Global Information Assurance Certification Paper

ISO 1799 ISMS for a Request Tracker System

GIAC Certified ISO-17799 Specialist (G7799)

Practical Assignment

Version 1.1

Luis Moreno
SANS Track 11 /
Monterey July 2004

Table of Contents

List of Figures

List of Tables

Abstract

Xnet is a nationwide Internet Service Provider (ISP). With more than 10 years of operation and evolution, it has now become one of the major Internet Service Providers (ISP) in Venezuela. Xnet offers different kinds of access for its clients to the Internet, for example, via Dial-Up, xDSL (broadband), Dedicated Leased Line access (frame relay links), Web, Database and Application Hosting Services, and other added value services like: content, games, personal web pages and email.

Due to the increase of spam email, the Xnet Security Team (secteam) has implemented public and private DNS black listing on the e-mail servers to protect its clients from unsolicited e-mails. As a result, the secteam has to deal with the collateral damage and false-positives caused by the deployment of such lists. Furthermore, the secteam does digital forensic analysis and offers consulting services to secure the deployment of IT projects on the ISP.

In the early days of this department, the requirements and tasks were managed and serviced entirely by email; as a consequence this has raised a few problems within the team referring to task management , and furthermore it presented the team with the inability to report the work being done and the effort hours/dedication from the staff on each task. In response to this, the secteam deployed a tool called RT (from Request Tracker http://www.bestpractical.com/), with the basic premise of minimizing task management problems and fulfilling the team's objectives.

After the RT tool was deployed and up-and-running, there has been a noticeable increase in the effectiveness on requirement's handling, and on reporting the time spent by each team member on daily tasks. The management has identified this system as being critical for the Xnet's security.

As the organization is moving on implementing ISO 1799 best practices on the ISP systems, a work on the RT system assurance based on these practices has been started. Our primary objective here is to develop an ISMS for the RT system, following the PDCA methodology and the 12 steps proposed at "SANS 17799 Security & Audit Framework" course.

Key Words: Information Security, ISMS, ISO 17799, RT.

Document Conventions

When you read this practical assignment, you may find that certain words are represented in different fonts and typefaces to highlight special meanings as follows:

`Command`	Operating system commands are represented in this font style. This style indicates a command that is entered at a command prompt or shell.
`Filename`	Filenames, paths, and directory names are represented in this style.
`computer output`	The results of a command and other computer output are in this style
URL	Web URL's are shown in this style.
Quotation	A citation or quotation from a book or web site is in this style.
[1]	A pointer to a reference located at References section (page 30).

Introduction

This document is oriented for a technical reader with knowledge in computer networks, operating system administration and information security.

The current scope of this work is to show the development of an ISMS for a Request Tracker system (RT) inside an organization called here Xnet. An ISMS is a "l*ife-cycle approach to implementing, maintaining and improving the interrelated set of policies, controls, and procedures that ensure the security of an organization's information assets in a manner appropriate for its strategic objectives*" [1].

This document is structured in five chapters, the first one shows the system to be assured together with the organization that uses the system. The following chapters explain the use of the methodology Plan, Do, Check and Act (PDCA) for develop the ISMS (one chapter per stage).

During the planning stage a risk analysis is conducted for the system, this analysis is the basis for identify policies and control. In the do phase the deployment of such controls is explained. Finally, during the Check and Act stages, measures for system improvement are identified and performed.

The System

RT is a complete open-source issue-tracker system, developed by Best Practical Solutions LLC (http://www.bestpractical.com) since 1996. Best Practical defines RT as "*an enterprise-grade task- and ticket-tracking platform, designed to simplify tracking of issues, user requests and project management in a community of users*" [2].

RT is a platform independent system developed in object-oriented Perl and it takes advantage of code reuse provided by the object-oriented paradigm; it has been made up of a bunch of modules, which are public at a Perl module repository called CPAN located at the web site: http://www.cpan.org/. Furthermore, RT has many of the advantages of an open source system, in which the code is being exposed to a big community of users, therefore it tends to be of a higher quality, for instance, since open source systems are not "black boxes" they have the following features: easier to isolate bugs, scaleable (enables tuning and improvement), and secure (issues are detected and corrected faster).

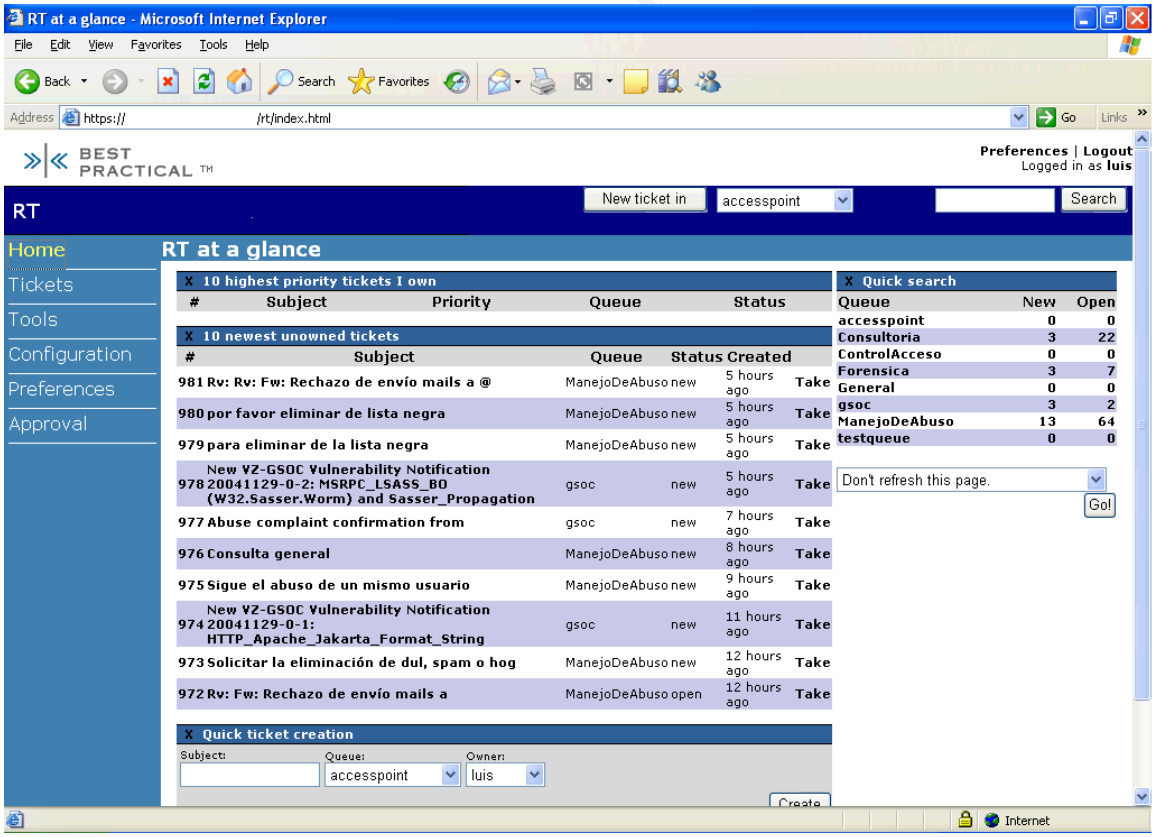


Figure 1 RT at a Glance

As a tool it is designed to improve efficiency in the organization by

improving the way a team receive, troubleshoot and resolve issues reported by a community of users like: clients, customers, partners, and another business units or users in general.

For every issue reported a ticket is created, tickets can be categorized into queues, and every queue has an email address to report an issue. For example, an email sent to the email address security@xnet creates a new ticket for the "information security team" queue.

Before we move ahead, the Xnet organization is introduced.

The Xnet Internet Service Provider

Xnet is a nationwide Internet Service Provider (ISP) with more than 10 years of operation and evolution; it has now become one of the majors ISPs in Venezuela. Xnet offers different kinds of Internet access to their customers via Dial-Up, xDSL (broadband), Leased Line Dedicated access (frame relay links), web, database and application hosting services, and other added value services like: content, games, personal web pages and email. Although the company employees are distributed over various offices dispersed on the same city, the datacenter is centralized on one location.

Xnet has a department that is responsible for Information Security in the organization. This department has the following objective: "To ensure Xnet high availability across all its services by mitigating the risk of loss associated or caused by information security incidents or breaches"[1].

Due to the increase of spam email, the Xnet Security Team (secteam) has implemented public and private DNS black listing on the e-mail servers to protect its clients from unsolicited e-mails. As a result, the secteam has to deal with the collateral damage and false-positives caused by the deployment of such lists. Furthermore, the secteam does digital forensic analysis and offers consultancy services to secure the deployment of IT projects on the ISP.

In the early days of this department, the requirements and tasks were managed and serviced entirely by email; as a consequence this has raised a few problems within the team regarding task management , and furthermore it presented the team with the inability to report the work being done and the hours/dedication effort from the staff on each task. In response to this, the secteam deployed a tool called RT (from Request Tracker http://www.bestpractical.com/) with the basic premise of minimizing task management problems and fulfilling the team's objectives.

[1] Xnet Information Security Deparment's mission statement.

