Global Information Assurance Certification Paper

GIAC IT Security Audit. Essentials (GSAE) – Practical Assignment version 1.1 Option 1

Contribution of Identity Management to the enterprise security

Soledad Bastías
August 10 2004

Abstract

The identity of a person within an organization has a set of attributes that must be administered during the life cycle of the identity that starts when the person arrives at the enterprise and it ends when the person goes away from it [1]. The management of the digital identity refers to “a group of business processes and an infrastructure that supports the creation, maintenance and use of digital identities”, that helps to mitigate the risks of security inside the enterprises.

The problem of identity management

As long as an organization business processes evolve, its mechanism of communications with its clients and commercial partners develop new and complex set of procedures, systems and applications that allow to support its business processes which are used by a wide range of users and applications within and outside the enterprise.

In general, each component that makes such network, that is to say, communication’s equipment , database, applications and data server, have its own security mechanism that is private or based in a standard, that allows to control the privileges of using such component. This way, each system or individual application implements a form to store users and permissions. Each one of these systems defines in a certain way the identity of the system or user that uses it.

The difficulties that this expansion have produced to users in several systems can be identified. Among them, we can distinguish:

- Information Technology Administrators have had a hard time dealing with the growth of a wide range of management interfaces. The lack of a global view of the users and their capacities within each system, redundancy in their labours (works, jobs) besides a distribution of the knowledge to carry on the administrative duties.

- Users experience less satisfaction in the use of the systems due to the use of different usernames and passwords. The constant reinsertion and its periodic updating drops the use of new systems that are introduced into the organization causing waste of productive time as users have to contact administrators and helpdesk to solve simple troubles such as change of passwords and the creation of new accounts.

- System developers need to integrate a wide range of systems of a different type. For instance: in the developing of a new system they meet the

alternative of using a repository of existing users or create a new one that actually fits the needs of the developing system. If an organization wishes to adopt a more robust authentication mechanism, such as changing user passwords for digital certificates or tokens, that means a high cost in time due to the amount of systems that need to be modified, this could imply that the only way to develop the system should be to reconstruct it completely.

The contribution of identity management and access to information security

When the community of users in an enterprise is in constant growing and change, the effective administration of the access to the resources is the key to maintain critic information safe. An identity management solution must keep the security controlled while lowering administrative cost[2].

Access control

With a comprehensively solution of identity management, TI administrators can instantly check, modify, and audit the privilege access of users and organizations. There is a quick and easy form to determine who has the access to which information, so that the access of certain users can be altered whenever it is necessary.

The ability to maintain an exact record and administer the user' access, has an important role when approving security audits, with the purpose of showing that users only have access to resources to which they need access in order to carry out their duties. In addition a solution must provide flexibility to align business needs and security. This means that the solution must provide the ability to exert control of policies over users, resources, roles and organizations independently of the environment. Only with this level of flexibility a solution can be aligned to the business needs.

Risk control

Solutions must detect proactively potential security risks, such as system accounts without any owner also called orphan accounts, or accounts which are not in compliance with the enterprise security policies, for example accounts with ID and password "guest". It is also critical for the solution to be able to have the ability of detecting changes in the environment and determining if these are legitimate or not. To give testimony of these risks that allow IT administration to act before the security is compromised.

Operational efficiency

Automatic duties

An IM solution that allows to automate most of the common IT processes, no matter how complex they are, associated with the administration of the identity life cycle, reducing the time that the staff requires for the developing of such processes,

permitting the saving of such costs and the dedication of the IT staff to strategic works. That is to say, this solution must provide a significant help in the IT operation, beyond simple tasks of approval associated with the user's creation.

Delegation of responsibilities

In addition to the automation of the administration procedures of the identity life cycle, a good IM system should allow the delegation of administrative responsibilities. From the IT department to the system owners or information users, or other departments or external agents like partners: so that the load of work on the IT administration group can be reduced. This capacity must be of intuitive nature, and possess web based interfaces, available to business users (Human resources, management) so that they can manage the provisioning process.

