International Journal of Advances in Science Engineering and Technology, ISSN(p): 2321 –8991, ISSN(e): 2321 –9009
Volume-6, Issue-4, Oct.-2018, http://iraj.in

CYBER SECURITY: RISK MANAGEMENT - IN CONTEXT OF ISO 2700X -

[1]SABHI CHAIMAE, [2]ELCHGAR HICHAM, [3]MOHAMMED KACHKOUCH SOUSSI, [4]CHAOUI HABIBA

[1]Master student: Security of Information Systems: National School of Applied Sciences Kenitra, Morocco
[2]IT6 Director: http://www.it6.ma/,37, Angle Avenue Fal ould Oumeir ET rue Oukeimeden Appt 4, Agdal - Rabat, Morocco.
[3]Information Security Consultant at IT6 Consulting: Telecommunications & networks engineer.
[4]Systems Engineering Laboratory, National School of Applied Sciences Kenitra, Morocco, http://www.ensa.uit.ac.ma
E-mail: [1]chaimae.sabhi@gmail.com, [4]hmina@univ-ibntofail.ac.ma

Abstract - Information systems are ubiquitous today in all businesses. The computer security of these systems must protect them from many threats of various origins. Risk management can determine, based on the vulnerability of the system, its criticality for each of these threats. It then makes it possible to propose the necessary and sufficient solutions to reduce the risks to an acceptable residual level.
The purpose of this article is to discuss the issue of cybersecurity within an organization and to analyze risk management activities across selected ISO standards to provide the basis for improving risk management in information systems. Then we discuss the different methodologies / tools for evaluating and managing the risks associated with information and its treatments. We also present an example based on ISO27001 set for risk assessment and risk management. The results of this research indicate that successful risk management helps protect the cyber-attack information system.

Keywords - Cyber Security, Risk Management, ISO Standards, Mehrai, Ebios, Risk Analysis, Standard Organisation, Information Security, ISO 27001.

I. INTRODUCTION

The world of cybersecurity has changed dramatically in the last 20 years. In the 1980s, the security of information systems was a rather confidential domain. In the early 2000s, the first security products began to be commercialized: firewalls, identity or event management systems. , detection probes, etc.
Cybersecurity is a problem that affects everyone, all businesses, and all administrations. The subject is so vast that we have limited ourselves to telecommunications and energy companies. Some of them were looted without knowing it.
Cyberspace is no longer safe. From business organizations to countries, the requirements of information security and assurance have become one of the most important functions to ensure continued operations. [1]

IT has become essential for any business. Because of its indispensability, risk management has also become vital. In all areas, risk management activities must be under control. This can be to dedicate risk management or a broader perspective in management system management systems is defined by ISO. [2]
The objective of this research is to study and understand risk management activities in various selected ISO standards and to show that a centralized and integrated risk management approach can serve as a basis for improving, protecting information systems in an organization and help identify and address the risks faced by a company and, in so doing, increase the likelihood of successfully achieving a company's goals.

In this article, we describe the topic of cybersecurity and we also identify emerging issues for companies in their information systems, network services, demonstrating the benefits of introducing and prioritizing risk management within information systems.
The document is organized as follows: Section 2 discusses cybersecurity issue; Section 3 presents the context of risk management; section 4 gives an overview of the process of risk management; Section 5 present a review about different security standards used for risk management; Section 6 describes a successful example that we have worked with to apply risk assessment for some companies and finally Section 7 concludes the paper and presents future directions on the subject.

II. CYBER SECURITY ISSUES

Cybersecurity refers to the tools, practices, approaches and safeguards implemented to protect information and information assets in the interconnected cyber world. [3]
Cybersecurity is about protecting information system against cyberattacks, cyberterrorism and cyberwarfare [4].
The risks are varied: breach of confidentiality of the data, unavailability of the network or certain documents, media risks for the company, cyber extortion.
In its latest annual report of flaws and attacks, the Cert-IST [5] points out that "the risk of intrusion has increased significantly in recent years. New attackers, specifically targeting companies (cyber-espionage,

cyber-sabotage, ransomware) have been identified. In addition, industrial systems and the connected objects sector have become popular targets of attackers and many vulnerabilities in these areas are being discovered.