Scope for the ISMS

The scope and primary goal of this paper is to develop an ISMS for the RT system in Xnet Information Security Department. This is going to be done following the PDCA[2] methodology and the 12 steps proposed at "SANS 17799 Security & Audit Framework" course. The hardware and software included in the system scope are: (see Figure 2):

- One front end server and one database backend server, located at the firewall DMZ; running Linux O.S, Apache web server, sendmail and RT3.
- One database backend server, located at the firewall DMZ; running Linux O.S, MySQL Database Management Server.
- One firewall that provides network perimeter security for the company network, running proprietary IOS.
- One switch that connects the servers to the firewall DMZ, running proprietary IOS.

Everything outside of the items listed above is not covered by the RT system ISMS.

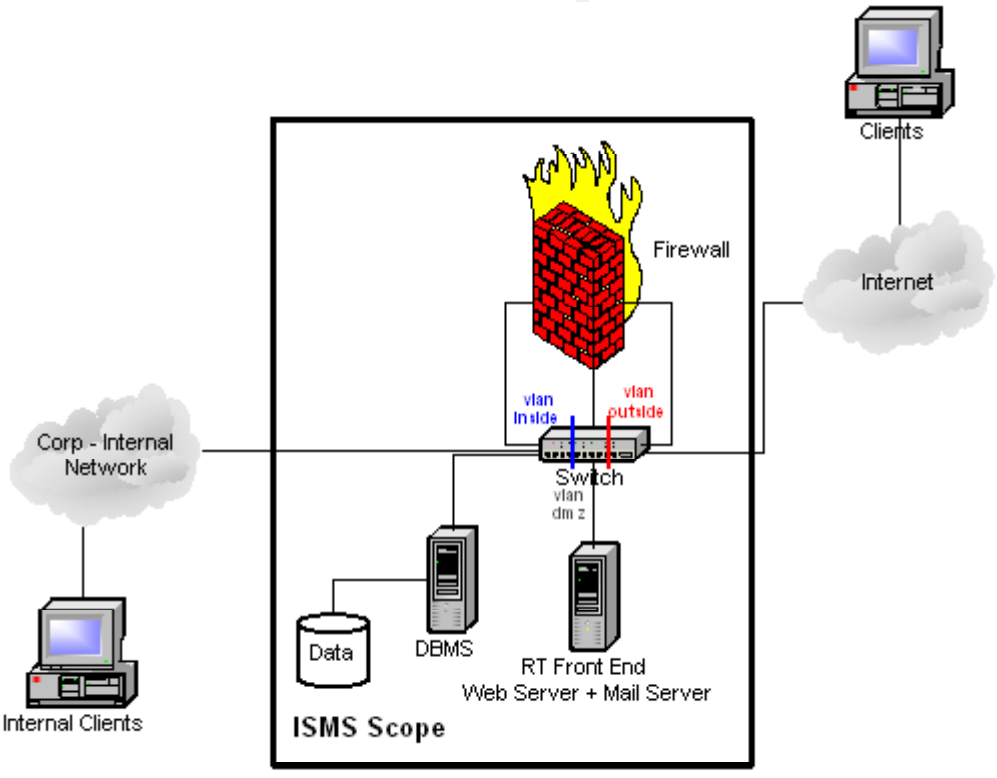


Figure 2 ISMS Scope and the RT System

[2] Also known as "The Deming Cycle", it was proposed by W. Edwards Deming in the 1950's. Mainly focused on business process improvement (BPI), he recommends that business process be placed in a feedback loop, in order to identify and change the components that need improvement [3].

The information assurance managed by this system is of great value to the department. There are several reasons why:

- The system facilitates and improves the communication with customers, business partners and peers, in order to manage complaints and resolve issues in general around information security.
- The information stored by the system is highly sensitive for the company.
- The system improves the department effectiveness; moreover, it is a powerful tool that enables the achieving of department goals.
- It provides statistics of what the department is doing in real time.

Current State of Security

As mentioned earlier in this document, the organization has a department responsible for Information Security. The major responsibilities of this department are:

- Define policies intended to protect the company's information assets.
- Implement the controls specified in the policies.
- Do forensic investigation of information security incidents.
- Manage and control the access to the systems in the organization and
- Offer consultancy to the ISP's new projects that revolve around the security topic and/or ensuring new projects and changes to the infrastructure to abide the security policies defined by the secteam.

The Information Security Officer has written a set of high-level security policies, and a set of controls have been deployed such as: perimeter security, antivirus, IDS and anti-spam systems. Furthermore, access to datacenter facilities is controlled trough a biometric system, although there is no formal revision and maintenance of access control database.

For every new IT project being deployed, the Information Security department has to evaluate the security impact of such project in the current ISP infrastructure; furthermore, the project must comply with a security checklist before going into production.

Xnet has a monitoring system in place to check the current use of systems via SNMP. Even though, a system can be monitored only when both the client (system to be scanned) and the monitoring server (system that performs the scan) have been properly configured. It is not mandatory for production systems to be monitored.

The Xnet organization is not actually looking for the ISO 17799 registration itself. In contrast, the secteam is adopting the standard as a best practice to secure the information assets on the company.

Plan

The plan phase is about to "*Design or revise business process components to improve results"* [3]. In this context and once defined the current baseline, and identified the ISMS objective and scope in the previous chapter, this one shows the steps used to develop the ISMS for the RT System, the process involved, the ISMS Management structure, an outline of the identified policies, and finally the main system risks.

Steps to develop the system.

The process to build the ISMS is motivated by the mitigation of the risk that surrounds the RT system. At a glance, the process will include the identification of assets, the threats and vulnerabilities that could damage those assets, and the associated controls that could mitigate the risk.

Based on that premise and the PDCA methodology steps, the project will be structured in four major phases: Plan, Do, Check and Act. The plan phase includes the ISMS analysis and design, the objective is to determine the current system state in order to find out:

- What processes are involved, which of them are considered critical and can be improved? The processes and its owners must be identified, using techniques like reverse engineering (see "Process Improvement" ahead).

- Who are the stakeholders, and which of them are the ideal candidates for the committees? This item includes the management structure. A selection of key people must be done, because they are going to write the policies for the system.

- Which policies are required for the system? This item includes the identification of required policies. Policies are needed to regulate elements like: physical security, access control, network security, operating system security, change control, password management and business continuity.

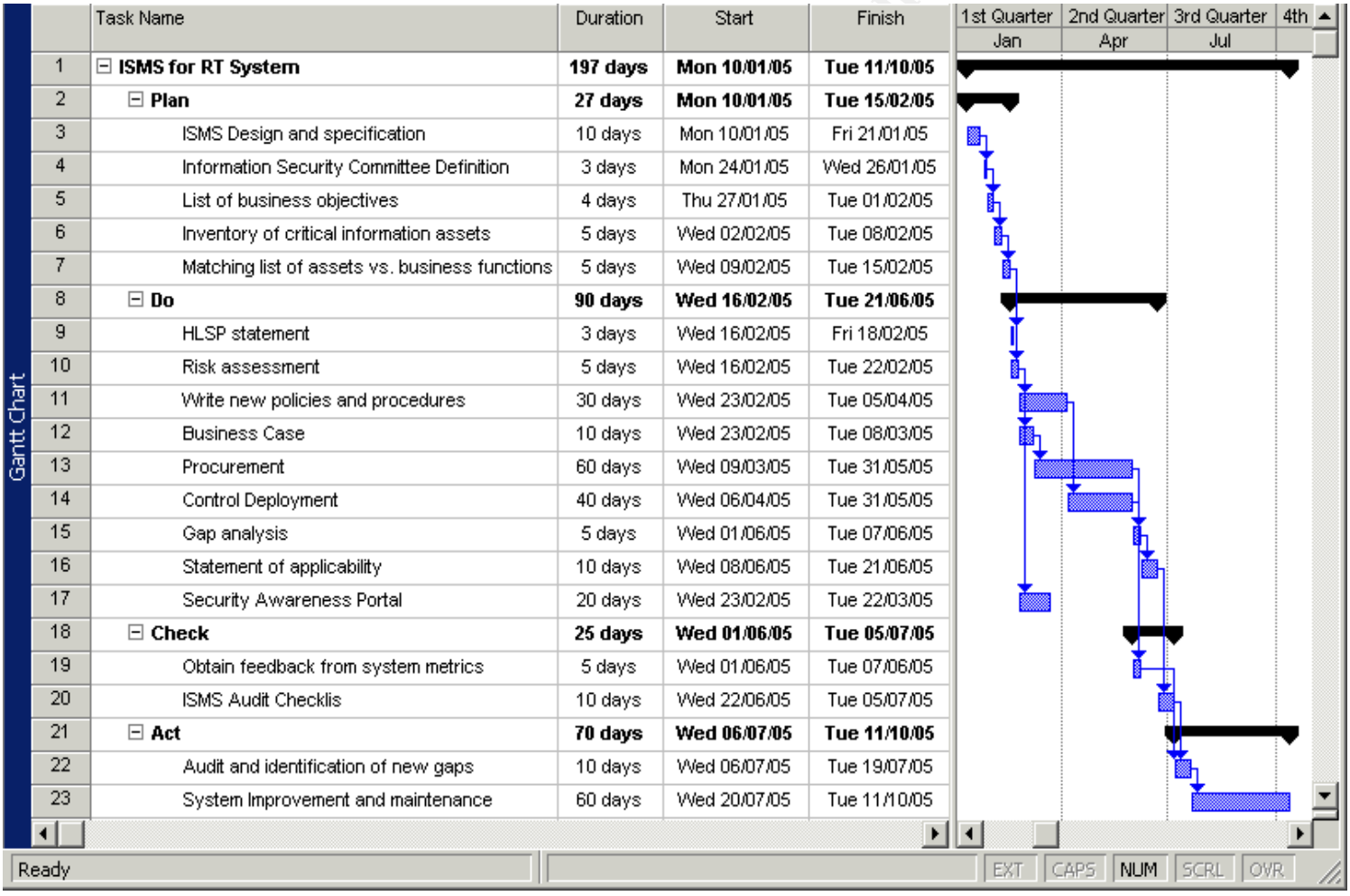
- Which information assets are exposed to which risks and how is the risk going to be managed? This item includes an inventory in order to identify critical assets, the process to identify risks and the plan for risk management. The FMECA risk analysis strategy is chosen because it facilitates the creation of corrective controls to prevent or detect failures, in the second case the application of identified correctives can bring a system back to a normal operation (business continuity).

