Global Information Assurance Certification Paper

GIAC Certified ISO-17799 Specialist

Practical Assignment

Version 1.1 (April 19, 2004)

Information Security Management System

For a

Regional Daily Newspaper

By

Luis J. Buezo

December 22, 2004

Table of Contents

Abstract

This document constitutes my response to the practical assignment Version 1.1 (April 19, 2004), to obtain the GIAC Certified ISO-17799 Specialist Certification.

In this document I will explain how to develop an Information Security Management System (ISMS) in accordance with the principles of 7799 in a Regional Newspaper.

In the Corporation XXX there are a variety of different business units, all related to Press and Magazines. The ISMS that I am going to develop is a specific part a one of these business units. The Business Unit XYZ is a Regional Newspaper that has two main products, a Regional daily newspaper and a weekly Sunday Supplement. The ISMS scope will be related to the most significant assets of the Regional daily newspaper.

This document is organized in five sections, following the PDCA (Plan-Do-Check-Act) model that will be used to develop the ISMS:

- Section one; System Definition where the scope and the environment of the ISMS that will be developed, are defined
- Section Two; **Plan** Activity, where policies and security organization will be identified and risk management activities based on CRAMM® are done.
- Section Three; **Do** Activity, where security countermeasures will be implemented.
- Section Four; **Check** Activity, where auditing process will check the security countermeasures implemented before.
- Section Five, **Act** Activity, where will be defined how will be maintained and improved the ISMS.

In order to protect the confidentiality of XXX and XYZ, information included in this document has been randomly mixed and changed. Any coincidence with the reality of XXX and XYZ is pure coincidence.

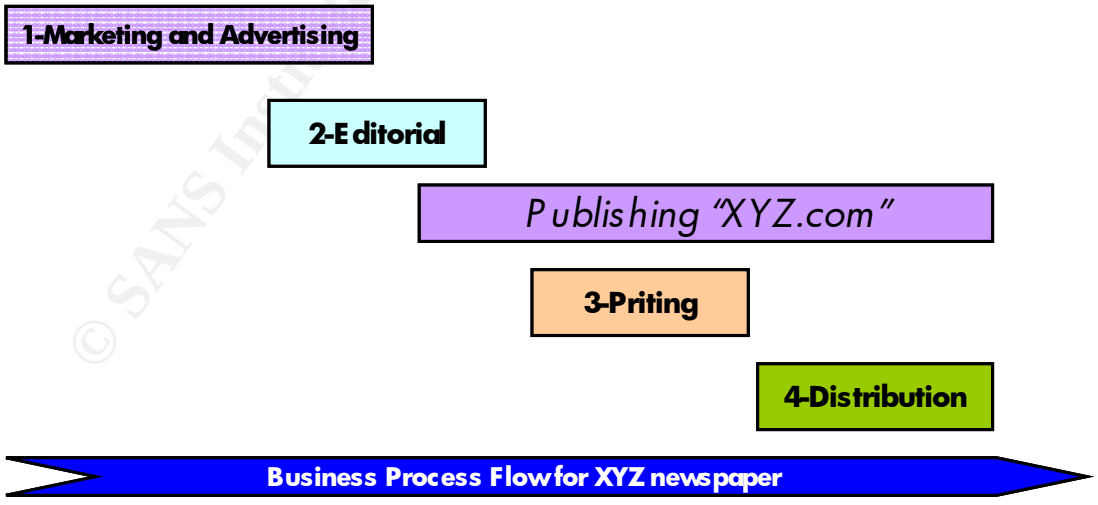
Part One: System Definition

From year 2000, the newspaper audience has been constantly increasing. Nowadays, the newspaper is implementing a technology modernization program. XYZ is able to produce and distribute the total daily diffusion using only one of the 2 rotary presses implemented in the region. But there is no a formal security governance and management process in the organization.

The organization structure of XYZ is leaded by a CEO (Chief Executive Officer) who reports to the president and General Manager of the Corporation XXX. The IT Manager of the newspaper reports directly to the newspaper CEO. The IT department organization is very similar to other organizations with Systems, Production, Development, Communications, and Help-desk department. Actually, there is no formal Security Organization, neither in the Newspaper nor in the corporation. One of the critical steps in the ISMS development will be to define the global security organization not only for the newspaper business unit but also for the rest of the Press Corporation.

In order to correctly select the ISMS scope (most significant assets of the regional daily newspaper), it is needed to analyze the business processes flows of the newspaper and identify the information assets. Once identified each asset and the total information flow, it is possible to select most significant assets related to the daily newspaper.

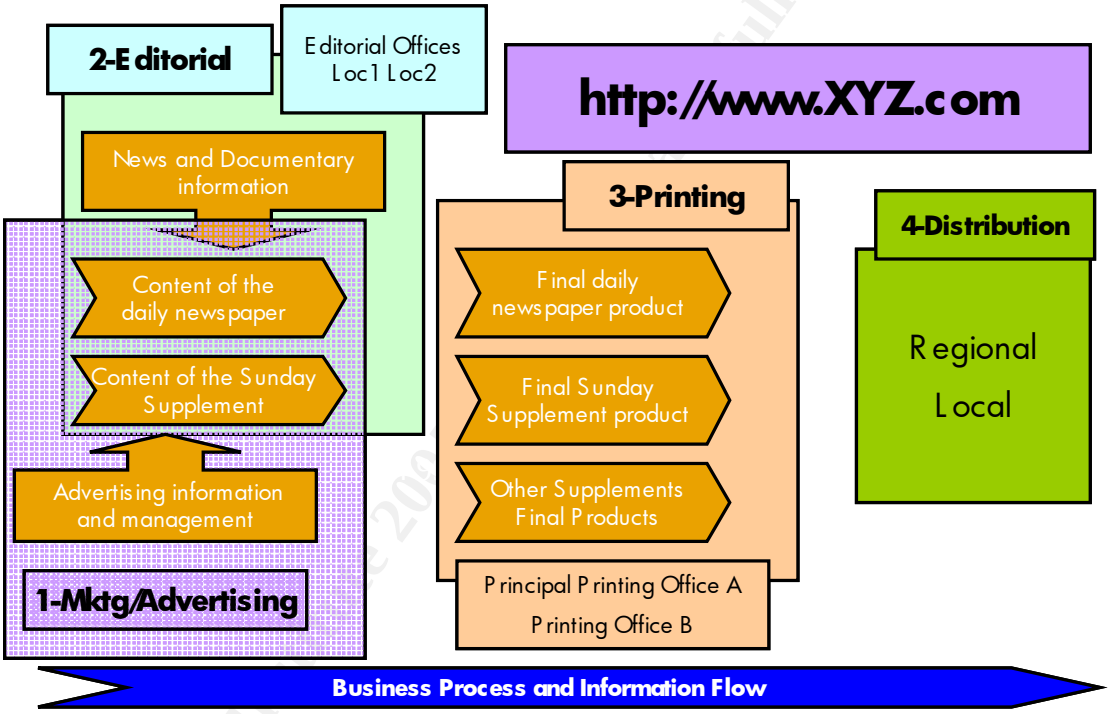
In the next figure, the main business process flow for a Newspaper business unit is described:



The business process flow for any press document is very similar. The first step is done by the marketing and advertising department (one of the main money income sources for the business unit), once this department has the

template with all the adds that have to be included in the final product, the editorial department fills the gaps with news, and relevant information; after this, this information can be published in Internet and printed for distribution to the final selling points. XYZ business is distributed in 2 Editorial office locations and 2 printing office locations.

XYZ has two main products, the national daily newspaper and the Sunday Weekly Supplement, and other less important Supplements (traveling, entertainment, business, technology, local news). The Business process flow described previously is very similar for all the products but the information assets in some cases are different. In the figure below is represented the relationship between the business process flow and the located information assets for the XYZ:



As you can see in the figure, the information assets that have been identified related to the business process are:

1. Advertising information and management.
2. News and Documentary information.
3. Content of the daily newspaper.
4. Content of the Sunday Supplement.
5. Final daily newspaper product.
6. Final Sunday Supplement product.
7. Other Supplements Final Products.

Other information assets identified are:

8. Documentation Management.
9. Economic and Financial Information.

10. Employee Information.
11. Subscription Information Management.
12. Special Offers and Promotion Information.
13. Distribution Information.
14. Partners Information Management.

Thinking that this is the first step of the business unit to formalize security, it is not recommended to develop de ISMS for all the Information Assets in this first step. The recommendation is to select the most representative information assets related to the "regional daily newspaper", because the regional daily newspaper is the principal product of the business unit.

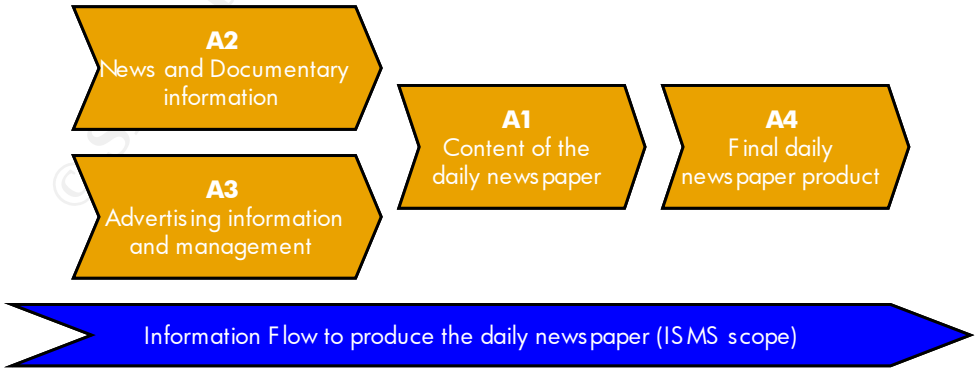
The Scope of the ISMS will be based on 4 Information Assets that are managed by the business unit to produce the regional daily newspaper:

- Asset 1: Content of the daily newspaper
- Asset 2: News and Documentary information
- Asset 3: Advertising information and management
- Asset 4: Final newspaper product

As you can see, there are information assets related to the Marketing, Advertising, Editorial and printing process flow. There are no assets related to the distribution process because this process is not a core competence business for XYZ newspaper. These activities are outsourced to other Companies. I don't want to say that this process is not important for the security of XYZ, but in order to select the most significant activities in the first scope of the ISMS there are other assets more representatives of the core business of the business unit.

As conclusion, the ISMS selected cover the systems and assets that are connected with the main business objective of XYZ business unit.

In the next figure you can see the Information Flow of the Information Assets selected for the ISMS to develop:



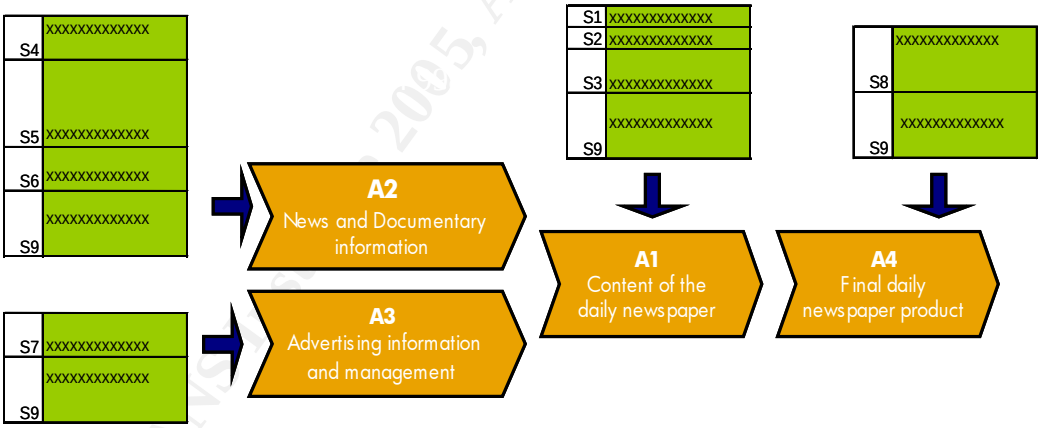
Now, it is needed to identify the Access Services used by XYZ to manage the information of the information assets (Access Service is defined as all the different ways to access to the information supported by the Assets). The access Services located in the ISMS scope are:

Nº	Access Service	Descripción	E	A2A	EDI	TF	I	B	W	Vo	Vi	Ot	Service Owner	Service Depositary
S1	S1 Access	xxxxxxxxxxxxxxxxxxxxxxxxxxxx					Y						yyyyyyyyyyyyyyy	fffffffffffff
S2	S2 Access	xxxxxxxxxxxxxxxxxxxxxxxxxxxx				Y			Y				yyyyyyyyyyyyyyy	fffffffffffff
S3	S3 Access	xxxxxxxxxxxxxxxxxxxxxxxxxxxx		Y					Y				yyyyyyyyyyyyyyy	fffffffffffff
S4	S4 Access	xxxxxxxxxxxxxxxxxxxxxxxxxxxx		Y		Y							yyyyyyyyyyyyyyy	fffffffffffff
S5	S5 Access	xxxxxxxxxxxxxxxxxxxxxxxxxxxx				Y			Y				zzzzzzzzzzzzzzz	fffffffffffff
S6	S6 Access	xxxxxxxxxxxxxxxxxxxxxxxxxxxx	Y			Y	Y		Y				zzzzzzzzzzzzzzz	fffffffffffff
S7	S6 Acess	xxxxxxxxxxxxxxxxxxxxxxxxxxxx	Y				Y						zzzzzzzzzzzzzzz	fffffffffffff
S8	S7 Access	xxxxxxxxxxxxxxxxxxxxxxxxxxxx		Y		Y	Y		Y				zzzzzzzzzzzzzzz	fffffffffffff
S9	S8 Acess	xxxxxxxxxxxxxxxxxxxxxxxxxxxx							Y			Y		

Where:

- **E** is an Email Service
- **A2A** is a communication between two Applications.
- **EDI**. Is an Electronic Data Interchange Service.
- **TF** is a File Transfer Service
- **I** is an Interactive Service.
- **B** is a Batch Service
- **W** is a Service based on Web
- **VO** is a Service based on Voice Signal communication
- **VI** is a Service based on Video Signal communication
- **O** Other Services.