1. Security Goals [6]

There are some specific security goals that must be achieved to ensure secrecy of the data/system. These goals are:

- Confidentiality: It states that the data must be accessible to authorized persons only, thus, maintaining the privacy and secrecy of the data.
- Integrity: It ensures that the data must be transmitted over the secure channel without unauthorized modification or the loss/destruction of data/information.
- Availability: It assures that the data and information is timely available for use. The services are not denied to the authorized users.
- Authenticity: Authentication means verifying that the user accessing the data is genuine. The identity of the sender and receiver of the information must be verified.
- Accountability: It helps to trace the responsible party/entity in case of any security breach. The actions of all the entities must be maintained for security purposes.
- Non-Repudiation: This prevents denial by one of the entities (sender or receiver) in the communication of having less or no participation.

2. Security Issues [7]

Hacking Terms	Descriptions
Denial of service	This is becoming a common networking prank, By hammering a website's equipment with too many request for information, an attacker can effectively clog the system, slowing performance or even crashing the site. This method of overloading computers is sometimes used to cover up an attack.
Scan	Widespread probes of the internet to determine type of computer, services and connections. The way the hackers can take advantage of weakness in a particular 'make' of computer or software program.
Sniffer	Programs that covertly search individual packets of data as they pass through the internet, capturing password or the entire content.
Spoofing	Faking an email address or webpage to trick users into passing along critical information like password or credit card number.
Trojan Horse	A program, that unknown to the user, contains instructions that exploit a known vulnerability in some software.
Backdoors	In case the original entry point has been detected, having a few hiding ways back make reentry easy and difficult to detect.
Malicious Applet	Tiny programs, sometimes written in the popular java computer language, that missus the computer resources, modifies files on the hard disk, sends fake emails and steals passwords.
War dialing	Programs that automatically dials thousands of telephone numbers in search of a way in though a modem connection.
Logic bombs	An instruction in a computer program that triggers a malicious act.
Buffer overflow	A technique for crashing or gaining control of a computer by sending too much data to the buffer in a computer's memory.
Password crackers	Software that can guess passwords.
Social engineering	A traffic used to gain access to computer system by talking unsuspecting company employee out of valuable information such as passwords.
Dumpster diving	Shifting through a company's garbage to find information to help break into their computers. Sometimes the information is use to make a stab at social engineering more credible.

Table1: Common hacking techniques.

III. RISK MANAGEMENT

In our fast paced world, the risks we have to manage evolve quickly. We need to make sure we manage risks so that we minimise their threats and maximise their potential.

Risk management is the identification, evaluation, and prioritization of risks (defined in ISO 31000 as the effect of uncertainty on objectives) followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events or to maximize the realization of opportunities [8]. So it must be proportionate to the complexity and type of organisation involved, Because risk is inherent in

everything we do, the type of roles undertaken by risk professionals are incredibly diverse. They include roles in insurance, business continuity, health and safety, corporate governance, engineering, planning and financial services. Awareness of the importance of risk management in the world's new high growth economies is increasing.

1. Risk Management Standard

[9] A number of standards have been developed worldwide to help organisations implement risk management systematically and effectively. These standards seek to establish a common view on frameworks, processes and practice, and are generally set by recognised international standards bodies or by industry groups. Risk management is a fast-moving discipline and standards are regularly supplemented and updated.

The different standards reflect the different motivations and technical focus of their developers, and are appropriate for different organisations and situations. Standards are normally voluntary, although adherence to a standard may be required by regulators or by contract.

