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

Student name: Plácido Rodal Castro

Degree: Master Program in Security of Information and Communication Technologies (MISTIC)
Area: Information security management system

Consultant: Antonio José Segovia Henares
Subject responsible teacher: Carles Garrigues Olivella
University: Universitat Oberta de Catalunya
Delivery Date: 12/30/2016

PROJECT DATA SHEET

Project Name:	*Implementation Plan for an ISMS according to ISO/IEC 27001:2013*
Author name:	*Plácido Jose Rodal Castro*
Consultant name:	Antonio José Segovia Henares
Subject responsible teacher name:	*Carles Garrigues Olivella*
Delivery Date:	12/2016
Degree:	Master Program in Security of Information and Communication Technologies (MISTIC)
Final Work Area:	*Information Security Management System*
Working language:	*English*
Key Words:	*Security, ISMS, IS0/IEC 27001:2013*

Project Summary:

The main objective of this project is to define the implementation plan for an ISMS (Information security management system) according to ISO/IEC 27001:2013 for Xintiba. This system includes all 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.

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.

The scope of the ISMS is the ISO/IEC 27001 entire organization certification. We have just two locations and no more than 50 employees so the best option is to cover the whole organization.

Xintiba has not established a ITSM and only has one employee to manage all security of the organization. We started defining a Security Strategic Plan to efficiently and effectively address the management, control and protection of the information assets.

The improvement a few weeks before the project kick-off is high. Nevertheless, more needs to be done to make the final target a reality.

Next initiatives are going to focus in move up nonexistence and initial controls and is expected to finish 2017 with a high maturity levels to start the ISO 27001 certification in 2018. It is noteworthy that employees are more compromised with the security since we start this project.

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1. Overview

There is no doubt, the computer security is a concern for most of companies. Xintiba is one of these companies that is looking to improve and invest in the security of each organization.

Xintiba develops therapeutic video games for children or handicapped people. They are concerned about ensuring the privacy of important data because any leak could have serious consequences for the operation of the company.

The objective of this document is to describe 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.

1.2. Project Objectives

The main purpose of the project is to establish the basis of an ISMS and it is divided into the following stages:

- Xintiba current situation and objectives: A process which starts identifying business objectives and priorities. To do so, understand Xintiba internal structure, processes, services and operation.
- Best practices of information security management: Most effective strategy for keeping organizations and users safe.
- ISO / IEC 27001: 2013 compliance audit: A process which Xintiba we are going to be review and report of the implemented controls of the standard.
- ISMS Scope: The selection of the ISMS proper scope implementation which helps to achieve the identified business objectives.
- Xintiba threat and risk analysis: Identification and evaluation of Xintiba threats and risks.
- Project proposals to achieve adequate safety management.

1.3. Methodology

Xintiba doesn't have an ISMS so we must start from the beginning. We will show the project as a completely new initiative that will help to improve Xintiba security.

Firstly, we should analyse if Xintiba is following some security practices and the level of security processes. It can be useful to start with some advantage.

Secondly, we are going to focus on protecting the most critical process of the company. Although we haven´t analysed Xintiba, we know that the current security level is low. These measurements were taken based on ISO 27001:2013 standard.

We are going to implement measurements into short deliverables in order to release them as we advance.

At the end of this project Xintiba will have an acceptable security level and the first steps done to start formally looking for the ISO 27001:2013 certification.

1.4. Project Planning

We divide project into two groups of tasks: Documentation and Implementation. Project implementations are more described into **6. Proposed Projects.**

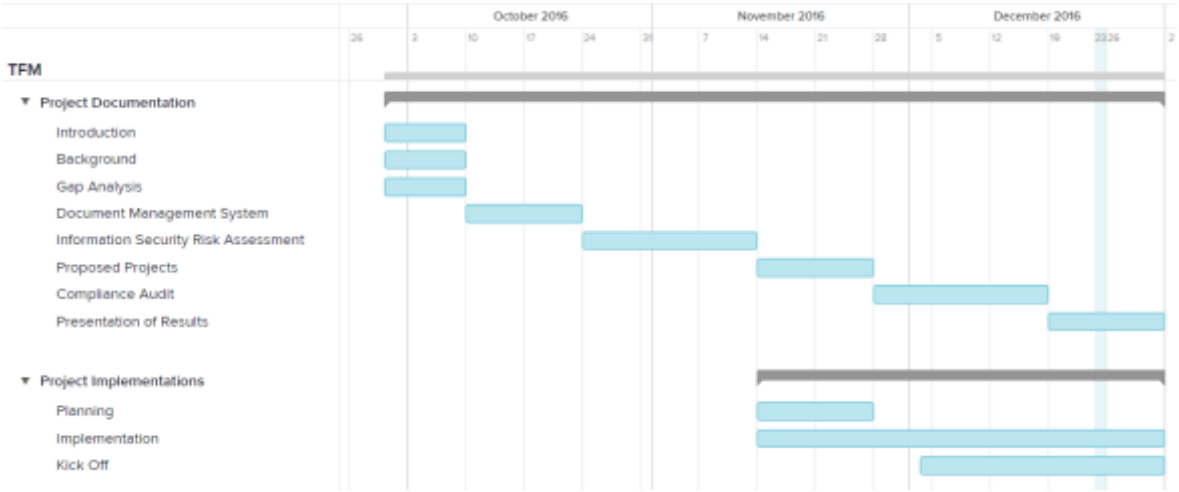

Figure 1: Project planning.

1.5. Deliverables

Below, as project deliverables:

- Gap analysis of ISO/IEC 27001:2013: An evaluation of the capability levels of the ISO/IEC 27001 controls according to the ISO/IEC 15504.

- Documents scheme of ISO/IEC 27001:2013: It contains the information security policy, the ISMS internal audit procedure, the ISMS Key performance indicators, the ISMS Management review, the ISMS roles and responsibilities, the Methodology for the risk management and the Statement of applicability.

- Xintiba threat and risk analysis: Enable Xintiba to systematically identify, analyze and evaluate the information security risks associated with an information system or service along with the controls required to manage it.
- Project plan: Contains documentation of the proposed projects to improve Xintiba Security.

- Compliance audit results of ISO/IEC 27001:2013.
- Conclusion and results report.

1.6. Brief Description of Chapters

We start this document with the background of Xintiba. It contains an overview of the company, the main line of business and how they organize. Also, it describes the project scope and objectives.

The document continues with a Gap Analysis to evaluate the capability levels of the ISO/IEC 27001. This standard is a set of technical standard documents for the software development process and related business management functions.
|
Once we know the security maturity of the company it is time to define some processes and policies that can help to start working on improving Xintiba information systems security. This chapter contains the descriptions of these deliverables that are annexes on this document.

It continues with the chapter of the Information security risk assessment. It describes how Xintiba can systematically identify, analyse and evaluate the information security risks associated with an information system or service along with the controls required to manage it.

The next chapter is about the proposed projects to mitigate the current risk in the organization and evolve ISO compliance to its proper level. The following chapter shows the results of security audit before the proposed projects implementation.

The documents finish with a conclusion section where we capture the most important lesson learned, the difficulties encountered and the next steps of Xintiba to continue enhancing its security levels.

2. Background

Xintiba is a company that grew quickly and a little out of control. A year and a half ago they hired a security specialist to improve the security of the organization. He has achieved a lot of initiatives but are not enough. The problem is that employees are not following up all his proposals and he has not resources to carry-out all the projects.

This section includes a deep description of Xintiba and a summary of the ISO/IEC 27001 -27002: 2013 standards.

2.1. 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. It will be focused on someone's daily life challenges, and the neurological exercises that may help patience improve certain cognitive skills.

The data collected is shown in a tool for visualizing and communicating important business data and is used by employees, parents and physicians. The dashboard shows graphical presentations, historical trends, performance indicators and some reports.

The company has around 40 employees located in two different offices. Developers, SysAdmins and more technical staff work in one of them. Marketing, finances, sales and others management areas work in the other office.

The organization is structured in the following way:

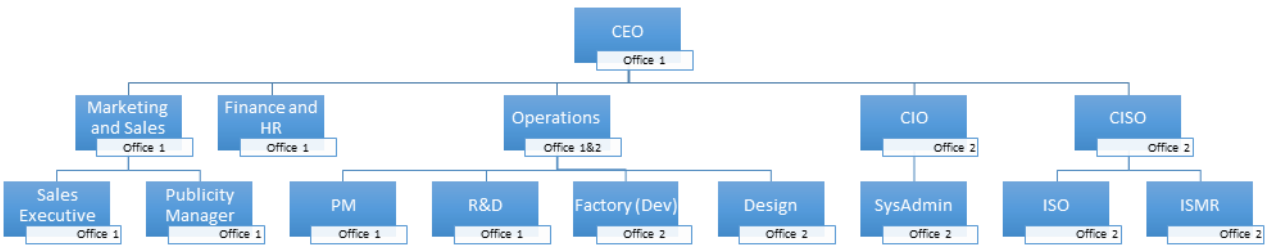

Figure 2: Xintiba hierarchy.

- **Chief Executive Officer (CEO)**

The CEO is the highest position and the founder of the company. She determines the goals of the company and is supportive with innovation projects. She follows closely every project of the company.

- **Marketing and Sales Department**

This is the department that handles every task of sales and marketing. The team includes a Manager, Sales Executive and an Advertising Manager. They work together setting strategies and deciding what marketing communications are needed to support their work. In addition, they help the R&D department to obtain customers feedbacks.

- **Finance and Human Resources Department**

Xintiba outsources hiring and recruiting tasks. An external accountant helps our accountant deal with the finances.

- **Operation Department**

This department handles the developing and innovations tasks; it is the core of the company. It is divide into the following four sub-areas:

  - **PM (Project Management)**

    There are two managers in charge of initiating, planning, executing, controlling and closing the work of the different operational areas.

  - **R&D (Research and development)**

    This sub-area is focused on all aspects of autism spectrum disorders and related developmental disabilities. Their outcomes are the heart of the games. They work with Design and PM area. The team consists of 6 psychologists.

  - **Factory (Software development)**

    Factory area is formed by specialized engineers (Analysts, Designers, Developers and Testers) who are managed by Project Managers. There are 15 people working together.

  - **Design**

    Design area is staffed by 7 people: 1 UX designer, 2 UI designers and 4 animation designers. They develop the audio-visual part of the games and help the Marketing area.

  - **Chief Information Officer (CIO)**

    Is the top executive for the information technology and computer systems that supports enterprise goals. There is one SysAdmin who is

working in data processing and storage and also, networks support and companies' security tasks.

- **Chief Information Security Officer (CISO)**

  Is the top executive for maintaining the enterprise vision, strategy, and program to protect assets and technologies. He is in charge of two persons:

  - **Information security management representative (ISMR)**

    Has the overall responsibility for the implementation, maintenance and improvement of an ISMS. He reports directly to CISO, he works in some projects with PM area.

  - **Information Security Officer (ISO)**

    The information security officer is responsible for implementing technical aspects of the security policy designed to protect information and some support. He reports to ISMR and works with the IT department. Moreover, he supports and the factory developing area code.

2.2. Scope

The scope of the ISMS is the ISO/IEC 27001 entire organization certification. We have just two locations and no more than 50 employees so the best option is to cover the whole organization. If Xintiba has a large organization with multiple divisions or business units, it may have separate ISMS.

The graph below shows the main areas, that the audit will focuses on:

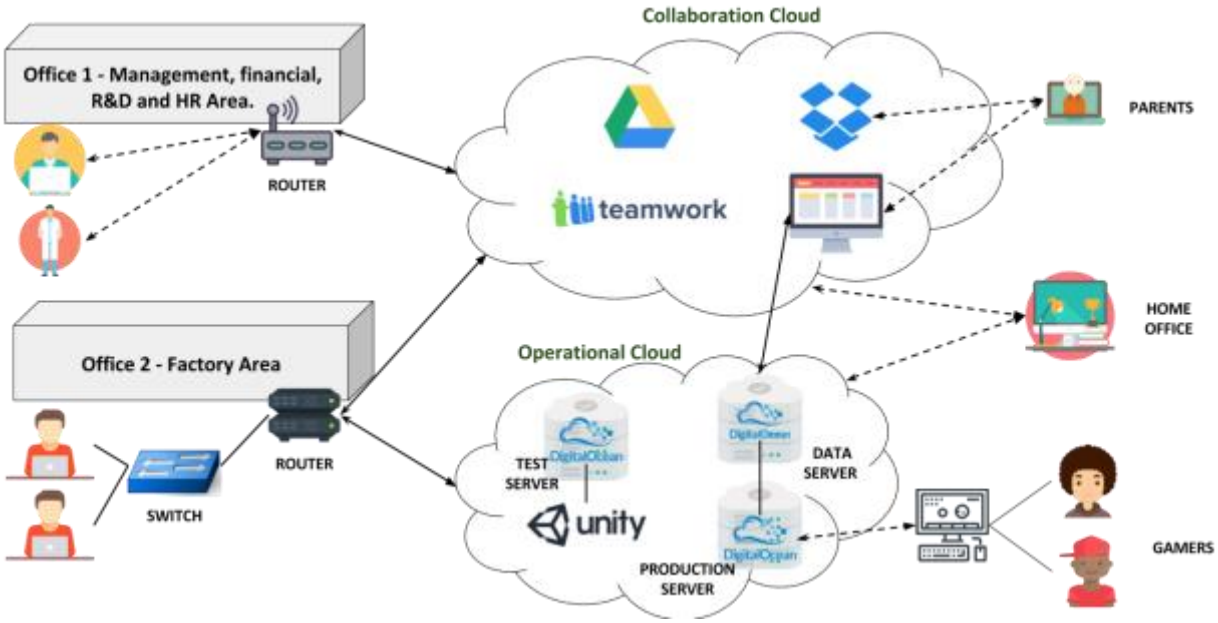

Figure 3: Xintiba main areas for the audit.

As we show in the graph the organization is divide into two different locations. We divide assets into two different supposed clouds with several connection types:

- Office 1 only uses Collaboration Cloud.
- Office 2 uses Collaboration and Operational Clouds.
- Home office is allowed and has access to the two clouds.
- Parents only have access to Dropbox and Xintiba Dashboard.
- Gamers don't have any direct access to the clouds.

In the first office, we have a wireless router and the second is connected via Ethernet to a wired router. There aren't any VPNs connections. Clouds are simulated to understand the organization.

Collaboration cloud groups all collaboration tools of Xintiba:

- G Suite (Internal use): Is the Google Cloud Suite which consists in Gmail, Docs, Drive and Calendar. Xintiba is trying to raise awareness for employees to save every document in Drive.
- Teamwork Projects (Internal use): This Project Management tool is used by every employee of Xintiba.
- Xintiba Dashboard (Internal and External use): Is a custom developed .NET platform.
- Dropbox (External use): Is used to share support documents, presentations and some reports.

Operational cloud has three servers with the following technical specifications:

Asset ID	**1**	**2**	**3**
Name	Data Server	Test Server	Production Server
Provider	Digital Ocean	Digital Ocean	Digital Ocean
SO	Ubuntu	Ubuntu	Ubuntu
RAM	8GB	4GB	16GB
Processor	4 Core	2 Core	8 Core
Memory	80GB SSD Disk	60GB SSD Disk	160GB SSD Disk
Transfer	5TB	4TB	6TB

Table 1: Xintiba Servers.

There are not controls and access restrictions to the servers, but the security provided by Digital Ocean.

Xintiba uses Unity, across-platform game engine used to develop video games for PC, consoles, mobile devices and websites. They use the Testing Server as part of the Testing Environment. Also, they have a Data Server to store and process data. Finally, the Production Server, which is connected by every gamer.

Data Server access is restricted to few users and there are not any disaster recovery plans (DRP).

Employees can use their personal mobile devices to access enterprise data and systems but there is not a BYOD (Bring Your Own Device) policy.

Only Windows computers use an antivirus program (Avast Endpoint Protection Plus) and the rest of the equipment is not protected. The are some Ubuntu and OS X computers.

2.3. ISO/IEC 27001 and 27002

ISMS protects its client and the companies' data against potential threats. Organizations can trust that the quality, safety, service and product reliability of their organizations have been protected to the highest level.

ISO/IEC 27001:2013 Information Technology – Security techniques – Information security management systems, is an information security management system (ISMS) managed by the International Organization for Standardization (ISO).

The main benefits of certificated of ISO 27001 is a greater added value to fight against competitors, have an efficient security cost management, comply with the law and help to effectively secure all confidential data. In addition, it can be used to improve the processes and services of the company.

ISO/IEC 27002: 2013 Information technology – Security techniques – Code of practice for information security controls, gives guidelines and details on how to implement the controls listed in ISO 27002. It can't be certificated.

ISO/IEC 27001 and its supporting document, ISO/IEC 27002, detail 133 security measures, which are organized into 11 sections and 39 control objectives. These sections specify the best practices for:

1. Business continuity planning.
2. System access control.
3. System acquisition, development and maintenance.
4. Physical and environmental security.
5. Compliance.
6. Information security incident management.
7. Personnel security.
8. Security organization.
9. Communication and operations management.
10. Asset classification and control.
11. Security policies.

We are going to start reviewing the implemented controls of the ISO 27001 on Xintiba. Based in the result we will be able to define a starting point.

2.4. Security Strategic Plan

A Security Strategic Plan sets priorities so Xintiba can efficiently and effectively address the management, control and protection of the information assets. This

plan also sets the strategic objectives for all futures initiatives that will be necessary and will constantly improve the companies' security. We are going to comply to the ISO/IEC 27001 standard.

The process is monitored and measured by an iteratively cycle which determines security requirements based on risk assessments and implements controls to mitigate them.