The do, check and act phase is the system synthesis, and has to do with implementing the risk mitigation strategy and executing the decisions taken during the planning phase.

The do, check and act phases involves among others:

- Implement the identified controls and changes.
- Spread the policies in the organization and Implement security awareness.
- Monitor and correct the deviations present in the system.

Having a brief description of each phase, the project plan is introduced:



	Task Name	Duration	Start	Finish
1	**ISMS for RT System**	**197 days**	**Mon 10/01/05**	**Tue 11/10/05**
2	**Plan**	**27 days**	**Mon 10/01/05**	**Tue 15/02/05**
3	ISMS Design and specification	10 days	Mon 10/01/05	Fri 21/01/05
4	Information Security Committee Definition	3 days	Mon 24/01/05	Wed 26/01/05
5	List of business objectives	4 days	Thu 27/01/05	Tue 01/02/05
6	Inventory of critical information assets	5 days	Wed 02/02/05	Tue 08/02/05
7	Matching list of assets vs. business functions	5 days	Wed 09/02/05	Tue 15/02/05
8	**Do**	**90 days**	**Wed 16/02/05**	**Tue 21/06/05**
9	HLSP statement	3 days	Wed 16/02/05	Fri 18/02/05
10	Risk assessment	5 days	Wed 16/02/05	Tue 22/02/05
11	Write new policies and procedures	30 days	Wed 23/02/05	Tue 05/04/05
12	Business Case	10 days	Wed 23/02/05	Tue 08/03/05
13	Procurement	60 days	Wed 09/03/05	Tue 31/05/05
14	Control Deployment	40 days	Wed 06/04/05	Tue 31/05/05
15	Gap analysis	5 days	Wed 01/06/05	Tue 07/06/05
16	Statement of applicability	10 days	Wed 08/06/05	Tue 21/06/05
17	Security Awareness Portal	20 days	Wed 23/02/05	Tue 22/03/05
18	**Check**	**25 days**	**Wed 01/06/05**	**Tue 05/07/05**
19	Obtain feedback from system metrics	5 days	Wed 01/06/05	Tue 07/06/05
20	ISMS Audit Checklis	10 days	Wed 22/06/05	Tue 05/07/05
21	**Act**	**70 days**	**Wed 06/07/05**	**Tue 11/10/05**
22	Audit and identification of new gaps	10 days	Wed 06/07/05	Tue 19/07/05
23	System Improvement and maintenance	60 days	Wed 20/07/05	Tue 11/10/05

Figure 3 Project Plan

The project should be developed in seven months by a team of three people: one project leader (the Information Security Officer) and two specialists (security team specialist and network operation specialist). In case of capital

investments (i.e. a new server or firewall procurement), a business case must be developed to justify the expenses generated by the project.

Process Improvement

For each process there is a RT queue associated, those processes are:

1. DNS black lists management.
2. Investigation and digital forensic.
3. Access control management.
4. Consultancy to the ISP's new IT projects.

Process improvement involves process change. In the company, the process change is driven in two ways: bottom-up and top-down. In the first way, technicians recognize the Information Security breaches and weakness in the company. This is an easy task for them, because they have to deal every day with new vulnerabilities and threats, for instance Figure 4 shows the number of incidents reported to CERT the last year.

From bottom-up the security specialist propone initiatives of investment to improve the security in the organization, for example adopting 17799 as a code of practice.

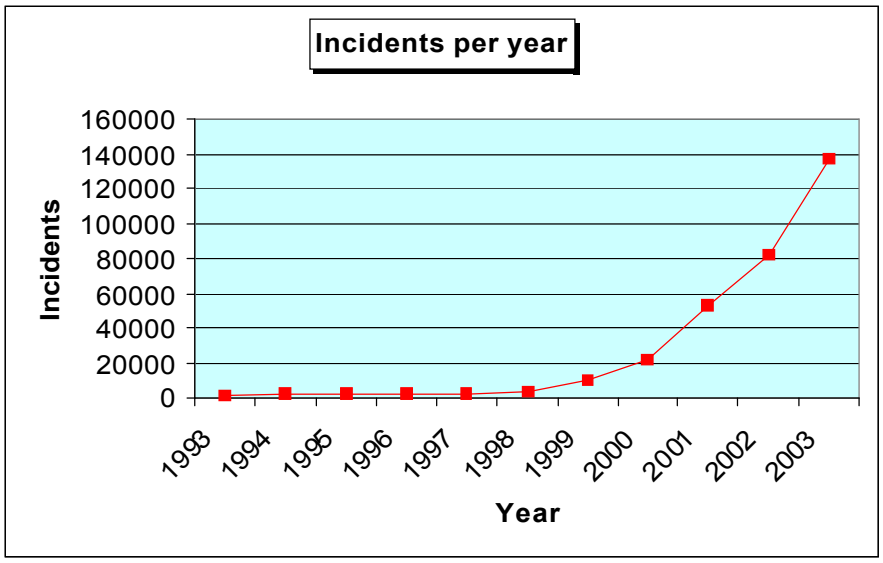


Figure 4 Incidents per year (source http://www.cert.org/stats/cert_stats.html)

From top down, the finance department, with the upper management committee evaluates which initiatives of investment are aligned with the company objectives, the selected initiatives evolve into projects.

ISMS Management Structure.

The ISMS management structure for the selected system is introduced in

the Figure 5

At the moment, the organization does not have an Information Security committee. For this reason, an Information Security Committee is proposed. The key individuals to be members of this committee are: Chief Executive Officer (CEO), Information Security Officer (ISO), the Network Operation Manager and a security team senior member. The roles and functions of each member are described below.

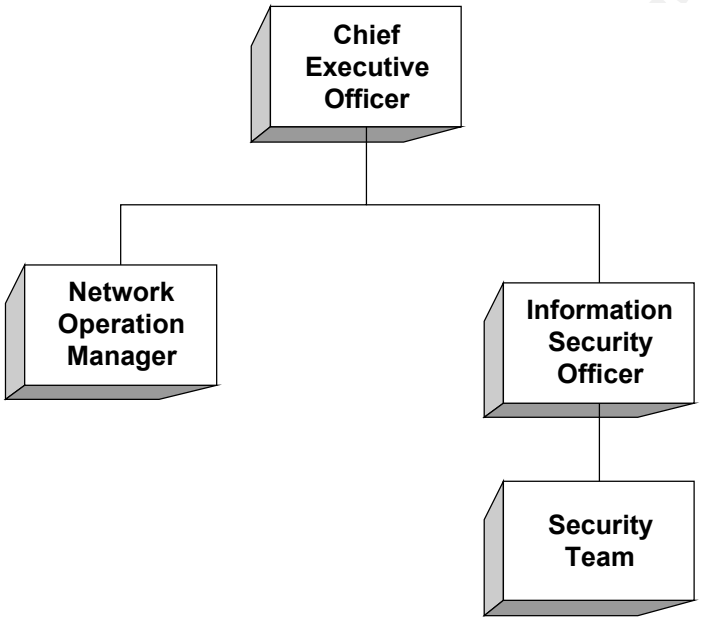


Figure 5 Information Security Committee.

Chief Executive Officer (CEO): Must have the highest commitment and responsibility for the company's information assets. The CEO's signature of the HLSP document is actually a probe of this commitment

Information Security Officer (ISO): responsible for the assurance of Xnet information assets, including: resources management, set priorities and scope to control deployment projects. In this case, the ISO is also the information owner.

Network Operation Manager: Responsible for Xnet systems operation, including: maintaining the service highest likely availability, applying vendor patches, servers hardening, updating and backing-up the systems.

Security Team (secteam): Highly specialized and accurate information security technical team, oriented to the deployment of information security controls like: network access controls, passwords audit, ethical hacking, forensic analysis

and access controls.

The Information Security Committee will have the responsibility for create and review business security policies, take decisions on Information Security matters, delegate the deployment of new controls, approve new Information Security initiatives, review the reports of incidents and so on.

Outline of policies.

Policies are considered to be laws or controls. The motivation of a policy or how it was written can actually influence its effectiveness [4]. The policies written will tend to be proactive and the following principles are taking into account: least privilege, complete mediation, openness, separation of duties and economy of mechanism.