Creating Self Services

Allowing users to worry about their own administrative requirements, such as password changes, a comprehensive IM system may dramatically reduce the amount of help desk calls. Self Service also permits IT to face big changes within organizations, no matter the amount of users that are incorporated or the quantity of changes produced. According to Gartner, 40% of the number of help desk calls are caused by password changes of latest users[3].

Reasons to implement an IM solution

According to Gartner, there are five reasons that should be taken into account to implement an IM solution in an enterprise , and correspond to Business facilitation, Cost Containment, Operational Efficiency, IT risk management and Regulatory Compliance. These demonstrate that IM is a solution that gives support to the different enterprise units, allowing hundred of thousands of users, that can no longer be administered manually.

Besides technologies used to implement an IM infrastructure permits to reduce operational costs decreasing the numbers help desk calls, for problems of password to users ,among others. It permits to provide an adequate segregation of responsibilities in case of outsourcing among different IT suppliers and the customer.

Without any doubt, one of the mayor contributions of IM, apart from what has already been mentioned corresponds to IT risk management, which provides the security for access control to an enterprise infrastructure. This is daily security requirement that must be considered in administrative activities, auditory, application of security policies for access control to the infrastructure and the fulfilment of the regulatory requirements in use.

The following are the specific items in which IM helps, according to Gartner[4]:

- Audit Management- Obtain audit reports in due time.
- Terminations- End of a person privilege to access information after he has ceased working for the enterprise.

- Policy- based compliance- Implementation and maintenance of policies such as password composition, changes, historical policies, roles and privileges which are centralized in an IM solution.
- Strong Authentication- provides compatibility with robust authentication mechanisms for industries such as health and financing are included in an IM solution.
- Strong audit trail- The importance of log records is a requirement that solves IM solution.

IM technology infrastructure

The term "*secure identity management*"[1][5] is used to describe the convergence of a group of disciplines and technologies that have been involved for years to give an answer to independent problems.

AI infrastructure corresponds to a set of related components, that include business processes as well as technological aspects. Within these business aspects it can be noticed the following areas.

Business processes:

- Administration of the Identity of Users (Identity Management)
- Systems that control the access of users to applications (Access control)
- System of supplying users, privileges and attributes within applications
- (Provisioning)
- Modelling business processes (workflow)

Normally, these business procedures of IM and access control are grouped together with the term " Identity and access management services", and the provisioning and workflow processes are known together as " provisioning."

From a technological point of view there are a variety of platforms that solve business processes in connection with IM solution.

Within the main technological platforms we can distinguish the following:

Technology platform

- Directory servers.
- Meta-directory servers.
- Synchronization password solutions.
- Access control servers and single sign-on.
- Provisioning and De-provisioning.
- Content administration system.
- Web portals.
- Workflow systems.

[1] Roughly equivalent terms from different analyst and vendors include "Identity Management", "Identity and Access Management", "Network Identity" and "Digital Identity"

Leaders and technology of IM

Chart 1 shows the main software suppliers that supply one or more solutions for an IM infrastructure, and chart 2 indicates products offered by every supplier for each requirement of IM solution [2][6].

Supplier	Suite IM	URL
Netegrity	SiteMinder	http://www.netegrity.com
IBM	Tivoli	http://www-306.ibm.com/software/tivoli/solutions/security/id/
Sun	Sun ONE Identity Management Waveset	http://wwws.sun.com/software/product_categories/directory_servers_identity_mgmt.html http://www.waveset.com/
CA	Etrust	http://www3.ca.com/Solutions/SubSolution.asp?ID=4347
RSA	RSA Security	http://www.rsasecurity.com/rsasecuritysolutions/iam/
BEA	BEA Enterprise Security	http://www.bea.com/framework.jsp?CNT=index.htm&FP=/content/products/security

Chart 1: Summary of main manufacturers of IM software products.

