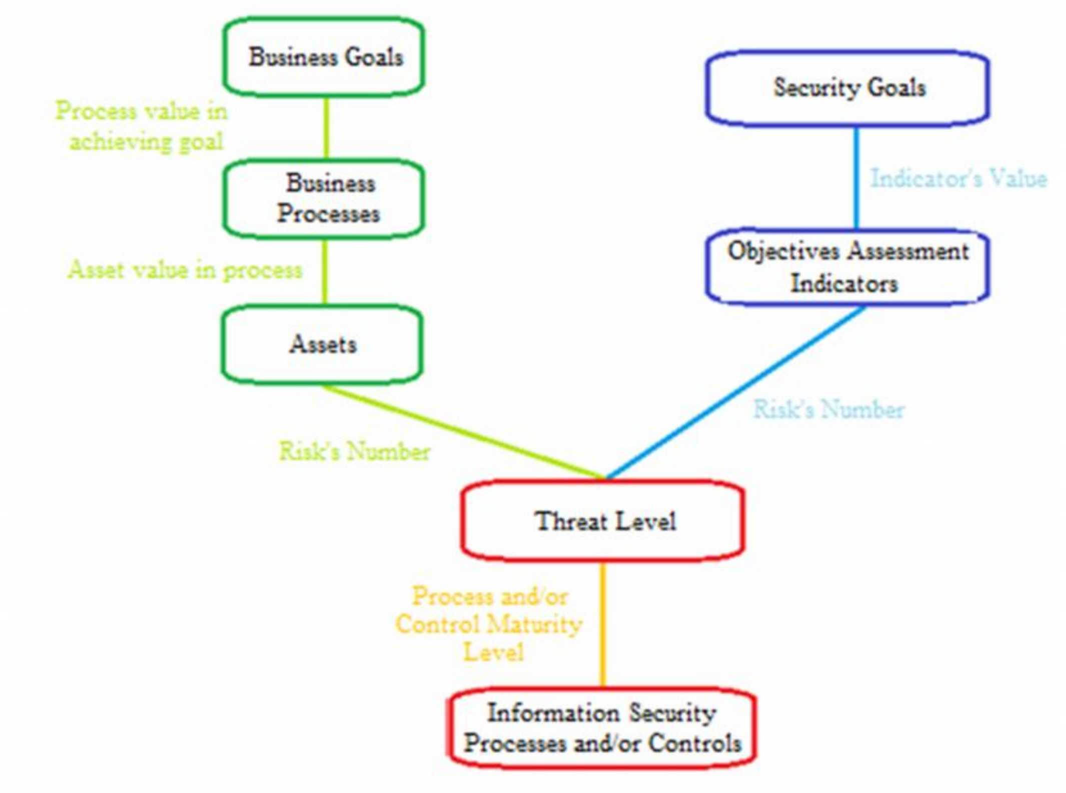
Business Goals
Process value in achieving goal
Business Processes
Asset value in process
Assets
Risk's Number
Security Goals
Indicator's Value
Objectives Assessment Indicators
Risk's Number
Threat Level
Process and/or Control Maturity Level
Information Security Processes and/or Controls

Figure 3. Relation between business and security goals

For example, if one of the organization's business goals is to increase the production of one product at n percent, we call it the G1 target, and P1 and P2 processes must be executed for the production of this product, and the implementation of these processes depends on the availability of assets A1, A2, A3 And A4, and this is not achieved due to the occurrence of R1 and R2 hazards occurring on these assets, then if the level of maturity of controls and information security processes and the level of risk associated with these assets are improved by n% Goal G1 will be realized. Therefore, security targeting in this example will improve the level of maturity of controls and information security processes and the degree of risk associated with these assets by n%.

Developing Readiness Assessment Model

The level of readiness is determined by the status of the organization in each of the six categories of information existence, the level of culture and organizational maturity, the status of processes, the status of defining objectives and strategy, management status, organizational structure, manpower and skills status. The number of evaluation indicators and its weight for each class is in accordance with Table 1.

Table 1. Readiness indicators classification

Category	No. of Indicators	Weight
Information Existence	13	14.9
Culture and Organization’s Maturity Level	18	20.7
Processes Status	20	22.0
Objectives & Strategy Definition Status	9	10.3
Management Status	17	19.5
Organizational Structure, Manpower and Skills	11	12.6

CRn: Category n readiness in percent
K: Number of categories
PFn: Indicators with positive situation
TFn: Category n total number of indicators
Wn: Category n weight
TR: Total readiness in percent

The percentage of readiness for each class is equal to the product of the number of indexes with the positive state of that class divided by the number of indexes of that class multiplied by 100.

$$CRn = PFn/TFn * 100 \tag{1}$$

And the overall readiness of the organization is equal to the sum of the total score of the level of readiness of each class in the weight of that class divided by 100.

$$TR = \sum_{n=1}^{k} C\quad W\quad /100 \tag{2}$$

References

زارعی، بهروز و ثقفی، فاطمه، تاثیر آمادگی الکترونیکی بر پیاده‌سازی پروژه‌های IT در بانک تجارت ایران

سیادت، سید حسین و ثقفی، نیاز، شناسایی چالشهاي پیاده سازي سیستم مدیریت امنیت اطلاعات در سازمان

تاج فر ، امیرهوشنگ و محمودي میمند، ﷴ و رضاسلطاني، فاطمه و رضاسلطاني، پوريا ، رتبه بندي موانع پیاده سازي سیستم مدیریت امنیت اطلاعات و بررسي میزان آمادگي مدیریت اکتشاف، مجله مدیریت فناوری اطلاعات، دورة 6، شمارة 4 زمستان 1393، 556-551

Basie von Solmsa, and Rossouw von Solmsb, The 10 deadly sins of information security management

Heru Susanto and Mohammad Nabil Almunawar and Yong Chee Tuan, Information Security Challenge and Breaches: Novelty Approach on Measuring ISO 27001 Readiness Level, International Journal of Engineering and Technology Volume 2 No. 1, January, 2012