Xintiba has not established a ITSM and only has one employee to manage all security of the organization. It is necessary to determine a CISO (Chief Information Security Officer) to lead the effort to deliver the objectives of this plan. This person must be responsible for the overall management, direction and security of Xintiba. CISO should report the progress to CIO (Chief Information Officer).

The plan set few strategic objectives outlined below:

- Integrate security requirement into Xintiba process's: Security requirements have not a separate agenda, they must be present into all the processes.
- Measure progress and support continuous improvement of the ISMS: Meet the demands of the continuously improving cycle described before.
- Compliance with regulations and laws of México.
- Ensure Xintiba can recover its system and services in an appropriate time frame: Set a procedure to recover and protect Xintiba IT infrastructure and systems.
- Security Policy Development and Assessment: Define, review, support and control security policies and procedures for Xintiba. Notably for BYOD (Bring Your Own Device) and home office policies.
- Security vision: Create a vision of the future environment that meets each security objective.

We are going to implement the ISO/IEC 27001 standard as the first key initiative. This standard will help us achieve all the objectives described before.

3. Gap Analysis

We evaluate the capability levels of the ISO/IEC 27001 controls per the ISO/IEC 15504. This standard is a set of technical standard documents for the software development process and related business management functions. It describes the capability levels of the companies' processes:

Capability Level	Capability Level ISO/IEC 15504
0. Nonexistence	There is not a process defined or is not easy to identify.
1. Initial	Processes are not strictly plan or track.
2. Managed	Process is planned and tracked.
3. Defined	Process is performed and managed using a defined process.
4. Quantitatively Managed	The defined process is performed consistently to achieve its defined process goals.
5. Optimizing	Performance of the process is optimized to meet current and future business needs.

Table 2: ISO/IEC 15004 Capability Level Description.

We stars evaluating the capability levels of the ISO/IEC 27001:

ID	Section Name	Maturity
4	**Context of the organization**	**10%**
4.1	Understanding the organization and its context	Initial
4.2	Understanding the needs and expectations of interested parts	Initial
4.3	Determining the scope of the information security management system	Nonexistence
4.4	Information security management system	Nonexistence
5	**Leadership**	**0%**
5.1	Leadership and commitment	Nonexistence
5.2	Policy	Nonexistence
5.3	Organizational roles, responsibilities and authorities	Nonexistence
6	**Planning**	**0%**
6.1	Actions to address risks and opportunities	Nonexistence
6.2	Information security objectives and planning to achieve them	Nonexistence
7	**Support**	**0%**
7.1	Resources	Nonexistence
7.2	Competence	Nonexistence
7.3	Awareness	Nonexistence
7.4	Communication	Nonexistence
7.5	Documented information	Nonexistence
8	**Operation**	**0%**

8.1	Operational planning and control	Nonexistence
8.2	Information security risk assessment	Nonexistence
8.3	Information security risk treatment	Nonexistence
9	**Performance evaluation**	**0%**
9.1	Monitoring, measurement, analysis and evaluation	Nonexistence
9.2	Internal audit	Nonexistence
9.3	Management review	Nonexistence
10	**Improvement**	**0%**
10.1	Nonconformity and corrective action	Nonexistence
10.2	Continual improvement	Nonexistence

Table 3: ISO/IEC 27001 Capability levels evaluation.

The graph shows that Xintiba has only few process implemented in the 4 section of the standard:

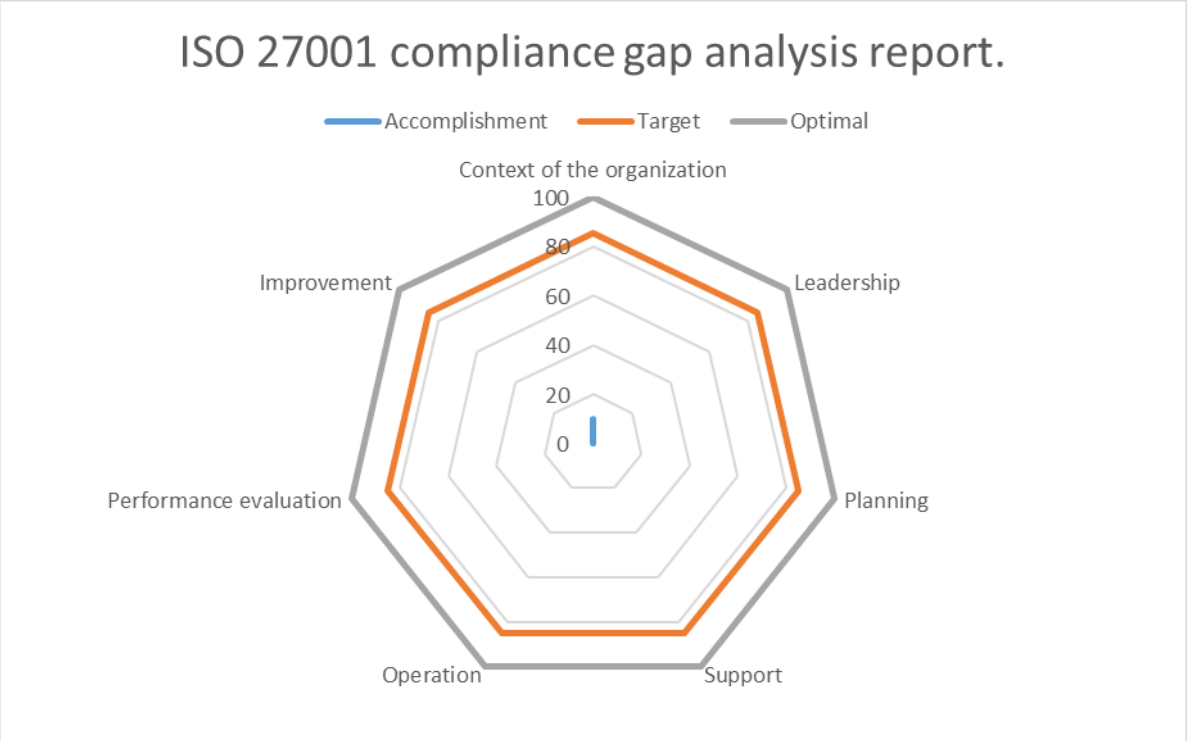

Figure 4: ISO 27001 compliance gap analysis report 1.

The following table reflects the results of the ISO/IEC 27002's process's controls capability level evaluation:

ID	Control	Applicable	Maturity
A.5 Information Security Policies			
A.5.1 Management direction for information security			
Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.			
A.5.1.1	Policies for information security	Yes	Nonexistence
A.5.1.2	Review of the policies for information security	Yes	Nonexistence

A.6 Organization of information security			
A.6.1 Internal organization			
Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.			
A.6.1.1	Information security roles and responsibilities	Yes	Initial
A.6.1.2	Segregation of duties	Yes	Initial
A.6.1.3	Contact with authorities	Yes	Nonexistence
A.6.1.4	Contact with special interest groups	Yes	Nonexistence
A.6.1.5	Information security in project management	Yes	Initial
A.6.2 Mobile devices and teleworking			
Objective: To ensure the security of teleworking and use of mobile devices			
A.6.2.1	Mobile device policy	Yes	Nonexistence
A.6.2.2	Teleworking	Yes	Nonexistence
A.7 Human resource security			
A.7.1 Prior to employment			
Objective: To ensure that employees and contractors understand the responsibilities and are suitable for the roles for which they are considered.			
A.7.1.1	Screening	Yes	Defined
A.7.1.2	Terms and conditions of employment	Yes	Defined
A.7.2 During employment			
Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.			
A.7.2.1	Management responsibilities	Yes	Nonexistence
A.7.2.2	Information security awareness, education and training		Nonexistence
A.7.2.3	Disciplinary process	Yes	Nonexistence
A.7.3 Termination and change of employment			
Objective: To protect the organization's interests as part of the process of changing or terminating employment.			
A.7.3.1	Termination or change of employment responsibilities	Yes	Nonexistence
A.8 Asset management			
A.8.1 Responsibility for assets			
Objective: To identify organizational assets and define appropriate protection responsibilities.			
A.8.1.1	Inventory of assets	Yes	Quantitatively Managed
A.8.1.2	Ownership of assets	Yes	Quantitatively Managed
A.8.1.3	Acceptable use of assets	Yes	Nonexistence
A.8.1.4	Return of assets	Yes	Managed
A.8.2 Information classification			
Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.			
A.8.2.1	Classification of information	Yes	Nonexistence
A.8.2.2	Labelling of information	Yes	Nonexistence

A.8.2.3	Handling of assets	Yes	Nonexistence
A.8.3 Media handling			
Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.			
A.8.3.1	Management of removable media	Yes	Nonexistence
A.8.3.2	Disposal of media	Yes	Nonexistence
A.8.3.3	Physical media transfer	Yes	Nonexistence
A.9 Access control			
A.9.1 Business requirements of access control			
Objective: To limit access to information and information processing facilities.			
A.9.1.1	Access control policy	Yes	Nonexistence
A.9.1.2	Access to networks and network services	Yes	Nonexistence
A.9.2 User access management			
Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.			
A.9.2.1	User registration and de-registration	Yes	Nonexistence
A.9.2.2	User access provisioning	Yes	Nonexistence
A.9.2.3	Management of privileged access rights	Yes	Initial
A.9.2.4	Management of secret authentication information users	Yes	Nonexistence
A.9.2.5	Review of user access rights	Yes	Nonexistence
A.9.2.6	Removal or adjustment of access rights	Yes	Defined
A.9.3 User responsibilities			
Objective: To make users accountable for safeguarding their authentication information.			
A.9.3.1	Use of secret authentication information	Yes	Nonexistence
A.9.4 System and application access control			
Objective: To prevent unauthorized access to systems and applications			
A.9.4.1	Information access restriction	Yes	Initial
A.9.4.2	Secure log-on procedures	Yes	Initial
A.9.4.3	Password management systems	Yes	Initial
A.9.4.4	Use of privileged utility programs	Yes	Nonexistence
A.9.4.5	Access control to program source code	Yes	Initial
A.10 Cryptography			
A.10.1 Cryptographic controls			
Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.			
A.10.1.1	Policy on the use of cryptographic controls	Yes	Nonexistence
A.10.1.2	Key management	Yes	Nonexistence
A.11 Physical and environmental security			
A.11.1 Secure areas			
Objective: To prevent unauthorized physical access, damage, and interference to the organization's information and information processing facilities.			

A.11.1.1	Physical security perimeter	Yes	Nonexistence
A.11.1.2	Physical entry controls	Yes	Nonexistence
A.11.1.3	Securing offices, rooms and facilities	Yes	Nonexistence
A.11.1.4	Protecting against external and environmental threats	Yes	Nonexistence
A.11.1.5	Working in secure areas	Yes	Nonexistence
A.11.1.6	Delivery and loading areas	Yes	Nonexistence
A.11.2 Equipment			
Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.			
A.11.2.1	Equipment siting and protection	Yes	Nonexistence
A.11.2.2	Supporting utilities	Yes	Nonexistence
A.11.2.3	Cabling security	Yes	Initial
A.11.2.4	Equipment maintenance	Yes	Nonexistence
A.11.2.5	Removal of assets	Yes	Nonexistence
A.11.2.6	Security of equipment and assets off-premises	Yes	Nonexistence
A.11.2.7	Secure disposal or reuse of equipment	Yes	Nonexistence
A.11.2.8	Unattended user equipment	Yes	Nonexistence
A.11.2.9	Clear desk and clear screen policy	Yes	Nonexistence
A.12 Operation Security			
A.12.1 Operational procedures and responsibilities			
Objective: To ensure correct and secure operations of information processing facilities.			
A.12.1.1	Documented operating procedures	Yes	Nonexistence
A.12.1.2	Change management	Yes	Nonexistence
A.12.1.3	Capacity management	Yes	Nonexistence
A.12.1.4	Separation of development, testing and operational environments	Yes	Defined
A.12.2 Protection from malware			
Objective: To ensure that information and information processing facilities are protected against malware.			
A.12.2.1	Controls against malware	Yes	Quantitatively Managed
A.12.3 Backup			
Objective: To protect against loss of data.			
A.12.3.1	Information backup	Yes	Quantitatively Managed
A.12.4 Logging and monitoring			
Objective: To record events and generate evidence			
A.12.4.1	Event logging	Yes	Nonexistence
A.12.4.2	Protection of log information	Yes	Nonexistence
A.12.4.3	Administrator and operator logs	Yes	Nonexistence
A.12.4.4	Clock synchronisation	Yes	Nonexistence
A.12.5 Control of operational software			
Objective: To ensure the integrity of operational systems.			
A.12.5.1	Installation of software on operational systems	Yes	Nonexistence
A.12.6 Technical vulnerability management			

Objective: To prevent exploitation of technical vulnerabilities.			
A.12.6.1	Management of technical vulnerabilities	Yes	Nonexistence
A.12.6.2	Restrictions on software installation	Yes	Initial
A.12.7 Information systems audit considerations			
Objective: To minimise the impact of audit activities on operational systems.			
A.12.7.1	Information systems audit controls	Yes	Nonexistence
A.13 Communications security			
A.13.1 Network security management			
Objective: To ensure the protection of information in networks and its supporting information processing facilities.			
A.13.1.1	Network controls	Yes	Nonexistence
A.13.1.2	Security of network services	Yes	Nonexistence
A.13.1.3	Segregation in networks	Yes	Initial
A.13.2 Information transfer			
Objective: To maintain the security of information transferred within an organization and with any external entity.			
A.13.2.1	Information transfer policies and procedures	Yes	Nonexistence
A.13.2.2	Agreements on information transfer	Yes	Nonexistence
A.13.2.3	Electronic messaging	Yes	Initial
A.13.2.4	Confidentiality or non-disclosure agreements	Yes	Managed
A.14 System acquisition, development and maintenance			
A.14.1 Security requirements of information systems			
Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.			
A.14.1.1	Information security requirements analysis and specification	Yes	Initial
A.14.1.2	Securing application services on public networks	Yes	Managed
A.14.1.3	Protecting application services transactions	Yes	Managed
A.14.2 Security in development and support processes			
Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.			
A.14.2.1	Secure development policy	Yes	Initial
A.14.2.2	System change control procedures	Yes	Managed
A.14.2.3	Technical review of applications after operating platform changes	Yes	Managed
A.14.2.4	Restrictions on changes to software packages	Yes	Managed
A.14.2.5	Secure systems engineering principles	Yes	Define
A.14.2.6	Secure developments environments	Yes	Define
A.14.2.7	Outsourced developments	Yes	Managed
A.14.2.8	System security testing	Yes	Quantitatively Managed

A.14.2.9	System acceptance testing	Yes	Managed
A.14.3 Test data			
Objective: To ensure the protection of data used for testing			
A.14.3.1	Protection of test data	Yes	Managed
A.15 Supplier relationships			
A.15.1 Information security in supplier relationships			
Objective: To ensure protection of the organization's assets that is accessible by suppliers.			
A.15.1.1	Information security policy for suppliers relationships	Yes	Define
A.15.1.2	Addressing security within supplier agreements	Yes	Managed
A.15.1.3	Information and communication technology supply chain	Yes	Managed
A.15.2 Supplier service delivery management			
Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.			
A.15.2.1	Monitoring and review of supplier services	Yes	Managed
A.15.2.2	Managing changes to supplier services	Yes	Managed
A.16 Information security incident management			
A.16.1 Management of information security incidents and improvements			
Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weakness.			
A.16.1.1	Responsibilities and procedures	Yes	Initial
A.16.1.2	Reporting information security events	Yes	Initial
A.16.1.3	Reporting information security weaknesses	Yes	Nonexistence
A.16.1.4	Assessment of and decisions on information security events	Yes	Initial
A.16.1.5	Response to information security incidents	Yes	Initial
A.16.1.6	Learning from information security incidents	Yes	Managed
A.16.1.7	Collection of evidence	Yes	Nonexistence
A.17 Information security aspects of business continuity management			
A.17.1 Information security continuity			
Objective: Information security continuity shall be embedded in the organization's business continuity management systems.			
A.17.1.1	Planning information security continuity	Yes	Nonexistence
A.17.1.2	Implementing information security continuity	Yes	Nonexistence
A.17.1.3	Verify, review and evaluate information security continuity	Yes	Nonexistence
A.18 Compliance			
A.18.1 Compliance with legal and contractual requirements			
Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security			

requirements.			
A.18.1.1	Identification of applicable legislation and contractual requirements	Yes	Initial
A.18.1.2	Intellectual property rights	Yes	Managed
A.18.1.3	Protection of records	Yes	Managed
A.18.1.4	Privacy and protection of personally identifiable information	Yes	Managed
A.18.1.5	Regulation of cryptographic controls	Yes	Managed
A.18.2 Information security reviews			
Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.			
A.18.2.1	Independent review of information security	Yes	Nonexistence
A.18.2.2	Compliance with security policies and standards	Yes	Nonexistence
A.18.2.3	Technical compliance review	Yes	Nonexistence

Table 4: ISO/IEC 27001's controls compliance audit.

Following a synthesis of the results, target and optimal.

ID	Section	Accomplishment	Target	Optimal
A.5	Information security policies	0 %	85%	100%
A.6	Organization of information security	8 %	85%	100%
A.7	Human resource security	2 %	85%	100%
A.8	Asset management	22 %	85%	100%
A.9	Access control	14 %	85%	100%
A.10	Cryptography	0%	85%	100%
A.11	Physical and environmental security	0.1 %	85%	100%
A.12	Operations security	2 %	85%	100%
A.13	Communications security	14 %	85%	100%
A.14	System acquisition, development and maintenance	46%	85%	100%
A.15	Supplier relationships	44%	85%	100%
A.16	Information security incident management	17%	85%	100%
A.17	Information security aspects of business continuity management	45%	85%	100%
A.18	Compliance	0%	85%	100%

Table 5: ISO 27001compliance summary; target and optimal.