2. Commonly used standards include:

The following standards and guidelines as we believe that they have been adopted most widely by member organizations, whether in full or in a modified version: [10]

- ISO 31000 2009 – Risk Management Principles and Guidelines.
- BS 31100: 2008.
- COSO 2004 – Enterprise Risk Management - Integrated Framework.
- OCEG "Red Book" 2.0: 2009 – a Governance, Risk and Compliance Capability Model.
- FERMA: 2002 A Risk Management Standard.
- SOLVENCY II: 2012 Risk Management for the Insurance Industry.

3. Risk definition

In enterprise risk management, a Risk is a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization. A threat-source does not present a risk when there is no vulnerability that can be exploited. A vulnerability is a weakness or flaw in system/organization security procedures, design, implementation, or internal controls that could be exploited (accidentally or intentionally) and result in a security breach or a violation of the system's security policy. [11]

Risks can come from various sources including uncertainty in financial markets, threats from project failures, legal liabilities, credit risk, accidents, and deliberate attack from an adversary.

Risk Category [12]

Here is one commonly used rating system for assessing criticality:

- Category 1: Critical Functions—Mission-Critical
- Category 2: Essential Functions—Vital
- Category 3: Necessary Functions—Important
- Category 4: Desirable Functions—Minor

Category 1 Mission-Critical

Mission-critical business processes and functions are those that have the greatest impact on your company's operations and potential for recovery. Almost everyone working in a company has an innate understanding of the mission-critical operations within their department. From an IT perspective, the network, system, or application outage that is mission-critical would cause extreme disruption to the business. Such an outage often has serious legal and financial ramifications.

Category 2 Vital

Some business functions may fall somewhere between mission-critical and important, From an IT perspective, vital systems might include those that interface with mission critical systems.

Category 3 Important

Important business functions and processes won't stop the business from operating in the near-term but they usually have a longer-term impact if they're missing or disabled. When missing, these kinds of functions and processes cause some disruption to the business. They may have some legal or financial ramifications and they may also be related to access across functional units and across business systems.

Category 4 Minor

Minor business processes are often those that have been developed over time to deal with small, recurring issues or functions. They will not be missed in the near-term and certainly not while business operations are being recovered. They will need to be recovered over the longer-term. Some minor business processes may be lost after a significant disruption and in some cases, From an IT perspective, these types of system outages cause minor disruptions to the business and they can be easily restored. The recovery time requirement for these types of processes often is measured in weeks or perhaps even months.

IV. PROCESS OF RISK MANAGEMENT

Since the early 2000s, several industry and government bodies have expanded regulatory compliance rules that scrutinize companies' risk management plans, policies and procedures. As a result, risk analysis, internal audits and other means of risk assessment have become major components of business strategy. In the other hand, risk management standards have been developed by several organizations, including the ISO. These standards are

designed to help organizations identify specific threats, assess unique vulnerabilities to determine their risk, identify ways to reduce these risks and then implement risk reduction efforts according to organizational strategy.[13]

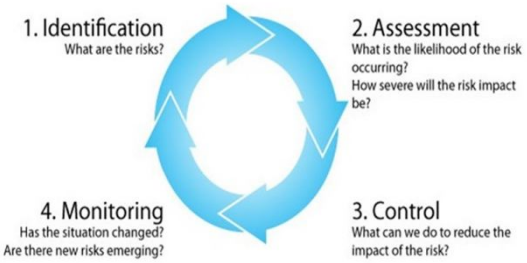

Fig.1. Risk management is a planned and systematic process consisting of 4 defined stages.

1. Risk Identification

The initial identification of risks and issues with the potential to impact on the objectives of a given procurement exercise is essential in terms of understanding, we can start with possible sources of problems (or the problems you need to focus). Once risks are identified they should be documented in the risk register.

2. Risk Assessment

The purpose of risk assessment is to assess the probability of risks occurring and their potential impact.

Probability (or likelihood)	Impact
The evaluated chance of a particular outcome actually happening (including a consideration of the frequency with which the outcome may arise).	The evaluated effect or result of a particular outcome actually happening (usually considered in terms of effect in cost, scheduling and quality).

Table2: Definition of probability and impact of risk.