As stated in the section “Steps to develop the system.” policies are needed to regulate elements like: physical security, access control, network security, operating system security, change control, password management and business continuity. In few words: the objective of a policy is to ensure business continuity by preventing or minimizing the impact of security incidents.

For the system selected, the ISO is the policies owner and Information Security Committee is responsible for the policies review and evaluation. Some of the policies are outlined here:

Physical Security

Policy name:	Entry control policy
Purpose:	This policy is motivated to protect the datacenter where the system is hosted, in order to prevent unauthorized access. It should include: physical entry controls, supervise visitor access, restrict the access only to authorized personal, validate identity. This policy is based upon the complete mediation principle
Audience:	All the network operation manager staff.
Areas covered[3]:	“*7.1.2 Physical entry Controls*”

Policy name:	Safeguard equipment policy
Purpose:	Protect the servers running the system. Including: protect the equipment from security and environmental threats and hazards, protect the data from loss or damage

[3] The quoted text was taken from "Information Security Management BS 7799.2:2002 Audit Check List for SANS" [9]

Audience:	Security Team and Network operation manager staff
Areas covered:	"*7.2.1 Equipment siting protection*".

Change Control

Policy name:	Change Control Policy
Purpose:	To establish change control procedures and approval process for systems and facilities. Including: development and deployment of change control procedures, assign management responsibility for system change control, equipments and procedures.
Audience:	Network operation manager staff
Areas covered:	"*8.1.2 Operation Change*"

Network Security

Policy name:	Network Security Policy
Purpose:	Provide network perimeter security for the system, emphasizing least privilege to access the system from the Internet
Audience:	Security team and Network Operation Manager staff
Areas covered:	"*8.5.1 Network Controls*"

Access Control

Policy name:	User Registration Policy
Purpose:	Enforce the development of a procedure for the creation of new users in the system
Audience:	Network Operation Manager staff
Areas covered:	"*9.2.1 User Registration.*"

Policy name:	User Registration Policy
Purpose:	Define the default access rights to the users, based on least privilege principle.
Audience:	Network Operation Manager staff
Areas covered:	"*9.2.4 Review of user access rights*"

Operating System Security

Policy name:	Identification and Authentication Policy
Purpose:	Define a secure mechanism to log into the servers, this mechanism must authenticate, authorize and account the user. This policy is based on the least privilege and complete mediation principles
Audience:	Network Operation Manager staff
Areas covered:	"*9.5.3 User identification and authorization."*

Policy name:	Inactive terminals Policy
Purpose:	Lock the terminal or logout the user after an inactive timeout, in order to prevent unauthorized access that could compromise the information availability, integrity and confidentiality. This policy is based on complete mediation principle.
Audience:	Network Operation Manager staff
Areas covered:	"*9.5.7 Terminal time-out.*"

Password Management

Policy name:	Password management Policy
Purpose:	Protect the access to system user interface, database and operating system, through a password management strategy.
Audience:	The whole staff
Areas covered:	"*9.2.3 User Password Management."*

Business Continuity

Policy name:	Business Continuity Policy
Purpose:	Develop and implement procedures to maintain the system operation in the presence of any event that could compromise it.
Audience:	Security Team
Areas covered:	"*11.1.3 Writing and implementing continuity plan*"

Procedures

To accomplish secure system operation and achieve business continuity, the administrators (Network Operation Staff) will develop and implement procedures for:

- System Installation
- Change Control: including system updates (Operating System, Web Server, Database Engine, RT Core System)

- Database Backup and Recovery.

Main Risks

The process used to identify the risk is based on a qualitative type of analysis called FMECA [6]. This method was chosen because it can be applied to all phases of an ISMS development. Furthermore, it allows to identify failures and to put controls in order to prevent or react in occurrence of a failure.

Step 1: Define the System.

The system is already defined on Chapter 1 (The System), and the interfaces with other systems are identified in the Figure 6. The Service Level Agreement (SLA) between the Operation Network Department and the Information Security Department establish the availability goal in 97% (maximum 7 days down in a year).

Step 2: Create Block Diagrams.

The system functional entities and interfaces are shown in the next block diagram.

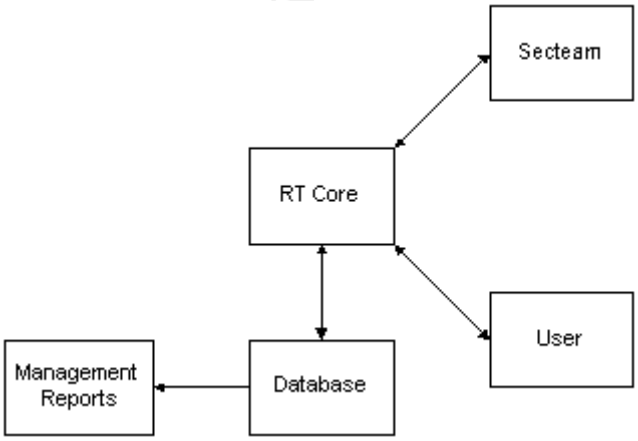


Figure 6 RT System Block Diagram

Step 3: Identify Failures.

Some of the potential points of failure identified in the systems and between them (interfaces) are:

- Server compromised (front-end interface, mail gateway)
- Database compromised (backend server)
- Hardware crash (servers, switch, firewall)
- Server attack from the Internet like: Malicious Code (email worms), Denial of Services (DoS) or Mail Bombing.

- Firewall IOS compromised
- Systems Updates (RT Core, Database Engine)

Each of the risks listed above could potentially affect overall system mission, because the risk involved could impact one or more of the main information security premises: availability, integrity or confidentiality.

Step 4: Assign a Severity level.

For each failure listed above, a "worst case scenario" analysis is done in order to assign a severity level; the results are shown in Table 1:

Failure	Nature Of Threat	Worst Case Scenario	Severity	Likely
Server compromised	Human negligence, deliberated attack from insiders or outsiders	Information disclosure or corruption, systems unavailable.	Catastrophic (I)	Medium
Database compromised	Human negligence, deliberated attack	Information disclosure or corruption	Catastrophic (I)	Medium
Hardware crash	Environmental, physical	The system is not available for its intended use	Critical (II)	Low
Attacks from the Internet	Human deliberated attack, malicious code like worms.	Service degradation	Marginal (III)	High
Firewall IOS compromised	Human Negligence to update the IOS, deliberated attack	The system could be exposed and then compromised	Marginal (III)	Medium
System Updates	Human Incompetence	The system is not available for its intended use.	Critical (II)	High

Table 1 Failures and severity levels

Step 5 to 7. Controls and Control Effects

The last steps of FMECA process are about creating controls. These controls could be preventive, detective or reactive. The objective is to mitigate or reduce the risk.

The risk dynamics analysis is based on Newton´s 2nd law: "for every action there is an equal and opposite reaction", based in that principle a new control can change or create new risks; according to Peter Senge: "today's solutions are tomorrow's problems" [7]. The Table 2 shows the proposed controls and their likely effects.

The security team is the unit responsible for the coordination of control deployment.

Risk	Control	Type	Reason	Effects
Server Compromised	*"4.2 Security of third party access".* *"6.3 Respond to security incidents and malfunctions".* *"9.2.3 Establish a process to manage passwords".* *"9.2.4 Review of user access rights".* *"9.4 Network Access Control".* *"9.5 Operating system access control".* *"9.7 Monitoring system access and use".*	Preventive Reactive Preventive Preventive Preventive Preventive Detective	The objectives of these controls are to detect, prevent and react to an unauthorized (physical or logical) access to system servers event	Could impact the system operation
Database Compromised	Idem	Idem	Idem	Idem
Hardware Crash	"*7.2 Equipment Security*". Have an stock of hardware for replacement "*11.1.3 Writing and Implementing continuity plan*."	Preventive Reactive Preventive	Hardware failure recovery in a reasonable lapse	Increases maintenance costs
Attacks from the Internet: Denial of Service (DoS), Mail Bombing, Malicious Code	Monitor and control the current connections to SMTP and HTTP services (9.7) "*8.1.3 Incident management procedures*" "8.3 Protection against malicious software" "*9.4. Network Access Control*"	Detective Reactive Preventive, Detective and Reactive Preventive	Control and react to attacks from the Internet. Detect and stop malicious code.	The SNMP service could be exploited

Mail Bombing	Idem	Idem	Control and react to Mail Bombing attack	Idem
Firewall IOS compromised	"*8.5.1 Network Controls*" (periodically review and audit of firewall rules). "*9.4 Network Access Control*" Patch regularly the equipments	Preventive Preventive Preventive	Avoid an attacker to run an IOS exploit and gain device control	Reduces level of threat
System Updates	"*8.1.1 Documented Operating procedures*". "*8.1.2 Operational Change*"	Preventive Preventive	Raise awareness. Reduce risk by improving the human competence	Reduces efficiency (more tasks to do)

Table 2 Proposed Controls[4]

Step 8. Residual Risks

Although desirable its almost unlikely that an organization have a 100% security level, one clear constraint is cost and furthermore new threats and vulnerabilities are very likely to keep appearing (as shown in Figure 4), for this reason –among others- residual risk is always present in an organization. The residual risks are those that cannot be managed by the implemented controls. An effective risk management strategy should minimize the residual risk to an acceptable level for the organization.