Software's Supplier	Access Management	User Management		MetaDirectory and Directory	Authentication
		Provisioning	Password		
Netegrity	Siteminder 6.0	IdentityMinder 5.6 Enterprise Edition	Siteminder 6.0	X	X
IBM	IBM Tivoli Identity Manager 5.1	IBM Tivoli Provisioning Manager 4.5	IBM Tivoli Identity Manager 5.1	IBM Directory Server 5.2	X
Sun	Identity Server 6.1	Waveset Lighthouse Provisioning Manager	Identity Server 6.1 Waveset Lighthouse Password Management	Directory Server 6.0 Metadirectory Server 5.1	X
CA	ETrust Access Control	ETrust Admin	ETrust admin.	ETrust Directory Server 3.6	X
RSA	RSA ClearTrust 5.5	X	X	X	RSA SecureID Passsanger
BEA	BEA Enterprise Security 4.1	X	X	Implementa MetaDirectorio(BEA Enterprise Security 4.1)	X

Chart 2: Summary of main IM products By manufacturers.

Conclusions

IM has become an strategic need to the enterprise[1]. Without any doubt implementing a complete IM solution, requires important efforts to the enterprise ,due to that many of these enterprises have grown without considering the life cycle of an identity, since the number of users allowed an administration and manual control. But at the beginning of relationship with partners, outsourcing of services, increase of internal and external users began to generate important gaps in security.

Given this, IM allows the mitigation of many risks because it manages the lifecycle of a users identity. Since the moment of its creation to its end. Delivering quick audit reports, policy compliance, risk management , and early warning alerts.

The ROI of this type of solutions is justified, because they help reduce security risks, lower operation costs and improve quality of service due to reduced help desk calls, it provides quick integration with new technologies, helps to keep clients and improves productivity. According to Gartner, the cost for identity systems and access administration goes from $5 to 25$ dollars per user. A 10.000 employees company, that automates the provisioning for 12 applications can save around $3.5 millions over 3 years and see a 295% of return of investment[3].

Reference

[1] Jaime Lewis, July 2003, Burton Group.
"Enterprise Identity Management: It's About the Business".
http://www.burtongroup.com/guests/signin.asp?id=142&source=idmbiz13
[2] IBM, International Technical Support Organization. July 2003. "Identity Management Design Guide with IBM Tivoli Identity Manager".
http://publib-b.boulder.ibm.com/Redbooks.nsf/RedbookAbstracts/sg246996.html
[3] George V. Hulme , March 15, 2004, Information Week. "The Need For Identity Management".
http://www.informationweek.com/story/showArticle.jhtml?articleID=18312163
[4] R. Witty, Research Note, Gartner, October 2003. "Five Business Drivers of Identity and Access Management",
[5] ePresence White Paper, 2002 "An introduction to Secure Identity Management"
http://www.u-curve.com/Documents/Intro_to_Secure_Identity_Management_ePresence.pdf
[6] Rutrell Yasin April 2002, Information Security. "What is Identity Management?"
http://infosecuritymag.techtarget.com/2002/apr/cover_casestudy.shtml
[7] Burton Group. "General Recommendations for creating Virtual Enterprise Network (VEN) Security Architecture"
[8]Archie Reed, Rainbow Technologies "The definitive Guide to Identity Management".
http://mktg.rainbow.com/mk/get/bitpipe_idebook

GIAC IT Security Audit. Essentials (GSAE) – Practical Assignment version 1.1
Option 1 – Assignment 2

Auditing a Security Operations Center
Soledad Bastías
August 10 2004

Scope: The purpose of this process is to authorize the security team to perform an audit of the systems and resources of the Security Operations Center (SOC) of Silicon Technology enterprises.

The auditors must supervise the following:

- Ensure the integrity, confidentiality and availability of resources and SOC Systems.
- Identify existing weaknesses associated to physical security and access control.
- Investigate security incidents associated with failure to stay in compliance with security policies.

Objectives: The auditor's team must watch over the following objectives during the audit process:

- Identify the control and classification of assets utilized by the SOC
- Identify physical and enviromental security of the SOC
- Identify any backup procedure used by the SOC
- Identify the group of security policies appliable to SOC and their level of comformity
- Investigate incidents related to unauthorized physical access as well as logical access
- Evaluate the level of patches and hotfixes in the SOC's infrastracture

To achieve this the auditor's team must request documentation associated to policies, standards and procedures applied within the SOC. The audit process must involve different roles and job positions within the SOC, from the SOC Senior Manager to the last Operators.