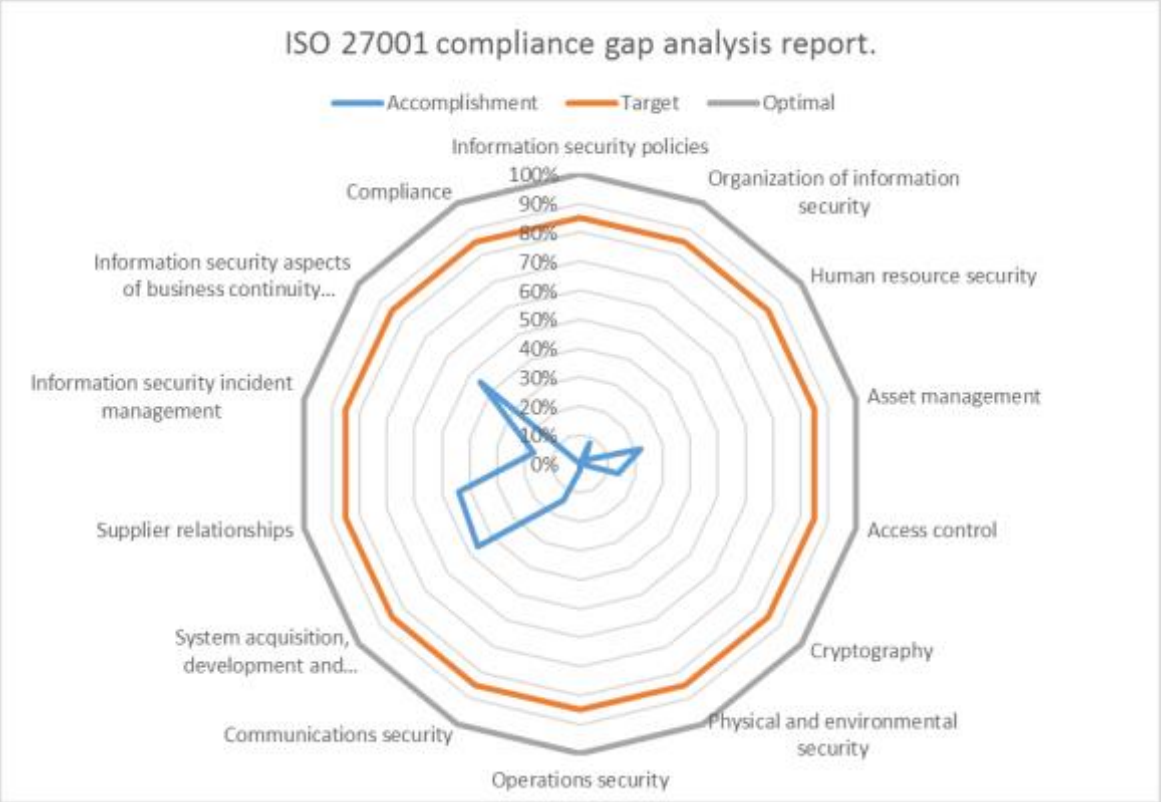

Figure 5: ISO 27001 compliance gap analysis report 2.

In conclusion, it can be determined that Xintiba processes are not capable, or maturate enough to meet the ISO 27001. So, we should work thoroughly in all Xintiba business processes if we want to be certified.

4. Document management system

4.1. Information security policy

The purpose of an information security policy is to provide a security framework that will ensure the protection of Xintiba' s physical and technological information assets. It is an open document that never finishes and is permanently updated as companies', technologies' and employee's requirements changed.

Xintiba privacy, access, confidentially, authentication and availability will be included and protected in this security plan. These will help to:

- Prevent waste or inappropriate use of Xintiba resources.
- Comply with contractual and legal requirements.
- Protect the reputation of Xintiba.
- Protect Xintiba IT from accidental or intentional damage.
- Protect the data stored from unauthorized accessed or alteration.
- Designate the required level of security for Xintiba.

The scope will cover entire organization. It includes all employees, third parties, and every guest who has access to Xintiba information technology resources.

It should address data, images, texts, programs, systems, hardware, paper and other technologies or assets.

Security plan is detailed in **Annex 1: Xintiba Information Security Policy.**

4.2. ISMS internal audit procedure

This internal audit is about management, validating the effectiveness of the ISMS. CISO is going to ensure Xintiba continually operates in compliance with the specified policies and procedures of ISO/IEC 27001 standard.

Internal audits include planning, executing, reporting and following up.

ISMS internal audit is detailed in **Annex 2: ISMS internal audit procedure.**

4.3. ISMS Key performance indicators

Xintiba evaluates the information security performance and the effectiveness of the information security management system.

The company uses key performance indicators (KPI) for monitoring, measuring, analysis and evaluating, as required, to ensure valid results. Xintiba holds appropriate documented information as evidence of the monitoring and measuring results.

Annex 3: ISMS Key Performance Indicators shows the procedure of performance evaluation.

4.4. ISMS Management review

Top management reviews the organization's information security management system on schedule dates to ensure its suitability and effectiveness.

Annex 4: ISMS Management Review Agenda define the management review process.

4.5. ISMS roles and responsibilities

Xintiba defines and communicates roles and authorities to ensure the security.

Annex 5: ISMS Roles and responsibilities contains more detail of ISMS roles and responsibilities.

4.6. Methodology for the risk management

Xintiba use MAGERIT V 3.0 methodology for the risk management. It implements the Risk Management Process within a working framework for government institutions to make decisions considering the risks derived from using information technologies.

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

Margerit is published and managed by the Spanish Ministry of Finance and Public Administration.

Annex 6: Methodology for the risk management contains more detail.

4.7. Statement of applicability

The applicability statement is a main link between the risk assessment and treatment and the implementation of ITSM. It is defined according with the ISO/IEC 27001:2013 suggested 114 controls in **Annex 7: Statement of applicability.**

5. Information Security Risk Assessment

The risk assessment process is designed to enable Xintiba to systematically identify, analyse and evaluate the information security risks associated with an information system or service along with the controls required to manage it.

This risk assessment has been carried out according to the methodology described in **Annex 6: Methodology for the risk management.**

5.1. Assets summary

Area	Asset		Value	Security elements				
	ID	Name	Avg	Con.	Int.	Ava	Auth.	Nonr.
[L] Installations	[L.1]	Office 1	4	3	3	3		
	[L.2]	Office 2	4	3	3	4		
[H] Hardware	[H.1]	Router Office1	2	3	4	4	3	3
	[H.2]	Router Office2	3	3	4	4	3	3
	[H.3]	Switch Office2	1	3	2	1	1	1
	[H.4]	Printer/Scanner Office1	1			2		
	[H.5]	Printer/Scanner Office2	1			1		
	[H.6]	Personal computing	3	4	5	5	5	5
	[H.7]	Mobile Phones	3	5	5	3	5	5
	[H.8]	Telephones	1	5	4	2	5	2
	[H.8]	Data Server	5	5	5	5	5	5
	[H.9]	Test Server	2	5	2	2	2	2
	[H.10]	Production Server	5	5	5	4	4	4
[SW] Software	[SW.1]	Xintiba Dashboard	4	5	5	4	5	3
	[SW.2]	Visual Studio	2	4	4	3	4	4
	[SW.3]	Endpoint Protection	2	3	3	2	3	3
	[SW.4]	Log App	2	2	5	2	2	2
[D] Data	[D.1]	Logs	4	2	5	2	2	2
	[D.2]	Backups	3	5	4	2	2	2
	[D.3]	Users Data	5	5	5	4	5	4
	[D.4]	Research Data	5	5	5	3	5	4
	[D.5]	Financial Data	4	4	5	2	4	5
[COM] Network	[COM.1]	Office1 Net	3	5	5	4	4	3
	[COM.2]	Office2 Net	4	5	5	4	4	3
	[COM.3]	Telephone Network	2	5	5	2	3	3
[S] Services	[S.1]	Unity	5	5	5	4	3	3
	[S.2]	G Suite	4	5	5	4	3	3
	[S.3]	Teamwork	2	2	2	3	1	1
[AUX] Auxiliary equipment	[AUX.1]	Air conditioning System	2			3		
[P] Personal	[P.1]	CEO	5			5		
	[P.2]	Financial	4			4		

		Manager						
	[P.3]	Sales and Marketing Manager	3			3		
	[P.4]	CIO	4			4		
	[P.5]	CISO	4			3		
	[P.6]	Security Specialist	3			3		
	[P.7]	Sys Admin	3			3		
	[P.8]	Researchers	5			5		

Table 6: Asset Summary.

Xintiba has no physical servers in their location so it easies assets protection. However, as a research company, employees become crucial for the company.

5.2. Threat analysis

The following table shows the assets described above relating them to the threats that they might be exposed to. Threats have been selected from the catalogue defined in Annex 6.

Area	Threat	Asset	Fre.	Security Elements			
				Con.	Int.	Ava.	Auth.
[N] Natural Disaster	[N.1] Fire	[L] Installations	1			5	
		[H] Hardware	1			5	
		[AUX] Auxiliary equipment	1			5	
	[N.2] Water Damage	[L] Installations	1			5	
		[H] Hardware	1			4	
		[AUX] Auxiliary equipment	1			4	
[I] Of Industrial origin	[I.1] Hardware of software failure	[SW] Software	2			4	
		[H] Hardware	2			4	
		[AUX] Auxiliary equipment	2			3	
	[I.2] Power Interruption	[HW] Hardware	2			5	
		[AUX] Auxiliary equipment	2			5	
	[I.3] Communications service failure	[COM] Network	3			5	
	[I.4] Interruption	[AUX]	3			2	

	of essential services	Auxiliary equipment					
[E] Errors and Unintentional Failures	[E.1] Users' errors	[SW] Software	4	2	2	2	
		[D] Data	4	2	2	2	
	[E.2] Administrator errors	[SW] Software	3	3	2	4	
		[D] Data	2	4	2	3	
		[COM] Network	2	3	2	5	
		[S] Services	2	2	2	4	
	[E.3] Monitoring logging	[S] Services	2			4	4
		[D] Data	2			4	4
		[SW] Software	2			4	4
	[E.4] Configuration errors	[S] Services	2	2	2	4	4
		[D] Data	2	3	3	3	
		[SW] Software	2	2	2	4	2
		[HW] Hardware	2			3	
		[COM] Network	2	2	2	5	
	[E.5] Organizational deficiencies	[P] Personal	4			3	
	[E.6] Malware diffusion	[SW] Software	3	2	3		4
	[E.7] Re-routing errors	[S] Services	1	3	2		4
		[SW] Software	1	2	1		3
		[COM] Network	2	2	1		3
	[E.8] Entry of Incorrect Information	[D] Data	4		3		
	[E.9] Information Degradation	[D] Data	3		4		
	[E.10] Destruction of information	[D] Data	1			5	
	[E.11] Disclosure of information	[D]Data	2	5			
	[E.12] Software Vulnerabilities	[SW] Software	4	4	2	3	
	[E.13] Defects in software maintenance	[SW] Software	3		3	2	

	[E.14] Defects in hardware maintenance	[HW] Hardware	2			4	
[A] Wilful attacks	[A.1] Manipulation of configuration	[S] Services	2	4	4	4	3
		[D] Data	2	4	4	3	3
		[SW] Software	2	4	3	3	2
		[HW] Hardware	2	4	3	4	3
		[COM] Network	2	4	2	4	3
	[A.2] Masquerading of user identity	[S] Services	2	4	2		3
		[SW] Software	2	4	2		3
		[COM] Network	2	4	4		3
	[A.3] Abuse of access privileges	[S] Services	2	4	3		
		[SW] Software	2	4	3		
		[HW] Hardware	2	3	3		
		[COM] Network	2	3	4		
	[A.4] Misuse	[S] Services	3			2	
		[SW] Software	3			3	
		[HW] Hardware	2			2	
		[COM] Network	2			4	
		[AUX] Auxiliary equipment	2			3	
		[L] Installations	2			2	
	[A.5] Malware diffusion	[SW] Software	3	3	4	5	2
	[A.6] Unauthorized access	[S] Services	2	4			3
		[D] Data	2	5			4
		[SW] Software	2	3			2
		[HW] Hardware	2	3			4
		[COM] Network	3	4			4
		[AUX] Auxiliary equipment	1	1			1
		[L] Installations	1	2			2

	[A.7] Traffic Analysis	[COM] Network	2	4			
	[A.8] Entry of false information	[D] Data	3		3		
	[A.9] Destruction of information	[D] Data	2		5		
	[A.10] Disclosure of information	[D] Data	3	3			
	[A.11] Software manipulation	[SW] Software	2	4	3		2
	[A.12] Denial of Service	[S] Services	2			4	
		[HW] Hardware	2			4	
		[COM] Network	3			5	
	[A.13] Destructive attack	[HW] Hardware	1		2	3	
		[COM] Network	2		4	4	
		[AUX] Auxiliary equipment	1		1	1	
		[L] Installations	1		2	4	
	[A.14] Extortion	[P] Personal	1	5	5		4
	[A.15] Social engineering	[P] Personal	3	4	4		4

Table 7: Threat Analysis Report.

5.3. Potential impact

Once the analysis of the assets presented in the previous tables and the analysis of the threats, has been completed we can calculate the impact that these can cause to the company.

The following table presents details of the results:

Asset		Value				Impact				Potential Impact			
ID	Name	Con.	Int.	Ava	Auth.	Con.	Int.	Ava.	Auth.	Con.	Int.	Ava.	Au.
[L.1]	Office 1	3	3	3				5				15	
[L.2]	Office 2	3	3	4								15	
[H.1]	Router Office1	3	4	4	3	4	2	4	2	12	8	16	6
[H.2]	Router Office2	3	4	4	3					12	8	16	6
[H.3]	Switch Office2	3	2	1	1					12	4	4	2
[H.4]	Printer/Scanner Office1			2								8	
[H.5]	Printer/Scanner Office2			1								4	

[H.6]	Personal computing	4	5	5	5					16	10	20	10
[H.7]	Mobile Phones	5	5	3	5					20	10	12	10
[H.8]	Telephones	5	4	2	5					20	8	8	10
[H.8]	Data Server	5	5	5	5					20	10	20	10
[H.9]	Test Server	5	2	2	2					20	4	8	4
[H.10]	Production Server	5	5	4	4					20	10	16	8
[SW.1]	Xintiba Dashboard	5	5	4	5	3	4	3	2	15	20	12	10
[SW.2]	Visual Studio	4	4	3	4					12	16	9	8
[SW.3]	Endpoint Protection	3	3	2	3					9	12	6	6
[SW.4]	Log App	2	5	2	2					6	20	6	4
[D.1]	Logs	2	5	2	2	5	4	3	1	10	20	6	2
[D.2]	Backups	5	4	2	2					25	16	6	2
[D.3]	Users Data	5	5	4	5					25	20	12	5
[D.4]	Research Data	5	5	3	5					25	20	9	5
[D.5]	Financial Data	4	5	2	4					20	20	6	4
[COM.1]	Office1 Net	5	5	4	4	4	3	5	3	20	15	20	12
[COM.2]	Office2 Net	5	5	4	4					20	15	20	12
[COM.3]	Telephone Network	5	5	2	3					20	15	10	9
[S.1]	Unity	5	5	4	3	3	4	5	2	15	20	20	6
[S.2]	G Suite	5	5	4	3					15	20	20	6
[S.3]	Teamwork	2	2	3	1					6	8	15	2
[AUX.1]	Air conditioning System			3				2				6	
[P.1]	CEO			5				5				25	
[P.2]	Financial Manager			4								20	
[P.3]	Sales and Marketing Manager			3								15	
[P.4]	CIO			4								20	
[P.5]	CISO			3								15	
[P.6]	Security Specialist			3								15	
[P.7]	Sys Admin			3								15	
[P.8]	Researchers			5								25	

Table 8: Threats potential impacts.

5.4. Residual Impact and Risk Value

It is impossible to completely eliminate a risk. However, according to the methodology of risk described in Annex 6, the possibility of those risks may decrease to a more acceptable level. This remaining risk after the measures are implemented is known as residual and the organization will make the decision to coexist with it.

We determine the Acceptable Risk of >=35/125 points according with the following formula:

Acceptable Risk = Active Value * Impact * Frequency.