In this study case, the Information Security Committee will define which residual risks are acceptable and which are not, for the last additional controls must be put in place. Having this in mind, the residual risks are listed below:

Failure	Nature Of Threat	Worst Case Scenario	Severity	Likely
Power shortage	Environmental	System Down	Catastrophic (I)	Low
Sabotage	Human attack	System Down	Catastrophic (I)	Low

Although the severity of every risk is of type (I), the possibility of occurrence is low, hence the Information Security Committee decided that the level of risk is acceptable (marginal) for the organization, though there is need for continue review of changes in the organization risk dynamics. To do this task; periodically risk analysis is suggested

[4] Note: *Quoted* controls were taken from: "Information Security Management BS 7799.2:2002 Audit Check List for SANS" [9]

Do

In the PDCA methodology, the "Do" stage is defined as: "implement the plan and measure its performance" [3]. This chapter describes the steps to be taken to implement the improvements previously identified; most of the improvements are controls that will mitigate the risks recognized during the risk analysis conducted in planning phase. At the end of the chapter, a statement of applicability is written for thee controls that have been considered for the system.

Implementing the improvements

A problem is related to an improvement opportunity, this section describes the problems associated with each risk, the actions required to solve the problem and finally the steps to implement each action.

Information Security Policies

Problem: The information security policies and procedures are incomplete.

Actions: The policies identified in planning phase must be developed and approved by the Information Security Committee (ISO 17799. 3.1.1).

Steps: For each policy write a policy statement, while writing the policies the information security principles should be taken into account: least privilege, complete mediation, openness, separation of duties and economy of mechanism. The policy statement[5] should include:

- Policy name.
- Purpose of the policy, describing the intent or the problems faced by the policy).
- Policy scope.
- Audience (who must be compliant with the policy) and the enforcement of the policy.
- Enforcement statement and mechanisms (if any)
- Audit controls.

System Compromised

Problem: New system vulnerabilities are continuously discovered. Those vulnerabilities might be potentially exploited by an attacker, gaining unauthorized access to sensible information. The system includes: servers operating system,

[5] According to "SANS 17799 Security & Audit Framework" course a good policy should be "SMART": Specific, Measurable, Achievable Realistic and Time based [8].

firewall and switch IOS, web server, database server, RT core modules.

Actions: A set of controls must be put in place by the security team to detect, prevent and react to unauthorized access (ISO 17799 4.2, 6.3, 9.2, 9.4, 9.5 and 9.7). Continuous vulnerabilities revision and system update procedures must be performed.

Steps:

1. Perform periodic revisions to biometric system to restrict third party access to facilities.
2. Continue revision of firewalls rules.
3. Develop system update procedures, including operating system and IOS updates.
4. To mitigate risks during operation, it is critical to develop procedures for update RT Core system and the Database Management System. Moreover, a development environment should be deployed to test the procedures and perform the updates prior to updating the production environment.
5. Perform penetration tests (see Penetration Tests appendix at page 30).
6. Develop an incident response procedure.
7. Do server hardening (see Server Hardening appendix at page 33).
8. Review user access rights (see RT Access Rights appendix at page 41)
9. Monitor the whole system activity and usage via SNMP.

Business Continuity

Problem: Hardware crash or disasters in datacenter facilities (i.e. fire or flooding) could stop the system.

Actions: Develop a business continuity plan for the system (ISO 17799 11.1.3, 11.1.5), including procedures for backup and recover the system.

Steps:

1. Write Procedures and scripts (see Database Backup at page 42) to backup the system.
2. Write Procedures to install or recover the system from scratch.
3. Write system operation procedures.
4. Backup the system.
5. Carry out periodical recovery tests in development environment.
6. Consider to rent a server in a third party datacenter facility.
7. Consider to have a stock of common server parts.

Internet Attacks

Problem: The HTTP, SMTP and Database services of RT System are highly vulnerable to a Denial of Service (DoS) attack. In addition, the SMTP server is vulnerable to a Mail Bombing attack and to could spread malicious code in the organization. This kind of attacks could cause service degradation and potential affect the system users.

Actions: Protect the server of attacks from the Internet by monitoring the system use (ISO 17799 9.7), identify operational thresholds, and set alarms in case the system operation breaks the thresholds. Restrict the web access to the system only to the organization networks (ISO 17799 9.4).

Steps:

1. Restrict access to web server and database server through the firewall.
2. Monitor the system use via SNMP and log revision. Particularly monitor and control the current connections to SMTP and HTTP services
3. Set operation thresholds and alarms.
4. Update the incident response procedure, to manage this kind of attacks.
5. Protect the web server using anti denial of service tools (like mod_dosevasive[6] in Apache web server).
6. Install antivirus systems for the SMTP service.

Statement of applicability.

This section presents statements of applicability for two controls considered for the system, and at the end a non applicability (or statement of exclusion) for a control that will not be implemented; because it does not apply to the system.

Statement of applicability for ISO 17799 9.7 “Monitor System access and review“:

These controls apply to the ISMS because they allow detecting system attacks from the Internet. To implement these controls, logs are going to be copied to a NAS Server for periodical review. The SNMP software will be updated and properly configured, in order to turn on the SNMP service in a secure way. Scanning will be allowed only from the monitoring system.

Statement of applicability for ISO 17799 9.5.7 ”Use time-outs to protect inactive terminals“:

This control prevents unauthorized access to the system. It will be implemented through a server hardening script (see Server Hardening appendix

[6] http://www.nuclearelephant.com/projects/dosevasive/

at page 33) and updating the IOS configuration of firewall and switch.

Statement of exclusion for (ISO 17799 4.3.1) "Use contracts to control outsourced services":

This control does not apply to the ISMS being discussed, because there are not outsourced services for the RT system, the whole system is administered by Xnet Network Operation staff.

Check

In the PDCA methodology, the "Check" phase is defined as: "*Assess the measurements and report the results to decision makers*" [3]. To perform the assessment, the ISMS has to be audited against the standard, at the end of the audit the decision makers (in this study case the Information Security Committee) will be able to know if the controls are working, and the ISMS is still effective.

The next table (Table 3) describes an audit checklist for the ISMS; it includes a set of selected controls from the standard pertaining to the system, and for each control:

1. The control objectives being evaluated by the checkpoint item.
2. Reason for audit the control.
3. The methods to audit or audit steps and the frequency to perform the audits

The audit checklist can be used to improve the ISMS, at the end of the check phase a set of gaps or control weakness will be identified, that issues are going to be solved during the Act phase.

ISO 17799 Control	Control Objective	Reason for audit	Audit steps and Frequency of tests

[7] Quoted ISO 17799 controls were taken from: "Information Security Management BS 7799.2:2002 Audit Check List for SANS" [9]

3.1.1 "*Information security policy document*" [7]	"*State management commitment and set out the organization's approach to managing information security*"[8]	Policies are the information security basement in any organization; they provide a framework for secure operation and define a set of controls to mitigate risk. It is necessary to audit them periodically to identify gaps between the policies and the business objectives.	Gather existing information security policies. Check whether the existing policies are signed by the Information Security Committee Identify at least one police aligned with the business objectives. Check whether the policies are published in the Intranet site, and check randomly whether employees have read the policies and have signed an acceptance form. Frequency of audit: Bi-annual.
6.3.1 "*Reporting security incidents*"	"*Minimize damage from information security incidents*"	Opportune communication of information security incidents through appropriate management channels could minimize the damage caused by the incident.	Look for formal incident response procedures Check whether exist any information security incident report Randomly select employees to verify whether procedures are known by the staff Frequency of audit: Bi-annual
8.1.1 "*Documented Operating procedures*"	"*To ensure the correct and secure operation of information processing facilities*"	Updated system operation procedures are needed to minimize the risk caused by human error.	Gather operation procedures, and check whether the procedure is current. Interview the Network Operations staff to determine whether their operational tasks correspond to the documented procedures. Frequency of audit: annual

[7] Quoted ISO 17799 controls were taken from: "Information Security Management BS 7799.2:2002 Audit Check List for SANS" [9]
[8] Quoted control objectives were taken from 7799 Implementation and Improvement [5]

8.1.2 "*Operational Change*"	Minimize the risk caused by human error.	Change control authorization can determine whether the control will maintain the system in a secure operation state.	Determine whether any change to the production environment must be authorized. Check how is the change authorization process and who is the owner of the process. Gather authorization process evidence, like electronic or physical forms. Frequency of audit: annual
8.1.3 "*Incident management procedures*"	"*To ensure a quick, effective and orderly response to security incidents and collect incident related data such as audit trails and logs*"	The RT system is vulnerable to attacks from the Internet like: DoS, Mail Bombing, exploits. In case of such attacks, an effective and quick response could minimize the damage.	Gather formal incident response and management procedures; verify whether the procedure covers different types of security information incidents. Review with the staff how is the process to manage an incident, compare the answers with the formal procedure. Look for evidence of incident (logs) and reports of incident response. Compare the actions reported with the formal procedures. Check whether the procedures are current. Frequency of tests: Annual
8.3.1 "Control against malicious software"	"To prevent against malicious software"	Stop malicious code propagation.	Check whether a antivirus system for the SMTP service is running in the frontend server. Review antivirus logs to verify its effectiveness. Verify whether the antivirus signature is up to date. Frequency of test: Quarterly