In the next figure you can see which services access to specific information assets:



Next elements are identified as IT-Dependencies from the XYZ and XXX IT Inventory that are related to the Information Assets Identified:

XYZ-Correspondent PCs	XYZ-User PCs	XYZ-VIP Users PCs
XYZ-RAS Dial Up	XYZ-Receiver Text News Agency	XYZ-DMZ Network XYZ.net XYZ-Internal Network XYZ.net
XYZ-SAN	XYZ-DB Correspondent Server	XYZ-DB Agency Server
XYZ-CiXYZ Server	XYZ-Correspondent Server	XYZ-HCXYZ Server
XYZ-HMXYZ Server	XYZ-External Agency Server	XYZ-Internal Agency Server
XYZ-Intranet Server	XYZ-PEXYZ Server	XYZ-PPXYZ Server
XYZ-SAXYZ Server	XYZ-SPXYZ Server	XYZ-PAXYZ Server
XXX-XYZ Cx Branch Off.	XXX-XYZ Cx Backbone	XXX-XYZ External Printers
XXX-Service Node	XXX-Backbone	XYZ-CiXYZ SW
XYZ-HCXYZ SW	XYZ-HMXYZ SW	XYZ-PEXYZ SW
XYZ-SAXYZ SW	XYZ-SPXYZ SW	

IT dependencies are divided in three different groups:

- XYZ IT Equipment, where there are clients systems, servers, SAN, Internal network, DMZ network, servers, etc. This equipment is directly managed by XYZ IT department
- XXX IT Equipment related to the corporative network that is managed by XXX IT department **that will not be considered inside the scope of XYZ ISMS**. The security controls that affect this IT equipment will be considered inside the Scope the XXX Corporate Network ISMS.
- XYZ specific software developed on demand for XYZ IT department.

In appendix I, the inventory is detailed for each IT Dependency group.

Eventually, it can be developed a model to identify the dependencies that apply to a specific service. The next dependency Model represents how IT dependencies support the activity of a specific Information asset for each access service.

Access Services	XYZ-S1	XYZ-S2	XYZ-S3	XYZ-S4	XYZ-S5	XYZ-S6	XYZ-S7	XYZ-S8	XYZ-S9
Assets	XYZ-A1	XYZ-A1	XYZ-A1	XYZ-A2	XYZ-A2	XYZ-A2	XYZ-A3	XYZ-A4	XYZ-A1-A2-A3-A4
IT Dependencies									
XYZ-Correspondent PCs				X		X			
XYZ-User PCs		X			X		x		X
XYZ-VIP Users PCs	X								
XYZ-RAS Dial Up					X			X	x
XYZ-Receiver Text News Agency			X			X			
XYZ-DMZ Network XYZ.net		X		X		X		x	x
XYZ- Network XYZ.net	X	X		X	X	X	X	X	
XYZ-SAN			X					X	
XYZ-DB Correspondent Server				X					
XYZ-DB Agency Server		X		X	X	X			
XYZ-CiXYZ Server			X				x		
XYZ-Correspondent Server				X					
XYZ-HCXYZ Server					X				
XYZ-HMXYZ Server	X	X						x	x
XYZ-External Agency Server			X			X			
XYZ-Internal Agency Server					X		X		
XYZ-Intranet Server	X			X					
XYZ-PEXYZ Server		X	X			X		x	
XYZ-PPXYZ Server					X			x	
XYZ-SAXYZ Server			X		X			x	
XYZ-SPXYZ Server							x	x	
XYZ-PAXYZ Server			X	X				x	
XXX-XYZ Cx Branch Off.	X	X			X		X		X
XXX-XYZ Cx Backbone	X			X	X		X		X
XXX-XYZ External RPs									x
XXX-Backbone	X	X	X		X		X	X	
XXX-Service Node						X			x
XYZ-CiXYZ SW			x				x		
XYZ-HCXYZ SW									
XYZ-HCXYZ SW	x		x					x	
XYZ-PEXYZ SW		x			x	x			
XYZ-SAXYZ SW			x		x			x	x
XYZ-SPXYZ SW				x			x		

In general, I can affirm that XYZ in the last 3 years has implemented a big variety of different security controls in order to mitigate specific threats in a reactive way based on bad incident experiences. XYZ has invested in Perimeter Security Technologies (firewalls, IDSs), malicious code prevention software (Desktop antivirus, Server Antivirus, Mail Server antivirus) and DMZ Servers are hardened and patched periodically. Actually, XYZ has not a formal security governance process because there is no a security policy implemented in the organization and there is not a security organization supporting this security policy; besides, there is not a continuous risk

management process as a primary tool to invest in security. The security invests decision criteria has been based on specific vendors selling skills, fashion security products and in a reactive way to security incidents.

A critical issue is that there is no Audit security control process, so there is no any mechanism to check once implemented a security control, how this security control is mitigating a determined risk.

In order to continue with de ISMS development there are people in the organization that has to be involved in the process. The people that has been identify are:

- Business Managers responsible for the Information Assets included in the ISMS
- XXX CIO
- XXX Corporative Network Manager
- XYZ IT Manager
- XYZ Systems Manager
- XXX Physical Security Responsible

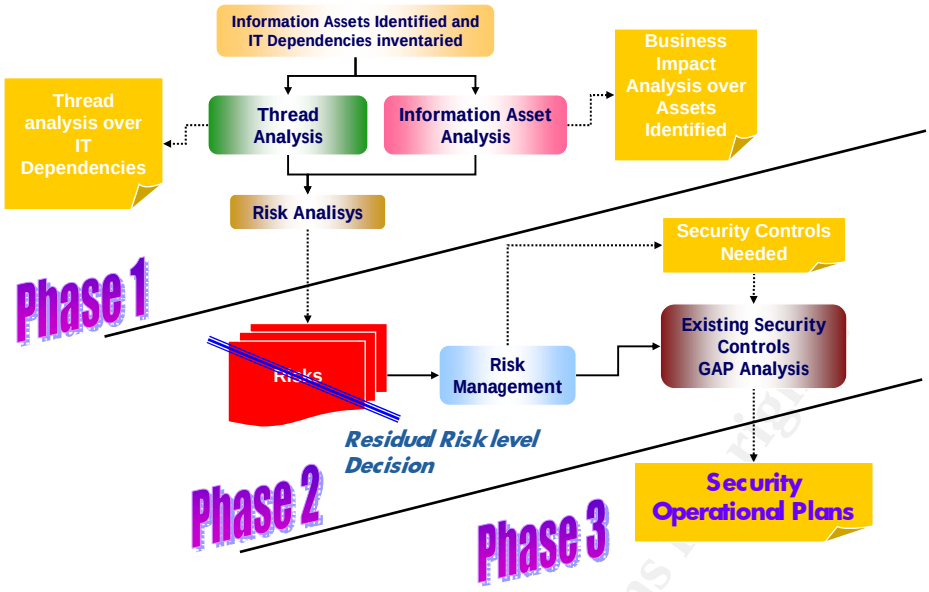
Part Two: Plan

Project Plan

XYZ Business Unit is beginning a Security governance project to formalize security. These are the project activities and phases that have been planned:

- **Phase 0**:
  - Start and Project Plan
  - ISMS Scope Definition for each business unit in which we obtain the Information assets and the IT Dependency Model (see Part One this practical)
  - ISMS Preparation
    - Corporate High level Security Policy Definition
    - Security Organization definition
    - Other Preparation activities
- **Phase 1**:
  - Business Information Assets Impact Analysis.
  - Thread Analysis over IT Dependencies identified
  - Risk Analysis
- **Phase 2**:
  - Risk Management. Residual Risk Decision
  - Identification of Security Controls needed.
  - Identification of existing Security Controls and Gap Analysis
- **Phase 3**:
  - Definition of the Security Operational Plan to achieve the security Objective and residual risk identified before
- **Phase 4**:
  - Implementation of controls following the Security Operation Plan
  - Managing the ISMS (Check and Act part of the PDCA Framework)
  - ISMS continuous Process Improvement

In the next figure is detailed the **Plan for Risk Management** based on **CRAMM®** methodology when finished the phase 0 of the ISMS developing process:



The **information Asset Analysis** activity is based on interviews with the business responsible of the information asset. In these interviews, different security objectives will be reviewed and different kinds of impacts based on different security scenarios will be assessed. In appendix II the 26 security scenarios that will be studied for each information asset are described:

In the **Thread Analysis activity** is very important to be efficient because the ISMS scope is not small. The different IT elements identified in the dependency model have been grouped in groups of IT elements with the same Threads (named Thread Groups).

Based on generic threads, a list with the threads that applies for each IT dependency Group will be defined. For example: theft only applies to tangible elements and fire applies to locations.

For each thread that applies to a specific IT dependency group, the frequency of the thread and the vulnerability level of the IT dependency group will be evaluated.

All this information will be taken in office templates and then will be introduced in CRAMM®. In appendix III are detailed the security threads that CRAMM® supplies to be analyzed for each IT dependency group:

The **Risk analysis** is calculated using CRAMM®, exchanging the results from the Information Asset analysis and the Thread analysis results.

The **Risk Management activity** is where XYZ will decide the Threshold of risk that will be accepted and therefore considered as “Residual Risk”; the rest of risks has to be mitigated, so that, it is necessary to define the security controls that mitigate any specific risk to manage.

In the next figure, you can see the risk management matrix where CRAMM® distributes the **risk level** based on the **Threat level**, **Vulnerability Level** and **Impact level**:

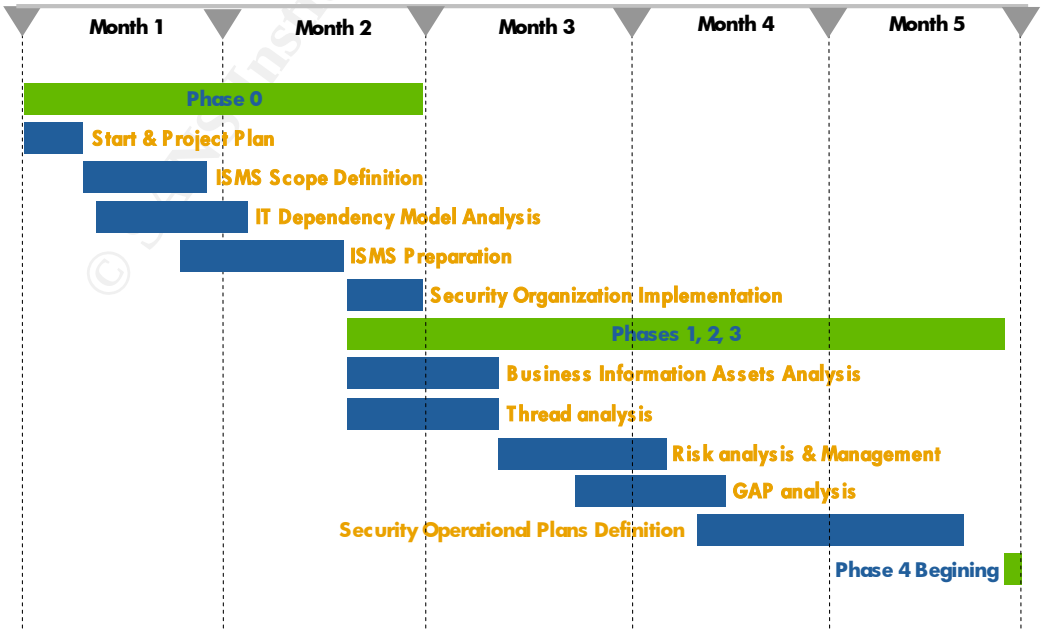
Thread	VL			L			M			H			VH		
Vulnerability	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H
Impact															
10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7
9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
3	1	2	2	2	2	3	2	3	3	3	3	4	3	4	4
2	1	1	2	1	2	2	2	2	3	2	3	3	3	3	4
1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3

The **Gap Analysis** activity will identify which security controls needed by the risk management decision that have to be implemented because they are not implemented at the moment.

The **Security Operation Plan design activity** is the most important part of the Risk management Plan because once the security controls that have to be implemented are identified, it is important to identify priorities, to group security controls in different security projects, assign resources, scheduling, assign responsibilities and to budget de project.

Detailed information and results from these activities will be included in the next steps of this practical.

The scheduling from Phase 0 to the beginning of Phase 4 is detailed in the next Gantt chart. The scheduling of phase 4 will be defined in the Security Operational Plans in phase 3 of the project:



One important issue in this planning process is that once finished the Gap analysis there will be accurate information of what security controls have to be implemented, where and how. At this moment, there will be done another planning process more detailed at operational level of whole security control implantation process.

Neither XXX nor XYZ has a security normative framework defined. This issue will be detected in the gap analysis and depending on the security controls needed there will be required specific security policies for specific areas, such as:

- Physical security
- Office Security
- Information systems utilization
- Information Classification
- Remote Access
- Communications
- Systems, networks and applications Administration
- IT Resource Planning
- Information systems Change Management
- Sw Development
- HW/SW Acquisitions
- Malicious code
- Credentials
- Cryptographic controls
- Incident detection
- Incident management
- Privacy
- Outsourcing Services
- Identity Management
- Privilege Management

Despite of these specific security policies and before this, in this Plan activity a Corporate High level Security Policy will be defined that together with the security organization will act as formal support for all the security implementation process of the ISMS.