Asset		Fre.	Potential Impact				Risk				Acceptable Risk
ID	Name		Con.	Int.	Ava.	Aut.	Con.	Int.	Ava.	Aut.	
[L.1]	Office 1	1			15				15		Acceptable
[L.2]	Office 2	1			15				15		Acceptable
[H.1]	Router Office1	1	12	8	16	6	12	8	16	6	Acceptable
[H.2]	Router Office2	1	12	8	16	6	12	8	16	6	Acceptable
[H.3]	Switch Office2	1	12	4	4	2	12	4	4	2	Acceptable
[H.4]	Printer/Scanner Office1	1			8				8		Acceptable
[H.5]	Printer/Scanner Office2	1			4				4		Acceptable
[H.6]	Personal computing	2	16	10	20	10	32	20	40	20	Nonacceptable
[H.7]	Mobile Phones	2	20	10	12	10	40	20	24	20	Nonacceptable
[H.8]	Telephones	2	20	8	8	10	40	16	16	20	Nonacceptable
[H.8]	Data Server	1	20	10	20	10	20	10	20	10	Acceptable
[H.9]	Test Server	1	20	4	8	4	20	4	8	4	Acceptable
[H.10]	Production Server	1	20	10	16	8	20	10	16	8	Acceptable
[SW.1]	Xintiba Dashboard	3	15	20	12	10	45	60	24	30	Nonacceptable
[SW.2]	Visual Studio	2	12	16	9	8	24	32	18	19	Acceptable
[SW.3]	Endpoint Protection	1	9	12	6	6	9	12	6	6	Acceptable
[SW.4]	Log App	2	6	20	6	4	12	40	12	8	Nonacceptable
[D.1]	Logs	2	10	20	6	2	20	40	12	4	Nonacceptable
[D.2]	Backups	2	25	16	6	2	50	32	12	8	Nonacceptable
[D.3]	Users Data	3	25	20	12	5	75	60	36	36	Nonacceptable
[D.4]	Research Data	1	25	20	9	5	25	20	9	5	Acceptable
[D.5]	Financial Data	1	20	20	6	4	20	20	6	4	Acceptable
[COM.1]	Office1 Net	3	20	15	20	12	60	45	60	36	Nonacceptable
[COM.2]	Office2 Net	3	20	15	20	12	60	45	60	36	Nonacceptable
[COM.3]	Telephone Network	2	20	15	10	9	40	30	20	18	Nonacceptable
[S.1]	Unity	3	15	20	20	6	45	60	60	18	Nonacceptable
[S.2]	G Suite	2	15	20	20	6	30	40	40	12	Nonacceptable
[S.3]	Teamwork	3	6	8	15	2	18	24	45	6	Acceptable
[AUX.1]	Air conditioning System	1			6				6		Acceptable
[P.1]	CEO	2			25				50		Nonacceptable
[P.2]	Financial Manager	2			20				40		Nonacceptable
[P.3]	Sales and Marketing Manager	2			15				30		Acceptable
[P.4]	CIO	1			20				20		Acceptable
[P.5]	CISO	1			15				15		Acceptable
[P.6]	Security	1			15				15		Acceptable

	Specialist										
[P.7]	Sys Admin	1			15				15		Acceptable
[P.8]	Researchers	1			25				25		Acceptable

Table 9: Acceptable assets risks.

5.5. Analysis of results

We have seen the results of the risk in the assets, as it may happen over and over.

Assets that exceed the acceptable risk threshold do not mean that they will not be included in the improvement plans. Priority will be given to assets that exceed the threshold and subsequently to those approved.

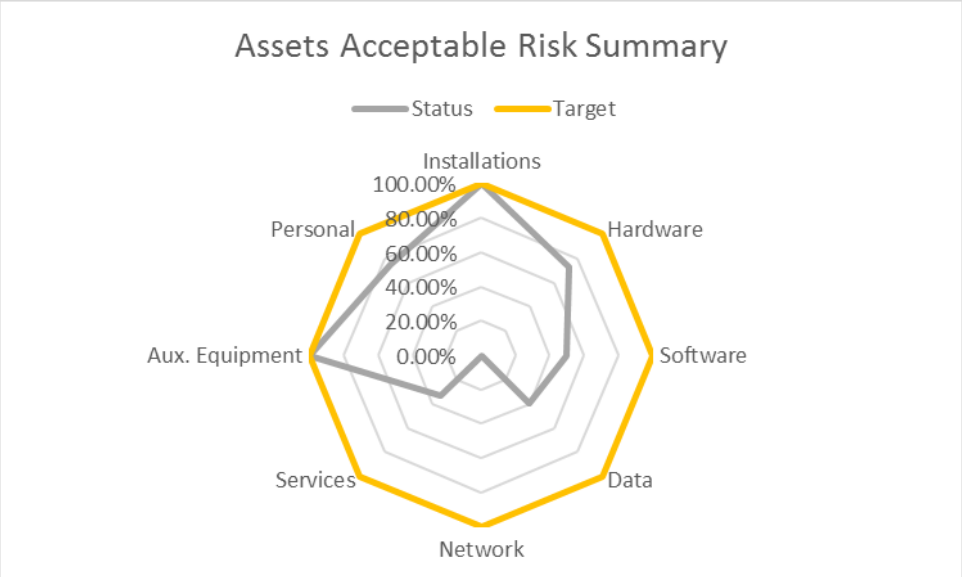

Figure 6: Assets Acceptable Risk Summary.

In the graph above we can see how services, network, data and software are the most critical asset categories and with higher levels of risk.

Figure 7: Assets Security Categories Summary.

We can see how availability and authenticity are the most exposed aspects of the organization. For example, application data contain confidential data that could undoubtedly identify an individual, therefore they are subject to additional risk.

6. Proposal Projects

At this point, we know the current level of risk of the assets in the organization and also, the main threats to the assets.

We are looking to mitigate the current risk in the organization and evolve ISO compliance to its proper level. The declaration of applicability defined all the controls that are suitable and therefore it is necessary to elaborate the corresponding project proposals to provide such controls.

The proposed projects gathers a set of recommendations identified in the risk analysis phase to facilitate their execution. Projects are economically quantified and planned over time, establishing deadlines for achieving their objectives.

6.1. Proposals

ID	**1.**
Name	**Xintiba Security Policies**
Starting date	10/11/2016
Finishing date	27/11/2016
Estimated budget	$90,000 MXN
Assets Involved	[P.1] CEO; [P.2] Financial Manager; [P.3] Sales and Marketing Manager; [P.4] CIO; [P.5] CISO; [P.6] Security Specialist; [P.7] Sys Admin; [P.8] Researchers
ISO Reference	5. Leadership
Scope	Whole Organization
Threats to mitigate	Avoid risk of breaking security policies, like confidentiality or integrity.
Objectives	Making sure every employee and partner complies with Xintiba Security Policies.
Description	Face-to-face security policies training shall take place.
KPIs	- Percentage of employees approving the training exam. - Security policies signed by the CEO.

Table 10: P – Xintiba Security Policies.

ID	**2.**
Name	**Xintiba Security Workshops**
Starting date	27/11/2016
Finishing date	01/12/2016
Estimated budget	$30,000 MXN
Assets Involved	[P.1] CEO; [P.2] Financial Manager; [P.3] Sales and Marketing Manager; [P.4] CIO; [P.5] CISO; [P.6] Security Specialist; [P.7] Sys Admin; [P.8] Researchers

ISO Reference	A.6 Organization of information security A.7 Human resource security A.8 Asset Management A.9 Access control
Scope	Whole Organization
Threats to mitigate	[E.1] Users' errors; [E.2] Administrator errors; [E.4] Configuration errors; [E.5] Organizational deficiencies; [E.6] Malware diffusion; [E.11] Disclosure of information; [A.14] Extortion; [A.15] Social engineering
Objectives	Educate Xintiba employees about the importance of security.
Description	Security training will be held for three days. It will review Xintiba's security policies, roles, responsibilities and security basis.
KPIs	1.- Percentage of employees aproving the training exam.

Table 11: P – Xintiba Security Workshops.

ID	**3.**
Name	**Asset Management**
Starting date	21/11/2016
Finishing date	23/12/2016
Estimated budget	$60,000 MXN
Assets Involved	[H.1] Router Office 1; [H.2] Router Office 2; [H.3] Switch Office2; [H.4] Printer/Scanner Office 1; [H.5] Printer/Scanner Office 1; [H.6] Personal Computing; [H.7] Mobile Phones; [H.8] Telephones; [H.9] Data Server; [H.10] Test Server; [H.11] Production Server
ISO Reference	8. Asset management
Scope	Whole Organization
Threats to mitigate	[E.1] Users' errors; [E.2] Administrator errors; [E.3] Monitoring logging; [E.4] Configuration errors; [E.5] Organizational deficiencies; [E.8] Entry of Incorrect Information; [E.9] Information Degradation; [E.10] Destruction of information; [E.11] Disclosure of information; [A.1] Manipulation of configuration; [A.6] Unauthorized access; [A.8] Entry of fake information; [A.9] Destruction of information; [A.10] Disclosure of information
Objectives	Making sure assets are in our owned inventory, properly used, and returned, when an employee or external party finishes their task.
Description	Identify organizational assets and define appropriate protection responsibilities. SysAdmin is going to be the owner of every asset. He is going to be audited monthly by the CISO.
KPIs	- Percentage of asset not inventoried. - Percentage of asset without owner. - Percentage of asset not returned.

Table 12: P – Asset Management.

ID	**4.**

Name	**Implementation of a Business Endpoint Protection**
Starting date	01/12/2016
Finishing date	15/12/2016
Estimated budget	$20,950.00 MXN (50 Keys) per year and $20,000 MXN for Xintiba management.
Assets Involved	[D.1] Logs; [D.2] Backups; [D.3] Users Data; [D.4] Research Data; [D.5] Financial Central
ISO Reference	A.12 Operations security
Scope	Whole Organization
Threats to mitigate	[A.5] Malware diffusion; [A.6] Unauthorized access; [A.9] Destruction of information; [A.11] Software manipulation; [E.6] Malware diffusion; [E.12] Software Vulnerabilities; [E.13] Defects in software maintenance
Objectives	Protect organization against malware and attacks.
Description	- Protect multiple platforms - PCs, Macs, and Servers. - Access to browser-based console with complete control over the behavior of antivirus on endpoint devices. - Firewall protection for remote endpoints. - Complete overview of current status of entire environment with immediate alerts. - Data Destructor.
KPIs	- Number of enrolled computers. - Number of malware cleaned up. - Amount of Spam blocked. - Amount of business information deleted. - Number of enrolled computers infected. - Number of enrolled servers infected. - Percentage of satisficed users. - Percentage of satisficed administrators.

Table 13: P – Implementation of a Business Endpoint Protection.

ID	**5.**
Name	**Set up a Third Party VPN Solution.**
Starting date	01/12/2016
Finishing date	15/12/2016
Estimated budget	$69,000.00 MXN (50 licenses) per year and $25,000 for Xintiba.
Assets Involved	[D.1] Logs; [D.2] Backups; [D.3] Users Data; [D.4] Research Data; [D.5] Financial Data
ISO Reference	A.6 Organization of information Security A.9 Access Control A.13 Communications Security
Scope	Whole Organization
Threats to mitigate	[E.4] Configuration errors; [E.11] Disclosure of information; [A.5] Malware diffusion; [A.7] Traffic Analysis; [A.10] Disclosure of information

Objectives	Secure communications.
Description	VPNs may allow employees to securely access to Internet everywhere.
KPIs	- Number of users using VPN connections. - Connection quality indicators. - Percentage of satisficed users.

Table 14: P – Set up a Third Party VPN Solution.

ID	**6.**
Name	**Renew Office Routers**
Starting date	01/12/2016
Finishing date	5/12/2016
Estimated budget	$10,000.00 MXN
Assets Involved	[COM.1] Office1 Net; [COM.2] Office2 Net
ISO Reference	A.9 Access Control A.13 Communications Security
Scope	Xintiba Routers
Threats to mitigate	[A.1] Manipulation of configuration; [A.7] Traffic Analysis; [A.12] Denial of Service
Objectives	Protect Xintiba Offices Networks.
Description	New routers will have firewall and the most up to date encryption protocols to protect network against attacks.
KPIs	- Number of successful intrusions. - Number of Spam and DDOS mitigated.

Table 15: P – Renew Office Routers.

ID	**7.**
Name	**Sucuri Website Protection**
Starting date	01/12/2016
Finish date	05/12/2016
Estimated budget	$6000 MXN per year and $4000 for Xintiba.
Assets Involved	[SW.1] Xintiba Dashboard
ISO Reference	A.12 Operations Security A.14 System acquisition, development and maintenance
Scope	Xintiba Websites
Threats to mitigate	[A.1] Manipulation of configuration; [A.2] Hiding of user identity; [A.3] Abuse of access privileges; [A.5] Malware diffusion; [A.6] Unauthorized access; [A.8] Entry of false information; [A.9] Destruction of information; [A.10] Disclosure of information; [A.11] Software manipulation; [A.12] Denial of Service
Objectives	Protect Xintiba Websites
Description	Website Malware Removal & Clean Up, Continuous Scans for Malware & Hacks, Website Blacklist Monitoring & Removal, Website Application Firewall (WAF), Distributed Denial of

	Service (DDoS)Mitigation and SSL & PCI Compliance.
KPIs	- Number of malware detected. - Number of malware cleaned up. - Number of Spam and DDOS mitigated.

Table 16: P – Sucuri Website Protection.

ID	**8.**
Name	**Black Box Audit by a Third Party**
Starting date	01/12/2016
Finishing date	31/12/2016
Estimated budget	$58,000.00 MXN
Assets Involved	[SW.1] Xintiba Dashboard; [SW.2] Visual Studio; [COM.1] Office1 Net; [COM.2] Office 2 Net; [D.1] Logs; [D.2]; Backups; [D.3] Users Data; [D.4] Research Data; [D.5] Financial Data
ISO Reference	A.12 Operations Security A.14 System acquisition, development and maintenance
Scope	Xintiba Websites and Servers
Threats to mitigate	[A.1] Manipulation of configuration; [A.2] Hiding users' identity; [A.3] Abuse of access privileges; [A.5] Malware diffusion; [A.6] Unauthorized access; [A.8] Entry of false information; [A.9] Destruction of information; [A.10] Disclosure of information; [A.11] Software manipulation; [A.12] Denial of Service
Objectives	Identify security vulnerabilities of Xintiba websites and servers.
Description	The team will only have access to public accessible information about the target environment. This type of test aims to simulate the real-world scenario of external attackers targeting and attempting to compromise Xintiba systems.
KPIs	- Number of vulnerabilities that could be exploited by an attacker. - Applicability of recommended mitigation strategies.

Table 17: P –Black Box Audit by a Third Party.

ID	**9.**
Name	**White Box Audit by a third party**
Starting date	01/12/2016
Finishing date	31/12/2016
Estimated budget	$68,000.00 MXN
Assets Involved	[SW.1] Xintiba Dashboard; [SW.2] Visual Studio; [COM.1] Office1 Net; [COM.2] Office 2 Net; [D.1] Logs; [D.2]; Backups; [D.3] Users Data; [D.4] Research Data; [D.5] Financial Data
ISO Reference	A.12 Operations security A.14 System acquisition, development and maintenance.
Scope	Xintiba Websites and Servers
Threats to mitigate	[E.1] Users' errors; [E.2] Administrator errors; [E.3] Monitoring logging; [E.4] Configuration errors; [E.5] Organizational deficiencies; [E.6] Malware diffusion; [E.7] Re-routing errors;

	[E.8] Entry of Incorrect Information; [E.9] Information Degradation; [E.10] Destruction of information; [E.11] Disclosure of information; [E.12] Software Vulnerabilities; [E.13] Defects in software maintenance;
Objectives	Tests internal structures or workings of an applications of Xintiba.
Description	White-box testing is a method of testing the application at the level of the source code.
KPIs	- Revealed hidden errors.

Table 18: P –White Box Audit by a Third Party.

6.2. Project Planning

Xintiba is a small company and every employee is located in the same place so this helps to the project implementations. The objective is to close all projects before finishing 2016. The following table summarize proposed projects deadlines:

ID	Name	Days	Budget	Start	Finish
1	Xintiba Security Policies	17	$90,000 MXN	10/11/2016	27/11/2016
2	Xintiba Security Workshops	4	$30,000 MXN	27/11/2016	01/12/2016
3	Asset Management	30	$60,000 MXN	21/11/2016	23/12/2016
4	Business Endpoint Protection	15	$40,950 MXN	01/12/2016	15/12/2016
5	Set up a Third Party VPN Solution	15	$85,000 MXN	01/12/2016	15/12/2016
6	Renew Office Routers	5	$10,000 MXN	01/12/2016	05/12/2016
7	Sucuri Website Protection	5	$10,000 MXN	01/12/2016	05/12/2016
8	Black Box Audit by a third party	31	$58,000 MXN	01/12/2016	31/12/2016
9	White Box Audit by a third party	31	$68,000 MXN	01/12/2016	31/12/2016

Table 19: P – Proposed plans time line.

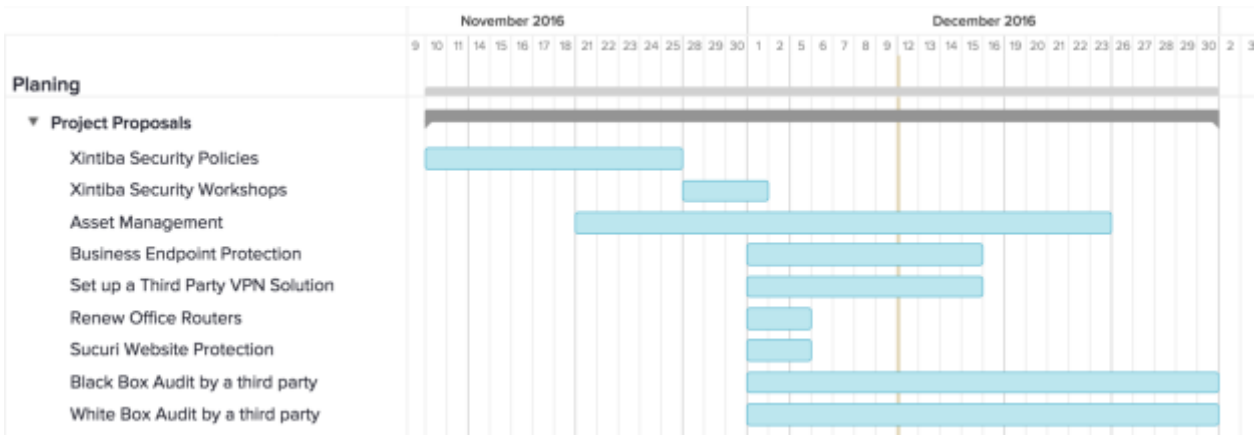

Figure 8: Proposed Projects Gantt Chart.

6.3. Summary of results

The action plan proposed through the implementation of the indicated projects is defined in order of the importance of the identified risks and priorities.