3. Risk Control

Once risks have been identified and assessed they must be addressed and controlled. The response must be proportionate to the level of the risk that will have been determined as part of the risk assessment. The table suggests four types of response that may be used to address risks at different levels.

Avoid	This includes not performing an activity that could carry risk. Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed. Not entering a business to avoid the risk of loss also avoids the possibility of earning profits.
Reduce	If we cannot completely avoid a risk, we can build some mechanism or take some sort of action that would reduce the damage to our project in case of risk occurrence. Risk reduction or "optimization" involves reducing the severity of the loss or the likelihood of the loss from occurring. Modern software development methodologies reduce risk by developing and delivering software incrementally.
Transfer	The term of 'risk transfer' is often used in place of risk sharing in the mistaken belief that you can transfer a risk to a third party through insurance or outsourcing. Before deciding to transfer a risk to a third party, you should consider who is best placed to manage the risk. It may be that the risk is best managed internally within your organisation. It is also possible that transferring risk to a supplier will result in a significant cost to your organisation and this should be considered before taking this course of action. Also remember that whilst you can transfer responsibility for an action, you cannot transfer accountability.
Accept	In some case, an identified risk cannot be avoided, reduced or transferred to a third party. This is a type of risk for which you can do nothing and you would need to accept the risk as integral part of project and hope for the best. This includes risks that are so large or catastrophic that either they cannot be insured against or the premiums would be infeasible. War is an example since most property and risks are not insured against war, so the loss attributed by war is retained by the insured.

Table3: Types of risk response level

4. Risk Monitor

One of the most common approaches to monitoring risks is the use of a risk register. The risk register should be set up at the start of the project and reviewed at each stage of the procurement and contract management process to keep this process and iterate during the project.

A risk register should contain the following information as a minimum:

- Risk identification number
- Risk Owner

- Description of Risk
- Results of assessment (Probability/Impact) and date of assessment
- Mitigating Actions - what are you going do to address the risk
- Date when the risks will next be reviewed.

V. SECURITY STANDARDS

The main methods used in Europe and North America will be discussed in this section: [14]

A. EBIOS (Expression of Needs and Identification of Security Objectives) makes it possible to identify the risks of an IS and to propose a security policy adapted to the needs of the company (or an administration). It was created by the DCSSI (Central Directorate for the Security of Information Systems), the Ministry of Defense (France). It is intended primarily for French administrations and companies.

B. Mehari (Harmonized Risk Analysis Method) has been developed by CLUSIF since 1995, Mehari's general approach consists of the analysis of security issues: what are the dreaded scenarios? , and the prior classification of IS entities in based on three basic security criteria (confidentiality, integrity, availability). These issues express the dysfunctions that have a direct impact on the company's activity. Then, audits identify the vulnerabilities of the IS. And finally, the risk analysis itself is done.

C. Octave (Operationally Critical Threat, Asset and Vulnerability Evaluation) was created by the University of Carnegie Mellon (USA) in 1999. Octave is intended for large companies, but recently a version adapted to small structures exists: Octave- S. Its purpose is to enable a company to carry out risk analysis of it IS by itself, without outside help (consultants). For this, a catalog of good security practices is provided with the method.

VI. APPLICATION RISK ASSESSMENT TOOL

The risk assessment is an important part of a risk management process designed to provide appropriate levels of security for information systems in a company. Assessing risks consists in identifying, as exhaustively as possible, all the risks which a company or organization is exposed to, estimating the seriousness of each risk and judging whether each risk is evaluated as acceptable or not [15] [16].

[17] There is no standard for risk assessment. Standards like ISO/IEC 27001 and 27002 [18], [19] do not define detailed steps of risk assessment, so if we want to use such standards we have to define our own security assessment method or we can use methods that have been developed by other organizations.

The method that we used for Risk Assessment is based on the ISO 27001. It help to identify all kind of vulnerability that can cause a threat for the processing of an information system.

In this section we present and explain each part of our application risk assessment tool.