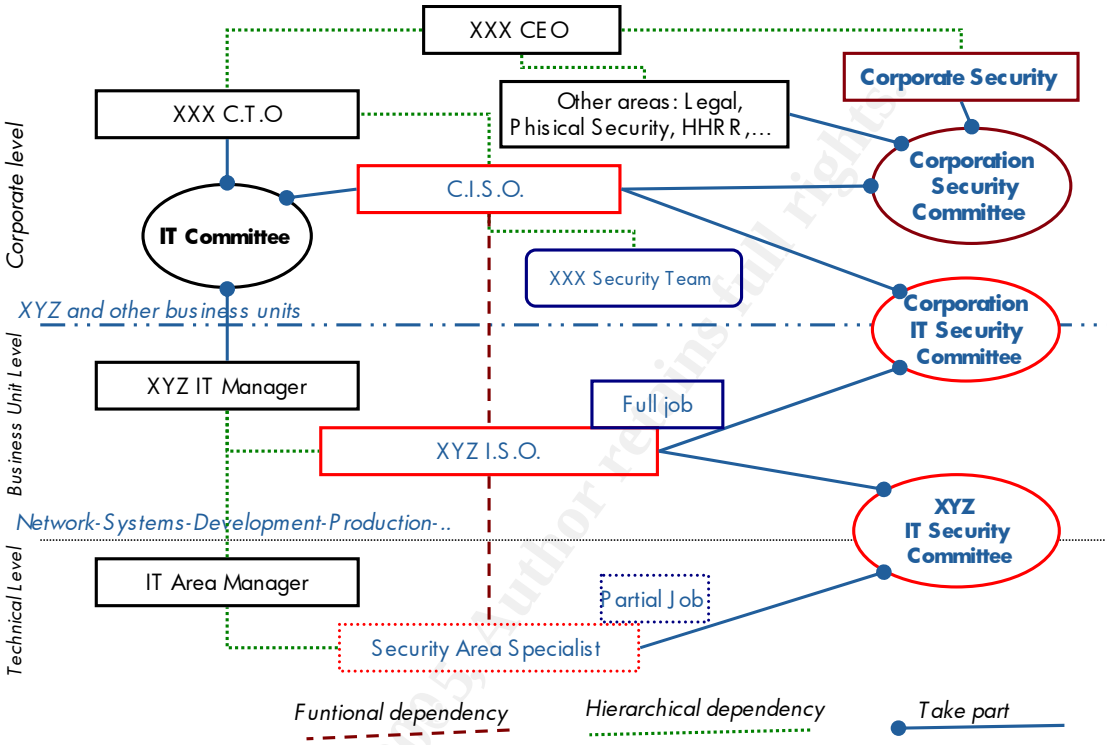
ISMS management structure:

The ISMS will not succeed if there is not a security organization that will take the responsibility of all the process in the entire PDCA framework. As I described before, neither XXX nor XYZ has a security organization defined. In consequence, one of the main objectives in the ISMS Preparation activity (see project Gantt chart) will be to define it.

This security organization has to be global, to solve security issues that could affect the global corporation, and also to achieve standardization and homogenization of objectives, but also has to be local, to adapt to the diversity

of different business that the corporation has and to be able to solve specific security issues that could affect to determined business units.

In the next figure is represented the organization that has been proposed to managed the security of XXX and XYZ:



As it is described in last figure, the committees and roles described in black already existed. The C.T.O (Chief Technology Officer) regarding to security at the moment is responsible:

- To establish the minimum quality and security level for the IT services in the corporate technology centers.
- As defined later, he will be responsible to establish one common high level strategic security policy for all technology centers in the corporation.
- To homogenize the security efforts of all corporate technology centers looking for synergies.
- Improve the interoperability of the different technology centers.

The XYZ IT Manager, regarding to security at the moment is responsible:

- To follow the Corporate high level security policy in XYZ
- To follow the minimum quality and security level for the XYZ IT services
- To Implement the Security controls needed in XYZ

As the maturity level XXX and XYZ about security is beginning it is not possible to implement a full security organization that supports all the areas in which security has to be present in a complex corporation.

This project has been leaded by IT people, and the ISMS scope defined is only related to IT departments, in consequence, the security organization that has been proposed now is only related to IT Security. The security organization proposed (roles and committees in red in last figure) is the minimum necessary to implement and manage the ISMS described before.

The most important new role defined is the **Corporate Information Security Officer (C.I.S.O)**, reporting to the C.T.O. with the next main responsibilities:

- To coordinate all the security interventions, identifying technical and economical synergies among Technology centers.
- To Lead the Corporate I.T. Security Committee.
- To take part of the Corporate Security Committee and in the I.T. Committee.
- To define, develop and Coordinate the implementation of the Corporate I.T. Security standards, such as policies, methodologies, procedures, technical aspects and homogenization
- Following and Monitoring the efficiency and efficacy of the security controls implemented
- To monitor the risk level of the critical information assets.

The C.I.S.O will have a **Security Team** working with him. At this step it is not possible to define the amount of people needed. After the risk management process, at the end of the Planning phase of all the ISMSs that will be developed, this team will be defined. In this team will be at least two people, one in charge of the development of all the policies, standards, guidelines, etc; and other in charge of the security homogenization process of the different security technologies that exist in the Corporation. Typical activities of the security team will be:

- Developing and communication of the security normative (policies, standards, guidelines, procedures, …)
- Security Management activities
- Risk Management activities
- Improvement in Security activities
- Following the implementation of the security projects
- Incident Management activities
- Monitoring Security activities
- Security Homogenization and standardization Laboratories activities
- Security Auditing activities for all the Corporation
- …

In the business unit level it has been identified a new role, the **XYZ Information Security Officer (I.S.O)** that will be responsible for the XYZ IT Security; reporting to the XYZ IT Manager with the next main responsibilities:

- To coordinate all the security interventions at XYZ Business Unit Level
- To Lead the XYZ I.T. Security Committee.
- To take part of the Corporate IT Security Committee
- To Define and develop the Security Procedures of XYZ
- To Coordinate the implementation of the I.T. Security standards, such as policies, methodologies, procedures, technical aspects and homogenization at XYZ
- Following and Monitoring the efficiency and efficacy of the security controls implemented in XYZ
- To monitor the risk level of the critical information assets in XYZ

When defining the XYZ I.S.O role, other choices suggested joining the role with the XYZ IT Manager or with one IT Area Manager, because XYZ has difficulties to find and implement this new role. The final decision was not to join these roles because XYZ recognizes that it is very important to have at least one person whose first priority is security and avoid conflict of interest with other responsibilities. Following the "Separation of Duties" Principle, the ISO role cannot be shared with IT Manager or IT area manager role.

The XYZ ISO has no team directly reporting to him. The security implementation process in XYZ will be in the different IT areas. In consequence there will be specific security area specialists (network security specialist, sw development security specialist, etc) in each IT department sharing his role with other XYZ IT activities. The **Security Area Specialist** partial job assignment reporting to specific IT area manager will have the next main responsibilities:

- To implement all the security interventions in his specific IT area
- To report and study all the security issues in his specific IT area.
- To take part of the XYZ IT Security committee

When the security maturity level of XXX and XYZ improve, the security organization will be able to be extended to other areas in the organization and at this moment will be implemented a global Corporation Security committee and a corporate security department (roles and committees in brown in last figure) that will lead all security aspects related to the business of XXX and XYZ.

Policies:

Neither XXX nor XYZ have a security normative framework defined. This issue will be detected in the gap analysis and depending on the security controls needed, specific security policies for specific areas will be required; as it was identified before, in this step a corporate global Strategic security Policy will be generated.

This is the outline of what will be covered in this Corporate High level Security Policy:

Policy Name: Strategic Security Policy for XXX Corporation

Purpose: Before implementing the ISMS it is very important that management from XXX to transmit every employee the importance of security, the main security objectives of XXX related to their business and their commitment for all the security processes that will be developed.

Audience: All people employed or contracted by XXX who have access to XXX information Services.

Areas of standard that will be addressed: Section 3 “Security Policy” including objective 3.1 “Information Security Policy”.

Some examples of Security Policies that will be implemented are:

Policy Name: Information Access Policy

Purpose: XXX manages specific information that must be protected from unauthorized access. In some cases, information will have to be segregated. A classification scheme must be defined and implemented; establishing handling procedures for each class of information.

Audience: People employed or contracted by XXX who have access to this information.

Areas of standard that will be addressed: Section 5. “Asset Classification and Control” including objective 5.2 “Information Classification”.

Policy Name: Malicious Software Policy

Purpose: XXX has to guaranty the availability and integrity of critical information systems. In these critical information systems, it is necessary to implement security controls to prevent, detect and correct the impact of any malicious software.

Audience: People employed or contracted by XXX who have access to critical information systems

Areas of standard that will be addressed: Section 8.3.1: “Controls against malicious software”

There will be more Security Policies that will have to be implemented. In the gap analysis activity these policies will be identified and the Security Operation Plan will define how these policies will be developed.

Risks:

Following the Risk Management Plan detailed before based on CRAMM® methodology, these are the results form each activity:

Information Asset Analysis

In this activity, Business information asset managers are interviewed. In the next figure (business impact analysis table) you can see the results of these interviews with the impact level assigned to each of the 26 security incident scenarios that were suggested for each information asset:

		Unavailability										Revelation			Modif.			Dest.		Incorrect Interchange							
	Information Assets	15m	1h	3h	12h	1d	2d	1s	2s	1m	2m	DI	SP	DO	SE	WE	DM	PD	TD	In	RO	RC	Nd	Rp	Mr	TM	OS
XYZ	A1: Content of the Daily Newspaper	3	3	3	5	7	7	7	7	7	7			4	3		3	3					4				
XYZ		6	6		5	5								3	5		4	6					6				
XYZ	A2: News and Documentary information	3	3	5	5	7	7	7	7	7	7			3	4			4	6				4				
XYZ		6		5	5									3	5			6	6				6				
XYZ	A3: Advertising information and management					3	3	4	4	8	8			7	3			1	5								
XYZ						6		4		4				4	4			6	6								
XYZ	A4: Final newspaper product		5	5	7	7	7	7	7	7	7				3		4						6				
XYZ			5	5	5										5		5						5				

For each information asset and each security scenario that applies (if it doesn't apply it is in blank) you can see the impact level in color (Red, orange or yellow) and bellow the scale that have been used to estimate the impact.

For any of the security incident scenarios, the impact level can be estimated using 6 impact scales that CRAMM® supplies; in appendix IV are detailed each of this 6 impact scales that have been used.

This is an example to understand the Impact analysis table: "The Impact level that it is estimated because of not having access available to the content of the daily newspaper (Asset 1) for 1 day is **7.** This impact was estimated by the asset manager responsible using the scale **5,** because this scenario affects negatively the relationship with other organizations, with public and the negative publicity can be extended beyond the nearby geographic environment."

Thread Analysis

In order to make the thread analysis as efficient as possible, all IT elements that **have the same threats have been grouped**:

First of all, groups that can be affected by "Generic Threats" have been identified. These are some example of XYZ Generic groups with Generic threats:

- **GE Fixed PC**: Generic Threats applies to fixed PCs. Threats below will be considered in this group:
    - HW Maintenance Error
    - SW Maintenance Error
    - Malicious Software
    - System Resources Abuse
- **GE Mobile PC**: Generic Threats applies to Mobile PCs. Threats below will be considered in this group:

- HW Maintenance Error
- SW Maintenance Error
- Malicious Software
- System Resources Abuse
- Theft by outsiders

- **GE 200x Server & GE NT Server**: Generic Threats applies to 200x & NT Servers. Threats below will be considered in this group:

  - Operation Error
  - HW Maintenance Error
  - SW Maintenance Error
  - Lack of staff
  - Host Error
  - Air conditioning Error
  - Network or System Software Error
  - Malicious Software
  - System Resources Abuse

There are some issues that affect to specific IT elements from XYZ Technology Centers, so it is necessary to add some specific threats. These are some example of XYZ specific groups with specific threats:

- **XYZ Mobile PC**: Specific Threats that applies to Mobile PCs from XYZ Technology Center. The hardware and software maintenance of these equipment is different because we are talking of equipment that in normal conditions is in another places so one hardware incidence can cause the equipment to be unavailable for more than 1 week.

- **XYZ Electricity Location A:** This is the best and new building in XXX Corporation and the electricity incidents have lower frequency than in other XXX buildings.

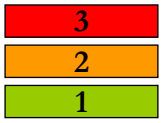
In appendix V is detailed the list of threats groups that apply to each IT Dependency group.

When analyzing the threats and vulnerabilities for each group the next CRAMM® scale is applied:
Threat: Represents the frequency of a security incident event.

VH (Very High): Every Month	5
H (High): Three times a year	4
M (Medium): Once a year	3
L (Low): Once each Three years	2
VL (Very Low): Once each Ten years	1

Vulnerabilities: Represents the impact when a threat happens.

H (High): Always happens the worst case (Probability > 66%)
M (Medium). Possible to happen the worst case (33% < P < 66%)
L (Low). Difficult to happen the worst case (P < 33%)



In appendix VI, it is summarize the results of the Threat analysis for XYZ IT Dependency groups.

Risk analysis

Once we have the asset impact analysis information and the results from the IT dependencies threat analysis, the information is introduced in CRAMM® in order to obtain the risk table where the risks that can affect the information assets will be identified.

There have been identified **358** risks that apply to the ISMS IT dependencies. In this table you can see the **risk distribution Matrix applied to XYZ** classified by Threat level and Impact level:

XYZ	**Threat Frequency**					
	10 years	3 years	1 year	3 x year	month	
N. of Risks	**Threat L.**					
Impact L.	VL	L	M	H	VH	Total
8	1					1
7	30	19	25	8	16	98
5	8	18	40	23	22	111
3	14	16	34	30	54	148
Total	53	53	99	61	92	358

Then, once the risks that affect the ISMS IT dependencies are identified, it is the moment to select which of them have to be mitigated and which of them have to be accepted; this is the risk management activity.

