Implementation Plan for an ISMS according to ISO/IEC 27001:2013

MASTER PROGRAM IN SECURITY OF INFORMATION AND COMMUNICATION TECHNOLOGIES (MISTIC)

Student: Plácido Rodal Castro
Consultant: Antonio José Segovia Henares

Index of Content

Introduction

- The objective of this document is to present the implementation plan for an ISMS (Information security management system) according to ISO/IEC 27001:2013 for Xintiba.

- This system includes all of the policies, procedures, plans, processes, practices, roles, responsibilities, resources, and structures that are used to protect and preserve the information and assets of the company.

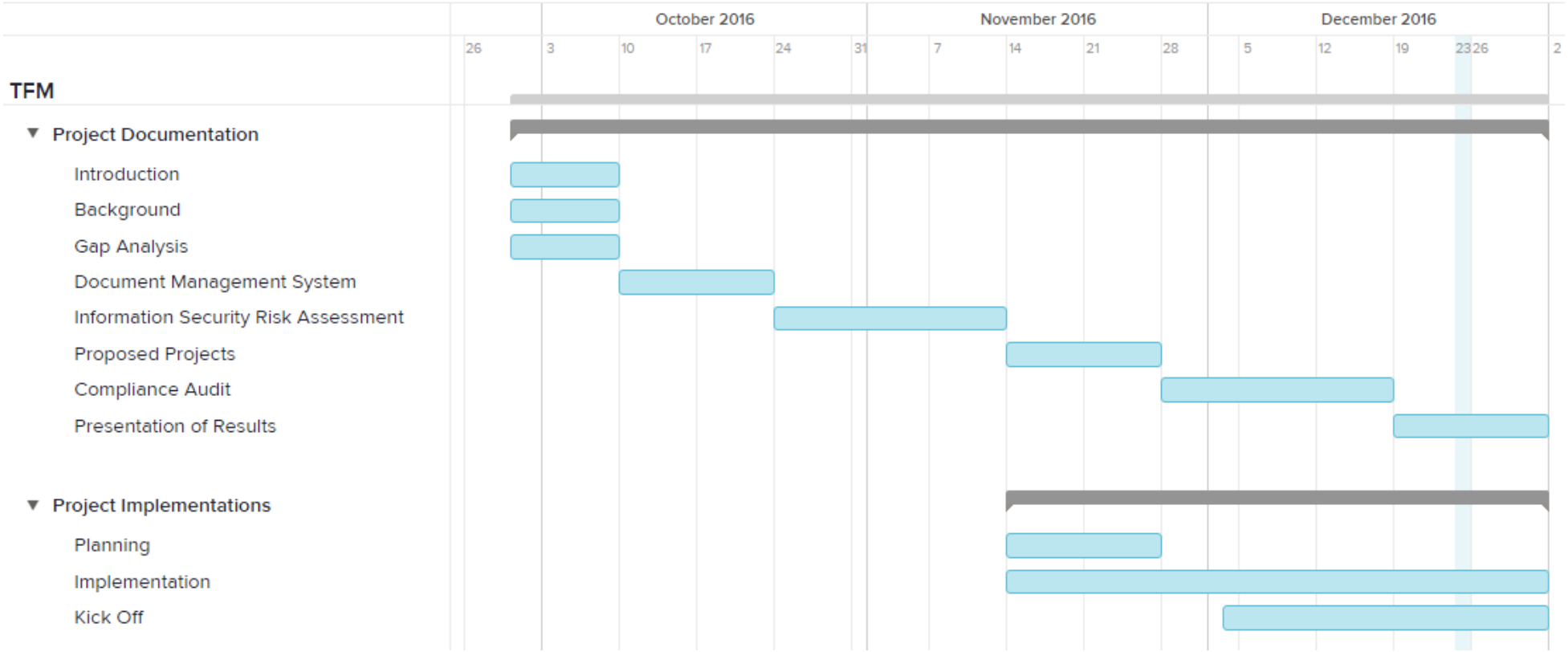
UOC Universitat Oberta de Catalunya www.uoc.edu
UAB Universitat Autònoma de Barcelona
Universitat Rovira i Virgili
UIB Universitat de les Illes Balears

Objectives

Best practices of information security management: Most effective strategy for keeping organizations and users safe.