8.5.1 "*Network controls*"	"*Achieve and maintain security in networks*"	To minimize the risk of attacks from the Internet, the access to RT system from public networks should be allowed only trough SMTP protocol (i.e. via email). The backend (database) server should be isolated from public networks.	Verify that the network is segmented and there is a firewall in place protecting the corporate network from the Internet Verify that the firewall is allowing communication from public networks to the front-end server only through SMTP protocol (i.e. perform a penetration test) Ask a system administrator to remotely connect to the server, verify whether is using encrypted protocols like SSH. Frequency of audit: Quarterly
9.2.4 "*Review of user access rights*"	"*To ensure that access rights to the system are appropriately allocated"*	RT system has a wide range of user access rights, the correct management of access rights assignment could minimize the risk of unauthorized access to sensible information	Gather formal policies and procedures that defines a periodical revision process of user access rights Together with a system administrator, review access rights for random selected users in the system. Frequency of audit: Bi-annual
9.5.3 "*User identification and authorization*"	"*To prevent unauthorized computer access"*	To prevent unauthorized computer access it is mandatory to identify and authenticate all user access to operation system and to the Web system interface.	Try to login into the operative system without password or in anonymous mode Try to get access to Web interface without having a valid user and password. Check whether there are generic accounts in the system. Frequency of audit: annual
9.5.7 "*Terminal time-outs*"	Idem	An unattended administration console is an area of concern, because it offers unauthorized access to the system.	Open an administration console and check whether the operating system logout the user after a period of inactivity. Frequency of audit: annual

9.7.1 "*Event logging*"	"*To detect unauthorized activities*"	Periodic review of system logs allows detecting suspicious activities. For RT system, the sources of logs are: syslog files, httpd logs, and the DBMS access logs.	Gather policies and procedures for logs management and review. Determine for how long are logs maintained Verify the log files date in the log repository. Check with the staff to know the nature of tasks performed with the logs and contrast them against the procedures Frequency of audit: annual
9.7.2 "*Monitoring system use*".	Idem	System monitoring allows setting thresholds for normal system operation, any deviation must be investigated.	Verify the monitoring system console whether the RT system is being monitored. From an authorized server do a `snmpwalk` command to check whether the server is answering to SNMP requests. Frequency of audit: annual
11.1.3 "*Writing and implementing continuity plan*"	"*To protect critical business processes from the effects of major failures or disasters*"	A business continuity plan mitigates the risk in case of major failures. In addition, the documented procedures (installation, backup and recovery) allow the recovery from a simple and frequent failure like a hardware crash.	Gather installation, backup and recovery procedures. Verify whether the procedures are up to date. Verify that backups and recovery tests are periodically performed

Table 3 ISMS Audit checklist

Act

The final stage of the Deming Cycle is Act: "*Decide on changes needed to improve the process*". One feature of open systems is their adaptability capacity, which allows the system to change continually in order adapt to its environment changes[9]. This chapter shows the strategy to maintain and improve the ISMS for the RT system. The strategy is just to detect system anomalies or gaps and to make changes to correct them.

One clear system anomaly is an information security incident. In addition to activate incident respond and management procedures -every time an incident is reported-; the incident itself could have positive effects in the ISMS improvement process, but only if the organization can take advantage of the knowledge involved in any incident.

In order to achieve learning from incidents, it is suggested to maintain incident statistics. Such numbers could include:

1. Total incidents per month.
2. Assets involved.
3. Source and type of attacks.
4. Vulnerabilities exploited and
5. Overall incident cost (if available).

Periodic statistics revision allows to set thresholds for normal ISMS "operation" (system metrics), a significant amount of incidents, i.e. a 10% increment above the thresholds in Mail Bombing or DoS attacks against an RT frontend server; imply control failures and policy need to be reviewed. Other cause of policy review is change in business objectives.

Another source of improvements is to carry out periodic (monthly) logs revision of firewalls and servers; also, periodic (annual) ISMS independent audits, both internal and external[10], should be performed.

Audits can be performed using checklists like the one introduced in the previous chapter (Table 3). Audits will detect system gaps that must be corrected applying correctives and preventives procedures (see Table 4) in order to maintain the system effectiveness. The steps to maintain the system are a control maintenance process; where new controls are added, existing controls are changed or deleted (of course this process involves updating the statement of applicability).

[9] Concept introduced by Bertalanffy in his theory of open systems.
[10] According to "SANS 17799 Security & Audit Framework" course, the auditor competence in information security, its critical for a success audit.

Audit	Gap	Improvement	Owner
Information Security Policies	Outdated policies and not aligned with business objectives	Review business objectives and polices to identify possibly breaches Update policies.	Information Security Committee
Operational Change	Change authorization process is not accomplished	With the process owner, review the authorization process. Identify the process weakness. Consider to apply business process reengineering (BPR).	Security Team staff and Network Operation staff
Network Controls	Outdated firewall rules.	Review firewall rules, group rules by network segment will make easy the revision	Security Team staff
User access rights	There are system users with more privileges as they need.	Determine why the periodic access rights revision is failing. Group users into RT groups according with their functionality, revoke user permissions and assign permissions to groups.	Security Team staff and Network Operation Staff

Table 4 System Gaps and Improvements

Conclusions

1. The Plan, Do, Check and Act (PDCA) methodology is suitable for an ISMS development; in fact, it is a guide for the development process.

2. A critical success factor is to have a management structure that support and empower the ISMS deployment.

3. The risk analysis process is basic for focus the efforts of risk mitigation, to those assets highly vulnerable and whose lost could actually impact the achieving of business objectives.

4. Server and database compromise, and attacks from the Internet are common risks for the RT system.

5. The risk analysis process could guide the creation of preventive, reactive and detective controls.

6. Network access controls, antivirus system for the SMTP service, restricted access rights, monitor system use and incident response procedures; are part of the controls identified for the RT system.

7. The check and act phase allows the ISMS to remain effective.

8. Two key concepts in ISMS deployment is periodic revision and continuous improvement.

References

[1] Brykczynski, Bill. Small, Bob. "Securing your Organization's Information Assets". Cross Talk Journal. May 2003.

[2] Best Practical Solutions, LLC. http://www.bestpractical.com/

[3] Arveson, Paul. "The Deming Cycle". Online at: http://www.balancedscorecard.org/bkgd/pdca.html

[4] Teledesign Security. "Enterprise Security Policy". Online at: http://www.teledesignsecurity.com/policy.asp

[5] Hoelzer, David. "7799 Implementation and Improvement". SANS Institute. 2004

[6] "MIL-STD-1629A Military Standard Procedures For Performing a Failure Mode, Effects And Criticality Analysis". Department of Defense. Washington, DC. USA. 1980. Online at: http://jcs.mil/htdocs/teinfo/software/ms18.html

[7] Senge, Peter. "The Fifth Discipline". DoubleDay. 1990

[8] Hoelzer, David. "SANS 17799 Security & Audit Framework". SANS Institute, page 138-140. 2004.´

[9] Val, Thiagarajan. "Information Security Management BS 7799.2:2002 Audit Check List for SANS".

Appendices

Penetration Tests

This section shows an extract of RT System penetration tests, the server scanning were performed using Retina Network Scanner with scanner version: 5.0.17.1124. Systems where patched and updated after the tests.

Frontend server

Retina - Network Security Scanner

Network Vulnerability Assessment & Remediation Management

Jueves, 21 de Octubre de 2004

TOP 20 VULNERABILITIES

The following is an overview of the top 20 vulnerabilities on your network.

Rank
Vulnerability Name
Count

1.
EXPN Command Enabled
2

2.
VRFY Command Enabled
2

3.
Apache-SSL Client Certificate Forging
2

4.
Mod_SSL Off-By-One HTAccess Buffer Overflow Vulnerability
2

5.
OpenSSL ASN.1 Parsing Error Denial Of Service Vulnerability
2

6.
OpenSSL CBC encryption timing attack vulnerability
2

7.
RPC nlockmgr service
1

8.
RPC rpc.portmap service
1

9.
RPC rpc.statd service
1

10.
RPC statd format string attack
1

11.
OpenSSH 3.3 PAMAuth Integer Overflow
1

12.
OpenSSH 3.3 Remote Challenge Integer Overflow
1

13.
OpenSSH 3.7.0 Buffer Overflow
1

TOP 20 OPEN PORTS

The following is an overview of the top 20 open ports on your network.

Rank
Port Number
Description
Count

1.
TCP:22
SSH - SSH (Secure Shell) Remote Login Protocol
1

2.
TCP:25
SMTP - Simple Mail Transfer Protocol
1

3.
TCP:80
WWW-HTTP - World Wide Web HTTP (Hyper Text Transfer Protocol)
1

4.
TCP:110
POP3 - Post Office Protocol - Version 3
1

5.
TCP:111
SUNRPC - SUN Remote Procedure Call
1

6.
TCP:443
HTTPS - HTTPS (Hyper Text Transfer Protocol Secure) - SSL (Secure Socket Layer)
1

7.
TCP:587
SUBMISSION -
1

8.
TCP:32768

1

TOP 20 RUNNING SERVICES

The following is an overview of the top 20 running services on your network.