Firstly, we start working on Xintiba security policies. Having defined them, employee face-to-face training is planned to ensure every employee and partner complies with Xintiba Security Policies. Also, some security workshops are planned to educate Xintiba employees about the importance of security. This first part is focused on raising the awareness of end users.

Secondly, we are going to define an Assets Management procedure to identify organizational assets and define appropriate protection responsibilities. Afterwards, there is a Business Endpoint Protection implementation, a Third Party VPN solution and the Sucuri Website Protection deployment. We are going to finish with a Black and White audits by a Third Party company to Xintiba websites and servers.

Assuming that every project is properly executed, these proposals are going to improve the current ISO 27001 compliance level, as we can see in the following charts:

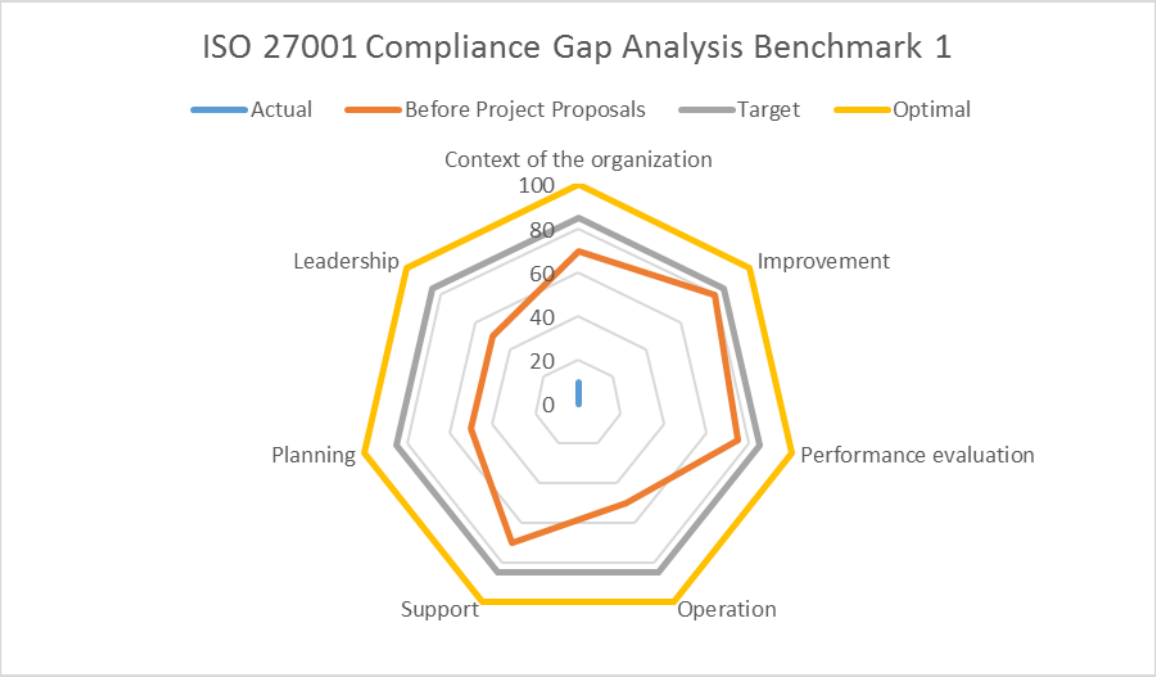

Figure 9: ISO 27001 Compliance Gap Analysis Benchmark 1.

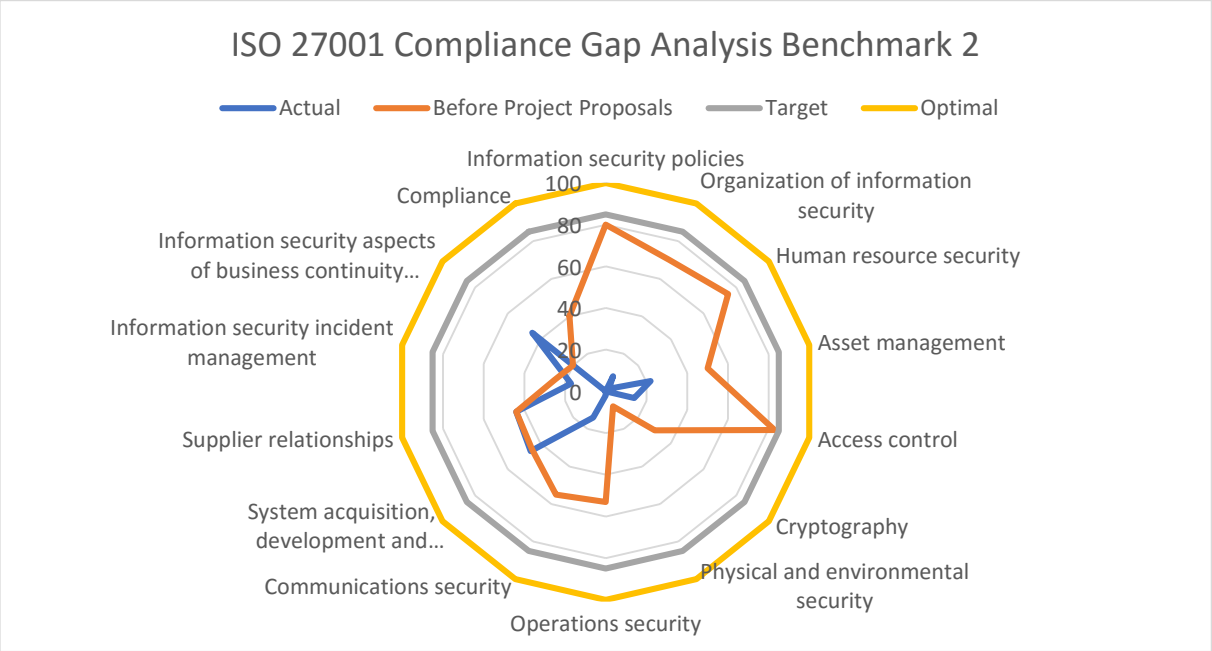

Figure 10: ISO 27001 Compliance Gap Analysis Benchmark 2.

7. Compliance Audit

For the moment we haven't finish all proposed project but we can estimate, according to the work done up until now, the final compliance results:

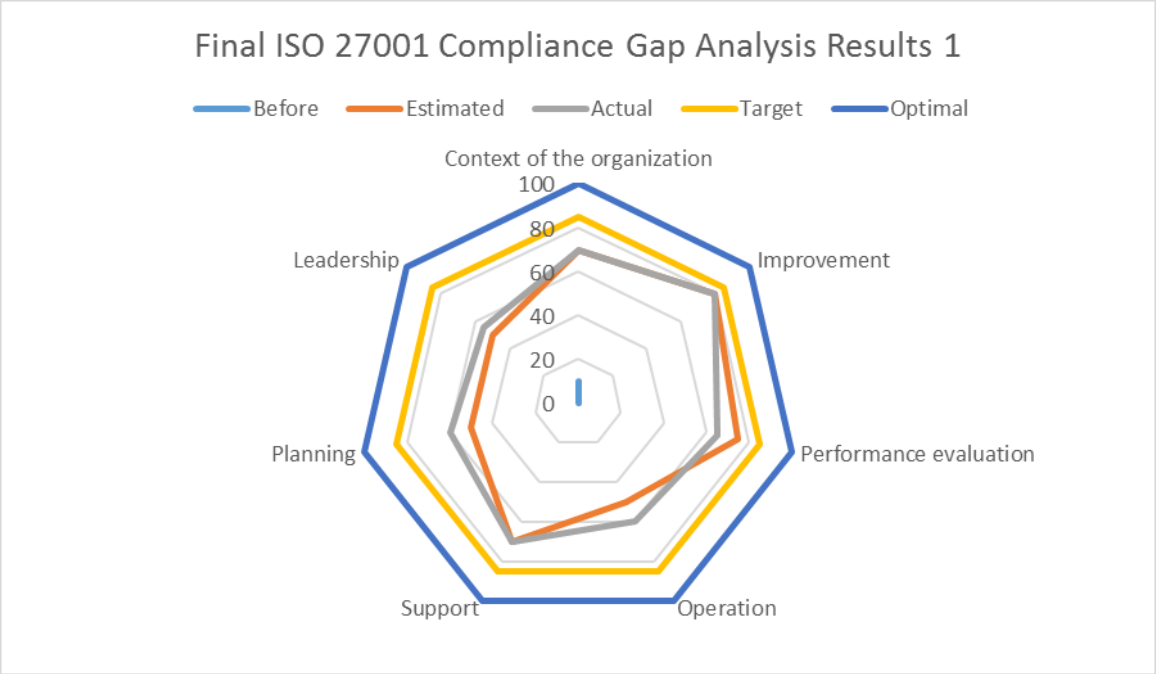

Figure 11: Final ISO 27001 Compliance Gap Analysis Results 1.

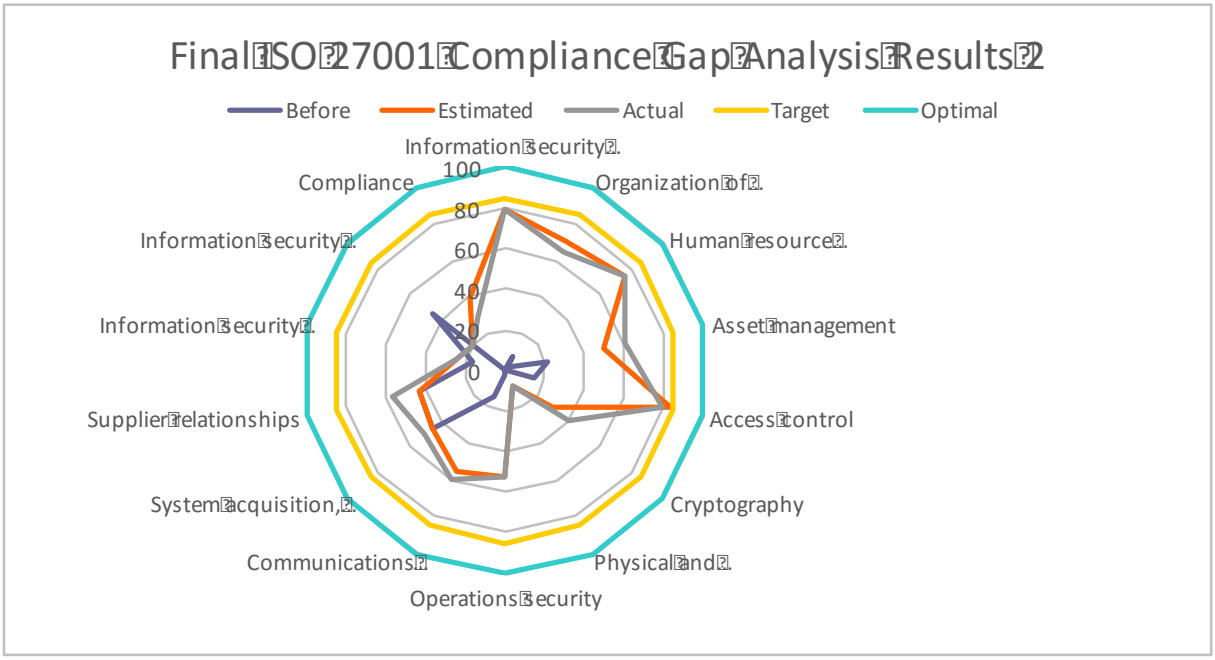

Figure 12: Final ISO 27001 Compliance Gap Analysis Benchmark 2.

As we can see in the following graphs, the improvement in a few weeks is high. Nevertheless, more needs to be done to make the final target a reality.

Next initiatives are going to focus in move up Nonexistence and Initial controls and is expected to finish 2017 with a high maturity levels to start the ISO 27001 certification in 2018.

It is noteworthy that employees are more compromised with the security since we start this project. This is very important because it's going to help keeping and improving faster the maturity of the organization security.

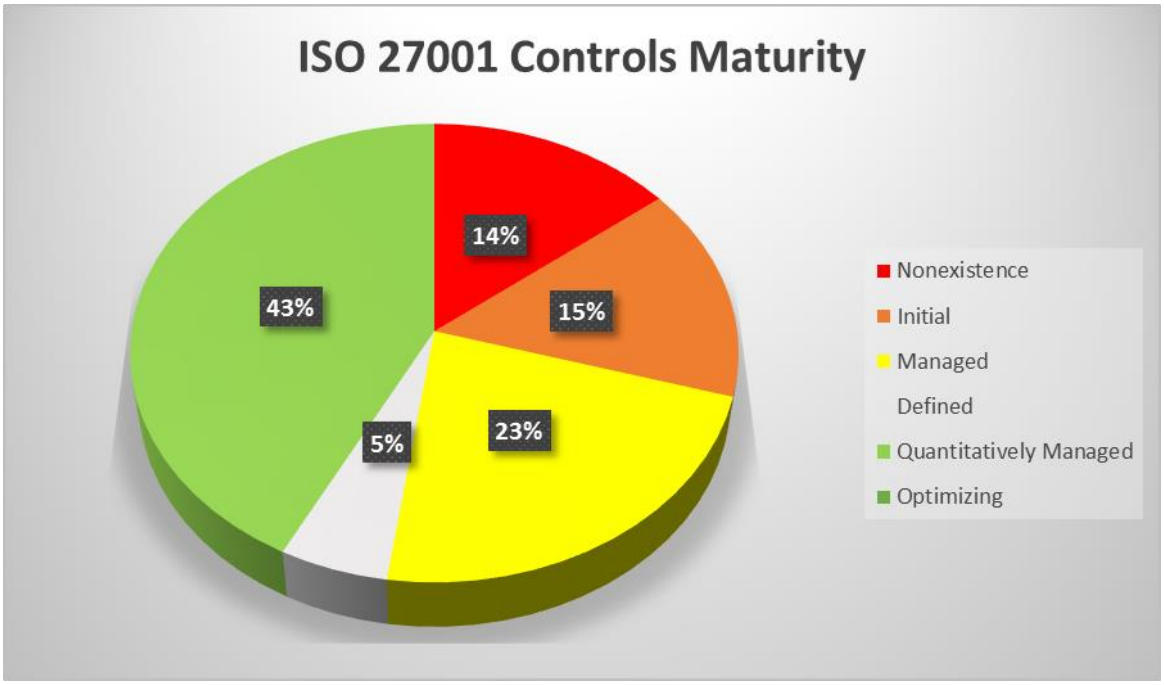

Figure 13: ISO 27001 Controls Maturity.

Compliance audit report is detailed in **Annex 8: Compliance Audit Report.**

8. Conclusions

We have finished the project complying with the proposed objectives but we expected to reach more maturity level of security. First steps were easy but as we advance it´s becoming more difficult. Therefore, we haven´t gotten last maturity level in any category but we've reached 43% percent of Quantitatively Managed level.

We want to point out that Xintiba employees were committed for the beginning and this helped to the success of the project. Some employees were less focused but the CEO talked to them personally to guarantee that that was not going to be a problem.

We had some problems with Third Party employees and companies. It was hard to explain them that from now on we must follow some security measures. But finally, they are doing their part correctly.

We have realized that it is important to work with third-party employees who can provide another point of view because we ourselves sometimes do not realize how exposed we are. For this reason, in the 2017 budget is contemplated external audit services. Also, they are going to help us defining the business processes related with the security of information.

At the beginning, we follow the project planning properly but finally we closed some projects in parallel because the year was to end and we wanted to finish before. Despite of this fact, the planning and methodology was fulfilled properly.

Now it is very important not to lose focus and maintain security as a daily task.

We see this project as the first step to introduce security as a key element in Xintiba. We are going to continue working hard to start the ISO/IEC 27001 certification at the final semester of 2017. Employee are motivated and looking forward to continuing working on these kinds of projects.

9. Glossary

- ISMS: An information security management system (ISMS) is a set of policies concerned with information security management or IT related risks.

- ISO/IEC 27001:2013: Is an information security standard that was published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint ISO and IEC subcommittee, ISO/IEC JTC 1/SC 27. It is a specification for an information security management system (ISMS).

- ISO/IEC 27002: Is an information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC), titled Information technology – Security techniques – Code of practice for information security management.

- ISO/IEC 15504: Is a set of technical standards documents for the computer software development process and related business management functions. It is one of the joint International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) standards.

- Magerit: Is a methodology for Information Systems Risk Analysis and Management published by Spanish Ministry of Finance and Public Administration.

- Capability Maturity Model Integration: Is a process level improvement training and appraisal program. Administered by the CMMI Institute, a subsidiary of ISACA. CMMI defines the following maturity levels for processes.

- Asset: Resources of the information system or related with it that are necessary for the organisation to operate correctly and to attain the objectives proposed by its management.

- Threat: Potential cause of an incident which may result in harm to a system or organisation. [ISO/IEC 27000:2014].

- Vulnerability: Weakness of an asset or control that can be exploited by one or more threats. [ISO/IEC 27000:2014].

- Authenticity: Property that an entity is what it claims to be. [ISO/IEC 27000:2014].

- Availability: Property of being accessible and usable upon demand by an authorized entity. [ISO/IEC 27000:2014].

- Integrity: Property that data has not been modified or deleted in an unauthorised and undetected manner.

- Confidentially: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [ISO/IEC 27000:2014].

- Statement of applicability: A formal document for a group of safeguards that states whether they apply to the information system being studied or whether they are meaningless.

- Residual Impact: The impact remaining in the system after the implementation of the safeguards described in the information security plan.

- Residual Risk: The risk remaining in the system after the implementation of the safeguards described in the information security plan.

- Disaster Recovery Plan: Is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster.

