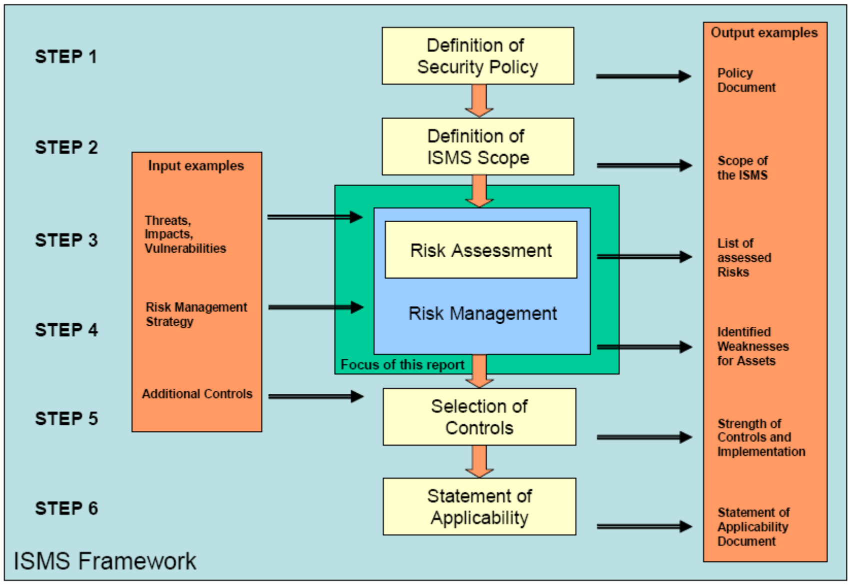
Information is valuable and important for organization, like other business assets. Maintaining the confidentiality, authenticity and availability of information in an appropriate measurable level must ensure. Along with the rapid growth of using network and Internet, Security is a major concern of worldwide organizations. Information security is a very hot topic of today’s networks and with the increase in Internet connections and implementation of large volumes of business operations, made this topic crucial important. Electronic information is the companies’ main resources to achieve their business objectives. The use of computer networks, especially the internet has fundamentally changed the business interactions. While these conditions have created many advantages and put the information in the distance of your few clicks, however they have brought the risk of disclosure and information loss.

As a matter of fact, the cases which were the corporate excellence points in delivery of services, now changes to their vulnerabilities to attack by the opportunistic and individual’s jobber. In such circumstances, any organization requires ISMS. Acceptance of ISMS should be a strategic decision in any company. Security in producing software process is not limited to the relevant units and software assets, in other words, the security should be a comprehensive and action-oriented. For this purpose, several standards have been provided. Designing and implementing information security management system in any organization is influenced by needs and objectives, security requirements, applied processes, size and structure of organization. ISO27001 standard provided for creating, establishing, implementing, operating, monitoring, reviewing, maintaining and improving information security management system which have a Process-oriented perspective.

The process-oriented perspective that submitted in this international standard makes the user consider the following cases:

- Understand the organization’s information security requirements and necessity of establishing policy and related objectives.
- Implementation and execution of controls for information security risks management.
- Monitoring and reviewing the performance and effectiveness of information security management system.
- Continuous improvement based on measurement objectives

According to ISO27001 standard, following regulations can be defined:



There are 5 fundamental approaches to security analysis and immunization organization and removing the risks which include:

- Control approach such as ISO27001 standard.
- Process approach such as ISM3.
- Approach based on risk management –such as ISO27005 standard.
- The approach which based on the products manufactures security recommendations such as “MS Baseline Security Analyzer”.
- The approach which based on best practices.

Developed methodology by the Terminus System, provides the best level of possible security for your organization using the combination of all these approaches. The unique structure of this methodology is based on four main phases of design, implementation, monitoring and improving the Deming Cycle and includes the following 23 steps:

Phase Zero: Project Management

The first condition for being successful in any project is to define it properly. For this reason, extensive research have done on implementing Information Security Management System challenges in Iranian organizations according to these researches, The reasons for the failure of information security projects include:

Challenges due to wrong assumptions and paradigms

- The concept of implementing ISMS is a systematic linear process
- Lack of priority of security in organization
- View of project-based to ISMS
- Lack of requirement to implement the ISMS
- Background and Organizational Culture
- Unwillingness to implement audit
- Lack of necessary training to staff
- Imagination of how ISMS makes the impossible possible