- Improved reputation and stakeholder confidence.
- Comply with relevant legislation.
- Builds trust and credibility in the market.
- Cost savings by minimizing incident.
- Ensures information is protected and available.

Planning


October 2016
November 2016
December 2016
26
3
10
17
24
31
7
14
21
28
5
12
19
23
26
2
TFM
Project Documentation
Introduction
Background
Gap Analysis
Document Management System
Information Security Risk Assessment
Proposed Projects
Compliance Audit
Presentation of Results
Project Implementations
Planning
Implementation
Kick Off

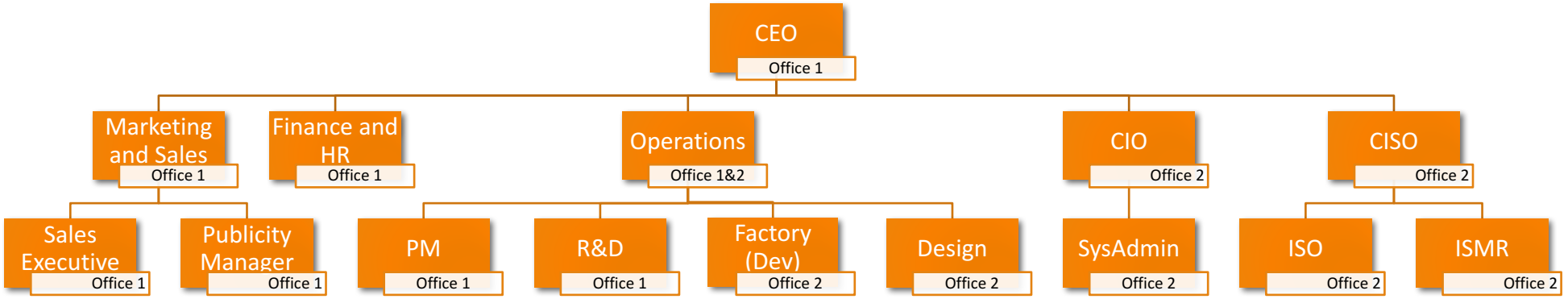
Xintiba

- Xintiba is a company from the north of Mexico that develops video games for children and handicap people. By using these video games, they attempt to accelerate the acquisition of certain cognitive skills that may help these people adapt and perform in society.

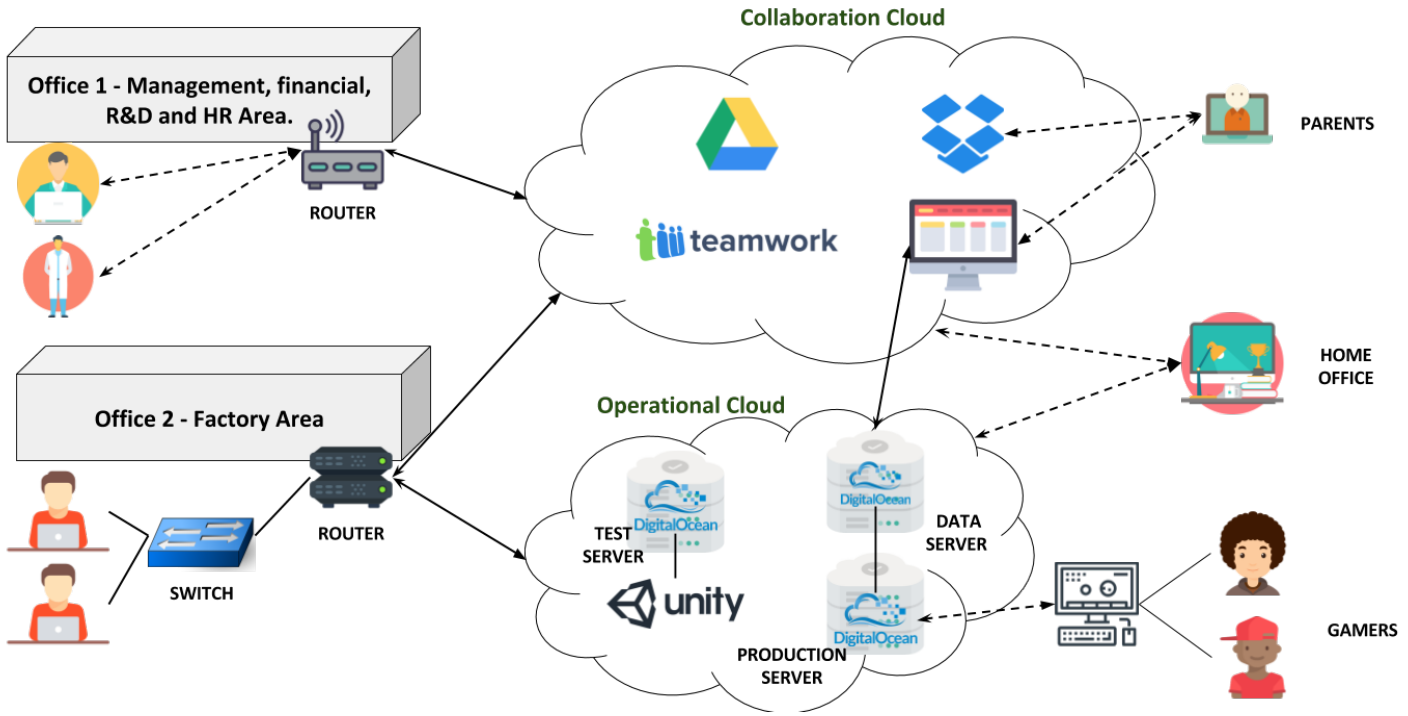
- They have published the first video game specifically designed for children with autism.