10. References

1. ISO/IEC 27001:2013

1.1. Wikipedia
1.2. ISO/IEC 27001:2013 standard
1.3. Planning for ISO 27001
http://www.isaca.org/Journal/archives/2011/Volume-4/Documents/jpdf11v4-Planning-for-and.pdf
1.4. ISO 27001 FAQ
http://advisera.com/27001academy/faqs/
1.5. Problem defining scope
http://advisera.com/27001academy/blog/2010/06/29/problems-with-defining-the-scope-in-iso-27001/
1.6. CISO
https://en.wikipedia.org/wiki/Chief_information_security_officer

2. Capability Maturity Model Integration
https://en.wikipedia.org/wiki/Capability_Maturity_Model_Integration

3. ISO/IEC 15504
https://en.wikipedia.org/wiki/ISO/IEC_15504

4. Overview of Threat and Risk Assessment
https://www.sans.org/reading-room/whitepapers/auditing/overview-threat-risk-assessment-76

5. Information Security Plan
5.1. MTU standard for acceptable use
http://www.security.mtu.edu/policies-procedures/standards-acceptable-use.pdf
5.2. Consensus standard for acceptable use
https://www.sans.org/security-resources/policies/general/pdf/acceptable-use-policy
5.3. Connecticut University
http://security.uconn.edu/wp-content/uploads/sites/251/2014/05/information-security-master-plan2.pdf
5.4. Backup policy Info
http://www.comptechdoc.org/independent/security/policies/backup-policy.html

6. Disaster recovery Plan
https://en.wikipedia.org/wiki/Disaster_recovery_plan

7. Internal audit procedure
7.1. Info
http://etc.ksu.edu.sa/sites/etc.ksu.edu.sa/files/ksu_etc_isms_pro_internal_audit_procedure_v1.1_0.pdf
7.2. Non-conformities Info

https://www.linkedin.com/pulse/iso27001-non-conformities-minor-major-almerindo-graziano

8. ISMS measure
8.1. KPI´s
http://advisera.com/27001academy/blog/2016/02/01/key-performance-indicators-for-an-iso-27001-isms/
8.2. Neupart measurement
http://www.neupart.com/hubfs/Pdf/iso27001isms-kpi.pdf?t=1439909692755
8.3. ISO 27001 management review
http://iso27001guide.com/isms-requirements/performance-evaluation/management-review/iso-27001-management-review-agenda/
8.4. CISO
http://advisera.com/27001academy/knowledgebase/what-is-the-job-of-chief-information-security-officer-ciso-in-iso-27001/

9. Risk Analysis and Management

9.1. Magerit – Version 3.0
9.2. Magerit described by Enisa
https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_magerit.html
9.3. Risk Analysis – Daniel Cruz Allende – PID_00177810

10. Information Security Risk Assessment

10.1. Definitions
- http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA
- http://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the three-components-of-the-cia-triad/

11. Annexes

Annex 1 – Xintiba Information security policy

1. Purpose

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.

2. Reason for policy

These will help to:

- Prevent waste or inappropriate use of Xintiba resources.
- Comply with contractual and legal requirements.
- Protect the reputation of Xintiba.
- Protect Xintiba IT from accidental or intentional damage.
- Protect the data stored from unauthorized accessed or alteration.
- Designate the required level of security for Xintiba.

3. Scope

Scope might be the entire organization. It included all employees, third parties, and every guest, without exception, who has access to Xintiba information technology resources.

It should address data, images, text, programs, systems, hardware, paper and others technologies or assets.

4. Enforcement

Employees must report every known non-compliance with any requirement of this policy to the responsible of CISO (Chief Information Security Officer) (xxxx@xintiba.com).

Failure to comply with this policy may subject you to disciplinary action and to potential penalties. All violations of the policy will be recorded and monitored.

5. Acceptable use of IT resources

Xintiba technology resources may not be used for malicious or unlawful purposes. Users must comply with all policies, licensing, contractual agreement and legal requirements of those technologies.

Users must use only resources they are authorized to use and only in the manner and to the extent authorized.

All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 5 minutes or less. The screen must be locked or logged off when the device is unattended.

User must safeguard every physical key, password, computer account, or network account that allows one to access to their or Xintiba accounts. Xintiba accepts no responsibility for every personal or unauthorized use of the user's resources.

User must use extreme caution when using Public Internet or opening e-mail attachments received from unknown senders, which may contain malware.

User are responsible for exercising good judgment regarding the reasonableness of personal use. They have to take care Xintiba resources as if they were their own or even better.

6. Unacceptable use of IT resources

Users are prohibited from engage any activity that is illegal under regulations, laws, licensing or Xintiba policies while using owned resources.

Users are not permitted to share authentication details or provide access to their Xintiba accounts to anyone else.

User are not allowed to use a false identity and outside email account.

Users are not allowed to download or install any software in Xintiba resources. Any special requirement will be reviewed by CISO (Chief Information Security Officer) (xxxx@xintiba.com).

User are not allowed to use resources for private purposes during working hours.

Users are not allowed to use mobile storage.

7. Use of internet

Xintiba does not restrict internet access, employees are encouraged to use Internet as a tool to improve their work. During working hours, network is only for business purposes and may not be interfered or disrupted with personal use. Out of working hours, the personal use is allowed.
Xintiba will permanently monitor browsing time and pages visited by employees and / or third parts according to current legislation.

Users are responsible to exercise good judgement when accessing Internet sites. Sites which perform illegal activities, against moral ethics or that they can be unsafe are not permitted.

User are not allowed to unauthorized exchange of proprietary information of the company, its customers and / or employees, with third parties.

8. Email

The email account should be used exclusively for the performance of assigned duties. Mailboxes contained messages and information are owned by Xintiba.

User are not allowed to send unauthorized data or confidential information via the Internet.

User are not allowed to send files containing executable extensions under any circumstances.

User may not open attachments by email from unknown senders for security reasons.

All messages sent must comply with the standard and corporate image format defined by the organization and must remain in all cases the corporate legal message confidentiality.

Admins, for safety reasons or unacceptable uses, are able to temporarily disable email accounts of users.

9. Backup

Employees should not keep information relevant locally. All information must be stored in the cloud (Google Drive).

However, technologies infrastructure area defines together with heads of departments all critical data to back up. It includes, at least, each server of the company.

Every month an incremental backup tape shall be made. At the end of every year employee's data will be achieved.

Users that need files restored must submit a request to CISO (Chief Information Security Officer) (xxxx@xintiba.com).

10. Passwords

Employees are required to protect and use strong passwords. Also change them, according to an established time. System of the company are configured by IT to allow only passwords complying with the following requirements:

- Minimum length - 14 characters recommended.
- Four types of characters: Lowercase, Uppercase, Numbers and Special characters.
- Password history - Require a number of unique passwords before an old password may be reused.

- Maximum password age - 60 days

Passwords are not allowed to written, send or revealed under any circumstance. If anyone asks for a password, refer them to IT area.

11. Network

The network structure and configuration shall be documented by IT area.

Factory area, located in Office 2, has an isolated network. This is only available via Ethernet and is necessary to apply for a permit to CISO (Chief Information Security Officer) (xxxx@xintiba.com).

IT area will be monitoring and auditing network looking for threats.

Annex 2 – ISMS Internal Audit Procedure

1. Purpose

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 and best practices can be gathered and applied.

2. Scope

This procedure applies to Xintiba ISMS, which includes, data, images, systems, infrastructure, processes, services, technologies or assets. As well as all staff and users that are directly or indirectly employed, who uses information assets owned Xintiba.

3. Enforcement

Employees must report recommendations or any anomaly detected during the audit procedure to the CISO (Chief Information Security Officer) (xxxx@xintiba.com).

Compliance with this procedure is mandatory and ISMS (Information Security Manager) should ensure continuous compliance monitoring within Xintiba head departments. Compliance with the statements of this procedure is a matter of periodic review and any violation of the procedure will be reviewed by the ISMS Steering Committee.

4. Roles and responsibilities

4.1 ISMR (Information Security Management Representative)

- Leads the ISMS internal audit activities.
- Plans the audit, prepares the working documents and briefs the audit team.
- Reviews the corrective and preventive actions and the follow-up audits done based on the internal audit report submitted.
- Maintains the confidentiality of the audit results.
- Report to the auditee the audit results clearly and without delay.
- Approves the annual audit plan and ensure that all steps within this procedure are executed correctly and timely.

4.2 Audit team member

- Follow up ISMR Plan.
- Reports the non-conformities and recommends suggestions for improvement.
- Maintains the confidentiality of the audit findings.

- Acts in an ethical manner at all times.
- ISMR and the audit team member must develop a plan to follow up audit findings.

4.3 Auditee

- Assist ISMR and audit team member.
- Receives, considers and discusses the audit report.

5. Procedure

Internal audit process will be created and it will contain all the scheduled and potential audits for the whole calendar year (12 months).

This section reflects the broad activities/steps to be carried out in the procedure:

Step 1: Prepare and submit annual audit plan

First of all, security related incidents that have occurred since last audit and also the security relate personnel issues have to be reviewed. They will be included in the annual audit plan.

The audit plan shall include:

- A detailed work plan and time schedule.
- Audit objective and scope.
- Department responsible.
- Audit team members. The number of auditors depends on the audit area size.
- Definition of the work methodology to be used.

As soon as ISMR finishes, the internal annual audit plan will be reviewed and approved by the ISMS steering committee.

Upon approval of the annual audit plan, the ISMR communicates the plan to the interested parties (Auditees).

Step 2: Audit execution

The auditors will perform the internal audit using a customized checklist to be reviewed which includes:

- The agreed actions from previous audits and reviews that have been implemented.
- The ISMS compliance with ISO/IEC 2700:2013.
- The implementation of ISO/IEC 27002:2013 controls.
- Appropriate risk assessment methodology.

Audit team collected findings, through examinations of documents, observation of activities and interviews, in the checklist described above. The work of the audit team is not only to focus on the check-lists. Also they have to report

nonconformities and controls of ITSM that they believe that are not correct or inappropriate. Audit findings and their corresponding non-conformance must be communicated to the ISM manager at the end of each audit.

Step 3: Audit reporting

Based on the audit findings, the ISMS Audit Team prepares the audit report. This is a report referring to findings, non-compliance, unresolved issues, etc. Every audit finding must be labeled according to this priority levels:

- Major non-conformity –Affects the overall effectiveness of the ISMS and the ability of the organization to achieve its information security objectives. Non-conformities have a direct effect on information security specifically on the preservation of confidentiality, integrity and availability of information assets.

- Minor non-conformity – Affect the overall effectiveness of the ISMS and the ability of the organization to achieve its information security objectives. Minor non-conformity has an indirect effect on information security.

All conformity requires appropriate documented corrective actions. In addition, auditors may provide advice for process improvements or good practice suggestions. Also suggest preventive actions.

Finally, in a closing meeting, ISMR summarizes audit results to the ISMS Steering Committee.

Step 4: Audit Follow-up and closure

According to the audit findings and the non-conformance level, an action plan and follow up audit must be developed. Auditees are responsible for resolving these non-conformities.

Auditor and auditee agreed corrective actions to resolve non-conformities and they continue with a follow-up audit. They are limited to the nonconformance and the same audit mechanisms will be used.

An audit will not be considered completed and closed until all corrective actions or measures have been successfully implemented to the satisfaction of the ISMR.

6. Competence of auditors

6.1 Auditors competences

The following requirements apply to every auditor:

a) Audit principles, methods and processes.
b) Applicable laws, regulations and other obligations knowledge.

c) Organization/business context knowledge.
d) Managing the team, planning the audit, and audit quality assurance processes.
e) ISMS measurement techniques.
f) Related and/or relevant ISMS standards, industry best practices, security policies and procedures.

6.2 Demonstration of auditor competence

Auditors must be able to demonstrate their knowledge and experience for example through:

a) Holding recognized ISMS-specific qualifications.
b) ISMS training courses certification.
c) Updated continuous professional development records.

7. Records

ISMS internal audits should generate the following formal records:

- Audit Plan/Notification.
- Audit checklist/Observation sheet.
- Internal audit Report.
- Non-conformity/Corrective and Preventive Action report.

Annex 3 – ISMS Key Performance indicators

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

The following table shows how Xintiba is going to monitor, measure, analyse and evaluate the ISMS performance:

KPI	How	When	Who	Target	Optimized
Effective Security Policy	Frequent surveys to employees.	Monthly	ISM	< 70%	< 95%
Incident management	Number of security breaches reduced on a year on year basis.	Annually	CISO	10%	20%
Percent of business initiatives supported by the ISMS	Comparing all services/processes of the organization.	Annually	ISM	90%	100%
Number of security-related service downtimes	Reviewing operational reports.	Monthly	CISO	1	0
Duration of service interruptions	Reviewing operational reports.	Monthly	CISO	15 seconds	0 seconds
Incident resolution time	Reviewing operational reports.	Monthly	CISO	15 minutes	5 minutes
Number of improvement initiatives	Reviewing initiatives in order to improve ISMS.	Annually	ISM	3	5
Level of employee's satisfaction with ISMS	Data collected through interviews	Annually	ISM	High	Excellent
% of IT budgets used to managingIT risks	Relate working man hours spent on IT risks	Annually	ISM	15	20
Number of new threats and risks identified compared to previous risk	Compare total numbers of risk identified with previous IT-risk assessments.	Annually	CISO	10	30

assessment					
Time between identification of non-compliance and implementation of fixes	Relate time of reported noncompliance issues of security incidents with actual implementation time.	Monthly	CISO	48 hours	24 hours
Number of security incidents caused by attacks from the NET	Number of security incidents caused by attacks from the NET.	Monthly	CISO	2	0.5
Number of Security incidents caused by malicious software	Number of Security incidents caused by malicious software	Monthly	CISO	5	0.5

Table 1: ISMS Key Performance Indicators.

Annex 4 – ISMS Management review agenda

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.

The meeting consists of the following items:

1. Review purpose of the meeting and also the attendee list.
2. Review the status of actions from previous management reviews.
3. Reviews ISMS scope, objectives and performance.
4. Review external and internal issues that are relevant to the information security management system.
5. Discuss information security policies and procedures.
6. Review and discuss the results of KPI's performance.
7. Opportunities for continual improvement.
8. Confirm actions and people responsible for these.
9. Schedule next meeting.

Meeting agenda will be documented as evidence of the results of management reviews.

Annex 5 – ISMS Roles and Responsibilities

ISMS must be composed of a team that is responsible to create, maintain, monitor and improve the system. This document describes the different roles and responsibilities to carry out proper operation and management of information security are detailed.

Positions related directly to ISMS:

1. Chief Information Security Officer (CISO): Coordinates all the activities related to securing the information in a Company. It includes compliance, documentation, risk management, human resources, relationship with top managers, asset management, communication and business continuity.
2. Information security management representative (ISMR): Has the overall responsibility for the implementation, maintenance and improvement of an ISMS. He reports directly to CISO.
3. Information Security Officer: The information security officer is responsible for implementing technical aspects of the security policy designed to protect information and any support. He reports to ISMR and works with the IT department.

CISO is more executive, ISMR is the responsible of the ISMR and Information Security officer is the security soldier.

Related authorities to ISMS:

1. Security Committee: Consist in ISMS Steering Committee (CISO, ISMR, ISO and CIO), CEO and HR manager. However, outside consultants will be invited to some meetings. Some duties of the committee:

    a. Review performance of ISMS Steering Committee.
    b. Support initiatives of ISMS Steering Committee.
    c. Review with management programs to educate Company employees about information security issues and policies.
    d. Review and approve the risk governance structure, key risk policies and critical risk tolerances adopted by company.
    e. Review and approve internal audit working plan to ensure alignment with identified risks and company needs.
    f. Review policies and frameworks relating to access controls, critical incident response plans, business continuity and disaster recovery, physical and remote system access, and perimeter protection of IT assets.

2. ISMS Steering Committee: Include CISO, ISMR, ISO and CIO.

    Its main responsibility is to ensure the implementation, maintenance, control, monitoring and measurement of ISMS. Eventually they have to present results and initiatives to the Security Committee.

Annex 6 – 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.

The summary of steps is provided below:

Step	Task	Description
1.1	Identify Assets	Describe and assign assets for an employee.
1.2	Identify Threats	Identify threats that could affect to assets.
1.3	Valuation of Assets	Qualitative and quantitative evaluate assets.
1.4	Valuation of Threats	Determine the exposure of an affected asset by a threat.
1.5	Determination of the potential impact	Impact is the measurement of the damage to an asset arising from the occurrence of a threat.
1.6	Residual impact and risk value	The risk value its calculated by integrating the frequency that a specific event can occur in our systems.
1.7	Security control effectiveness	This parameter shows the effect of security controls to protect against detected risks.

Table 1: Risk management summary.

Risk analysis is a methodical approach to estimate the risk, following specific steps:

1. Assets

1.1. Identify Assets:

All assets must be valuated and assigned for an employee in the company. Each owner of the assets must have measures for treatment of risks. Assets include: information, data, services, software, hardware, communications, media, facilities, and personnel.

There are two essential types of assets in an information system determined by:

1. Information it contains: Is evaluate based on the loss of value caused by an incident.

2. Services it provides: Is evaluated based on the loss of value of an interruption to the service.

Both types of assets will be valued qualitative or quantitative. For qualitative scale, is not possible to estimate the value of each asset so we are going to order them by relevance:

1.2. Identify threats:

After evaluating the assets it's time to identify threats that could affect to them. Threats are things that could happen to our assets and affect their value.