Risk Management

In order to manage the risks, some criteria is needed to determine what risks have to be mitigated and how. Remembering the risk management matrix detailed at the beginning of part 2, the risk level criteria distinguished three types of risks:

- **Obligatory**: Critical risks that have to be mitigated
- **Recommended**: Major risks that it is recommended to be mitigated
- **Informative**. Identified Risks that have to be identified but not mitigated

For XYZ Business Unit, the thresholds criteria for these risks are:

- **Obligatory**: Risk level > 5
- **Recommended**: Risk Levels 4 & 5
- **Informative**: Risk level < 4

Thresholds

>5 **Obligatory** 4,5 **Recommended** <4 **Informative**

Following this criteria, this is how the 380 risks that applied to XYZ ISMS have been distributed:

Risks	Threat Vuln.															
	VL Threat			L Threat			M Threat			H Threat			VH threat			Total
Impact	L Vul	M Vul	H Vul	L Vul	M Vul	H Vul	L Vul	M Vul	H Vul	L Vul	M Vul	H Vul	L Vul	M Vul	H Vul	
8			1													1
7	16	6	8	11	7	1	9	5	11	3	2	3	4	8	4	98
5	4	2	2	1	11	6	10	19	11	3	12	8	2	17	3	111
3	12	2		7	6	3	11	12	11	5	16	9	6	43	5	148
Total	32	10	11	19	24	10	30	36	33	11	30	20	12	68	12	**358**

As conclusion of the risk management activity there are **15** risks that have to be mitigated, **206** risks that it is recommended to mitigate and **137** risks that have identified but it is not necessary to mitigate.

In appendix VII level 5 and level 6 risk examples has been detailed.

It is not possible in the scope of this document to detail the risk plan process for the 358 risks identified. In consequence, I am going to detail the risk plan process (risk analysis and risk management) for level 6 risks identified that have to be mitigated. The risk plan process for the rest of risks is analogous.

Case 1:

IT Dependency: XYZ-Correspondent PCs
Threat Group Assigned: XYZ Mobile PC
Risk level 6

1) Most Critical Risks Identified:

- Risk A:
  - **Nature of the threat:** Introduction of Damaging or Disruptive Software
  - **Vulnerability:** Medium Probability of unavailability for 1 Week.
  - **Likelihood of Occurrence:** Very High (once a month)
  - **Impact to the information Asset related:** 7
  - **Risk Level:** 6 (Obligatory to mitigate)

- Risk B:

  - **Nature of the threat:** Misuse of System Resources
  - **Vulnerability:** Medium Probability of unavailability for 1 Week.
  - **Likelihood of Occurrence:** Very High (once a month)
  - **Impact to the information Asset related:** 7
  - **Risk Level:** 6 (Obligatory to mitigate)

2) Description of the controls selected (proposed with CRAMM®):

- Unattended XYZ Mobile PC should be protected against an unauthorized person taking the opportunity to use the equipment (ISO 17799, Control 9.3.2: "*Unattended user equipment*")
- The potential for the introduction of malicious software into the XYZ Mobile PC should be minimized (ISO 17799, Control 8.3.1: "*Controls against malicious software*")
- The XYZ Mobile PC should be monitored for potential malicious software activity (ISO 17799, Control 8.3.1: "*Controls against malicious software*")
- Any malicious software should be identified, isolated, and removed (ISO 17799, Control 8.3.1: "*Controls against malicious software*")

3) Reason for selecting control: These are controls that are not difficult to implement; there are antivirus, anti-spam, content management and access control technology solutions in the market that make these controls feasible and mitigate directly the risks identified.

4) Risk level after implementing control: Because the risk level identified is 6, the security controls needed not only have to be implemented but also have to be audited. Once Implemented and satisfactory audited the risk level 6 would be mitigated. As these controls do not mitigate other identified level 5 risks, the risk level after implementing these controls will be reduced from 6 to 5.

Case 2:

IT Dependency: XYZ Location X
Threat Group Assigned: GE Buildings
Risk level 6

1) Most Critical Risks Identified:

- Risk A:

  - **Nature of the threat:** Willful Damage by Outsiders
  - **Vulnerability:** Medium Probability of unavailability for 1 day.
  - **Likelihood of Occurrence:** Very High (once a month)
  - **Impact to the information Asset related:** 7

- **Risk Level:** 6 (Obligatory to mitigate)

- Risk B:

  - **Nature of the threat:** Terrorism
  - **Vulnerability:** Medium Probability of unavailability for 2 days.
  - **Likelihood of Occurrence:** Very High (once a month)
  - **Impact to the information Asset related:** 7
  - **Risk Level:** 6 (Obligatory to mitigate)

2) Description of the controls selected (proposed with CRAMM®):

- Key staff should be distributed across several sites
- Pre-equipped stand-by accommodation should be available
- Where appropriate, non-critical staff should work from home
- Entrances to the site should be kept to a minimum
- The entrances to the site should be monitored
- The site should be surrounded by a security barrier that is designed to deter and delay a resourceful attacker
- All dark spots should be eliminated
- Lighting which illuminates the areas inside the perimeter fence should be installed.
- Surfaces (e.g. buildings or fences) which intruders must pass in front of should be illuminated
- Guards should monitor the site from an incident control room
- Guards should mount patrols of the external areas of the site or building
- Guards should visit the site during silent hours
- Surveillance of the site perimeter should be undertaken using Closed Circuit Television (CCTV)
- The security of the site should not be the responsibility of a single security guard
- When using a commercial guard force the company must be reputable
- Mechanisms should be in place to recognize a temporary increase in level of threat, and procedures to raise the state of vigilance should be implemented
- Technical measures should be implemented to identify suspicious packages
- Staff should be aware of the actions they must take during a bomb warning
- Staff should be able to recognize a suspect device and take appropriate action
- The procedures for the detection of suspect devices should be tested
- Ensure all critical activities are conducted as far away from any identified vulnerable point as possible
- The entrances to the site should be monitored
- The site should have a defined security perimeter
- Potential vulnerable points in the site or building should be identified

- Seek specialist advice on conducting a site survey to identify all vulnerable areas and document them
- Security reviews should be undertaken to ensure compliance with physical, procedural and technical countermeasures

3) Reason for selecting control: These are controls not easy and expensive to implement, but they are very common in physical security high protected environments; these controls mitigate directly the risks identified.

4) Risk level after implementing control: Because the risk level identified is 6, the security controls needed not only have to be implemented but also have to be audited. Once Implemented and satisfactory audited the risk level 6 would be mitigated. As these controls do not mitigate other identified level 5 risks, the risk level after implementing these controls will be reduce from 6 to 5.

Case 3:

IT Dependency: XYZ-DMZ Network XYZ.net
Threat Group Assigned: GE Exposed Network
Risk level 6

1) Most Critical Risks Identified:

- Risks A:
  - **Nature of the threat:** Communications Infiltration, Interception or Manipulation
  - **Vulnerability:** High Probability of Unauthorized disclosure to outsiders
  - **Likelihood of Occurrence:** Very High (once a month)
  - **Impact to the information Asset related:** 7
  - **Risk Level:** 6 (Obligatory to mitigate)
- Risk B:
  - **Nature of the threat:** Communications Interception
  - **Vulnerability:** High Probability of Non delivery
  - **Likelihood of Occurrence:** High (3 Times per year)
  - **Impact to the information Asset related:** 7
  - **Risk Level:** 6 (Obligatory to mitigate)
- Risk C:
  - **Nature of the threat:** Communications Failure
  - **Vulnerability:** High Probability of Non delivery
  - **Likelihood of Occurrence:** High (3 Times per year)
  - **Impact to the information Asset related:** 7
  - **Risk Level:** 6 (Obligatory to mitigate)

- Risk D:

  - **Nature of the threat:** Embedding of Malicious Code
  - **Vulnerability:** High Probability of Unauthorized disclosure to outsiders
  - **Likelihood of Occurrence:** Very High (once a month)
  - **Impact to the information Asset related:** 7
  - **Risk Level:** 6 (Obligatory to mitigate)

2) Description of the controls selected (proposed with CRAMM®):

- The network should be monitored
- All faults on the network should be reported
- The network service should be monitored
- The service provider's contract should formally define the security issues for the Network Service
- Independent audits and reviews should be performed regularly
- Network traffic volumes should be monitored
- Network devices should be checked to ensure that all known vulnerabilities have been eliminated
- Network traffic should be monitored for signs of unauthorized or hostile activity
- A policy should be formulated concerning the use of networks and network services
- Unauthorized access to remote access ports should be prevented
- The confidentiality of information being transmitted over the remote access links should be safeguarded
- The networking facilities available to users should be restricted to those for which there is a demonstrable business requirement
- Routing controls should be implemented in shared network to ensure that the flows of information do not breach the access control policy
- The flow of traffic between networks should be controlled
- General access to and from external networks should be prevented
- Individual network users should be identified and their functionality restricted
- Isolate specific hosts and control communications with hosts and networks
- Isolate the network from other networks
- Access to the Internet should be controlled
- Isolate Internet connections
- Control the network management traffic used to monitor and manage network devices
- The gateway/firewalls should have a defined access control policy
- Control physical access to network devices
- Restrict logical access to network consoles
- Restrict remote access to network devices
- Routing configuration information should be backed up on a regular basis
- All unused diagnostic and control equipment should be secured

- Only authorized users should use diagnostic and control equipment
- The accuracy of the inventory of diagnostic and control equipment should be checked regularly
- Use of diagnostic and control equipment to be checked to ensure that it is not being misused
- Access to all network distribution and termination equipment should be restricted to authorized personnel
- The network should be resilient to failure of individual components
- The network should be set up to ensure that traffic is delivered in a timely manner
- Connections to public networks should be set up in such a manner that they can resist 'denial of service' attacks
- A procedure should exist for handling 'denial of service' attacks
- Changes to IT facilities should be controlled
- Changes to the Operating System should be authorized
- The security impact of a change to the Operating System should be reviewed
- Access to the System Administration accounts should be strictly controlled
- Changes to packaged software should be carried out in such a manner that the change will not introduce further problems
- A stand-by Host should be available to take over processing in the event of a disaster or other incident
- Where appropriate it should be possible to revert to a manual process
- Emergency spares should be available
- Back-ups should be taken of all essential business data
- Back-ups should be taken of all software applications
- All data should be backed-up using suitable technology
- It should be possible to re-create data lost since last back-up
- The system should be resilient to the failure of individual storage disks
- Equipment should be sited to reduce the risks from environmental threats and hazards and opportunities for unauthorized access

3) Reason for selecting control: These are many controls but not difficult to implement to the DMZ specific environment; there are security and network technology solutions in the market that make these controls feasible and mitigate directly the risks identified.

4) Risk level after implementing control: Because the risk level identified is 6, the security controls needed not only have to be implemented but also have to be audited. Once Implemented and satisfactory audited the risk level 6 would be mitigated. As these controls do not mitigate other identified level 5 risks, the risk level after implementing these controls will be reduce from 6 to 5.

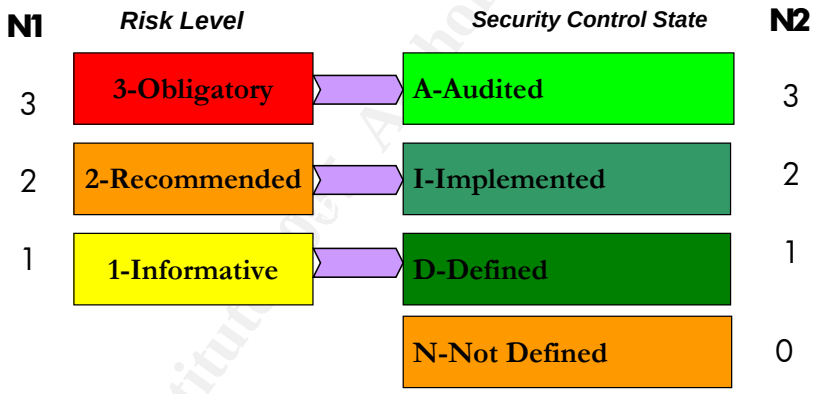
For the rest of this document, in order to achieve the detail level required and not to extend the document more than needed, I am going to develop the Do and Check Steps of the PDCA model for Case 1 and Case 2.

Part Three: Do.

Finishing the risk management process activity, CRAMM® tools proposed **150** security controls to mitigate informative level risks, **915** controls to mitigate recommended level risks and **662** controls to mitigate obligatory level risks.

Now, it is moment to begin the steps to implement the security controls. Based on the risk management decision, we know what security controls are needed, but also, it is very important to know how theses controls have to be implemented. **XYZ has decided the following criteria** that apply to the security controls that have to be implemented:

- **Audited Controls**: All countermeasures to mitigate Obligatory risks have to be implemented and appropriately audited
- **Implemented Controls**: All countermeasures to mitigate Recommended risks have only to be implemented but it is not necessary to be audited
- **Defined Controls**: All countermeasures needed to mitigate Informative risks only have to be defined.



$$XYZ\ Security\ Level = \sum (N2\text{-}N1)$$

Objetive Security Level = 0

Next step is the Gap analysis activity; we know what is needed to achieve the security objective, but following the methodology we also need to know what is the real state in XYZ of theses security controls. With this information a Gap Analysis related to the security objectives defined will be developed. And based on this gap analysis it is possible to define, and implement the security operational plans to achieve the security objective.