Rank
Name
Description
Count

1.
nlockmgrUDP1

4

2.
nlockmgrUDP3

4

3.
nlockmgrUDP4

4

4.
portmapperTCP2

4

5.
portmapperUDP2

4

6.
statusTCP1

4

7.
statusUDP1

4

Backend server

Retina - Network Security Scanner

Network Vulnerability Assessment & Remediation Management

Jueves, 21 de Octubre de 2004

TOP 20 VULNERABILITIES

The following is an overview of the top 20 vulnerabilities on your network.

Rank
Vulnerability Name
Count

1.
EXPN Command Enabled
2

2.
VRFY Command Enabled
2

3.
Apache-SSL Client Certificate Forging
2

4.
Mod_SSL Off-By-One HTAccess Buffer Overflow Vulnerability
2

5.
OpenSSL ASN.1 Parsing Error Denial Of Service Vulnerability
2

6.
OpenSSL CBC encryption timing attack vulnerability
2

7.
RPC nlockmgr service
1

8.
RPC rpc.portmap service
1

9.
RPC rpc.statd service
1

10.
RPC statd format string attack
1

11.
OpenSSH 3.3 PAMAuth Integer Overflow
1

12.
OpenSSH 3.3 Remote Challenge Integer Overflow
1

13.
OpenSSH 3.7.0 Buffer Overflow
1

TOP 20 OPEN PORTS

The following is an overview of the top 20 open ports on your network.

Rank
Port Number
Description
Count

1.
TCP:22
SSH - SSH (Secure Shell) Remote Login Protocol
1

2.
TCP:25
SMTP - Simple Mail Transfer Protocol
1

3.
TCP:80
WWW-HTTP - World Wide Web HTTP (Hyper Text Transfer Protocol)
1

4.
TCP:110
POP3 - Post Office Protocol - Version 3
1

5.
TCP:111
SUNRPC - SUN Remote Procedure Call
1

6.
TCP:443
HTTPS - HTTPS (Hyper Text Transfer Protocol Secure) - SSL (Secure Socket Layer)
1

7.
TCP:587
SUBMISSION -
1

8.
TCP:32768

1

TOP 20 RUNNING SERVICES

The following is an overview of the top 20 running services on your network.