The following is a catalogue of possible threats to the assets in an information system:

ID	Type	Threat
N.1	**Natural Disaster**	Fire
N.2		Water Damage
I.1	**Of Industrial Origin**	Hardware of software failure
I.2		Power interruption
I.3		Communications service failure
I.4		Interruption of utilities
I.5		Media degradation
E.1	**Errors and Unintentional Failures**	Users' errors
E.2		Administrator errors
E.3		Monitoring (logging) errors
E.4		Configuration errors
E.5		Organizational deficiencies
E.6		Malware diffusion
E.7		Re Routing errors
E.8		Entry of incorrect information
E.9		Information degradation
E.10		Destruction of information
E.11		Disclosure of information
E.12		Software vulnerabilities
E.13		Defects in software maintenance
E.14		Defects in hardware maintenance
A.1	**Wilful attacks**	Manipulation of the configuration
A.2		Masquerading of user identity
A.3		Abuse of access privileges
A.4		Missuse
A.5		Malware diffusion
A.6		Unauthorized access
A.7		Traffic Analysis
A.8		Entry of false information
A.9		Destruction of information
A.10		Disclosure of information
A.11		Software manipulation
A.12		Denial of service

A.13		Destructive attack
A.14		Extortion
A.15		Social engineering

Table 2: Threats.

1.3. Valuation of assets

The following tables shows defined criteria for giving a value to an asset that can be qualitative, quantitative or both:

Qualitative scale	Value	Description
VH: Very High	5	Crucial to accomplish ISMS objectives.
H: High	4	Very important to accomplish ISMS objectives.
M: Medium	3	Important to accomplish ISMS objectives.
L: Low	2	Relatively little important to accomplish ISMS objectives.
VL: Very low	1	Irrelevant to accomplish ISMS objectives.

Table 3: Qualitative Scale of Valuation of assets.

Quantitative scale	Value	Description (MXN Currency)
VH: Very High	5	$500.000 MXN
H: High	4	$300.000 MXN
M: Medium	3	$100.000 MXN
L: Low	2	$20.000 MXN
VL: Very low	1	$5.000 MXN

Table 4: Quantitative Scale of Valuation of assets.

In addition, there are four elements considered the most crucial components for assets security to take into account:

- Confidentiality: Involves a set of rules or a promise that limits access or places restrictions on certain types of information.
- Integrity: Involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle.
- Availability: Availability of information refers to ensuring that authorized parties are able to access the information when needed.
- Authenticity: Is the property that ensures that the identity of a subject or resource is the identity claimed

1.4. Valuation of threats

To determine the exposure of an affected asset by a threat is necessary to estimate considering two aspects:

- Degradation: The amount of damage done to the value of the asset.
- Likelihood: How often the threat occurs.

The possibility is numerically modeled as a rate of occurrence. It uses the annual rate of occurrence as a measure of the possibility of something happening:

Possibility scale	Value	Description
VH: Very high	5	Daily
H: High	4	Weekly
M: Medium	3	Monthly
L: Low	2	Annually
VL: Very Low	1	Every few years

Table 5: Likelihood qualitative modeled scale.

1.5. Determination of the potential impact

Impact is the measurement of the damage to an asset arising from the occurrence of a threat. By knowing the value of the assets (in various dimensions) and the degradation caused by the threats, the impact on the system can be calculated.

It's calculated with the following formula:

Potential Impact = Asset * Impact

To perform this analysis, it is estimate by range of impacts:

Potential Impact	Value	Percentage
VH: Very high	25	100%
H: High	20	75%
M: Medium	15	50%
L: Low	10	25%
VL: Very Low	5	5%

Table 6: Likelihood qualitative modeled scale.

1.6. Residual impact and risk value

The risk value it's calculated by integrating the frequency that a specific event can occur in our systems:

Risk = Potential Impact * Frequency

To define the acceptable level of risk we used the following formula:

Acceptable Risk = Active Value * Impact * Frequency

Before the determination of the risk, it's time to choose to avoid, to treat, to transfer or to accept the risk. The listed below:

- Avoid: Stop the activity that would give rise to the risk. Risk avoidance is only selected when the probabilities to exploit the associated opportunity are very high.
- Treat: Implement controls to reduce the likelihood and/or impact of the risk eventuating.
- Transfer: Transfer or share all or part of the impact of the risk eventuating with a third party.

- Accept: When a risk is being within the business's defined risk tolerance level it can be accepted.

1.7. Security control effectiveness.

This parameter shows the effect of security controls to protect against detected risks.

When reducing a risk, there are two ways of acting against it: Reduce vulnerability (frequency of occurrence) or reduce the impact caused by this risk.

Reduce Vulnerability frequency	Value	Percentage
VH: Very high	5	95%
H: High	4	75%
M: Medium	3	50%
L: Low	2	30%
VL: Very Low	1	10%

Table 7: Range of vulnerability frequency reduction.

Reduce Vulnerability Impact	Value	Percentage
VH: Very high	5	95%
H: High	4	75%
M: Medium	3	50%
L: Low	2	30%
VL: Very Low	1	10%

Table 8: Range of vulnerability impact reduction.

Annex 7 – Statement of applicability

Statement of applicability contains the necessary checks which the justification of inclusion or exclusion. The statement is contained in the following table:

ID	Control	Applicable	Justification
A.5 Information Security Policies			
A.5.1 Management direction for information security			
Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.			
A.5.1.1	Policies for information security	Yes	Provide support and guidance to the management of Xintiba information security.
A.5.1.2	Review of the policies for information security	Yes	The policies shall be reviewed to ensure their continuing suitability, adequacy and effectiveness.
A.6 Organization of information security			
A.6.1 Internal organization			
Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.			
A.6.1.1	Information security roles and responsibilities	Yes	Responsibilities shall be defined to initiate and control the information security.
A.6.1.2	Segregation of duties	Yes	Assign duties to avoid responsibility that can cause security weaknesses.
A.6.1.3	Contact with authorities	No	There are no authorities in Mexico that could help Xintiba.
A.6.1.4	Contact with special interest groups	Yes	Contact with special groups helps to stay up to date and have special support if it is required.
A.6.1.5	Information security in project management	Yes	Security should be addressed in every project of Xintiba.
A.6.2 Mobile devices and teleworking			
Objective: To ensure the security of teleworking and use of mobile devices			
A.6.2.1	Mobile device policy	Yes	To ensure the use of mobile devices is necessary to apply an special policy.
A.6.2.2	Teleworking	Yes	A policy shall be implemented to support security measures of teleworking.
A.7 Human resource security			
A.7.1 Prior to employment			
Objective: To ensure that employees and contractors understand the responsibilities and are suitable for the roles for which they are considered.			
A.7.1.1	Screening	Yes	It is necessary to verify all

			candidates for employment comply with a series of laws, regulations…
A.7.1.2	Terms and conditions of employment	Yes	Employees shall accept Xintiba's responsibilities for information security.
A.7.2 During employment			
Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.			
A.7.2.1	Management responsibilities	Yes	All employees and contractors are required to apply information security in accordance with the established policies and procedures of Xintiba.
A.7.2.2	Information security awareness, education and training	Yes	All employees and contractors shall receive appropriate security courses and training to comply with security requirements.
A.7.2.3	Disciplinary process	Yes	Disciplinary procedures may be applied to staff that have committed an information security breach.
A.7.3 Termination and change of employment			
Objective: To protect the organization's interests as part of the process of changing or terminating employment.			
A.7.3.1	Termination or change of employment responsibilities	Yes	After termination or change of employment information security responsibilities that remain valid should be communicated to employees.
A.8 Asset management			
A.8.1 Responsibility for assets			
Objective: To identify organizational assets and define appropriate protection responsibilities.			
A.8.1.1	Inventory of assets	Yes	There must be an inventory of assets to identify for protection and maintenance.
A.8.1.2	Ownership of assets	Yes	Assets shall be owned.
A.8.1.3	Acceptable use of assets	Yes	Assets shall be uses according to rules and policies.
A.8.1.4	Return of assets	Yes	After termination or change of employment assets shall be returned.
A.8.2 Information classification			
Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.			
A.8.2.1	Classification of information	Yes	Information shall be identified in accordance with its importance to Xintiba.
A.8.2.2	Labelling of information	Yes	A set of procedures for information labelling shall be

			developed and implemented in accordance with its importance to Xintiba.
A.8.2.3	Handling of assets	Yes	Procedures for handling assets shall be developed and implemented in accordance with its importance to Xintiba.
A.8.3 Media handling			
Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.			
A.8.3.1	Management of removable media	Yes	To prevent unauthorized disclosure of information, procedure should be implemented.
A.8.3.2	Disposal of media	Yes	Media shall be disposed properly when it's no longer is required.
A.8.3.3	Physical media transfer	Yes	Media containing information shall be protected during transportation.
A.9 Access control			
A.9.1 Business requirements of access control			
Objective: To limit access to information and information processing facilities.			
A.9.1.1	Access control policy	Yes	An access control policy shall be established based on Xintiba business and information security requirements.
A.9.1.2	Access to networks and network services	No	Xintiba network services have no access restrictions.
A.9.2 User access management			
Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.			
A.9.2.1	User registration and de-registration	Yes	User registration and de-registration process shall be implemented to enable assignment of access rights.
A.9.2.2	User access provisioning	Yes	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all system and services.
A.9.2.3	Management of privileged access rights	Yes	The allocation and usage of privileged access rights shall be restricted and controlled.
A.9.2.4	Management of secret authentication information users	Yes	The allocation of secret authentication information shall be controlled through a formal management process.
A.9.2.5	Review of user access rights	Yes	Asset owners shall review users' access rights at regular interviews.

A.9.2.6	Removal or adjustment of access rights	Yes	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.
A.9.3 User responsibilities			
Objective: To make users accountable for safeguarding their authentication information.			
A.9.3.1	Use of secret authentication information	Yes	Users must follow Xintiba practices in the usage of secret authentication information.
A.9.4 System and application access control			
Objective: To prevent unauthorized access to systems and applications			
A.9.4.1	Information access restriction	Yes	Xintiba information shall be restricted in accordance with the access control policy.
A.9.4.2	Secure log-on procedures	Yes	Access to applications shall be controlled by a secure log-on procedure.
A.9.4.3	Password management systems	Yes	Password management system shall be interactive and shall ensure quality passwords.
A.9.4.4	Use of privileged utility programs	Yes	The usage of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
A.9.4.5	Access control to program source code	Yes	Access to program source code shall be restricted.
A.10 Cryptography			
A.10.1 Cryptographic controls			
Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.			
A.10.1.1	Policy on the use of cryptographic controls	Yes	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
A.10.1.2	Key management	Yes	A policy on the usage, protection, lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.
A.11 Physical and environmental security			
A.11.1 Secure areas			
Objective: To prevent unauthorized physical access, damage, and interference to the organization's information and information processing facilities.			
A.11.1.1	Physical security	Yes	Security perimeters shall be

	perimeter		defined to protect sensitive areas.
A.11.1.2	Physical entry controls	Yes	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed to access.
A.11.1.3	Securing offices, rooms and facilities	No	Xintiba has not physical servers or especial rooms.
A.11.1.4	Protecting against external and environmental threats	Yes	Physical protection against natural disaster, malicious attack and accidents shall be designed and applied.
A.11.1.5	Working in secure areas	Yes	Procedures for working in secure areas shall be designed and applied.
A.11.1.6	Delivery and loading areas	No	Xintiba has not delivery and loading areas.
A.11.2 Equipment			
Objective: To prevent loss, damage, theft or compromising assets and interruption to the organization's operations.			
A.11.2.1	Equipment setting and protection	Yes	Equipment shall be set and protected to reduce the risks form environmental threats and opportunities for unauthorized access.
A.11.2.2	Supporting utilities	Yes	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
A.11.2.3	Wiring security	Yes	Power and telecommunications wiring carrying data or supporting information services shall be protected from interception, interference or damage.
A.11.2.4	Equipment maintenance	Yes	Equipment shall be correctly maintained to ensure its continued availability and integrity.
A.11.2.5	Removal of assets	Yes	Equipment, information or software shall not be taken off-site without prior authorization.
A.11.2.6	Security of equipment and assets off-premises	Yes	Security shall be applied to off-site assets taking into account the different risks of working outside Xintiba premises.
A.11.2.7	Secure disposal or reuse of equipment	Yes	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely erased prior to disposal or re-use.
A.11.2.8	Unattended user	Yes	Users shall make ensure that

	equipment		unattended equipment has appropriate protection.
A.11.2.9	Clear desk and clear screen policy	Yes	A clear desk policy for papers and removable storage media and a clear screen policy information processing facilities shall be adopted.
A.12 Operation Security			
A.12.1 Operational procedures and responsibilities			
Objective: To ensure correct and secure operations of information processing facilities.			
A.12.1.1	Documented operating procedures	Yes	Operating procedures shall be documented and made available to all users who need them.
A.12.1.2	Change management	Yes	Changes to the Xintiba, business processes, information processing facilities and systems that affect information security shall be controlled.
A.12.1.3	Capacity management	Yes	The usage of resources shall be monitored and tuned up in order to ensure future system requirements will be met.
A.12.1.4	Separation of development, testing and operational environments	Yes	Developing, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.
A.12.2 Protection from malware			
Objective: To ensure that information and information processing facilities are protected against malware.			
A.12.2.1	Controls against malware	Yes	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness..
A.12.3 Backup			
Objective: To protect against loss of data.			
A.12.3.1	Information backup	Yes	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.
A.12.4 Logging and monitoring			
Objective: To record events and generate evidence			
A.12.4.1	Event logging	Yes	Event logs, recording user activities, exceptions, faults and information security events shall be recorded, kept and regularly reviewed.
A.12.4.2	Protection of log	Yes	Logging facilities and log

	information		information shall be protected against unauthorized access.
A.12.4.3	Administrator and operator logs	Yes	System administrator activities shall be logged and the logs protected and regularly reviewed.
A.12.4.4	Clock synchronisation	Yes	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.
A.12.5 Control of operational software			
Objective: To ensure the integrity of operational systems.			
A.12.5.1	Installation of software on operational systems	Yes	Procedures shall be implemented to control the installation of software on operational systems.
A.12.6 Technical vulnerability management			
Objective: To prevent exploitation of technical vulnerabilities.			
A.12.6.1	Management of technical vulnerabilities	Yes	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities, shall be evaluated, and appropriate measures shall be taken to address the associated risk.
A.12.6.2	Restrictions on software installation	Yes	Rules governing the installation of software by users shall be established and implemented.
A.12.7 Information systems audit considerations			
Objective: To minimise the impact of audit activities on operational systems.			
A.12.7.1	Information systems audit controls	Yes	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.
A.13 Communications security			
A.13.1 Network security management			
Objective: To ensure the protection of information in networks and its supporting information processing facilities.			
A.13.1.1	Network controls	Yes	Networks shall be managed and controlled to protect information in systems and applications.
A.13.1.2	Security of network services	No	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements.

A.13.1.3	Segregation in networks	Yes	Groups of information services, users and information systems shall be divided on networks.
A.13.2 Information transfer			
Objective: To maintain the security of information transferred within an organization and with any external entity.			
A.13.2.1	Information transfer policies and procedures	Yes	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communications facilities.
A.13.2.2	Agreements on information transfer	Yes	Agreements shall be addressed the secure transfer of business information between the organization and external parties.
A.13.2.3	Electronic messaging	Yes	Information involved in electronic messaging shall be properly protected.
A.13.2.4	Confidentiality or non-disclosure agreements	Yes	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.
A.14 System acquisition, development and maintenance			
A.14.1 Security requirements of information systems			
Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.			
A.14.1.1	Information security requirements analysis and specification	Yes	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.
A.14.1.2	Securing application services on public networks	Yes	Information involved in application services surfing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure or modification.
A.14.1.3	Protecting application services transactions	Yes	Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

A.14.2 Security in development and support processes			
Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.			
A.14.2.1	Secure development policy	Yes	Rules for the development of software and systems shall be established and applied to developments within Xintiba.
A.14.2.2	System change control procedures	Yes	Changes to systems within the development lifecycle shall be controlled by using of formal change control procedures.
A.14.2.3	Technical review of applications after operating platform changes	Yes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
A.14.2.4	Restrictions on changes to software packages	Yes	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.
A.14.2.5	Secure systems engineering principles	Yes	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.
A.14.2.6	Secure developments environments	Yes	Xintiba shall establish and properly protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.
A.14.2.7	Outsourced developments	No	Xintiba have not outsourced development.
A.14.2.8	System security testing	Yes	Testing of security functionality shall be carried out during development.
A.14.2.9	System acceptance testing	Yes	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.
A.14.3 Test data			
Objective: To ensure the protection of data used for testing			
A.14.3.1	Protection of test data	Yes	Test data shall be selected carefully, protected and controlled.
A.15 Supplier relationships			
A.15.1 Information security in supplier relationships			

Objective: To ensure protection of the organization's assets that is accessible by suppliers.			
A.15.1.1	Information security policy for suppliers relationships	No	Suppliers have no access to Xintiba information.
A.15.1.2	Addressing security within supplier agreements	Yes	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for Xintiba information.
A.15.1.3	Information and communication technology supply chain	Yes	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.
A.15.2 Supplier service delivery management			
Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.			
A.15.2.1	Monitoring and review of supplier services	Yes	Xintiba shall regularly monitor, review and audit supplier service delivery.
A.15.2.2	Managing changes to supplier services	Yes	Xintiba should managed changesgti9 with suppliers.
A.16 Information security incident management			
A.16.1 Management of information security incidents and improvements			
Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weakness.			
A.16.1.1	Responsibilities and procedures	Yes	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.
A.16.1.2	Reporting information security events	Yes	Information security events shall be reported through appropriate management channels as quickly as possible.
A.16.1.3	Reporting information security weaknesses	Yes	Employees and contractors using Xintiba information systems and services shall be required to report any observed or suspicious information security weaknesses in systems or services.
A.16.1.4	Assessment of and decisions on information security events	Yes	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.