First part contain:

- **Asset Category**: Choose an Asset Category: Primary Asset or Support Asset [Hardware / Network Infrastructure].
- **Asset Designation**: Assign a name for the Asset.
- **Asset ID**: Assign a Unique Asset Reference in order to be able to identify each Asset unambiguously.
- **Risk Owner**: Who is the Information Asset Owner, the person who will be held to account if the risk treatments are inadequate, incidents occur and the organization is adversely impacted? It is in this person's interest to assess and treat the risks adequately, or face the consequences.

Asset Categorg	Asset Designation	Asset ID	Risk Owner
Software	DES1		USER1
Software	DES2		USER2

Fig.2First part of Application Risk Assessment tool

Second part contain:

- **Vulnerability**: Describes the vulnerabilities that can be exploited regarding the threat.
- **Threat**: Describe the information security threat briefly so that people will understand what risk you are assessing.

Vulnerability	Threat
Wrong allocation of access rights	Abuse of rights/Error in use
Lack of documentation	Corruption of data
Incorrect parameter set up	Error in use
Incorrect dates	Error in use
Lack of identification and authentication mechanisms like user authentication	Error in use
Unprotected password tables	Error in use
Poor password management	Forging of rights
Unnecessary services enabled	Forging of rights
Immature or new software	Forging of rights
Absence of change impact analysis	Error in use
Lack of effective change control	Software malfunction
Lack of back-up copies	Software malfunction
Wrong allocation of access rights	Abuse of rights/Error in use
Lack of documentation	Corruption of data
Incorrect parameter set up	Error in use
Incorrect dates	Error in use

Fig.3 Second part of Application Risk Assessment tool

Third part contain:

- **Confidentiality:** Property that information is not made available or disclosed to unauthorized individuals, entities or processes, Incident on Confidentiality would cause this effect: internal disclosure, external disclosure.
- **Integrity:** Property of protecting the accuracy and completeness of assets; Incident on Integrity would cause this effect: accidental modification, deliberate modification, incorrect results, and incomplete results.
- **Availability**: Property of being accessible and usable upon demand by an authorized entity. Incident on Availability would cause this effect: performance degradation, short-term/long-term interruption, total loss (destruction).

Confidentiality	Integrity	Availability
high	high	high
high	high	high
high	high	high
low	high	low
high	high	high

Fig.4Third part of Application Risk Assessment tool

Fourth part contain:

- **Asset Rank**: Assign a criticity rank to the asset to define the priority.
- **Impact:** The global impact on business calculated by establishing the Maximum between confidentiality, integrity and availability impacts.
- **Likehood**: Enter the likelihood of the risk's occurrence regarding statistics and historical facts (how Often Security Incidents did occur?).
- **Current Risk Score**: The Risk global score, calculated by multiplying the likelihood and the impact.
- **Risk Treatment**: Describe how the risk is to be treated (Avoidance / Reduction / Transfer/ Retention).

Asset Rank	Impact	Likelihood	Current Risk Score	Risk Treatment
3	9	1	9	Reduct
3	9	1	9	Reduct
3	9	1	9	Retain
3	9	1	9	Retain
3	9	1	9	Retain

Fig.5Fourth part of Application Risk Assessment tool

Last part contain:

- **Recommended Controls**: Controls that should be implemented to treat the risk. Ref 27002.
- **Implemented Controls:** Controls that have been or being actually implemented.
- **Notes**: Keep notes about the risks.
- **Last Checked**: Record the date on which the risk was last reviewed, updated and/or approved by management.

Recomended controls	implemented controls	Notes	Last Checked
A9.2.5, A9.2.6	A9.1.1, A9.1.2		
A12.1.1			
	A14.1.3		
	A12.4.4		

Fig.6Last part of Application Risk Assessment tool

This table present the risk score matrix which allows us to choose the adequate treatment for the risk based on his score.