Rank
Name
Description
Count

1.
nlockmgrUDP1

4

2.
nlockmgrUDP3

4

3.
nlockmgrUDP4

4

4.
portmapperTCP2

4

5.
portmapperUDP2

4

6.
statusTCP1

4

7.
statusUDP1

4

Server Hardening

The next post install server script was used to carry out the servers operating

system hardening.

```
# Operating System postinstall script
# luismoreno@gmail.com
#
#!/bin/bash
echo Doing postinstall
# Network interfaces issues and increase syn queue to combat DoS
attacks
cat <<END_NETPARAM_ENTRIES >>/etc/sysctl.conf
net.ipv4.ip_forward = 0
net.ipv4.conf.default.arp_filter = 1
net.ipv4.conf.all.arp_filter = 1
net.ipv4.conf.eth0.arp_filter = 1
net.ipv4.conf.eth1.arp_filter = 1
net.ipv4.tcp_max_syn_backlog = 4096
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
END_NETPARAM_ENTRIES
#
# Full Duplex
echo Configuring eth driver
module=`/sbin/modprobe -c|egrep "^alias eth0"|cut -d" " -f 3`
echo Driver: $module
if [ "${module}" == "eepro100" ]; then
     echo options eepro100 options=0x30,0x30 >>
/etc/modules.conf
fi
if [ "${module}" == "tg3" ]; then
     cat <<TG3 > /sbin/ifup-local
#!/bin/bash
#
# Thomas Eriksson thomas.eriksson@slac.stanford.edu
#
# This script is run after a network interface is started
# The calling script passes one parameter; the devicename.
#
DEVICE=\${1}
[ -z \${DEVICE} ] && exit 0
[ -x /usr/sbin/ethtool ] || exit 0
driver=\`/sbin/modprobe -c | awk "/^alias \${DEVICE}/ { print
\\\\\$3 }"\`
if [ \${driver} == "tg3" ]; then
     /usr/sbin/ethtool -s \${DEVICE} speed 100 duplex full
autoneg off
fi
```

```
exit 0
TG3
     /bin/chmod 755 /sbin/ifup-local
fi
echo Done Configuring eth
echo Server Hardening...
#Server Hardening

#Disable netfs script
/sbin/chkconfig netfs off

# Disable core dumps
cat <<END_COREDUMP_ENTRIES >>/etc/security/limits.conf
*    soft  core  0
*    hard  core  0
END_COREDUMP_ENTRIES

# Add nosuid option for removable media in /etc/fstab
cp /etc/fstab /etc/fstab.old
awk '($2 ~/^\/m.*\/(floppy|cdrom)$/ && $3 != "supermount") \
     {$4 = sprintf("%s,nosuid", $4) }; \
     { print }' /etc/fstab > /etc/fstab.new
mv /etc/fstab.new /etc/fstab
# Add nodev
awk '($3 ~ /^ext[23]$/ && $2 != "/") \
{ $4 = $4 ",nodev" }; \
{ print }' /etc/fstab >/etc/fstab.new
/bin/mv /etc/fstab.new /etc/fstab
chown root:root /etc/fstab
chown 0644 /etc/fstab

# Disable user-mounted removable filesystems
cd /etc/security
awk '($1 == "<console>") && ($3 !~ \
/sound|fb|kbd|joystick|v4l|mainboard|gpm|scanner/) \
{ $1 = "#<console>" };
{ print }' console.perms >console.perms.new
/bin/mv console.perms.new console.perms
chown root:root console.perms
chmod 0600 console.perms

grep -v supermount /etc/fstab > /etc/fstab.new
mv /etc/fstab.new /etc/fstab

# Create /etc/ftpusers
for name in `cut -d: -f1 /etc/passwd`
do
     if [ `id -u $name` -lt 500 ]
     then
          echo $name >> /etc/ftpusers
     fi
done
chown root:root ftpusers
chmod 600 /etc/ftpusers
```

```
# Restrict permissions on crontab files
/bin/chown root:root /etc/crontab
/bin/chmod 400 /etc/crontab
/bin/chown -R root:root /var/spool/cron
/bin/chmod -R go-rwx /var/spool/cron
/bin/chown -R root:root /etc/cron.*
/bin/chmod -R go-rwx /etc/cron.*

# Purge or lock system accounts
for user in news lp operator games gopher ftp
do
     /usr/sbin/userdel $user
done

# Set default umask for users
echo "umask 022" >> /etc/profile
echo TERM=\"linux\" >> /etc/profile
echo TMOUT=3600 >> /etc/profile
echo export TERM TMOUT >> /etc/profile
chmod 444 /etc/profile
rm /etc/csh.login
rm /etc/csh.cshrc
# Restrict root logins to system console
/bin/cp /dev/null /etc/securetty
for i in 1 2 3 4 5 6; do
echo tty$i >>/etc/securetty
echo vc/$i >>/etc/securetty
done
echo console >>/etc/securetty
/bin/chown root:root /etc/securetty
/bin/chmod 400 /etc/securetty

# Restrict cron and at exec
echo root > /etc/cron.allow
echo root > /etc/at.allow

# Restrict init scripts
/bin/chmod 700 /etc/rc.d/init.d

#Remove .rhosts support in PAM configuration files
for file in /etc/pam.d/* ; do
grep -v rhosts_auth $file > ${file}.new
/bin/mv ${file}.new $file
/bin/chown root:root $file
/bin/chmod 644 $file
done

if [ "`egrep -l Authorized /etc/motd`" == "" ]; then
echo "Authorized uses only. All activity may be \
monitored and reported." >>/etc/motd
echo "Solo usuarios autorizados. Toda actividad \
puede ser monitoreada y reportada." >>/etc/motd
```

```
fi
if [ "`egrep -l Authorized /etc/issue`" == "" ]; then
echo "Authorized uses only. All activity may be \
monitored and reported." >>/etc/issue
echo "Solo usuarios autorizados. Toda actividad \
puede ser monitoreada y reportada." >> /etc/issue
fi
if [ "`egrep -l Authorized /etc/issue.net`" == "" ]; then
echo "Authorized uses only. All activity may be \
monitored and reported." >>/etc/issue.net
echo "Solo usuarios autorizados. Toda actividad \
puede ser monitoreada y reportada." >> /etc/issue.net
fi
/bin/chown root:root /etc/motd /etc/issue /etc/issue.net
/bin/chmod 644 /etc/motd /etc/issue /etc/issue.net
if [ -e /etc/X11/xdm/kdmrc ] ; then
cd /etc/X11/xdm
awk '/GreetString=/ \
{ print "GreetString=Authorized uses only!"; next };
{ print }' kdmrc >kdmrc.new
/bin/mv kdmrc.new kdmrc
/bin/chown root:root kdmrc
/bin/chmod 644 kdmrc
fi
if [ -e /etc/X11/gdm/gdm.conf ] ; then
cd /etc/X11/gdm
awk '/^Greeter=/ && /gdmgreeter/ \
{ printf("#%s\n", $0); next };
/^#Greeter=/ && /gdmlogin/ \
{ $1 = "Greeter=/usr/bin/gdmlogin" };
/Welcome=/ \
{ print "Welcome=Authorized uses only!"; next };
{ print }' gdm.conf >gdm.conf.new
/bin/mv gdm.conf.new gdm.conf
/bin/chown root:root gdm.conf
/bin/chmod 644 gdm.conf
fi

#Create "authorized only" banners for network services using TCP
Wrappers
mkdir /etc/banners ; cd /etc/banners
if [ -e /usr/doc/tcp_wrappers-7.6/Banners.Makefile ]; then
file=/usr/doc/tcp_wrappers-7.6/Banners.Makefile
else
file=/usr/share/doc/tcp_wrappers-7.6/Banners.Makefile
fi
cp $file Makefile
echo "Solo usuarios autorizados. Toda actividad \
puede ser monitoreada y reportada."> prototype
echo "Authorized uses only. All activity may be \
monitored and reported." >> prototype
make
cd /etc/xinetd.d
for file in telnet krb5-telnet ; do
```

```
if [ -f $file ]; then
awk '( $1 == "}" ) \
{ print "banner = /etc/banners/in.telnetd" };
{ print }' $file >$file.new
/bin/mv $file.new $file
fi
done
for file in wu-ftpd gssftp ; do
if [ -f $file ]; then
awk '( $1 == "}" ) \
{ print "banner = /etc/banners/in.ftpd" };
{ print }' $file >$file.new
/bin/mv $file.new $file
fi
done
for file in rsh kshell ; do
if [ -f $file ]; then
awk '( $1 == "}" ) \
{ print "banner = /etc/banners/in.rshd" };
{ print }' $file >$file.new
/bin/mv $file.new $file
fi
done
for file in rlogin klogin eklogin ; do
if [ -f $file ]; then
awk '( $1 == "}" ) \
{ print "banner = /etc/banners/in.rlogind" };
{ print }' $file >$file.new
/bin/mv $file.new $file
fi ; done
/bin/chown root:root {krb5-,}telnet gssftp wu-ftpd rsh \
kshell rlogin klogin eklogin
/bin/chmod 644 {krb5-,}telnet gssftp wu-ftpd rsh kshell \
rlogin klogin eklogin

#Require authentication for single-user-mode
cd /etc
if [ "`grep -l sulogin inittab`" = "" ]; then
awk '{ print };
/^id:[0123456sS]:initdefault:/ \
{ print "~~:S:wait:/sbin/sulogin" }' \
inittab >inittab.new
/bin/mv inittab.new inittab
/bin/chown root:root inittab
/bin/chmod 644 inittab
fi

#Block system accounts
for name in `cut -d: -f1 /etc/passwd`; do
uid=`id -u $name`
if [ $uid -lt 500 -a $name != 'root' ]; then
/usr/sbin/usermod -L -s /dev/null $name
fi
done
```

```
#Set account expiration parameters on active accounts
cd /etc
awk '($1 ~ /^PASS_MAX_DAYS/) { $2="90" }
($1 ~ /^PASS_MIN_DAYS/) { $2="7" }
($1 ~ /^PASS_WARN_AGE/) { $2="28" }
($1 ~ /^PASS_MIN_LEN/) { $2="6" }
{ print } ' login.defs > login.defs.new
/bin/mv login.defs.new login.defs
/bin/chown root:root login.defs
/bin/chmod 640 login.defs
for name in `cut -d: -f1 /etc/passwd`; do
uid=`id -u $name`
if [ $uid -ge 500 -a $uid != 65534 ]; then
/usr/bin/chage -m 7 -M 90 -W 28 $name
fi
done

# Set default umask for users
touch /etc/csh.login
touch /root/csh.login
touch /etc/csh.cshrc
touch /root/csh.cshrc
cd /etc
for file in profile csh.login csh.cshrc bashrc
do
if [ `egrep -c umask\.\*77 $file` -eq 0 ];
then
echo "umask 077" >> $file
fi
/bin/chown root:root $file
/bin/chmod 444 $file
done
cd /root
for file in .bash_profile .bashrc .cshrc .tcshrc
do
echo "umask 077" >>$file
/bin/chown root:root $file
done

#Confirm permissions on system log files
cd /var/log
/bin/chmod o-w boot.log* cron* dmesg ksyms* httpd/* \
maillog* messages* news/* pgsql rpmpkgs* samba/* \
scrollkeeper.log secure* spooler* squid/* vbox/* wtmp
/bin/chmod o-rx boot.log* cron* maillog* messages* pgsql \
secure* spooler* squid/*
/bin/chmod g-w boot.log* cron* dmesg httpd/* ksyms* \
maillog* messages* pgsql rpmpkgs* samba/* \
scrollkeeper.log secure* spooler*
/bin/chmod g-rx boot.log* cron* maillog* messages* pgsql \
secure* spooler*
/bin/chmod o-w gdm/ httpd/ news/ samba/ squid/ vbox/
/bin/chmod o-rx httpd/ samba/ squid/
```

```
/bin/chmod g-w gdm/ httpd/ news/ samba/ squid/ vbox/
/bin/chmod g-rx httpd/ samba/
/bin/chown -R root:root .
/bin/chgrp utmp wtmp
/bin/chown -R news:news news
/bin/chown postgres:postgres pgsql
/bin/chown -R squid:squid squid

# Limit xinetd connections
cd /etc
for file in xinetd.conf; do
if [ -f $file ]; then
awk '( $1 == "}" ) \
{ print "only_from =127.0.0.1/24" };
{ print }' $file >$file.new
/bin/mv $file.new $file
fi
done

/sbin/sysctl -p

echo Done Hardening
#
echo Configuring daemons
# Configure SSH
cd /etc/ssh
awk '($1=="Protocol") { print "Protocol 2"; next };
{ print }' ssh_config >ssh_config.new
/bin/mv ssh_config.new ssh_config
/bin/chown root:root ssh_config
/bin/chmod 644 ssh_config
if [ "`egrep -l ^Protocol ssh_config`" == "" ]; then
echo 'Protocol 2' >>ssh_config
fi
awk '/^#?Protocol/ { print "Protocol 2"; next };
/^#?X11Forwarding/ \
{ print "X11Forwarding yes"; next };
/^#?IgnoreRhosts/ \
{ print "IgnoreRhosts yes"; next };
/^#?RhostsAuthentication/ \
{ print " RhostsAuthentication no"; next };
/^#?RhostsRSAAuthentication/ \
{ print "RhostsRSAAuthentication no"; next };
/^#?HostbasedAuthentication/ \
{ print "HostbasedAuthentication no"; next };
/^#?PermitRootLogin/ \
{ print "PermitRootLogin no"; next };
/^#?PermitEmptyPasswords/ \
{ print "PermitEmptyPasswords no"; next };
{print}' sshd_config >sshd_config.new
/bin/mv sshd_config.new sshd_config
/bin/chown root:root sshd_config
/bin/chmod 600 sshd_config
```

```
# ntp
cat <<END_NTP >/etc/ntp.conf
#
# ntp.conf: Configuration for the ntp servers
# 19980916: Initial release <alvaro@xnet>
#

server w.x.y.z
peer a.b.c.d

driftfile /var/log/ntp.drift
END_NTP

# resolv.conf
cat <<END_RESOLV >/etc/resolv.conf
search xnet
nameserver w.x.y.z
nameserver w.x.y.z
END_RESOLV
# syslog.conf
cat <<SYSLOG > /etc/syslog.conf
*.*                                     /dev/console
*.*                                     @logger-01.x.y.z
*.*                                     @logger-02.x.y.z
SYSLOG
echo Done configuring daemons
#
echo Disabling services
echo Configuring daemons
# Disable services
cd /etc/rc.d/rc3.d/
mv S05kudzu K05kudzu
mv S08ip6tables K08ip6tables
mv S08iptables K08iptables
mv S08ipchains K08ipchains
mv S09isdn K09isdn
mv S24pcmcia K24pcmcia
mv S26apmd K26apmd
mv S28autofs K28autofs
mv K50snmpd S50snmpd
mv S56rawdevices K56rawdevices
mv S56xinetd K56xinetd
mv S60lpd K60lpd
mv K75netfs S75netfs
mv S80sendmail K80sendmail
mv S85gpm K85gpm
mv S90xfs K90xfs
mv S95atd K95atd
mv S97rhnsd K97rhnsd
mv S95anacron K95anacron
mv S99local K99local
echo Done disabling services
echo Done postinstall...
echo reboot the server!
```

RT Access Rights

The users are grouped by his role in the system, the following permissions were given to the groups.

Group: Everyone

```
CommentOnTicket, CreateTicket, ModifySelf, ReplyToTicket
```

Group: Staff

```
CommentOnTicket, OwnTicket, SeeQueue, ShowTicket,
ShowTicketComments, StealTicket, TakeTicket, Watch.
```

The `ModifyTicket` permission is given to the “owner” role for each queue.

Database Backup

The next script performs the MySQL database backup and is executed by the crond daemon in the database server.

```
#!/bin/sh
backupserver=xyz.xnet
date=`date -I`

/usr/bin/mysqldump --flush-logs --opt  --all-databases |gzip -c
> /var/backup/databasebackup-$date.sql.gz
/usr/bin/md5sum /var/backup/databasebackup-$date.sql.gz >
/var/backup/databasebackup-$date.sql.gz.md5
/usr/bin/scp /var/backup/databasebackup-$date.sql.*
$backupserver:/var/backup/
```