Challenges due to implementing environment

- Lack of sufficient budget allocation for implementing ISMS
- Lack of reaching to security organizational maturity
- Lack of reaching to necessary infrastructure for implementing ISMS
- Lack of experts in the field of information security in organization
- Contractor wrong impression of organization objectives for implementing ISMS

Emerging challenges in process

- Ignoring ISMS in organization strategy
- Failure of determining someone to take the responsibility for implementing ISMS
- Lack of coordination and cooperation of involved departments in the project
- Wrong implementation of PDCA Cycle
- Describing instead of deepening

Challenges due to project management and technology

- Failure of determining specific individuals for implementing ISMS in the organization
- Tool-oriented versus pivotal question
- Poor organizing the project
- Poor scope definition
- Underestimated the cost and time
- Reducing the concept of ISMS to network security project
- Focusing on procedures rather than outcomes

As matter of fact, preparation of organization for acceptance and implementation of this system is an important fact in project success. A questionnaire has been provided to identify the preparation level of organization for acceptance and implementation ISMS. After completing this questionnaire, probable challenges of implementing in organization is determined and according to it the appropriate project management structure is presented.

In this structure, project management regulation PMBOK combined with ISO27001 standard and developed the following model:

Early coordination

This stage has two parts, first referrals and development of project management structure.

Referrals mutual acquaintance

In inaugural session the following options discuss:

- Introducing the owner, the executive team and a person who in charge of it and project beneficiaries in organization.
- Introducing the manager, the executive team and considered specialties
- Describing the objectives, methodology of this work and the standards, we use.
- Determining facilities
- Developing a commitment to non-disclosure
- Determining audience of training programs and seminars during implementing
- Developing to follow up implementing provisions of the contract
- Determining and managing required resources (human, time, …)

Developing project management structures

After inaugural session and determining mutual the executive teams, project management document shall be ultimate which includes the following components:

- Project implementation chart
- Determining component duties of chart
- Communication plan
- Documentation plan
- Ensuring and quality control plan
- Completing and delivery of the project plan
- Determining project implementation risks and coping strategies
- Problem solving plan

The First Phase: Designing

This phase is a base of implementing Information Security Management System (ISMS) and includes more than 50% weight of this project. This phase includes different steps which are as follows:

The First Step: Implementing initial training programs

To create the best interaction between your executive team and the organization and also necessary coordination and exchanging ideas, the following initial training programs presented:

- Concepts of information security
- Implementation procedure
- Determining objectives and effectiveness
- Internal audit

The Second Step: Understanding organization

In this step organization are identified and documented by the following aspects:

- The organizational structure
- Mission and mid-time measurable goals
- Processes
- Services/ products
- Beneficiaries
- Requirements and commitments

The Third Step: Developing Organization information security structure

In this step the existing information security structures of organization, their components and duties description is identified and documented, then the wackiness points of this structure determined and the desired structure offered.

The Forth Step: Defining project scope

This is one of the most important and essential parts of the project which determines the project scope.

For this reason, enough recognition of organizational structure and the way they distribute on departments and different geographical regions is needed. Determining included components of the plan are mentioned below, is required in determination of scope:

- Business profile
- Organizational Units
- Departments
- Type of assets
- Technology
- Exceptions

The Fifth Step: Asset management

This stage has two parts, Census assets and their valuation.

Census assets

In this step list of assets is provided. Assets are divided to main categories, units (safe areas) such as sites, datacenter or server rooms, hardware such as switches and routers, software such as applications and operating system, information such as documents and office appliances, human resource such as staff, customers and services such as telephone and network systems.

Asset Evaluation

After compiling a list of assets should be valued. Criteria of this valuing is the level of importance and impact on the business cycle and to achieve the goals of organization.

The Sixth Step: Reviewing the current status and gap analysis

This step has two parts: review of current situation and gap analysis.

Review of current situation:

In the present situation, the current status of information security based on implementation of controls ISO / IEC 27001, maturity levels ISM3, should be determined.

Gap analysis:

Compare the current security situation and the relevant standards with gap analysis of organization.

The Seventh Step: Risk Assessment

This stage includes risk analysis, risk identification; identifying threats and vulnerabilities for various assets.

