UNIVERSITY OF MACEDONIA
MASTER OF SCIENCE IN APPLIED INFORMATICS
DEPARTMENT OF APPLIED INFORMATICS

MSC DISSERTATION

CHATZIDIMITRIOU ELPINIKI

SUPERVISOR

ASSOCIATE PROFESSOR KITSIOS FOTIOS

30 OCTOBER 2019

THE IMPLEMENTATION OF INFORMATION SECURITY POLICY USING ISO 27001: A CASE STUDY IN A SOFTWARE COMPANY

Introduction

Literature overview – Theoretical background

Case Study – Venus

Results

Concluding Remarks

Introduction

The information has always been an essential asset to every company, and this asset needs to be protected

Throughout the years, cyber-attacks targeting confidential/sensitive information are on the rise

The establishment of an Information Security Management System (ISMS) is imperative to attract more customers and keep the existing ones

In literature, we encountered different approaches to develop and implement an ISMS in a company

However, there are few case studies

The objective of this study and contribution

The purpose of this study was twofold:

On the one hand, to provide the theoretical background of the research and, on the other hand, to present a case study of a successful company of the Information Technology sector and the process followed to comply with ISO 27001

Implementing an ISMS, is creating, applying and enforcing a set of changes and strategy to achieve and maintain them. An ISMS team needs to make sure that the selected set of the above are the optimal for the company.

Information Security Management Systems (ISMS)

Information Security is considered a subset of IT governance

The implementation of an ISMS is not an easy task, and poor planning can even negatively affect a company

Adjustment and cost-effectiveness are key elements of a successful Information Security Management System (ISMS).

Information Security Management Systems (ISMS)

The fundamental concept of an ISMS is to ensure the “CIA”:

- Confidentiality
- Integrity
- Availability

ISO 27000

ISO 27000 provides an overview and vocabulary, it is a guide to best practice for the overall information security management system

The ISO/IEC 27001presents itself as the standard that specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.

ISO 27002 provides the essential guidance and framework to implement the controls defined in ISO 27001

Roles of ISMS

CISO – Chief Information Security Officer

ISM – Information Security Manager

- Coordinating all information security activities and staff involved in these
- Developing IT security governance mechanisms
- Implementing security awareness programs for employees through mentoring and training sessions
- Advanced Technical skills
- Managerial skills
- Incidence response skills
- Business skills
- Core Information security skills

Risk Assessment, Risk Management

As in ISO 27000:2013 is originally stated “The information security management system preserves the confidentiality, integrity, and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed”

Risk assessment is a tool to analyze and interpret risk. It is the process of identifying and assessing the organization's vulnerabilities. It requires defining an assessment’s scope and methodology, gathering and analyzing data, and go through the risk analysis results. The implementation team should collect and analyze the risk data.

Risk Assessment

We can break risk assessment to the following activities

- Identification of the assets that are at risk and definitions of the status of importance according to the value, sensitivity, and criticality
- Identify potential threats
- Identify how possible is a threat to occur to a specific asset
- Define the impact. This usually includes the expected losses, damage and recovery cost
- Reduce risk by embedding risk-limiting controls that are accepted by the company as regards to the budget like introducing new policies and procedures
- Export the conclusions and organize an action plan

Risk Assessment

Quantitative analysis assigns a value to each risk component and the residual risk is calculated providing the loss expectancy. This type of analysis is trying to evaluate the cost of the risk, taking into consideration factors like the likelihood, the costs of potential damage and the cost of possible controls

Qualitative, on the other hand, combines elements from quantitative, in order to assess the level of risk, likelihood and the impact of possible incidents should be estimated and at this point is imported to the analysis the experience and personal judgment of the team that performs the risk assessment

Semi-quantitative assessment examines threats according to the consequences and probabilities of occurrence. This approach is based on the opinion of the people making assessment. For example, probabilities can be divided into five classes: 0 – very unlikely, 1 – unlikely, 2 – rather unlikely, 3 – rather likely, 4 – likely

Case Study – Venus

The company's real name will be concealed for security reasons

Venus automates and optimizes data-driven business processes with software and services

Venus is a company which is "project based".

Company's technology consultants are assigned to each project of each client.

The teams are dynamic- people are assigned or moved out of the team according to the phase and workload of the project.