Based on security controls proposed with CRAMM®, begins the GAP Analysis activity. The security controls are revised grouped by control type; it is easier, because there are many cases that the same control applies to one o more IT dependencies. In the Gap Analysis every countermeasure is associated to one of these states:

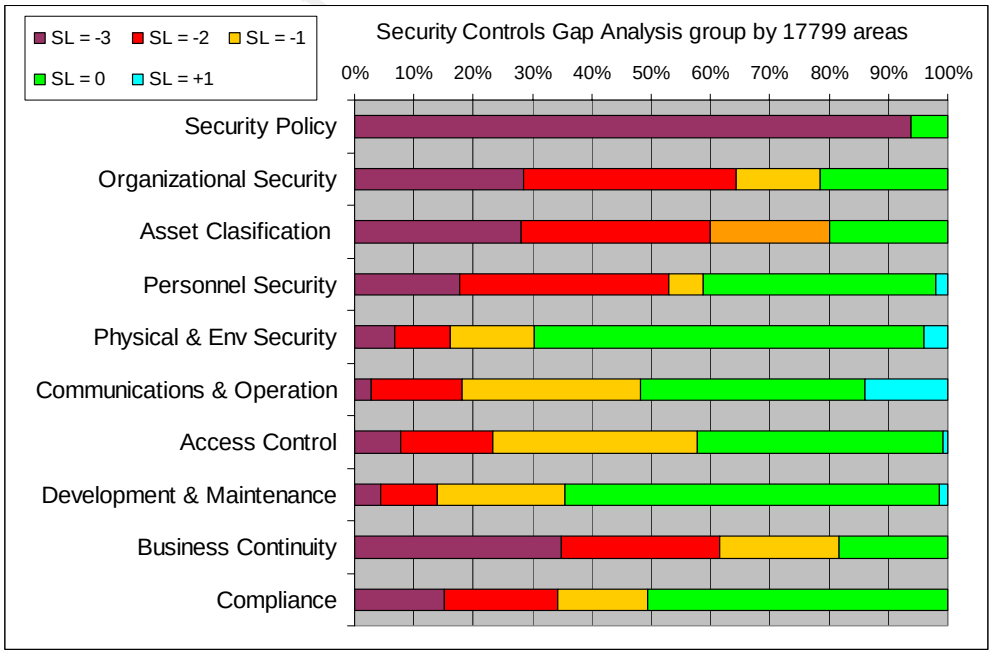
- **0 – Not Defined**: XYZ has not thought before about this countermeasure.
- **1 – Defined**: XYZ has thought before, knows that this countermeasure is useful to mitigate a particular risk but has decided not to implement it. In this state, have also been included all countermeasures that are even implemented but the efficacy of the control does not mitigate the risk or the implementation level is not adequate.
- **2 – Implemented**: countermeasure totally and correctly implemented.
- **3 – Audited**: In addition to implemented, the countermeasure, is periodically revised of being correctly implemented with the desired efficacy level.
- **Evaluation Pending**: It is not possible to check the real state of the countermeasure
- **Not Applicable**: Countermeasure that has non sense and doesn't mitigate the risk

Once, all countermeasures have its state assigned, the security level of the countermeasure is obtained:

Security Level (**SL**) = Countermeasure State – Countermeasure Objective

The Global Security level is the addition of all countermeasure security levels. With these criteria, we have now a very simple metric to measure the real security controls implantation state of the ISMS. Now, we know that the Global Security Level (**GSL**) Objective (related to control implementation) of our ISMS has to be equal o higher than 0.

The next figure graphically represents the results of the Gap analysis activity, the countermeasures has been grouped in the 10 different areas of the standard ISO-IEC 17799:2002:



Following the figure, it is possible to differentiate the next Security levels (**SL**) in each 17799 area:

- **SL = -3**; Identify these countermeasures that are required to be audited but its actual state is not defined.
- **SL = -2**; Identify this countermeasures not defined that have to be implemented; or countermeasures defined that have to audited
- **SL = -1**; identify countermeasures in one state level below the objective
- **SL = 0**; identify countermeasures whose state is correct, there is no action needed with them
- **SL = 1**; identify countermeasures that are over-secured; there is no action needed with them.

Next step is to begin to correct the Security Level (**SL**) of the countermeasures identified before. The Gap analysis is done countermeasure per countermeasure (see next examples), but the corrective actions are grouped in Security Projects. Each project will have specific priority, dependencies with other projects, security controls to be corrected, budged, resources needed, scheduling and a Project Manager assigned. The criteria to assign controls to project are more dependent in the way of XYZ of doing things. There are some projects that are grouped following the criteria of countermeasures that affect to one specific department, other criteria can be the skills needed to implement de countermeasures (governance management skills versus security technical skills).

The security projects that XYZ have developed to correct the security level of the countermeasures identified are:

- Security Organization and Security Management
- Security Policies, standards and guidelines for XYZ
- Security Audit
- HHRR Framework Improvement
- Identity Management
- Remote Access
- Incident management
- Business Continuity
- Security Awareness Program
- Active Directory Security
- Security Procedures development
- Inventory management
- Security Monitoring
- Security practices in SW development
- Security in networks and communications
- Development Security Best Practices
- Password Management
- Physical security

These are 2 cases of the Gap analysis activity related to the specific risks and countermeasures detailed in part 2.

As this is Part 3 (Do activity of the PDCA model), I am going to explain the corrective action related to Implement controls; once implemented, in part 4 (Check activity of the PDCA model), I will explain the audit process needed. So the objective in this phase is to implement the corrective actions, it is no time yet to audit.

Case 1:

IT Dependency: XYZ-Correspondent PCs
Threat Group Assigned: XYZ Mobile PC
Risk Level 6

Gap Analysis

In the next table we can see the countermeasure Gap Analysis results for risk level 6 countermeasures that apply to XYZ-Correspondent PCs:

Code	Group	Sub-Group	Description	IT Dependency	Problem Description	CM State	Risk Level	CM Objetive	Security Level (SL)	Action
20. L55. 1.	20. Logical Access Control	55. Workstation Time-out/Password Protected Screen Savers	1. Unattended workstations should be protected against an unauthorised person taking the opportunity to use the workstation	XYZ-Correspondent PCs	There are some doubts about the implementation level of this control	1- Defined	6	3 - Audited	-2	Implement & Audit
80. P170.1.	80. Protection Against Malicious Software	170. Prevention Against Malicious Software	1. The potential for the introduction of malicious software into the IT system should be minimised	XYZ-Correspondent PCs	The antivirus software is supposed to be installed but there is no certain of its effectiveness	2- Implemented	6	4 - Audited	-1	Audit
80. P175.1.	80. Protection Against Malicious Software	175. Detection of Malicious Software	1. The system should be monitored for potential malicious software activity	XYZ-Correspondent PCs	The antivirus software is supposed to be installed but there is no certain of its effectiveness	2- Implemented	6	5 - Audited	-1	Audit
80. P180.1.	80. Protection Against Malicious Software	180. Removal of Malicious Software	1. Any malicious software should be identified, isolated, and removed	XYZ-Correspondent PCs	The antivirus software is supposed to be installed but there is no certain of its effectiveness	2- Implemented	6	6 - Audited	-1	Audit

Based on this Gap analysis, we know the specific problems that we need to address in this phase:

Control Description: Unattended workstations should be protected against an unauthorized person taking the opportunity to use the workstation

Problem: There are some doubts about the implementation level of this control. Security level (**SL**) Assigned **-2**

Action: For all XYZ-Correspondent PCs enforce an automatic timeout session lock. Session Lock out has to be enforced with Correspondent Authentication Credentials supply. Inform and train all XYZ Correspondent about manually locking and unlocking their PCs when unattended.

(Related to ISO 17799 Control 9.3.2: "*Unattended user equipment*")
(Related to ISO 17799 Control 6.2.1: "*Information security education and training*")

Steps:

- Based on XYZ-Correspondent PCs inventory, develop an assessment to check the current state of this control for each XYZ-Correspondent PC.

- All the equipment belongs to an Active Directory Domain, so the solution is to enforce this control based on Active Directory Policies.
- Coordination with **XXX/XYZ Active Directory Security Project** to add this countermeasure.
- Test the control in a lab environment to check the real enforcement of the control
- Check that the final user cannot disable by himself the control
- Prepare a roll-out implementation plan
- Notice the help-desk department before beginning to implement the changes in order to make them able to deal with possible incidents
- In the implementation process check the number of equipments that have been enforced and identify which equipments has not been enforced
- Identify the reasons why some equipments have not been enforced (perhaps these equipments are usually in remote areas, not connected, outside the AD Domain)
- Through help desk department contact these users and enforce the new policy.
- Coordination with **XXX/XYZ Security Awareness Program** to add this countermeasure.
- When designing the security awareness courses material, include information about these topics:
  - Inform Correspondent about the importance of locking the PC when unattended.
  - Train the Correspondent on locking and unlocking the PC
- Plan and Coordinate the security awareness courses implementation with HHRR department.
- Check that all XYZ Correspondents have received the course.

Case 2:

IT Dependency: XYZ Location X
Threat Group Assigned: GE Buildings
Risk level 6

Gap Analysis

In the next table we can see the countermeasure Gap Analysis results for risk level 6 countermeasures that apply to XYZ Location X Building:

Code	Group	Sub-Group	Description	IT Dependency	Problem Description	CM State	Risk Level	CM Objetive	Security Level (SL)	Action
370. 555.3.	370. Recovery Options for Accommodation	555. Recovery of Accommodation	Key staff should be distributed across several sites	XYZ Location XXX Building	xxxxxxxxxxxxxxxxxx	0-Not Defined	6	0-Not Applicable	0	
370. 555.1.	370. Recovery Options for Accommodation	555. Recovery of Accommodation	Pre-equipped stand-by accommodation should be available	XYZ Location XXX Building	xxxxxxxxxxxxxxxxxx	0-Not Defined	6	0-Not Applicable	0	
370. 555.2.	370. Recovery Options for Accommodation	555. Recovery of Accommodation	Where appropriate, non-critical staff should work from home	XYZ Location XXX Building	xxxxxxxxxxxxxxxxxx	0-Not Defined	6	0-Not Applicable	0	
430. 640.3.	430. Site / Building Physical Security	640. Perimeter of the Site	Entrances to the site should be kept to a minimum	XYZ Location XXX Building	xxxxxxxxxxxxxxxxxx	3-Audited	6	3-Audited	0	
430. 640.5.	430. Site / Building Physical Security	640. Perimeter of the Site	The entrances to the site should be monitored	XYZ Location XXX Building	xxxxxxxxxxxxxxxxxx	3-Audited	6	3-Audited	0	
430. 640.4.	430. Site / Building Physical Security	640. Perimeter of the Site	The site should be surrounded by a security barrier that is designed to deter and delay a resourceful attacker	XYZ Location XXX Building	There is a perimeter zone where Security Barrier is not effective	1-Defined	6	3-Audited	-2	Implement & Audit
430. 645.2.	430. Site / Building Physical Security	645. Security Lighting	All dark spots should be eliminated	XYZ Location XXX Building	xxxxxxxxxxxxxxxxxx	3-Audited	6	3-Audited	0	
430. 645.1.	430. Site / Building Physical Security	645. Security Lighting	Lighting which illuminates the areas inside the perimeter fence should be installed	XYZ Location XXX Building	xxxxxxxxxxxxxxxxxx	3-Audited	6	3-Audited	0	
430. 645.3.	430. Site / Building Physical Security	645. Security Lighting	Surfaces (e.g. buildings or fences) which intruders must pass in front of should be illuminated	XYZ Location XXX Building	xxxxxxxxxxxxxxxxxx	3-Audited	6	3-Audited	0	
430. 660.4.	430. Site / Building Physical Security	660. Site Monitoring	Guards should monitor the site from an incident control room	XYZ Location XXX Building	xxxxxxxxxxxxxxxxxx	3-Audited	6	3-Audited	0	
430. 660.5.	430. Site / Building Physical Security	660. Site Monitoring	Guards should mount patrols of the external areas of the site or building	XYZ Location XXX Building	xxxxxxxxxxxxxxxxxx	3-Audited	6	3-Audited	0	
430. 660.1.	430. Site / Building Physical Security	660. Site Monitoring	Guards should visit the site during silent hours	XYZ Location XXX Building	xxxxxxxxxxxxxxxxxx	3-Audited	6	3-Audited	0	
430. 660.3.	430. Site / Building Physical Security	660. Site Monitoring	Surveillance of the site perimeter should be undertaken using Closed Circuit Television (CCTV)	XYZ Location XXX Building	xxxxxxxxxxxxxxxxxx	3-Audited	6	3-Audited	0	
430. 660.6.	430. Site / Building Physical Security	660. Site Monitoring	The security of the site should not be the responsibility of a single security guard	XYZ Location XXX Building	xxxxxxxxxxxxxxxxxx	3-Audited	6	3-Audited	0	
430. 660.2.	430. Site / Building Physical Security	660. Site Monitoring	When using a commercial guard force the company must be reputable	XYZ Location XXX Building	xxxxxxxxxxxxxxxxxx	3-Audited	6	3-Audited	0	
480. 700.1.	480. Terrorist / Extremist Warnings	700. States of Vigilance	Mechanisms should be in place to recognise a temporary increase in level of threat, and procedures to raise the state of vigilance should be implemented	XYZ Location XXX Building	xxxxxxxxxxxxxxxxxx	3-Audited	6	3-Audited	0	
500. 715.1.	500. Bomb Detection	715. Bomb Identification	Technical measures should be implemented to identify suspicious packages	XYZ Location XXX Building	xxxxxxxxxxxxxxxxxx	3-Audited	6	3-Audited	0	
500. 720.1.	500. Bomb Detection	720. Bomb Alarms	Staff should be made aware of the actions they must take during a bomb warning	XYZ Location XXX Building	The Procedure is only defined; not implemented	1-Defined	6	3-Audited	-2	Implement & Audit
500. 725.1.	500. Bomb Detection	725. Bomb Identification procedures	Staff should be able to recognise a suspect device and take appropriate action	XYZ Location XXX Building	The Procedure is only defined; not implemented	1-Defined	6	3-Audited	-2	Implement & Audit
500. 725.2.	500. Bomb Detection	725. Bomb Identification procedures	The procedures for the detection of suspect devices should be tested	XYZ Location XXX Building	The Procedure is only defined; not implemented	1-Defined	6	3-Audited	-2	Implement & Audit
510. 730.2.	510. Internal and External Bomb Protection	730. Site Layout	Ensure all critical activities are conducted as far away from any identified vulnerable point as possible	XYZ Location XXX Building	xxxxxxxxxxxxxxxxxx	3-Audited	6	3-Audited	0	
510. 730.3.	510. Internal and External Bomb Protection	730. Site Layout	The entrances to the site should be monitored	XYZ Location XXX Building	xxxxxxxxxxxxxxxxxx	3-Audited	6	3-Audited	0	
510. 730.1.	510. Internal and External Bomb Protection	730. Site Layout	The site should have a defined security perimeter	XYZ Location XXX Building	There is a perimeter zone where Security Barrier is not effective	2-Implemented	6	3-Audited	-1	Audit
510. 735.1.	510. Internal and External Bomb Protection	735. Site Layout Procedures	Potential vulnerable points in the site or building should be identified	XYZ Location XXX Building	There is a perimeter zone where Security Barrier is not effective	2-Implemented	6	3-Audited	-1	Audit
510. 735.2.	510. Internal and External Bomb Protection	735. Site Layout Procedures	Seek specialist advice on conducting a site survey to identify all vulnerable areas and document them	XYZ Location XXX Building	xxxxxxxxxxxxxxxxxx	3-Audited	6	3-Audited	0	
620. 870.2.	620. Compliance Checks	870. Compliance Checks	Security reviews should be undertaken to ensure compliance with physical, procedural and technical countermeasures	XYZ Location XXX Building	xxxxxxxxxxxxxxxxxx	3-Audited	6	3-Audited	0	

Based on this Gap analysis, we know the specific problems that we need to address in this phase:

Control Description: The site should be surrounded by a security barrier that is designed to deter and delay a resourceful attacker.