Develop methods for risk analysis:

After identifying and valuing their assets, identifying risks is a mandatory part of implementing the Information Security Management System. This section identifies methods and Risk Assessments based on methodologies of qualitative and quantitative and ISO27005 standards are developed.

Asset risk identification:

At this point, the list of risks for each type of asset being acquired. METT methodology is a way to do.

Identify security threats to assets:

After identifying the risks of each asset, Identifying security threats that may lead to the risk will be carried.

Determining the vulnerability of assets:

Determination of the Vulnerabilities that risk using it becomes threats. Determining vulnerabilities in network is executed by penetration test. Penetration testing is Simulation methods that disruptors for unauthorized access to network resources and systems are used in an organization.

The Eight Step: Risk Management

This step including acceptance level of risk and provide solutions to cope with various risks.

Acceptance level of Risk:

In this section, the level of acceptable risk is Determined based on 3 parameters asset value, risk probability and the consequences.

Technical strategies to deal with risks:

At this point, a solution is presented to deal with the risk and Security plan includes hardware, software, schematic connections and how to configure them is the ultimate.

The Ninth Step: Compiling the applicable Statement

At this stage, to provide a system solution

Determine necessary controls and developing applicable Statement

In this part among the 113-fold controls the necessary and implemented controls are selected.

The Tenth Step: Compilation Security policies

At this stage in order to provide a systematic approach to deal with security risks, Security policies need to be developed. These policies include:

- Access policies Explains Permissions and access levels and different individuals.
- Operational Policies Defines the responsibilities of users, operational staff and management. In this policy the ability to monitor security policies must be defined and recommendations for how to report the problem should be predicted.
- Identifying policies which deal with users' identification when they enter to the network which includes passwords and user names.
- Recommendations for how to purchase equipment security systems.
- Recommendations for security hardware and accessories.
- Recommendations for access controlling to information and resources.
- Recommendations for processing data and documentation.
- Recommendations for purchase and maintenance of commercial software.
- Recommendations for dealing with electronic crime.
- Recommendations for Physical and perimeter security.
- Recommendations for the development of internal software and related codes.
- Recommendations for personnel security.

The Step Eleventh step: Develop instructions and procedures

Security regulations are defined to enforce security policies. Regulations define Security mechanisms adjustments, how to enter to network and monitoring of safety issues. These regulations must be written down for network administrators, users and security managers. In this regulation the way they should face with security threats is determined.

The Twelfth Step: Compilation disaster mitigation plan

In the structure of Security must plan for disaster mitigation and accurate definition of the duties and responsibilities of security personnel in the different conditions in each group.

The Thirteenth Step: Compilation educational programs and information

Definition of informing and training program at different levels is the output of this stage. A factor in information security and the continuation is staff awareness of rights, tasks, responsibilities and accountability in the field of information security program plays an important role, a significant portion of corporate security policies is dedicated role of personnel to provide information security. In the information security plans, the forms and executive procedures required for the implementation of plans which should be predicted; On the other hand, it is necessary that the information security group have knowledge of information security and also has the ability to deal with risks.

The Fourteenth Step: Determine Goals and Effectiveness

In order to measure success in implementing Information Security Management System, the goals and methods of measurement should be determined. In this way, the effectiveness of this system and the concept of security is an intangible concept which is measurable.

The Fifteenth Step: Developing a security policy

The statement of the security policy in terms of the following content is developed:

- Determine goals and overall understanding of the course
- Legal requirements, regulations and security obligations
- The provision of risk management
- Risk assessment criteria
- Defining acceptable risk levels and risk acceptance criteria

One of the essential steps in designing a security system is to develop a security policy statement. Security policy is a high-level document that explains the security requirements.

The Sixteenth Step: Implementing management

Resource Management and implementing operations before starting the implementation phase is required. The first step is to design and it should be presented to the stakeholders and obtain the necessary approval of the remaining risks and after executing permission, implementation begins.