- The data collected is shown in a tool for visualizing and communicating important business data and is used by employees, parents and physicians.

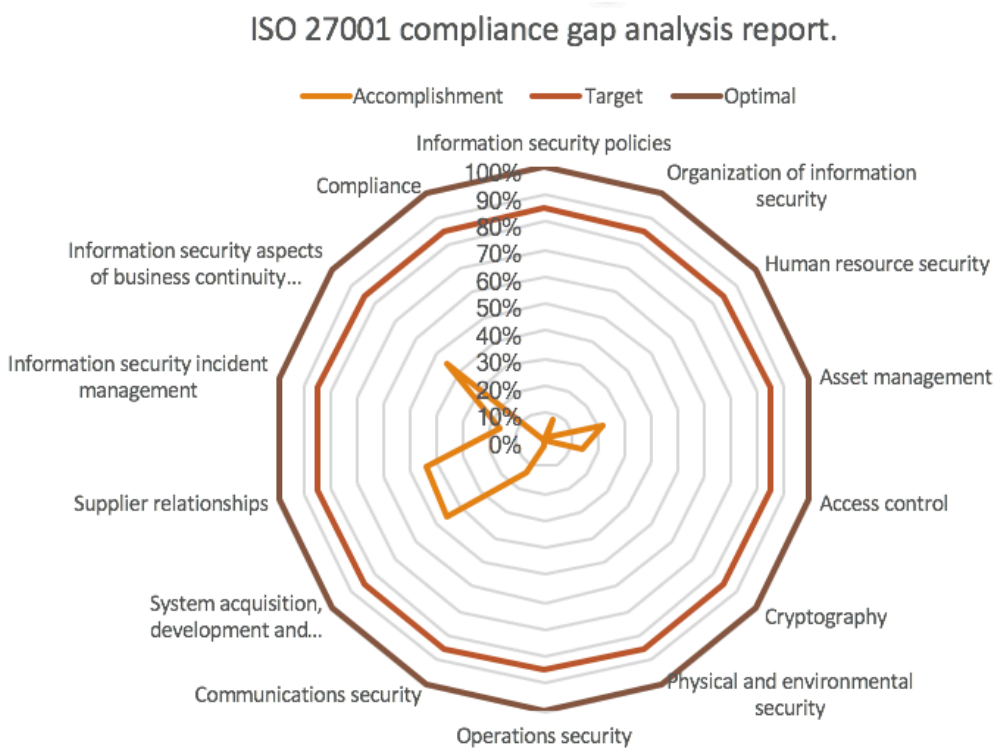
Xintiba


CEO
Office 1
Marketing and Sales
Office 1
Finance and HR
Office 1
Operations
Office 1&2
CIO
Office 2
CISO
Office 2
Sales Executive
Office 1
Publicity Manager
Office 1
PM
Office 1
R&D
Office 1
Factory (Dev)
Office 2
Design
Office 2
SysAdmin
Office 2
ISO
Office 2
ISMR
Office 2