A.16.1.5	Response to information security incidents	Yes	Information security incidents shall be address in accordance with the documented procedures.
A.16.1.6	Learning from information security incidents	Yes	Knowledge obtain from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.
A.16.1.7	Collection of evidence	Yes	Xintiba shall define and applying procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.
A.17 Information security aspects of business continuity management			
A.17.1 Information security continuity			
Objective: Information security continuity shall be stored in the organization's business continuity management systems.			
A.17.1.1	Planning information security continuity	Yes	Xintiba shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.
A.17.1.2	Implementing information security continuity	Yes	Xintiba shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.
A.17.1.3	Verify, review and evaluate information security continuity	Yes	Xintiba shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.
A.18 Compliance			
A.18.1 Compliance with legal and contractual requirements			
Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.			
A.18.1.1	Identification of applicable legislation and contractual requirements	Yes	All relevant legislative statutory, regulatory, contractual requirements and Xintiba approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and Xintiba.
A.18.1.2	Intellectual property	Yes	Appropriate procedures shall be

	rights		implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and usage of owner's soft- ware products.
A.18.1.3	Protection of records	Yes	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.
A.18.1.4	Privacy and protection of personally identifiable information	Yes	Privacy and protection of personal information shall be ensured as required in relevant legislation and regulation where applicable.
A.18.1.5	Regulation of cryptographic controls	Yes	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.
A.18.2 Information security reviews			
Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.			
A.18.2.1	Independent review of information security	Yes	Xintiba approach to managing information security and its implementation (e.g. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.
A.18.2.2	Compliance with security policies and standards	Yes	Managers shall regularly review the compliance of information processing and procedures within their areas of responsibility with the appropriate security policies, standards and any other security requirements.
A.18.2.3	Technical compliance review	Yes	Information systems shall be regularly reviewed to comply with the Xintiba information security policies and standards.

Table 1: Statement of applicability.

Annex 8 – Compliance Audit Report

Detail of findings and evidence

We are going to show the main audit findings referring to findings labelled according to this priority levels:

- Major non-conformity –Affects the overall effectiveness of the ISMS and the ability of the organization to achieve its information security objectives. Non-conformities have a direct effect on information security specifically on the preservation of confidentiality, integrity and availability of information assets.

- Minor non-conformity – Affect the overall effectiveness of the ISMS and the ability of the organization to achieve its information security objectives. Minor non-conformity has an indirect effect on information security.

All conformity requires are documented with its corrective actions or suggested preventive actions.

Evidence	Affected Control	Type	Corrective / Suggested Action
1.- No responsible defined to be update of external outcomes.	4.1	Minor	Define a responsible to be review periodically the external outcomes.
2.- Employees explained that some processes are not completely optimized.	4.4	Minor	Work optimizing the processes to the maximum level.
3.- The actions taken placed to acquire the necessary competence are not evaluated.	7.2	Minor	Evaluate the actions taken placed.
4.- Employees not knowing the implications of not conforming with the information security management system requirements.	7.3	Mayor	Broadcast campaign to ensure every employee knows the implications.
5.- Complexity of processes and the competence of employees is not documented.	7.5	Minor	Document and maintain the complexity of processes and the competences of employees.
6.- Outsourced processes are not reviewed in detail.	8.1	Minor	Review in detail all the processes.

7.- Corrective actions taken place are not documented.	10.1	Minor	Document corrective actions taken place.
8.- Not contact with authorities.	A.6.1.3	Mayor	Seek a private authority instead of a public.
9.- There is no contact with special interest groups.	A.6.1.4	Mayor	Make appropriate contacts with special interest groups.
10.- Only for few actions a disciplinary process is taken.	A.7.2.3	Mayor	Be more strict and open disciplinary process for all actions defined.
11.- SysAdmin didn't know that two users have use usage permits.	A.9.4.4	Mayor	Track properly all users with usage permits.
12.- There aren't processes defined to control media handling.	A.8.3.1, A.8.3.2, A.8.3.3	Mayor	Take actions to defined the process properly.
13.- Offices don't have physical access, protection.	A.11.1	Mayor	Implement security measures to protect physically offices.
14.- No events recorded and evidence generated.	A.12.4	Mayor	Start logging events and generating evidences.
15.- Information is transferring to external entities without following defined processes.	A.12.4	Mayor	Warn employees or take disciplinary actions.

Table 1: Audit main findings.

Audit Results Summary

We summarize the ISO/IEC 27001:2013 compliance audit results according to the ISO/IEC 15504. This standard is a set of technical standard documents for the software development process and related business management functions. It describes the capability levels of the companies' processes:

Below charts are composed by the following outputs:

Capability Level	Capability Level ISO/IEC 15504
0. Nonexistence	There is not a process defined or identifiable.
1. Initial	Processes are not rigorously plan or track.
2. Managed	Process is planned and tracked.
3. Defined	Process is performed and managed using a defined process.
4. Quantitatively Managed	The defined process is performed consistently to achieve its defined process goals.
5. Optimizing	Performance of the process is optimized to meet current and future business needs.

Table 2: ISO/IEC 15004 Capability Level Description.

ID	Section Name	Maturity
4	**Context of the organization**	**%70**
4.1	Understanding the organization and its context	Defined
4.2	Understanding the needs and expectations of interested parts	Quantitatively Managed
4.3	Determining the scope of the information security management system	Quantitatively Managed
4.4	Information security management system	Defined
5	**Leadership**	**80%**
5.1	Leadership and commitment	Quantitatively Managed
5.2	Policy	Quantitatively Managed
5.3	Organizational roles, responsibilities and authorities	Quantitatively Managed
6	**Planning**	**75%**
6.1	Actions to address risks and opportunities	Quantitatively Managed
6.2	Information security objectives and planning to achieve them	Quantitatively Managed
7	**Support**	**50%**
7.1	Resources	Quantitatively Managed
7.2	Competence	Managed
7.3	Awareness	**Initial**
7.4	Communication	Managed
7.5	Documented information	**Initial**
8	**Operation**	**70%**
8.1	Operational planning and control	Managed
8.2	Information security risk assessment	Quantitatively Managed
8.3	Information security risk treatment	Quantitatively Managed
9	**Performance evaluation**	**50%**
9.1	Monitoring, measurement, analysis and evaluation	Managed
9.2	Internal audit	Managed
9.3	Management review	Quantitatively Managed
10	**Improvement**	**50%**
10.1	Nonconformity and corrective action	Initial
10.2	Continual improvement	Defined

Table 3: ISO 27001 compliance gap analysis report 1.

ID	Control	Applicable	Maturity
A.5 Information Security Policies		**Yes**	**80%**
A.5.1 Management direction for information security			

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.			
A.5.1.1	Policies for information security	Yes	Quantitatively Managed
A.5.1.2	Review of the policies for information security	Yes	Quantitatively Managed
A.6 Organization of information security		**Yes**	**70%**
A.6.1 Internal organization			
Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.			
A.6.1.1	Information security roles and responsibilities	Yes	Quantitatively Managed
A.6.1.2	Segregation of duties	Yes	Managed
A.6.1.3	Contact with authorities	Yes	Nonexistence
A.6.1.4	Contact with special interest groups	Yes	Nonexistence
A.6.1.5	Information security in project management	Yes	Quantitatively Managed
A.6.2 Mobile devices and teleworking			
Objective: To ensure the security of teleworking and use of mobile devices			
A.6.2.1	Mobile device policy	Yes	Quantitatively Managed
A.6.2.2	Teleworking	Yes	Quantitatively Managed
A.7 Human resource security		**Yes**	**75%**
A.7.1 Prior to employment			
Objective: To ensure that employees and contractors understand the responsibilities and are suitable for the roles for which they are considered.			
A.7.1.1	Screening	Yes	Quantitatively Managed
A.7.1.2	Terms and conditions of employment	Yes	Quantitatively Managed
A.7.2 During employment			
Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.			
A.7.2.1	Management responsibilities	Yes	Quantitatively Managed
A.7.2.2	Information security awareness, education and training		Quantitatively Managed
A.7.2.3	Disciplinary process	Yes	Initial
A.7.3 Termination and change of employment			
Objective: To protect the organization's interests as part of the process of changing or terminating employment.			
A.7.3.1	Termination or change of employment responsibilities	Yes	Managed
A.8 Asset management		**Yes**	**50%**
A.8.1 Responsibility for assets			
Objective: To identify organizational assets and define appropriate			

protection responsibilities.			
A.8.1.1	Inventory of assets	Yes	Quantitatively Managed
A.8.1.2	Ownership of assets	Yes	Quantitatively Managed
A.8.1.3	Acceptable use of assets	Yes	Quantitatively Managed
A.8.1.4	Return of assets	Yes	Managed
A.8.2 Information classification			
Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.			
A.8.2.1	Classification of information	Yes	Quantitatively Managed
A.8.2.2	Labelling of information	Yes	Quantitatively Managed
A.8.2.3	Handling of assets	Yes	Quantitatively Managed
A.8.3 Media handling			
Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.			
A.8.3.1	Management of removable media	Yes	Nonexistence
A.8.3.2	Disposal of media	Yes	Nonexistence
A.8.3.3	Physical media transfer	Yes	Nonexistence
A.9 Access control		**Yes**	**83%**
A.9.1 Business requirements of access control			
Objective: To limit access to information and information processing facilities.			
A.9.1.1	Access control policy	Yes	Quantitatively Managed
A.9.1.2	Access to networks and network services	Yes	Quantitatively Managed
A.9.2 User access management			
Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.			
A.9.2.1	User registration and de-registration	Yes	Quantitatively Managed
A.9.2.2	User access provisioning	Yes	Quantitatively Managed
A.9.2.3	Management of privileged access rights	Yes	Quantitatively Managed
A.9.2.4	Management of secret authentication information users	Yes	Quantitatively Managed
A.9.2.5	Review of user access rights	Yes	Quantitatively Managed
A.9.2.6	Removal or adjustment of access rights	Yes	Quantitatively Managed
A.9.3 User responsibilities			
Objective: To make users accountable for safeguarding their authentication information.			
A.9.3.1	Use of secret authentication information	Yes	Quantitatively Managed

A.9.4 System and application access control			
Objective: To prevent unauthorized access to systems and applications			
A.9.4.1	Information access restriction	Yes	Quantitatively Managed
A.9.4.2	Secure log-on procedures	Yes	Quantitatively Managed
A.9.4.3	Password management systems	Yes	Managed
A.9.4.4	Use of privileged utility programs	Yes	Initial
A.9.4.5	Access control to program source code	Yes	Quantitatively Managed
A.10 Cryptography		**Yes**	**30%**
A.10.1 Cryptographic controls			
Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.			
A.10.1.1	Policy on the use of cryptographic controls	Yes	Nonexistence
A.10.1.2	Key management	Yes	Managed
A.11 Physical and environmental security		Yes	**8%**
A.11.1 Secure areas			
Objective: To prevent unauthorized physical access, damage, and interference to the organization's information and information processing facilities.			
A.11.1.1	Physical security perimeter	Yes	Nonexistence
A.11.1.2	Physical entry controls	Yes	Nonexistence
A.11.1.3	Securing offices, rooms and facilities	Yes	Nonexistence
A.11.1.4	Protecting against external and environmental threats	Yes	Nonexistence
A.11.1.5	Working in secure areas	Yes	Nonexistence
A.11.1.6	Delivery and loading areas	Yes	Nonexistence
A.11.2 Equipment			
Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.			
A.11.2.1	Equipment siting and protection	Yes	Nonexistence
A.11.2.2	Supporting utilities	Yes	Nonexistence
A.11.2.3	Cabling security	Yes	Initial
A.11.2.4	Equipment maintenance	Yes	Nonexistence
A.11.2.5	Removal of assets	Yes	Nonexistence
A.11.2.6	Security of equipment and assets off-premises	Yes	Nonexistence
A.11.2.7	Secure disposal or reuse of equipment	Yes	Nonexistence
A.11.2.8	Unattended user equipment	Yes	Quantitatively Managed
A.11.2.9	Clear desk and clear screen policy	Yes	Quantitatively Managed
A.12 Operation Security		**Yes**	**53%**
A.12.1 Operational procedures and responsibilities			
Objective: To ensure correct and secure operations of information processing facilities.			
A.12.1.1	Documented operating procedures	Yes	Initial
A.12.1.2	Change management	Yes	Initial

A.12.1.3	Capacity management	Yes	Initial
A.12.1.4	Separation of development, testing and operational environments	Yes	Defined
A.12.2 Protection from malware			
Objective: To ensure that information and information processing facilities are protected against malware.			
A.12.2.1	Controls against malware	Yes	Quantitatively Managed
A.12.3 Backup			
Objective: To protect against loss of data.			
A.12.3.1	Information backup	Yes	Quantitatively Managed
A.12.4 Logging and monitoring			
Objective: To record events and generate evidence			
A.12.4.1	Event logging	Yes	Quantitatively Managed
A.12.4.2	Protection of log information	Yes	Quantitatively Managed
A.12.4.3	Administrator and operator logs	Yes	Quantitatively Managed
A.12.4.4	Clock synchronisation	Yes	Nonexistence
A.12.5 Control of operational software			
Objective: To ensure the integrity of operational systems.			
A.12.5.1	Installation of software on operational systems	Yes	Quantitatively Managed
A.12.6 Technical vulnerability management			
Objective: To prevent exploitation of technical vulnerabilities.			
A.12.6.1	Management of technical vulnerabilities	Yes	Quantitatively Managed
A.12.6.2	Restrictions on software installation	Yes	Initial
A.12.7 Information systems audit considerations			
Objective: To minimise the impact of audit activities on operational systems.			
A.12.7.1	Information systems audit controls	Yes	Quantitatively Managed
A.13 Communications security		**Yes**	**55%**
A.13.1 Network security management			
Objective: To ensure the protection of information in networks and its supporting information processing facilities.			
A.13.1.1	Network controls	Yes	Quantitatively Managed
A.13.1.2	Security of network services	Yes	Quantitatively Managed
A.13.1.3	Segregation in networks	Yes	Quantitatively Managed
A.13.2 Information transfer			
Objective: To maintain the security of information transferred within an organization and with any external entity.			
A.13.2.1	Information transfer policies and procedures	Yes	Nonexistence
A.13.2.2	Agreements on information transfer	Yes	Nonexistence

A.13.2.3	Electronic messaging	Yes	Initial
A.13.2.4	Confidentiality or non-disclosure agreements	Yes	Managed
A.14 System acquisition, development and maintenance		**Yes**	**45%**
A.14.1 Security requirements of information systems			
Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.			
A.14.1.1	Information security requirements analysis and specification	Yes	Initial
A.14.1.2	Securing application services on public networks	Yes	Managed
A.14.1.3	Protecting application services transactions	Yes	Managed
A.14.2 Security in development and support processes			
Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.			
A.14.2.1	Secure development policy	Yes	Initial
A.14.2.2	System change control procedures	Yes	Managed
A.14.2.3	Technical review of applications after operating platform changes	Yes	Managed
A.14.2.4	Restrictions on changes to software packages	Yes	Managed
A.14.2.5	Secure systems engineering principles	Yes	Define
A.14.2.6	Secure developments environments	Yes	Define
A.14.2.7	Outsourced developments	Yes	Managed
A.14.2.8	System security testing	Yes	Quantitatively Managed
A.14.2.9	System acceptance testing	Yes	Managed
A.14.3 Test data			
Objective: To ensure the protection of data used for testing			
A.14.3.1	Protection of test data	Yes	Managed
A.15 Supplier relationships		**Yes**	
A.15.1 Information security in supplier relationships			
Objective: To ensure protection of the organization's assets that is accessible by suppliers.			
A.15.1.1	Information security policy for suppliers relationships	Yes	Define
A.15.1.2	Addressing security within supplier agreements	Yes	Managed
A.15.1.3	Information and communication technology supply chain	Yes	Managed
A.15.2 Supplier service delivery management			
Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.			
A.15.2.1	Monitoring and review of supplier services	Yes	Managed
A.15.2.2	Managing changes to supplier	Yes	Managed

	services		
A.16 Information security incident management		**Yes**	**25%**
A.16.1 Management of information security incidents and improvements			
Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weakness.			
A.16.1.1	Responsibilities and procedures	Yes	Quantitatively Managed
A.16.1.2	Reporting information security events	Yes	Managed
A.16.1.3	Reporting information security weaknesses	Yes	Managed
A.16.1.4	Assessment of and decisions on information security events	Yes	Initial
A.16.1.5	Response to information security incidents	Yes	Initial
A.16.1.6	Learning from information security incidents	Yes	Managed
A.16.1.7	Collection of evidence	Yes	Initial
A.17 Information security aspects of business continuity management		**Yes**	**20%**
A.17.1 Information security continuity			
Objective: Information security continuity shall be embedded in the organization's business continuity management systems.			
A.17.1.1	Planning information security continuity	Yes	Initial
A.17.1.2	Implementing information security continuity	Yes	Initial
A.17.1.3	Verify, review and evaluate information security continuity	Yes	Initial
A.18 Compliance		**Yes**	**40%**
A.18.1 Compliance with legal and contractual requirements			
Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.			
A.18.1.1	Identification of applicable legislation and contractual requirements	Yes	Initial
A.18.1.2	Intellectual property rights	Yes	Managed
A.18.1.3	Protection of records	Yes	Managed
A.18.1.4	Privacy and protection of personally identifiable information	Yes	Managed
A.18.1.5	Regulation of cryptographic controls	Yes	Managed
A.18.2 Information security reviews			
Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.			
A.18.2.1	Independent review of information security	Yes	Quantitatively Managed

Table 4: ISO 27001 compliance gap analysis report 2.