- Exchange of information with stakeholders
- Determining priority of risk management strategies
- Obtain approval of residual risks
- Determining different responsibilities when implementing
- Determining Schedule of Implementation
- The estimation cost of implementing and Funding
- Getting a permission on implementing

The second phase: Implementation

In this phase, the implementation of information security management system based on design has done in the previous phase. This phase has the following structure:

The Seventeenth Step: Implementation

This section deals with the implementation of plan and includes the following options:

- Run the configuration plan to deal with risks
- Preparation RFP implementation of the project plan to deal with risks
- Justifying the implementation of the Guidelines to the audience

The third phase: Monitoring

In this phase, the effectiveness evaluation of implementing information security management system has reviewed. This phase has the following structure:

The Eighteenth Step: Monitoring

- Effectiveness

In this part the following option is done:

- Measuring the effectiveness of controls

The Nineteenth Step: Review

- Review

In this part the following options are done:

- Management Review
- Reviewing plans to deal with risks

The Twentieth Step: Internal Audit

- Internal Audit

In this part the following option is done:

- Internal Audit
-

The Fourth phase: Improvement

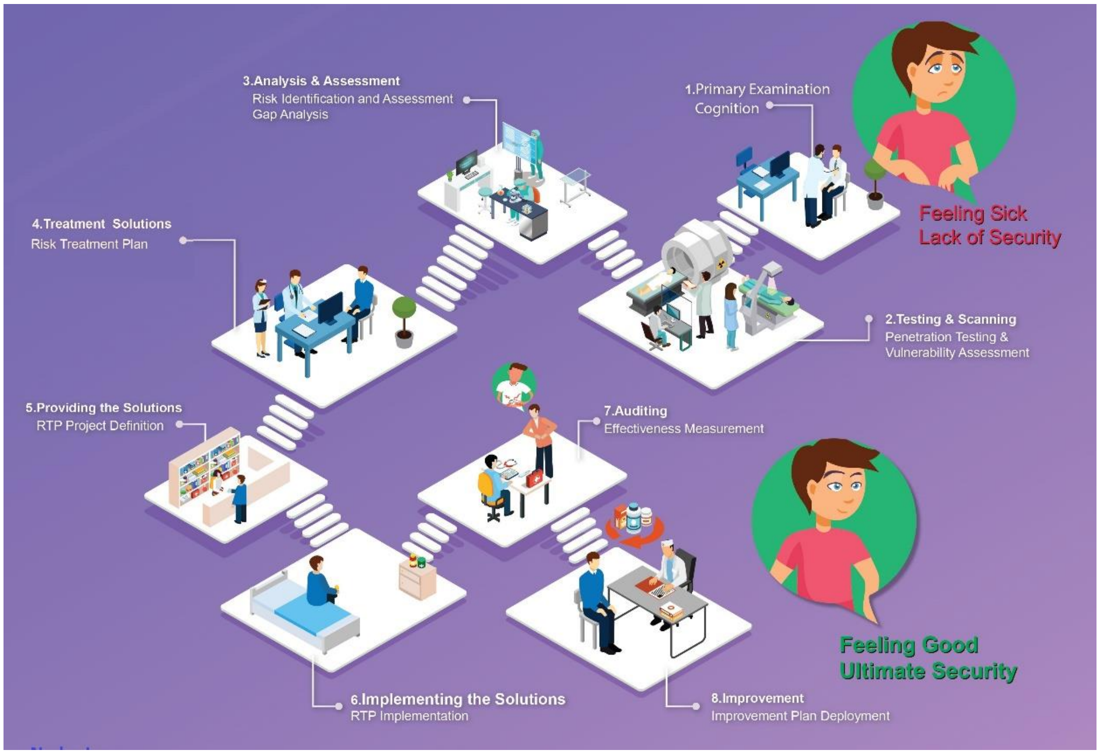
It is to turn to the problems observed in the monitoring phase and final reforming the system that includes the following components:

The Twenty first Step: Improvement

- Improvement

In this part the following options are done:

- Implementation of corrective plans
- Insurance of improvement
- Being awareness of improvement


3.Analysis & Assessment
Risk Identification and Assessment
Gap Analysis
1.Primary Examination
Cognition
Feeling Sick
Lack of Security
4.Treatment Solutions
Risk Treatment Plan
2.Testing & Scanning
Penetration Testing &
Vulnerability Assessment
5.Providing the Solutions
RTP Project Definition
7.Auditing
Effectiveness Measurement
Feeling Good
Ultimate Security
6.Implementing the Solutions
RTP Implementation
8.Improvement
Improvement Plan Deployment