Current Risk Score	Definition
1	Acceptable risk[*]
2 3	Low risk
4 6	Medium risk
8 9 12	High risk
18 27	Critical Risk

Fig.7Risk score matrix

CONCLUSIONSAND FUTURE WORKS

Cybersecurity is not a new threat, but it is increasing. The pirates are more and more talented. And they have always more ways to break into a network. Inadequately protected information and information technology infrastructure provides immense opportunities for malefactors as well as dedicated and hardened criminals, state actors and terrorists. Corporate espionage, spying, financial crimes, identity theft, privacy compromises have become matters of concern from a national, commercial as well as individuals perspective.

In this paper we present a global idea about cyber security issues in organisation, then we describe the process to apply risk management to prevent any malicious attack to happen in the information system and we introduce our Application Risk Assessment Tool based on ISO 27001 that we have implemented with many cases. The Risk Assessment presented in this article help to keep the information system protected against any threats and we can anytime apply this method periodically because each day new risk come out to ruin our information system..

REFERENCES

[1] National Information Security Policy And Its Implementation: A Case Study In Taiwan, Cheng-Yuankua1yi-Wenchanga2david C.Yenb.
[2] Iso/Iec Directives, Part1. Annex Sl Proposals For Management System Standards. International Organization For Standardization, Geneva (2014).
[3] Improving Cybersecurity Using Nist Framework, Csi Communications, Volume No. 39 • Issue No. 2 • May 2015.
[4] Palo Alto Networks, Inc.;"What Is Cyber Security," 2016, Www.Paloaltonetworks.Com/Documentation/Gloassary/What-Is-Cyber-Security.
[5] Https://Www.Cert-Ist.Com/Doc/Cert-Ist_Bilan2011_En_V10.Pdf
[6] Comparative Evidence Of Cryptographic Based Algorithms Under The Cloud Computing Environment To Ensure Data/System Security, Csi Communications, Volume No. 39 • Issue No. 2 • May 2015.
[7] Adapted From Sager, Ira Et Al. 2000. "Cyber Crime", Business Week, Feb 21, 2000, P.40, Cited In O'brien. 2004, P385).
[8] Https://En.Wikipedia.Org/Wiki/Risk_Management.
[9] Https://Www.Theirm.Org/Knowledge-And-Resources/Risk-Management-Standards/
[10] Https://Www.Rims.Org/Resources/Erm/Documents/Rims%20executive%20report%20on%20widely%20used%20standards%20and%20guidelines%20march%202010.Pdf
[11] Eric Cole,Ronald Krutz, James W. Conley, Network Security Bible.
[12] Https://Searchitchannel.Techtarget.Com/Feature/Understanding-Security-Risk-Management-Criticality-Categories
[13] Https://Www.Procurementjourney.Scot/Risk-Management-Process
[14] Https://Cyberzoide.Developpez.Com/Securite/Methodes-Analyse-Risques.
[15] Davis R., Information Systems Auditing: The Is Audit Testing Process, Usa, 2011.
[16] Weber R., Information Systems Control And Audit, Editura Prentice Hall, Usa, 1998.
[17] Comparison Of Risk Analysis Methods: Mehari, Magerit, Nist800-30 And Microsoft's Security Management Guide, Amril Syalim, Yoshiaki Hori And Kouichi Sakurai, 2009 International Conference On Availability, Reliability And Security.
[18] Bs Iso/Iec 27001:2005, Information Technology - Security Techniques - Information Security Management Systems - Requirements. Bsi, 2007.
[19] Bs Iso/Iec 27002:2005, Information Technology - Security Techniques - Code Of Practice For Information Security Management. Bsi, 2007.
[20] C. Giolli, A. Scrivani, G. Rizzi, F. Borgioli, G. Bolelli, and L. Lusvarghi, "Failure mechanism for thermal fatigue of thermal barrier coating systems", Journal of Thermal Spray Technology,vol.18,pp.223–230,2009.
[21] C. Zhou, Q. Zhang, and Y. Li, "Thermal shock behavior of nanostructured and microstructured thermal barrier coatings on a Fe-based alloy", Surface & Coatings Technology,vol.217,pp. 70–75,2013.

★★★