Scope


Collaboration Cloud
Office 1 - Management, financial, R&D and HR Area.
ROUTER
teamwork
PARENTS
Office 2 - Factory Area
HOME OFFICE
Operational Cloud
ROUTER
SWITCH
TEST SERVER
DATA SERVER
unity
PRODUCTION SERVER
GAMERS

Gap Analysis



ID	Section	Accomplishment
A.5	Information security policies	0 %
A.6	Organization of information security	8 %
A.7	Human resource security	2 %
A.8	Asset management	22 %
A.9	Access control	14 %
A.10	Cryptography	0%
A.11	Physical and environmental security	0.1 %
A.12	Operations security	2 %
A.13	Communications security	14 %
A.14	System acquisition, development and maintenance	46%
A.15	Supplier relationships	44%
A.16	Information security incident management	17%
A.17	Information security aspects of business continuity management	45%
A.18	Compliance	0%

UOC Universitat Oberta de Catalunya www.uoc.edu
UAB Universitat Autònoma de Barcelona
Universitat Rovira i Virgili
UIB Universitat de les Illes Balears

Document Management System

- **Information security policy.**
- **ISMS internal audit procedure.**
- **ISMS Key performance indicators.**
- **ISMS Management review.**
- **ISMS roles and responsibilities.**

Document Management System

- **Information security policy**

  - The purpose of an information security policy is to provide a security framework that will ensure the protection of Xintiba physical and information technology assets.

  - All users must follow and accept responsibilities shown in this policy. It is the user's responsibility to carefully use and protect those resources, as well as comply with all Xintiba policies, regulations, laws and contractual obligations.

  - Xintiba will periodically audit and check the Information Security policy.

Document Management System

- **ISMS internal audit procedure**

  - The purpose of the internal audit procedure is to check, at least once every 12 months, that all aspects of the ISMS are functioning as intended and the compliance of the ISMS to the ISO/IEC 27001 standard is maintained at an acceptable level.

  - This will help ensure that not only policies and procedures are being applied but new best practices can be gathered and applied.

Document Management System

ISMS Key performance indicators

- Xintiba will evaluate the information security performance and the effectiveness of the information security management system.

- **Effective Security Policy**
- **Incident management**
- **Percent of business initiatives supported by the ISMS**
- **Number of security-related service downtimes**
- **Duration of service interruptions**
- **Incident resolution time**
- **Number of improvement initiatives**

- **% of IT budgets used to managing IT risks**
- **Number of new threats and risks identified compared to previous risk assessment**
- **Time between identification of non-compliance and implementation of fixes**
- **Number of security incidents caused by attacks from the NET**
- **Number of Security incidents caused by malicious software**

Document Management System

- **ISMS Management review**

  - Top management reviews the organization's information security management system at scheduled intervals to ensure its continuing suitability, adequacy and effectiveness.

  - Management meeting reviews should be held periodically in order to measure the effectiveness of the management system. Firstly, time frames between meetings start as monthly but probably they could be increased when the system becomes more mature.

  - The attendees of management review meetings consist in ISMS Steering Committee (CISO, ISMR, ISO and CIO), CEO and HR manager. However, outside consultants will be invited to some meetings.

Document Management System

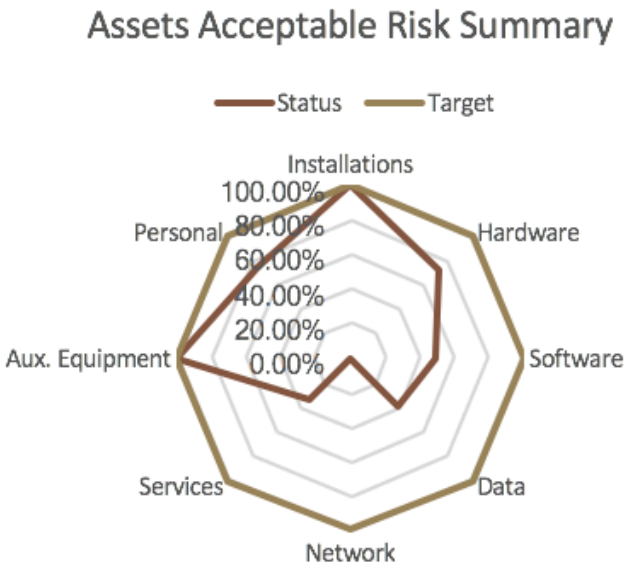
- **Methodology for the risk management**