A team might consist of 4-30 members

Client Projects

For each client a separate, concrete infrastructure is created. This infrastructure includes:

- a centralized code repository, a code file archive which allows to multi-developer projects to handle various versions
- a centralized document library
- a dedicated directory in a project management tool
- dedicated distribution lists
- dedicated containers for the development and testing
- an issue-tracker for the project
- a separate entry to a time management tool

Risk assessment in Venus

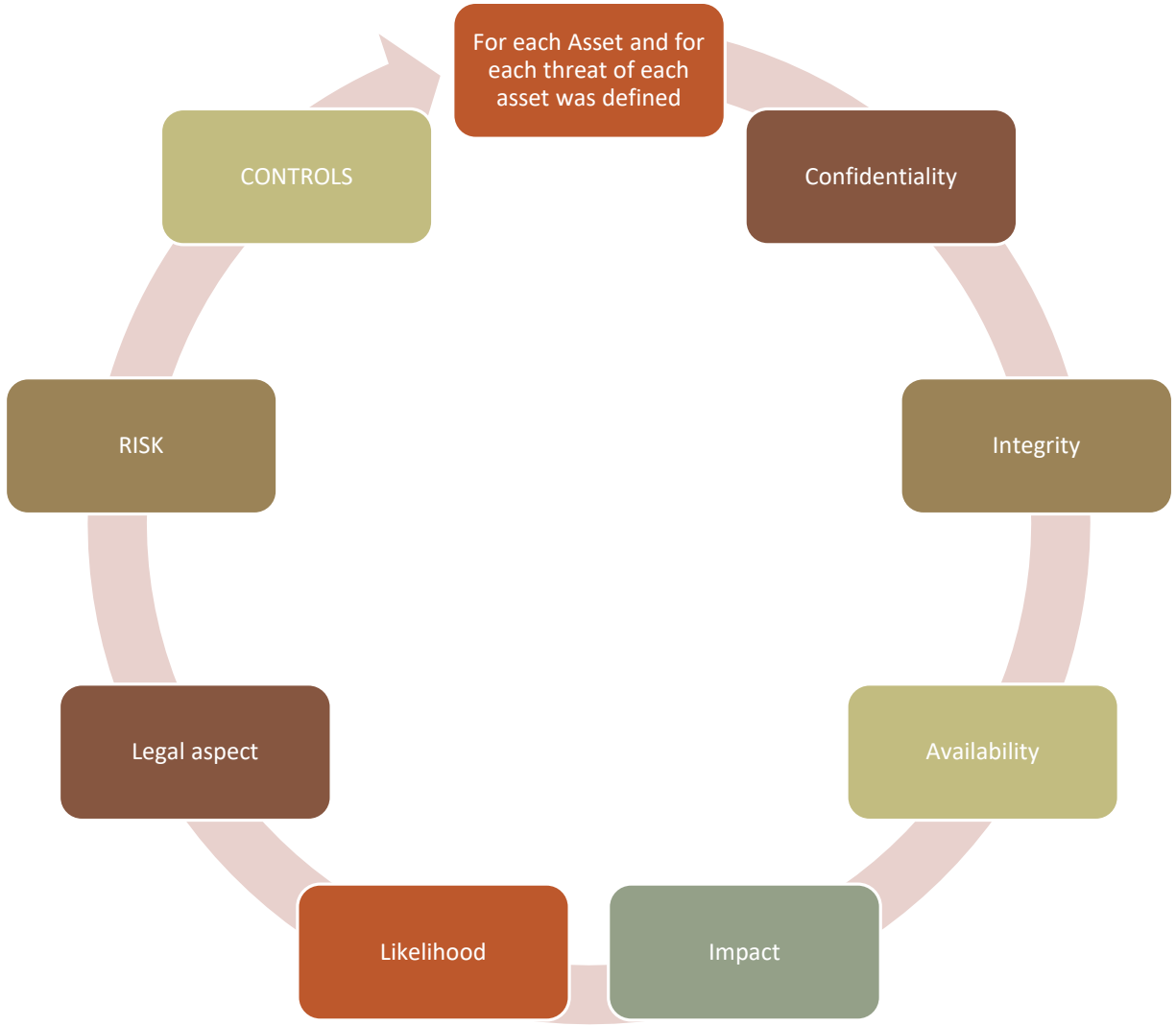
A risk assessment must be conducted at least:

- For every new information processing system.
- Following the introduction of a new information asset.
- Following modifications to systems or processes
- Modifications which might change the nature of threats and vulnerabilities.
- When there has been no review for a relatively long period (e.g., three years).