Checklist

A checklist is described inmediately base don ISO 17799:2000 and BS 7799-2:2002 and must be used by the auditors team for each of the sections to be evaluated.

Ítem: Security Policies The objective of this section is to identify the existance of security policies, documentation, maintenance and applicability of these.	**Yes**	**No**
The security policy is documented and updated. *Objective: To verify the existance of a document that describes the security policies that*		

must be applied. **Auditor Observations:**		
The policy is signed by the enterprise's administration (or equivalent) to indicate administration approval. *Objective:To verify administration support to policy.* **Auditor Observations:**		
The policy is written in a clear way and summarized. **Objective:To verify that the policy is clear to be understood by the final user.** **Auditor Observations:**		
All the envolved personnel (staff) knows the exitence of the document referring to policies. *Objective:If it has existed internal difusión of the document referring o security policies.* **Auditor Observations:**		
The policy indicates the use and administration of accounts and passwords ***Objective:*** **Identify if there are policies associated to the use and management of passwords.** **Auditor Observations:**		
The policy indicates how incidents of security will be reported and the channels for that. **Objective: Identify if there is a structure in the organization with identified responsable to inform security incidents and if these are known.** **Auditor Observations:**		
The policy indicates how should control access to facilities be handled *Objetive: To verify that exists a policy that controls access to by authorized personnel to facilities within the organization.* **Auditor References:**		
The policy indicates that the personnel will receive training according to the job they perform. *Objective: To verify the existence and compliance with a policy that indicates security training for the personnel.* **Auditor observation:**		
Ítem: Asset Control and Classification Determine the existance of an assets inventory (Software, Hardware, Information, among others) where it is identified the owner, location, security classification and an identifier. *Objective: To identify the existance of an inventory of assets where its recorded its owner, security classification, location and verification of the information.* *Auditor observations:*		
1.- Manteinance for the inventory is contemplated for all information assets. *Objective: To verify that the inventory is updated verifiying the information of the assets present in the inventory.* **Auditor observations:**		

2.- There is a classification for the security of information *Objective: To verify the existance of a security classification, written and approved.* **Auditor observations:**		
3.- Information assets have been assigned a security classification *Objective: To verify that information assets have a security classification that is known and applied.* **Auditor Observation:**		
4.-This security classifications are reviewed with the security senior manager or equivalent. *Objetive: To verify that security classifications are known and approved by the security senior manager or equivalent.* **Auditor observations:**		
5.- Information is labeled according to their security level. *Objetive: To verify that information is labeled according to their classification level of existing information.* **Auditor observations:**		
Item: Physical and Enviromental Security Identify the eficiency of implemented controls regarding physical and enviromental security, identifying access controls, location, doors security, fire controls.		
1.- Information assets are located in an enviroment that has a security perimeter. *Objective: To verify that information assets are located and protected by a security perimeter, according to their level of security.* **Auditor observations:**		
2.- The security perimeter is in compliance with the objective of preventing unathorized access. *Objective: To verify the existance of controls mechanisms in the security perimeter that prevents unathorized access to facilities.* **Auditor observations:**		
3.- The security perimeter is consistent with the risks associated to the assets. *Objective: To verify that the security perimeter has apropiate controls according to the assets that secures.* **Auditor observations:**		
4.- Access to activities within the security perimeter is restricted in a need to have basis. *Objective: To verify that only authorized personnel has access within the perimeter* **Auditor observations:**		
5.- A physical device (Example: key, card) is required at the access control besides something he knows (PIN, Password). *Objective: To verify the existance of an access control that protects the entrance within the security perimeter to prevent unauthorized access.*		