(Related to ISO 17799 Control 7.1.1: "*Physical security perimeter*")

Problem: There is a perimeter area where the Security Barrier is not effective. Security level (**SL**) Assigned **-2**

Action: Enforce a complete and effective security barrier for the whole XYZ Location X Security Perimeter.

Steps:

- Develop an assessment to check the current vulnerabilities in XYZ Location X Security Barrier.
- Coordination with **XXX/XYZ Physical Security Project** to add this countermeasure.
- Design a new external door, fence and security controls for these area with the same security criteria as the rest of the XYZ Location X Perimeter barrier.
- Plan and Coordinate the implementation processes with all possible XYZ employees and partners affected.
- Implement a new external door and new fence.
- Pay special attention when works are running with specific security guards watching this area.

Control Descriptions:

- Staff should be aware of the actions they must take in case of a bomb warning
- Staff should be able to recognize a suspect device and take appropriate action
- The procedures for the detection of suspect devices should be tested

(Related to ISO 17799 Control 6.2.1: "*Information security education and training*")

Problem: The Procedure is only defined; not implemented. Security level (**SL**) Assigned **-2**

Action: All XYZ Location X employees have to receive appropriate training about bomb warning, and suspect devices detection.

Steps:

- Develop an assessment with some XYZ Location X employees to check the current state about employee Security Awareness.
- Coordination with **XXX/XYZ Security Awareness Program** to add this countermeasure.
- When designing the security awareness courses material, include information about these topics:
  - Inform employees to check the origin of any package they can receive. If the origin is not trusted, don't do anything, and immediately call the security department.
  - Inform employees about the procedure they have to follow when evacuating a Location and key recommendation to success the evacuation.
- Plan and Coordinate the implementation of security awareness courses with HHRR department.
- Check that XYZ Location X employees have received the course.

Statements of applicability & exclusion

Following the security controls defined before, these are some examples of **statements of applicability and exclusion** that have been defined:

ISO 17799 Control 6.2.1: "*Information security education and training*"

XYZ security is responsibility of all XYZ employees. Due to critical risk identified that can affect the normal business of XYZ is absolutely necessary that all XYZ employees and where relevant, partners, should receive and understand the appropriate information to follow the XYZ policies, standards, guidelines and security procedures.

ISO 17799 Control 7.1.1: "*Physical security perimeter*"

Due to critical risks that have been identified, it is absolutely necessary that all XYZ locations must have a Physical Security perimeter clearly defined and implemented. This physical security perimeter must be respected by any person who wants to get in or get out from any XYZ Location. The Physical Security Perimeter must be enforced by a security barrier to deter and delay a resourceful attacker.

ISO 17799 Control 9.3.2: "*Unattended user equipment*"

XYZ security is responsibility of all XYZ employees. Every XYZ employee is responsible of the security of any assigned equipment. It is absolutely necessary to implement the security controls needed to protect unattended equipment from unauthorized accesses. It is responsibility of the user to lock the equipment when unattended.

This is an example of an ISO 17799 control that **doesn't apply** to XYZ ISMS developed.

ISO 17799 Control 10.5.5 "*Outsourced software development"*
(Does Not Apply)

XYZ has decided not to apply Outsourced software development security controls because at the moment there is no software development outsourced to other entities.

Part Four: Check.

Following the Separation of Duties Security Principle, XXX has decided to centralize the Security Audit Process. As the security countermeasure implementation process is responsibility of the different Technology centers (for example XYZ), the audit process has to be responsibility of another department to avoid conflict of interests. That's why a Security Audit corporate Project has been defined to cover and coordinate all the security audits needed. The Corporate Security Team (reporting to the CISO) will be responsible of coordinating all the audits needed in XYZ.

After the implementation process (Do Activity of the PDCA Model), the security level of the countermeasures that have been implemented to mitigate risk level 6 is now **-1,** because the audit process is pending.

Based on the 2 cases detailed in part 2 and 3, in this section I am going to specify how is going to be implemented the audit processes that are pending. In the next Gap Analysis table we can see the countermeasure that need Audit process after the Do Activity of the PDCA model.

											ISO 17799		
Code	Group	Sub-Group	Description	IT Dependency	Problem Description	CM State	Risk Level	CM Objetive	Security Level (SL)	Action	I1	I2	I3
20. L55. 1.	20. Logical Access Control	55. Workstation Time-out/Password Protected Screen Savers	1. Unattended workstations should be protected against an unauthorised person taking the opportunity to use the workstation	XYZ-Correspondent PCs	There is no Audit process Implemented	2- Implemented	6	3 - Audited	-1	Audit	9	3	2
80. P170.1.	80. Protection Against Malicious Software	170. Prevention Against Malicious Software	1. The potential for the introduction of malicious software into the IT system should be minimised	XYZ-Correspondent PCs	There is no Audit process Implemented	2- Implemented	6	4 - Audited	-1	Audit	8	3	1
80. P175.1.	80. Protection Against Malicious Software	175. Detection of Malicious Software	1. The system should be monitored for potential malicious software activity	XYZ-Correspondent PCs	There is no Audit process Implemented	2- Implemented	6	5 - Audited	-1	Audit	8	3	1
80. P180.1.	80. Protection Against Malicious Software	180. Removal of Malicious Software	1. Any malicious software should be identified, isolated, and removed	XYZ-Correspondent PCs	There is no Audit process Implemented	2- Implemented	6	6 - Audited	-1	Audit	8	3	1
430. 640.4.	430. Site / Building Physical Security	640. Perimeter of the Site	The site should be surrounded by a security barrier that is designed to deter and delay a resourceful attacker	XYZ Location XXX Building	There is no Audit process Implemented	2- Implemented	6	3-Audited	-1	Audit	7	1	1
500. 720.1.	500. Bomb Detection	720. Bomb Alarms	Staff should be made aware of the actions they must take during a bomb warning	XYZ Location XXX Building	There is no Audit process Implemented	2- Implemented	6	3-Audited	-1	Audit	6	2	1
500. 725.1.	500. Bomb Detection	725. Bomb Identification procedures	Staff should be able to recognise a suspect device and take appropriate action	XYZ Location XXX Building	There is no Audit process Implemented	2- Implemented	6	3-Audited	-1	Audit	6	2	1
500. 725.2.	500. Bomb Detection	725. Bomb Identification procedures	The procedures for the detection of suspect devices should be tested	XYZ Location XXX Building	There is no Audit process Implemented	2- Implemented	6	3-Audited	-1	Audit	6	2	1
510. 730.1.	510. Internal and External Bomb Protection	730. Site Layout	The site should have a defined security perimeter	XYZ Location XXX Building	There is no Audit process Implemented	2-Implemented	6	3-Audited	-1	Audit	7	1	1
510. 735.1.	510. Internal and External Bomb Protection	735. Site Layout Procedures	Potential vulnerable points in the site or building should be identified	XYZ Location XXX Building	There is no Audit process Implemented	2-Implemented	6	3-Audited	-1	Audit	7	1	1

Based on this Gap analysis, we know the specific problems that we need to address:

In consequence the ISO 1799 sections that have to be audited based on this gap analysis are:

1. **ISO 17799 Control 6.2.1**: "*Information security education and training*"
2. **ISO 17799 Control 7.1.1**: "*Physical security perimeter*"
3. **ISO 17799 Control 8.3.1**: "*Controls against malicious software*"
4. **ISO 17799 Control 9.3.2**: "*Unattended user equipment*"

These are the audit checklists defined for each of the ISO 17799 sections identified before:

1) Audit Checklist for ISO 17799 Control 6.2.1; **"*Information security education and training*"**

Control Objective: To inform and train XYZ employees and partners when necessary, about how to follow and understand XYZ Security policies, standards, guidelines and procedures.

Reason to Audit the control: There are risks level 6 that are mitigated by this control.

Where to Audit: XYZ Employees and partners where necessary

Frequency: Once a month

Audit Test Description: Corporate Security Team will implement two audit processes for this control:

- Implementation Level Audit:
  - HHRR department will be required to supply the list of employees who have received the Security awareness training last month.
  - A random sample of these employees will be phoned by security team to ask for feedback about the course:
    - If the course meet their expectations
    - If the course is relevant for them
    - If they have learned something
    - If Security become different after receiving the course
    - What they propose to **improve** the course
  - Security Department will keep an updated list of the employees who have received the course, when they have received the course and course version.
- Efficacy Level Audit:
  - A random sample of XYZ employees (independent of having received the course or not) will be required to fill an anonymous web based survey to check the real security awareness level of XYZ employees with question related to the most critical risk identified.
  - These are some questions that must be done:
    - ¿Do you know what to do in case of an Evacuation alarm? Have you tested it anytime?
    - If you receive a package, and you don't know who is the package from. What do you do?
    - Do you know criteria to recognize a suspect device?
    - If you are connected to XYZ from a hotel lobby, if you have to leave for a minute, what do you do?

- It is very important to introduce some dummy questions to confuse the interviewed person in order not to have obvious answers.

2) Audit Checklist for ISO 17799 Control 7.1.1: "*Physical security perimeter*"

Control Objective: To deter and delay a resourceful attacker.

.

Reason to Audit the control: There are risks level 6 that are mitigated by this control.

Where to Audit: XYZ Locations.

Frequency: Twice a year

Audit Test Description: Corporate Security Team will implement two audit processes for this control:

- Implementation Level Audit:
  - Corporate Audit Team will visit the locations **without prior notice** to check the implementation level of the specific security perimeter controls implemented:
    - If the security Perimeter is defined
    - if the site is surrounded by a security barrier in the whole security perimeter
    - If there are potential vulnerable points not detected before.
    - If the entrances to the location are monitored
    - If there is any dark spot
    - Check the current state of the walls and fences.
    - Check if the Guards are actually monitoring
    - Ask for the Security room "Event Sheet" to guaranty that is updated.
    - Check the current state of the CCTV system
  - Corporate Audit Team in the same visit will study the physical security implemented in the location in order to look for possible **improvements**:
    - If it is possible, how to reduce the number of entrances?
    - How to improve the lighting in the security perimeter?
    - How many guards are necessary?
    - Verify the commercial Guard company reputation?
- Efficacy Level Audit:
  - Corporate Audit Department will contract external security Service to check the real efficacy of physical security controls.
    - Using different techniques (such us social engineering) an outsider not authorized will try to get in a specific XYZ location.

- It is very important to be careful with this audit process, because there are some potential dangers. That is why it is very important to contract an external trusted security professional company to do this. In other words: It is a physical penetration test.

3) Audit Checklist for ISO 17799 Control 8.3.1: "*Controls against malicious software*"

Control Objective: To protect XYZ equipment from malicious software
.
Reason to Audit the control: There are risks level 6 that are mitigated by this control.

Where to Audit: XYZ equipments.

Frequency: Once a week

Audit Test Description: Corporate Security Team will implement two audit processes for this control:

- Implementation Level Audit:
  - Corporate Audit Team will have access to a Security Console in XXX Corporate Security Department to check online the current state related to engine and virus pattern of the antivirus software installed in the XYZ PCs paying special attention to XYZ Correspondent-PCs.
  - Implement a continuous audit process to check the current state of the antivirus software in XYZ-Correspondent PCs inventory.
  - All equipments, whose current state information is not updated, through the help desk department, contact the user and the PC administration team to check the current antivirus state and causes of not having the updated information and take the appropriate decisions.
  - Corporate Audit Team will study possible improvements to the security controls implemented:
    - How to improve the current capacity of detection, response, correction and eradication of the malicious software?
    - What about implement an internal IPS solution?
    - What about implement two malicious software control vendors?
- Efficacy Level Audit:
  - Corporate Audit Department, every time there is a high level virus Threat, will track the impact of the virus in XXX and XYZ, with information like these:
    - If the virus impacted any system in XXX or XYZ.
    - If yes, how many?
    - How much time it was necessary to mitigate the virus?

- There were any re-infections? And Why?

4) Audit Checklist for ISO 17799 Control 9.3.2: "*Unattended user equipment*"

Control Objective: To protect XYZ equipment from unauthorized access
.
Reason to Audit the control: There are risks level 6 that are mitigated by this control.

Where to Audit: XYZ equipments.