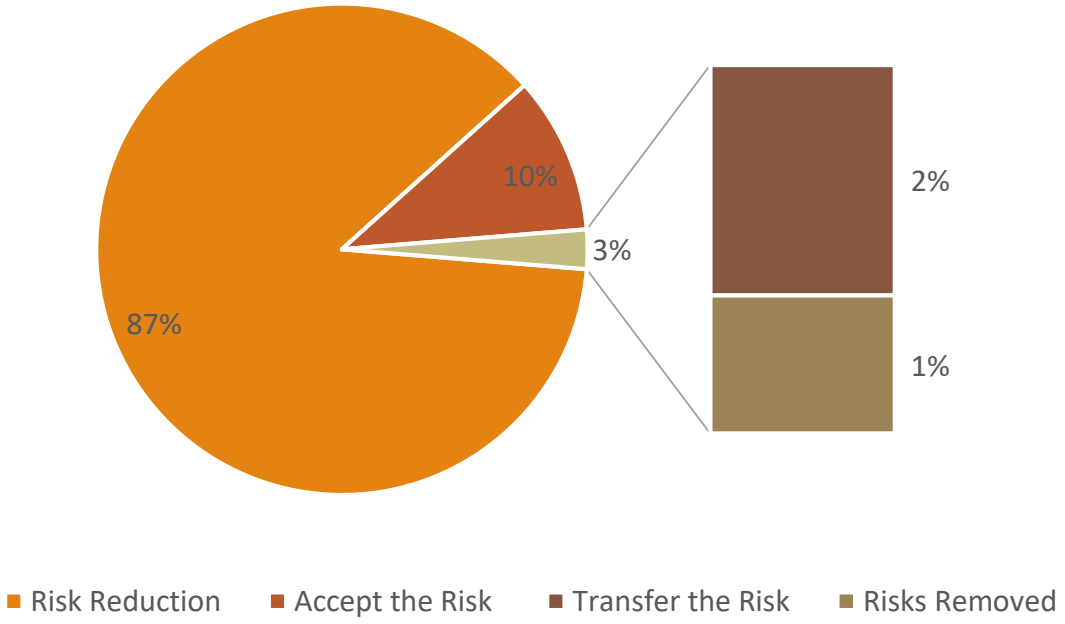
A risk assessment must be conducted with access and an understanding of

- Venus' business processes.
- The risk-related impact on Venus' business assets.
- The technical systems in place, supporting the business needs.
- The legislation and regulations to which Venus is subject.
- Up to date vulnerability and threat assessments.

Category	Threats
Theft	Theft, Vandalism
Software Error	Software Error
Software Error	Malware
Software Error	Unauthorized Access
Outage	Power Outage
Outage	Telecommunications Outage
Network Error	Network Attack
Natural Disaster	Earthquake
Natural Disaster	Flood
Natural Disaster	Fire
Legal	Breach of Contractual Relations
Legal	Breach of Legislation
Human Error	Information Misuse
Human Error	Operator Error
Human Error	Misuse of User Privileges
Human Error	Destruction of Records
Hardware Error	Hardware Error
Hardware Error	Damage to Cabling
Access Error	Locked Out
Software Error	Errors in Maintenance
Hardware Error	Malfunction of Equipment
Human Error	Unauthorized Installation of Software
Hardware Disposal	Non-safe Deletion of Media
Hardware Reuse	Non-safe Reassignment of Hardware
Removable Media	Use of Non-Encrypted Removable Media



Risk Assessment Procedure



Risk Treatment Results

Problems during the implementation

Dedicated Security Team

Complexity of the company’s project-oriented security model

The change management challenge

Concluding remarks

Summary and final remarks

Companies should be and verified to be committed to protecting the confidentiality, availability, and integrity of all types of information within their control in order to manage information risk and meet business, legal and regulatory obligations and to maintain trusted business relationships

Research restrictions and limitations

Future research directions

What will be the findings of the audit?

Will there be any nonconformities?

Thank you