  - Xintiba methodology for the risk management is based on Magerit V 3.0 methodology.

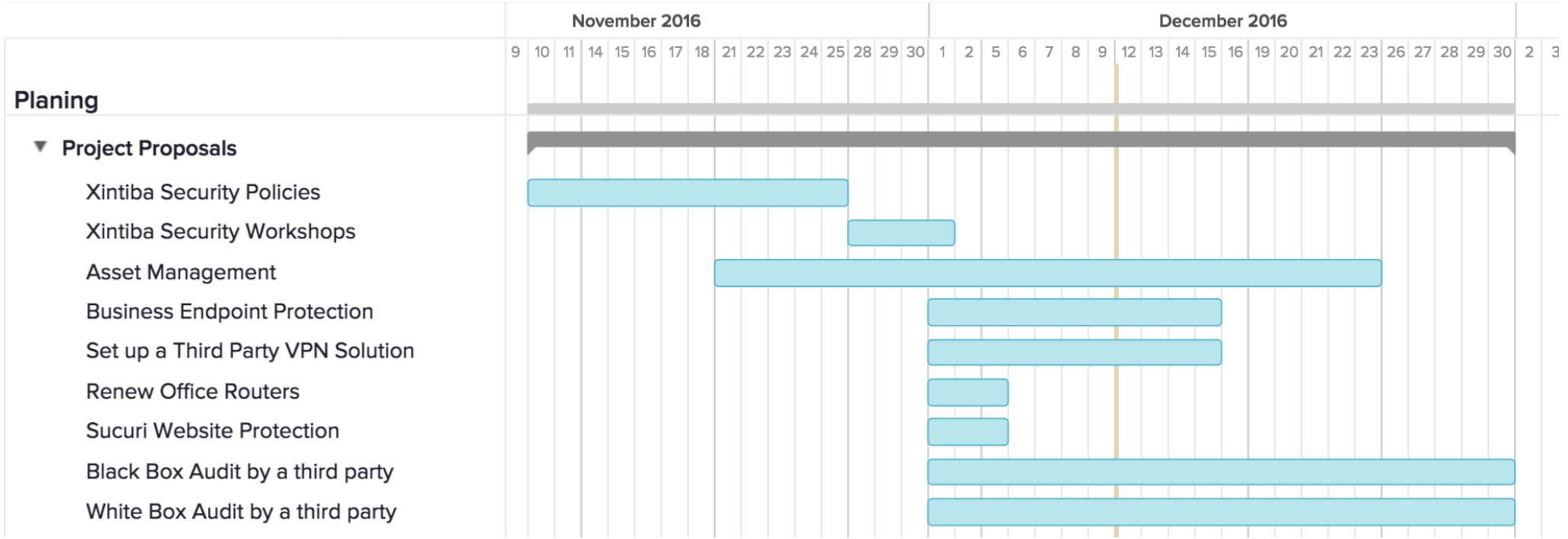
  - Magerit implement the Risk Management Process within a working framework for governing bodies to make decisions taking into account the risks derived from the usage of information technologies.

  - The objective is to protect the organization’s mission taking different security dimension´s requirements into account.