Frequency: Once a week

Audit Test Description: Corporate Security Team will implement two audit processes for this control:

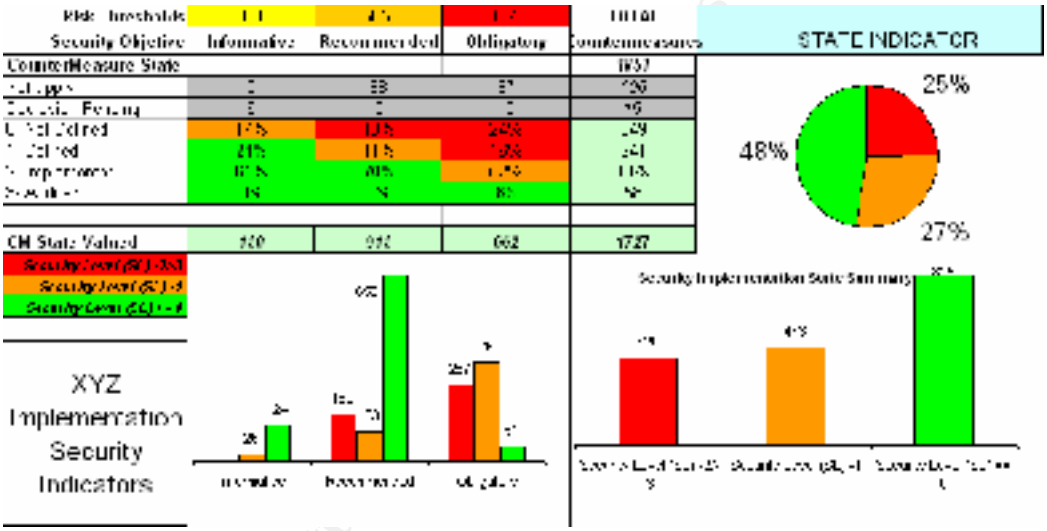
- Implementation Level Audit:
  - Corporate Audit Team will have access to XYZ Active Directory Console to check online the current state of this AD policy in XYZ PCs paying special attention to XYZ Correspondent-PCs.
  - Implement a continuous audit process to check the current state of the automatic timeout session lock in XYZ-Correspondent PCs inventory.
  - All equipments, whose last month information is not updated, through the help desk department, contact the user and the PC administration team to check the current timeout session lock state and causes of not having the updated information and take the appropriate decisions.
  - Corporate Audit Team will study possible **improvements** to the security controls implemented:
    - Strong authentication based on a smartcard (XXX/XYZ Corporate Badge) and automatic lock when release de card?
    - What about installing a host IPS in XYZ-Correspondent PCs to detect suspicious activity?
    - What about creating a log that correlates the XYZ-Correspondent PC idle time with the session timeframes?
- Efficacy Level Audit:
  - Corporate Audit Department will contract external security Service to check the real efficacy of this control
    - An external security auditor will check without previous notice in XYZ Locations if there are equipments unattended with the session open.

It is very important to realize that audit process is not only valid to check if security controls are correctly implemented; it is the best process to investigate and innovate to improve the security controls current implemented. In all of the checklists detailed, there are activities more focused on the ISMS improvement than simple testing the security controls implemented.

Part Five: Act

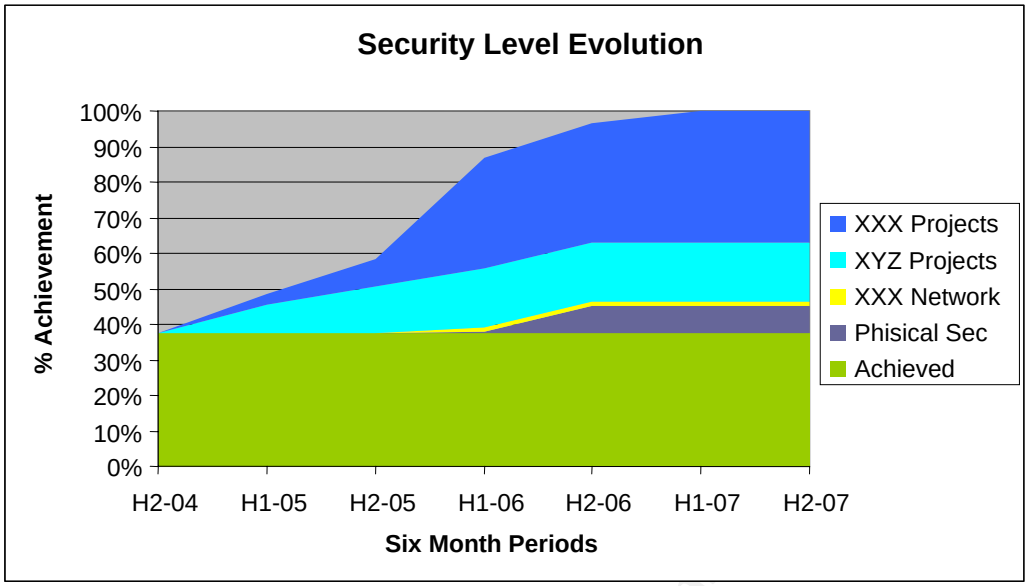
It is very important to remark that this ISMS that has been developed has to be managed day by day. The implementation control process has been planned for 3 years from the start date, this is too much time and it is very easy to lose one's bearing. **These are some tools that have been designed and implemented to help the security organization to maintain the ISMS**.

In the next figure it is an example of a Security Implementation Scorecard, very useful to check graphically XYZ ISMS state related to the controls that have been implemented and audited. As you can see these are some security indicators that can give CISO and XYZ ISO measures of the real XYZ security level:



In this moment, XYZ has 46% of countermeasures the security objective is fulfilled, 28% are near to security objective and 26% are far from security objective. As you can see, in this moment, XYZ was working in implementing countermeasure projects more than auditing.

This is other graphical tool that permits to see how XYZ ISMS is following the security controls implementation planning:



In this graph you can see that XYZ has planned to achieve the Security Level Objective by second half 2007, but it is very important to remark that this security level objective is not static. Security is always changing, new threats will appear, XYZ business is continually changing, and so on the security scenarios. That's the reason why conclusions from the risk analysis done in the ISMS plan activity will expire.

In order to improve the ISMS, XYZ has defined and implemented a **continuous risk management process** that will improve the ISMS defined to the concept of adaptive security to the changing security environment explained before.

The main activities of this continuous risk management process that will evolve the XYZ ISMS are:

- Design, implementation and management of a Security Scorecard as principal tool to administrate the security of XYZ.
- Design and implementation of a Communication Plan to include the security projects advances to all the stakeholders
- Every 6 months, Corporate Security Team will coordinate a differential risk analysis process related to information assets scope of the ISMS to check the validity of the previous conclusions. It is not to begin a new complete risk analysis, but to review the risk analysis done before, to check for changes in threats, vulnerabilities or impacts. In the first reviews, there will be more changes, accordingly with XYZ maturity level related to risk management.
- Every 6 months after reviewing the risk analysis conclusions, there will be also a review of the security operational plans defined before, and, in consequence, there will be changes in the security projects where needed.

- In these revisions security team will study new possible technologies based on the security state of the art, to check other possible countermeasures for the risk identified.

Other sources for improvements are conclusions from **Auditing Process** as explained before in this document. Auditing process has to be focused not only on looking for countermeasures fails (reactive way), but also looking for security possible improvements (proactive way). In last section (Check activity from the PDCA model) every audit checklist has definitions about how to improve a specific security control.

In each auditing checklist, there are two auditing process. Generally, one auditing process is **internal**, coordinated and developed by Corporate Security Team, but in many cases there is another auditing process for the same countermeasure, normally this second process is conducted **externally** with the main objective to complement the conclusions from the first auditing process. The first auditing process will focus on checking if the countermeasure is correctly implemented; and the second auditing process will focus on checking if the countermeasure is really effective.

Now we have two ways to improve, based on the continuous risk management process and auditing conclusions and suggestions. But there is another way, that well conducted can be very useful to learn, I am referring to Security Incidents.

Security Staff hate Incidents; I think this is because there is a bad fallacy that says that Security Staff is paid not to have incidents in their company. That is not true. This is the same than trying to implement a 100% secure system; that is not possible. Security Incidents always can happen, and it is very important to manage this expectation with management. **The difference is how the security incident is managed** and **to learn** from the incident.

In previous sections of this document, a Security Operation Plan related to Incident management was defined and implemented. Incident Management has to be prepared from the beginning, from the threat analysis, and implement the required processes to detect, contain, repair and react from a security Incident. Concerning to this section, the **react** activity process, after the incident has been controlled, require the security team to:

- Study the whole incident: Threat that provokes the incident, vulnerability that was exploited, and Impact caused by the incident.
- Check if the Threat and the Vulnerability was studied and appropriate assessed in the risk management process; if not, review the threat analysis concerning to this Threat.
- Check if the Impact caused by the Incident was appropriate assessed in the risk management process; if not, review the Business Impact analysis concerning to this Impact.
- Check if preventative security controls implemented could protect from this incident; if yes, study why they haven't work.

- Check if corrective security controls implemented have worked appropriately; if not, study why.
- Perform a differential risk analysis taking the new information and formalize a new risk management decision.
- Based on the risk management decision, Implement the corrective changes needed to adapt the Security Operational Plans that are affected.
- Communicate and Train to learn from the incident, in order to minimize the probability of next occurrence, paying special attention in what has been improved related with the incident.

Appendix I: IT Dependencies Inventory

This is not the real inventory of XYZ. For confidentiality reasons, data has been mixed and changed.

IT Elements		Location				Classification		
Identification	Qty	BU	Centre	Building	Room	Class 1	Class 2	Class 3
XYZ-Intranet Server	1	XYZ		Building X	CPD	HOST	Application Server	
						HOST	Database Server	
						HOST	Application Server	
						Storage Device	Magnetic Disk Device	
XYZ-HMXYZ Server	1	XYZ	Location A	Building Y	CPD	HOST	Magnetic Disk Device	
						HOST	Application Server	
XYZ-User PCs	100	XYZ			Offices	WORKSTATION	Fixed Location Intelligent Workstation	
XYZ-Correspondent PCs	20	XYZ				WORKSTATION	Fixed Location Intelligent Workstation	
XYZ-VIP Users PCs	5	XYZ				WORKSTATION	Portable	
						EXTERNAL NETWORK SERVICE	DATA	ADSL
XYZ-SAXYZ Server	1	XYZ	Location A	Building Y	CPD	HOST	File Server	
						HOST	File Server	
						HOST	Database Server	
XYZ-CiXYZ Server	1	XYZ	Location A	Building Y	CPD	HOST	Database Server	
						HOST	Application Server	
						HOST	File Server	
						COMMUNICATION PROTOCOL	HIGH LEVEL COMMUNICATION PROTOCOL	FTP
XYZ-DB Agency Server	1	XYZ	Location A	Building Y	CPD	Storage Device	Magnetic Disk Device	
XYZ-Receiver Text News Agency		XYZ	Location A	Building Y	CPD	HOST	Database Server	
XYZ-SAN		XYZ	Location A	Building Y	CPD	HOST	Multiplexer	
						NETWORK COMPONENT	Multiplexer	
XYZ-PPXYZ Server		XYZ	Location A	Building Y	CPD	HOST	Application Server	
						HOST	Application Server	
						COMMUNICATION PROTOCOL	HIGH LEVEL COMMUNICATION PROTOCOL	FTP
						COMMUNICATION PROTOCOL	HIGH LEVEL COMMUNICATION	http

IT Elements		Location				Classification		
Identification	Qty	BU	Centre	Building	Room	Class 1	Class 2	Class 3
							PROTOCOL	
XYZ-DB Correspondent Server		XYZ	Location A	Building Y	CPD	HOST	Application Server	
XYZ-Correspondent Server		XYZ	Location A	Building Y	CPD	HOST	Application Server	
						HOST	Application Server	
						COMMUNICATION PROTOCOL	HIGH LEVEL COMMUNICATION PROTOCOL	HTTP
XYZ-SPXYZ Server		XYZ	Location A	Building Y	CPD	HOST	Database Server	
						HOST	File Server	
						HOST	File Server	
						COMMUNICATION PROTOCOL	HIGH LEVEL COMMUNICATION PROTOCOL	HTTP
XYZ-PAXYZ Server	>40	XYZ	Location A	Building Z	xxxxxx	HOST	Database Server	
						HOST	Application Server	
						HOST	File Server	
						COMMUNICATION PROTOCOL	HIGH LEVEL COMMUNICATION PROTOCOL	HTTP
						COMMUNICATION PROTOCOL	HIGH LEVEL COMMUNICATION PROTOCOL	FTP
XYZ-External Agency Server		XYZ	Location A	Building Y	CPD	HOST	Application Server	
						COMMUNICATION PROTOCOL	HIGH LEVEL COMMUNICATION PROTOCOL	HTTP
XYZ-HCXYZ Server		XYZ	Location A	Building Y	CPD	HOST	Database Server	
						HOST	Application Server	
						HOST	File Server	
XYZ-PEXYZ Server		XYZ	Location A	Building Y	CPD	HOST	Application Server	
						COMMUNICATION PROTOCOL	HIGH LEVEL COMMUNICATION PROTOCOL	HTTP
XYZ-RAS Dial Up	1	XYZ	Location A	Building Y	CPD	NETWORK COMPONENT	Router	
						EXTERNAL NETWORK SERVICE	DATA	Dial-up
XYZ- Network XYZ.net	1	XYZ	Location A	Generic Building		NETWORK COMPONENT	Layer 3 Switch	
						NETWORK CABLING	UTP	
						COMMUNICATION PROTOCOL	LOW LEVEL COMMUNICATION PROTOCOL	TCP/IP

IT Elements		Location				Classification		
Identification	Qty	BU	Centre	Building	Room	Class 1	Class 2	Class 3
						COMMUNICATION PROTOCOL	LOW LEVEL COMMUNICATION PROTOCOL	FTP
XYZ-DMZ Network XYZ.net	1	XYZ				NETWORK COMPONENT	Layer 3 Switch	
						NETWORK COMPONENT	Firewall/Security Gateway	
						EXTERNAL NETWORK SERVICE	DATA	Internet
						NETWORK MANAGEMENT	TTP/CA/PKI Management System	