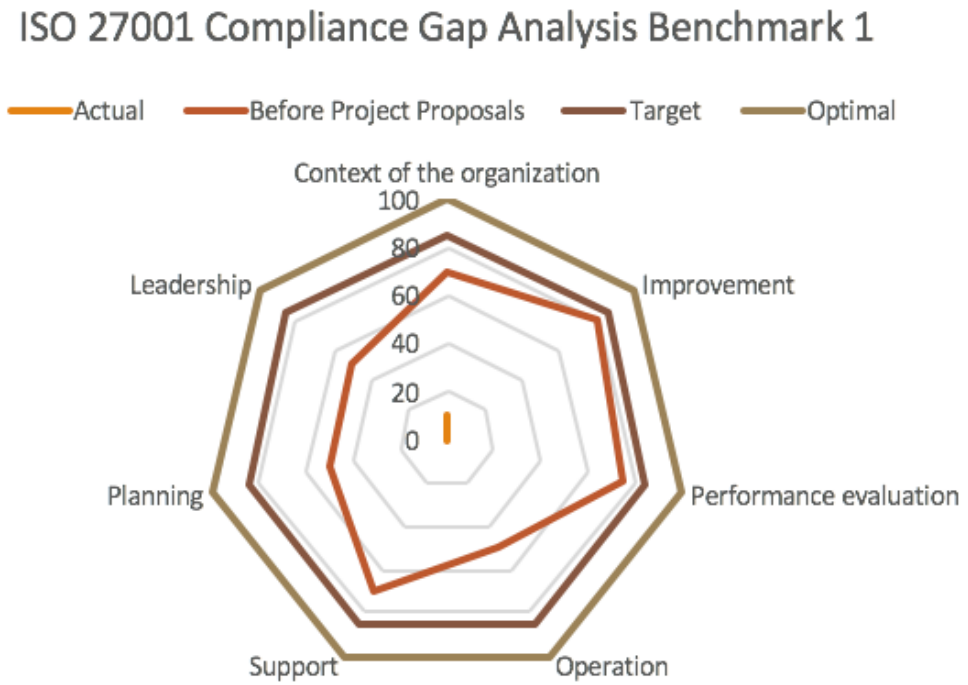
Information Security Risk Assessment

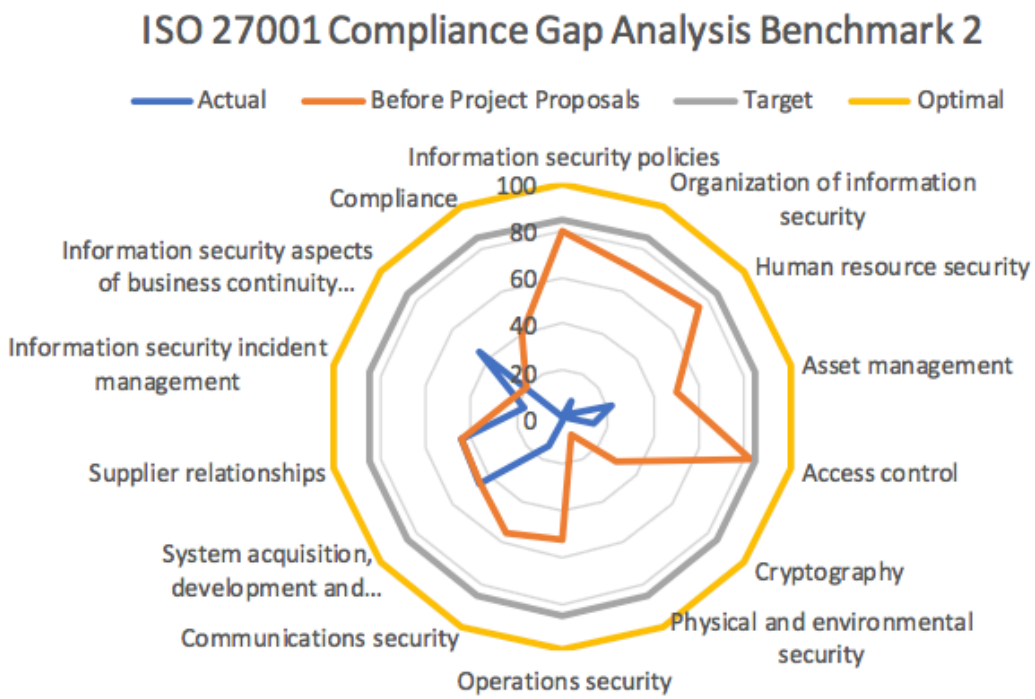


Project Proposal

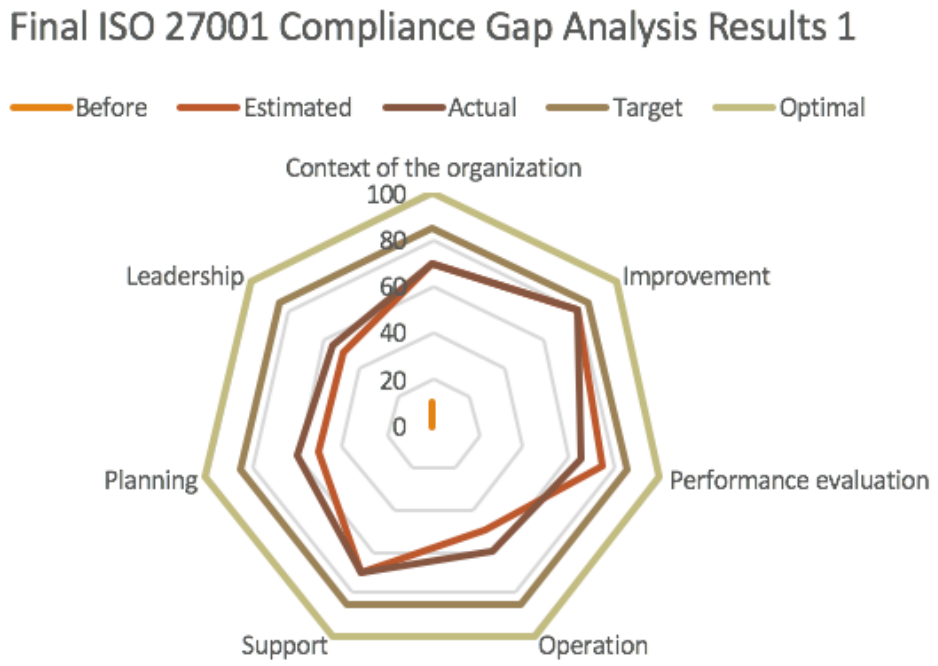


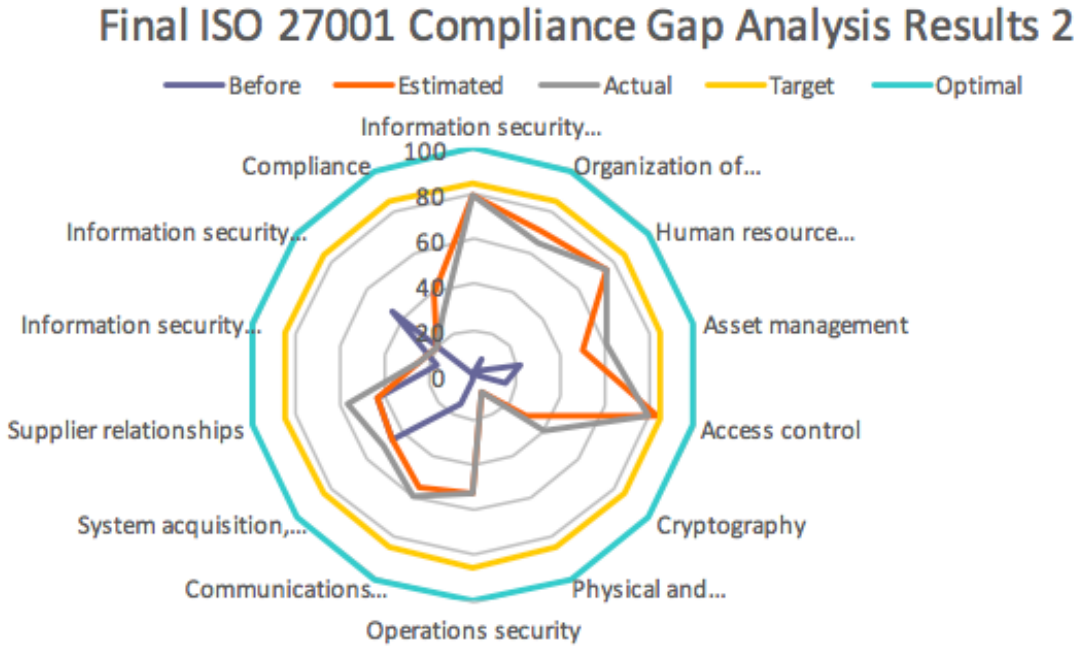
Project Proposals



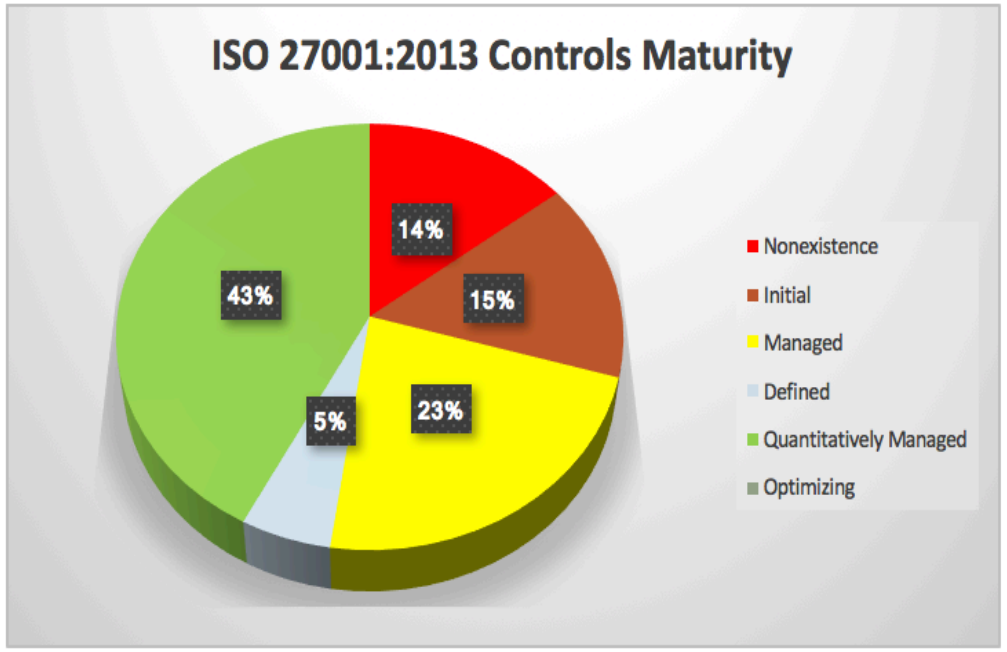


Compliance Audit





Compliance Audit



ID	Section	Before	Now
A.5	Information security policies	0 %	80 %
A.6	Organization of information security	8 %	70 %
A.7	Human resource security	2 %	75 %
A.8	Asset management	22 %	50 %
A.9	Access control	14 %	83 %
A.10	Cryptography	0 %	30 %
A.11	Physical and environmental security	0.1 %	8 %
A.12	Operations security	2 %	53 %
A.13	Communications security	14 %	55 %
A.14	System acquisition, development and maintenance	46 %	45 %
A.15	Supplier relationships	44 %	44 %
A.16	Information security incident management	17 %	25 %
A.17	Information security aspects of business continuity management	45 %	20 %
A.18	Compliance	0 %	40 %

Lessons Learned

1. It is very important to explain in detail to the employees the projects that the company wants to carry out. If they don’t understand what the target is, they will not cooperate properly.
2. Security is not a project, it is a key piece of the company. It is very important to devote time and patience to explaining to managers how important it is.
3. The first stages in a securitization project are the easiest. The complexity begins when we reach high levels of process maturity, and it is also harder to maintain safety levels than to achieve them.
4. Computer security requires to be updating daily, therefore, it is important to devote time to research, have contact with authorities and periodically work with an outsides consultants.

Conclusions

- We have finish the project complying with the proposed objectives but we expect reach more maturity level of security.
- This project is the first step to introduce security as a key element in Xintiba. The plan is continue working hard to start the ISO/IEC 27001 certification at the final semester of 2017.
- The project planning was followed properly at the beginning, but on the final weeks the projects were closed in parallel because we were short of time.
- We had some issues with third party employees and companies. Also, with some internal employees who were low focused on the project.

Thanks for your attention!

Student: Plácido Rodal Castro
Consultant: Antonio José Segovia Henares