Appendix II: Security Impact Scenarios

	Information not available
15mn	Less than 15mn
1h	Less than 1hour
3h	Less than 3 hours
12h	Less than 12 hours
1d	Less than 1 whole day
2d	Less than 2 days
1s	Less than 1 week
2s	Less than 2 weeks
1m	Less than 1 month
2m	Less than 2 months
	Information Destruction
dp	Partial lost from last backup
dt	Total lost from last backup
	Information revelation
DI	To non authorized XXX Employees
DCSP	To non authorized XXX Subcontracted People
DO	To non authorized Outsider
	Information Modification
SE	Precise or accidental entrance error, keyboard, etc.
WE	generalized error in the whole information due to, for example, to a failure in the programming
DM	deliberate error due to a malicious intend
	Inappropriate information exchange
IN	False messages insertion, such as inadequate request
RO	Origin Repudiation: rejected message by whom it sent it
RC	Destiny Repudiation: Receiver denies it to have received
ND	No Delivery: a request does not arrive at its destiny in accidental or deliberate form
Rp	Request duplication
Mr	Wrong Receiver
TM	Traffic Monitoring: one knows volume and interlocutors without knowing the content
OS	Wrong order in the processes

Appendix III: Threats Table

COD	APLI	Threads
AL1	YES	Masquerading of User Identity by Insiders
AL2	YES	Masquerading of U. Identity by Contracted Service Providers
AL3	YES	Masquerading of User Identity by Outsiders
AL4	YES	No authorized use of an application
AL5	YES	Embedding of Malicious Code
AL6	YES	Misuse of System Resources
AC1	YES	Communications Infiltration
AC2	YES	Communications Interception
AC3	YES	Communications Manipulation
AC4	YES	Repudiation
AC5	YES	Communications Failure
AC6	YES	Introduction of Damaging or Disruptive Software
AC7	YES	Wrong delivery
AFT1	YES	Technical Failure of Host
AFT3	YES	Technical Failure of Storage Facility
AFT4	YES	Printing failure
AFT2	YES	Technical Failure of Network Gateway
AFT5	YES	Technical Failure of Network Distribution Component
AFT6	YES	Network management failure
AFT7	YES	Network interface failure
AFT8	YES	Technical Failure of Network Service
AFT9	YES	Power Failure
AFT10	YES	Air Conditioning Failure
AFT11	YES	System and Network Software Failure
AFT12	YES	Application Software Failure
AEH1	YES	Operations Error
AEH2	YES	Hardware Maintenance Error
AEH3	YES	Software Maintenance Error
AEH4	YES	User Error
AF1	YES	Fire
AF2	YES	Water Damage
AF3	YES	Natural Disaster
AF4	YES	Staff Shortage
AF5	YES	Theft by Insiders
AF6	YES	Theft by Outsiders
AF7	YES	Willful Damage by Insiders
AF8	YES	Willful Damage by Outsiders
AF9	YES	Terrorism

Appendix IV: 6 Impact analysis scales

	Scale 1	Scale 2	Scale 3
	Personal Information	Legal Liabilities	Economic and Commercial Interests
1	To cause slight nuisances to a person but without failing to fulfill the legality		Of interest for a competitor, but without commercial value
2	To cause uneasiness to a person but without failing to fulfill the legality	Crime or fault with a fine of 3.000€ or less	It can suppose a number of business of 15.000€ or less to a competitor
3	Failure to comply with Data Protection Legislation and to cause slight nuisances to someone	Crime or fault with a fine between 3.001€ and 15.000€	It can suppose a number o business between 15.001€ and 150.000€ to a competitor
4	Failure to comply with Data Protection Legislation and to cause slight nuisances to a group of people	Crime or fault with a fine between 15.001€ and 75.000€, or with a sentence to prison up to 2 years	It can suppose a number of business between 150.001€ and 1.500.000€ to a competitor
5	Failure to comply with Data Protection Legislation and to cause major nuisances to someone	Crime or fault with a fine between 75.001€ and 375.000€, or with a sentence to prison between 2 years and up to 10 years	It can suppose a number of business between 1.500.001€ and 15.000.000€ to a competitor
6	Failure to comply with Data Protection Legislation and to cause major nuisances to a group of people	Crime or fault with a fine of more than 375.000€ or a sentence to prison of more than 10 years	It can suppose a number of business of more than 15.000.000€
7			It could caused a considerable damage to national economy and commercial interests
8			
9			Probably it could caused a considerable damage to national economy and commercial interests
10			Probably it would damage the national economy in a lasting and harshly way

	Scale 4	Scale 5	Scale 6
	Financial Losses	Image Losses	Business Management and Activities
1	Direct o indirect losses of 1.500€ or less		Inefficient working of one part of the company
2	Direct or indirect losses between 1.501€ and 15.000€	It affects negatively the relationships with other company's parts	
3	Direct or indirect losses between 15.001€ and 45.000€	It affects negatively the relationships with other companies or with general public, but the negative publicity is reduced to a nearer geographical environment and without lasting effects	To damage the company suitable management and its operations
4	Direct or indirect losses between 45.001€ and 150.000€		
5	Direct or indirect losses between 150.001€ and 450.000€	It affects negatively the relationships with other companies or with general public, and the negative publicity expands beyond the nearer geographical environment	To prevent the development or effective implementation of the company's policies
6	Direct or indirect losses between 450.001€ and 1.500.000€		It puts the company at disadvantage in negotiations with third parties in policies and commercial issues
7	Indirect losses of more than 1.500.000€	It affects in a very significant way the relationships with other companies or with the general public, involving a negative publicity with great repercussion	To obstruct the deployment or implementation of the most important company's policies or to cause the closure or the interruption of the most important operations in a substantial way
8	Indirect losses of more than 1.500.000€		
9			
10			

Appendix V: Threats groups & IT Dependency groups

IT Dependencies Groups	Threat Group that applies	Threat Group that applies
XYZ-Correspondent PCs	XYZ Mobile PC	
XYZ-User PCs	GE Fixed PC	
XYZ-VIP Users PCs	GE Mobile PC	XYZ ADSL PC
XYZ-RAS Dial Up	XYZ RAS	
XYZ-Receiver Text News Agency	GE 200x Servers	XYZ Agency Receptor
XYZ-DMZ Network XYZ.net	GE Own Network	GE Exposed Network
XYZ-Internal Network XYZ.net	GE Own Network	GE Local Network
XYZ-SAN	XYZ SAN	
XYZ-DB Correspondent Server	GE 200x Servers	
XYZ-DB Agency Server	GE 200x Servers	
XYZ-Correspondent Server	GE 200x Servers	
XYZ-CiXYZ Server	GE 200x Servers	
XYZ-HCXYZ Server	GE 200x Servers	
XYZ-HMXYZ Server	GE 200x Servers	
XYZ-External Agency Server	GE 200x Servers	
XYZ-Internal Agency Server	GE 200x Servers	
XYZ-Intranet Server	GE 200x Servers	
XYZ-PEXYZ Server	GE 200x Servers	
XYZ-PPXYZ Server	GE 200x Servers	
XYZ-SAXYZ Server	GE 200x Servers	
XYZ-SPXYZ Server	GE 200x Servers	
XYZ-PAXYZ Server	GE NT Servers	
Locations		
Centers		
XYZ-Location A	GE Buildings	
XYZ-Other Locations	GE Buildings	
Buildings		
XYZ-Building X	GE Buildings	
XYZ-Building Y	GE Buildings	
XYZ-Building Z	GE Buildings	
Rooms		
XYZ- Offices	GE Office	GE electricity
XYZ- CPD	GE CPD Room	XYZ- Electricity Location A
XYZ- Other CPDs	GE CPD Room	XYZ- Electricity Other Loc.
XYZ-Room PA	GE CPD Room	GE electricity

Appendix VI: Threat analysis Results

For confidentiality reasons, it is not possible to include the complete thread analysis. This an example of the thread analysis result referred to Generic Threats that apply to a Windows 2003 Server:

			Unavailability														Destr.		Revelation				Modification			Incorrect Interchange									
			U15		U1H		U3H		U12		U1D		U2D		U1W		U2W		U1M		U2M		DP		DT		DI		DCS		DO		SE		WE		DM		In		RO		RC		Nd		Rp		Mr		TM		OS	
Cod	Group	Threat	T	V	T	V	T	V	T	V	T	V	T	V	T	V	T	V	T	V	T	V	T	V	T	V	T	V	T	V	T	V	T	V	T	V	T	V	T	V	T	V	T	V	T	V	T	V	T	V	T	V
AFT10	GE 200x Servers	Air Conditioning Failure	2	3	2	3	2	3															2	2																														
AL5	GE 200x Servers	Embedding of Malicious Code	5	2	5	2	4	2	2	1													5	2							3	1	1	1	1	2			3	1					3	1			1	1			
AEH3	GE 200x Servers	Error mantenimiento software	4	2	4	2	3	2	1	2													2	2																														
AEH2	GE 200x Servers	Hardware Maintenance Error	3	2	2	2	2	2	2	2	1	1	1	1	1	1							2	2			2	1			4	1																				
AL6	GE 200x Servers	Misuse of System Resources	5	1	3	1																	3	1																														
AEH1	GE 200x Servers	Operations Error	4	2	4	2	3	2	1	2													1	1			1	1	1	1	1	1	1	1	1	1																
AF4	GE 200x Servers	Staff Shortage	3	2	3	2																																															
AFT11	GE 200x Servers	System and Network Software Failure	4	3	4	2	4	2															2	1							4	2																				
AFT1	GE 200x Servers	Technical Failure of Host	3	3	3	2	2	2	2	2	2	2	1	1									2	2																														

Appendix VII: Level 5 & Level 6 Risk identified

For confidentiality reasons, it is not possible to include the XYZ real risk analysis. This is an example of risk analysis results:

Threat Description	IT Elements Group	Impact Description	Threat	Vuln.	Imp.	Risk
Threat: Wilful Damage by Outsiders	GE Buildings	*Unavailability - 1 day*	VH	M	7	6
Threat: Communications Infiltration	GE Exposed Network	*Unauthorised disclosure to outsiders*	VH	H	7	6
Threat: Communications Interception	GE Exposed Network	*Unauthorised disclosure to outsiders*	VH	H	7	6
Threat: Communications Manipulation	GE Exposed Network	*Unauthorised disclosure to outsiders*	VH	H	7	6
Threat: Embedding of Malicious Code	GE Exposed Network	*Unauthorised disclosure to outsiders*	VH	H	7	6
Threat: Communications Interception	GE Exposed Network	*Non-delivery*	H	H	7	6
Threat: Communications Failure	GE Exposed Network	*Non-delivery*	H	H	7	6
Threat: Terrorism	GE Buildings	*Unavailability - 2 days*	VH	M	7	6
Threat: Masquerading of User Identity by Outsiders	GE External Access Services	*Unauthorised disclosure to outsiders*	VH	M	7	6
Threat: Communications Infiltration	GE External Access Services	*Unauthorised disclosure to outsiders*	VH	M	7	6
Threat: Communications Interception	GE External Access Services	*Unauthorised disclosure to outsiders*	VH	M	7	6
Threat: Communications Failure	GE External Access Services	*Non-delivery*	H	H	7	6
Threat: Introduction of Damaging or Disruptive Software	GE Mobile PC	*Unavailability - 12 hours*	VH	M	7	6
Threat: Introduction of Damaging or Disruptive Software	XYZ Mobile PC	*Unavailability - 1 week*	VH	M	7	6
Threat: Misuse of System Resources	XYZ Mobile PC	*Unavailability - 1 week*	VH	M	7	6
Threat: Fire	GE CPD Room	*Unavailability - 1 month*	VL	H	5	5
Threat: Hardware Maintenance Error	GE 200x Servers	*Unauthorised disclosure to outsiders*	H	L	5	5
Threat: User Error	GE Assets	*Unauthorised disclosure to outsiders*	H	L	5	5
Threat: Communications Infiltration	GE External Access Services	*Unavailability - 12 hours*	H	M	5	5
Threat: Technical Failure of Network Distribution Compone	GE Own Network	*Unavailability - 12 hours*	M	M	5	5
Threat: System and Network Software Failure	GE Own Network	*Non-delivery*	M	M	5	5
Threat: Theft by Outsiders	GE Mobile PC	*Unavailability - 12 hours*	M	H	5	5
Threat: Theft by Outsiders	GE Mobile PC	*Unavailability - 1 day*	M	H	5	5
Threat: Theft by Outsiders	GE Mobile PC	*Unavailability - 2 days*	M	H	5	5
Threat: Theft by Outsiders	GE Buildings	*Unavailability - 12 hours*	M	H	5	5
Threat: Theft by Outsiders	GE Buildings	*Unavailability - 1 day*	M	H	5	5
Threat: Communications Infiltration	GE External Access Services	*Unavailability - 1 day*	M	M	5	5
Threat: Application Software Failure	XYZ HCXYZ SW	*Unavailability - 12 hours*	M	M	5	5
Threat: Theft by Outsiders	XYZ Mobile PC	*Unavailability - 1 day*	M	H	5	5
Threat: Theft by Outsiders	XYZ Mobile PC	*Total destruction including back-ups*	M	H	5	5
Threat: Embedding of Malicious Code	GE External Access Services	*Unauthorised disclosure to outsiders*	VH	L	5	5
Threat: Communications Interception	GE Exposed Network	*Unavailability - 1 hour*	H	H	5	5
Threat: Communications Interception	GE Exposed Network	*Unavailability - 3 hours*	H	H	5	5

Appendix VIII: References

- Track 11 – SANS 17799 Security & Audit Framework. Course Material. SANS Institute
- CISSP All in One Certification Exam Guide. Shon Harris.
- CRAMM Version 5. http://www.cramm.com from Insight Consulting
- ISO/IEC TR 13335-1 Information Technology: Guidelines for the management of IT Security. Part1: concepts and models for IT Security
- ISO/IEC TR 13335-2 Information Technology: Guidelines for the management of IT Security. Part2: Managing and Planning IT Security
- ISO/IEC TR 13335-3 Information Technology: Guidelines for the management of IT Security. Part3: Techniques for the management of IT Security
- ISO/IEC 17799. Information technology — Code of practice for information security management