Auditor observations:		
6.- There are procedures to control unauthorized access to facilites *Objective: To verify the existance of procedures that indicate how should personnel colaborate to prevent or detect unauthorized access.* **Auditor observations:**		
7.- SOC personnel is aware of this access control procedures *Objective: Verify that SOC personnel knows and uses these existing access control procedures.* **Auditor observations:**		
8.- SOC visitors are supervised within the perimeter at all times. *Objective: Verify that SOC visitors within the perimeter are supervised at all times by a person belonging to the enterprise and proper authorization has been issued.* **Auditor observations:**		
9.- Information servers are located away from public access places and/or roadways *Objective: Verify that the processing center is located away from public access places or roadways that represent a risk to instalation security.* **Auditor observations:**		
10.- Dangerous materials or fuels are kept outside the data center or servers room. *Objective: Verify that there is no flammable material either within or outside the data center, such as paper, or any other flammable material.* **Auditor observations.:**		
11.- It is forbidden to smoke, eat or drink in locations that possess technology equipment. *Objective: Verify that activities that can damage or affect equipment inside locations that contain tecnology equipment are not carried out. Example smoking, drinking, eating.* **Auditor observations:**		
12.- If the equipments performs critical business process, is it protected by a uninterrumped power suply (UPS)? *Objetive: To verify that in case of power supply interruption there are power sources available that ensures operational continuity.* **Auditor observations.:**		
13.- UPS are available to workstations for operators or end users *Objective: Verify that if there are UPS in the system, this is available to workstations.* **Auditor observations:**		
14.- Communication and electricity wires are installed in separated panels. *Objective:To verify that there is proper separation of communication wires and electricity.* **Auditor observations::**		
15.- All storage media is wiped before being reused. *Objective: Verify thatstorage media, such as CDRW, Hard Disks, Diskettes are wiped by reliable procedures before they are reused.* **Auditor observations::**		

16.- Information chosen for deletion is destroyed by reliable means. (paper grinder, media destruction). *Objective:Verify that media and disposed information is destroyed by reliable means to ensure that it cannot be reassembled.* **Auditor observations::**		
17.- It exists a policy of clean desktop and screen. *Objetive: Verify that confidential documents are not left on operators desktops and workstations are locked when left unattended.* **Auditor observations::**		
Item: Communication and Operations Management Corresponds to verify the existence of procedures that watch over proper operational enviroment, including operational changes, incident report, capacity planning, information back up and system maintenance.		
1.- There is existence of procedures for the operation of all systems and procesess. *Objective: Identify procedures that indicate the workings and operation for the existing systems.* **Auditor observations::**		
2.- There is existence of procedures for databases administration. *Objective: Verify the existence of procedures for the administration of databases.* **Auditor observations::**		
3.- It exists procedures of restoration and restart of systems *Objective: Verify the existence of processes that indicate the steps required to restore the systems and its restart.* **Auditor observations:**		
4.- It exists procedures for equipment maintenance *Objective: Verify the existence of procedures that indicate how equipment maintenance should be done for the different equipments.* **Auditor observations::**		
5.- There are documented procedures for change control. *Objective:Verify the existence of a change control procedure, that watches over changes, teir impact and level of importance to the business operational continuity.* **Auditor observations:**		
6.- There are documented procedures for configuration back up for the equipments. *Objective:Verify the existence of configuration backups for the SOC's equipments.* **Auditor observations::**		
7.- There are documented procedures to handle malicius software *Objective:Identify the existence of procedures and tools that allow to control malicius software (computer virus, worm, troyans)* **Auditor observations:**		
8.- There are documented procedures to report security incidents		

Objectives: Identify procedures that indicate which are the formal channels to report a security incident. **Auditor observations::**		
9.- Capacity planning is done for all information systems and assets. *Objetivo: Identify the existence of capacity planning focused on operational continuity.* **Auditor observations:**		
10.- There are documented procedures that allow early detection of computer viruses, so as to prevent network infection. *Objective: Identify which are the procedures and/or tools that allow to detect viruses or to protect the network from malicius software.* **Auditor observations:**		
11.- There are controls to mitigate risks associated to files downloaded from internet or other external source. *Objective: Identify controls mechanisms for downloading and installation of files tools from Internet by the end users.* **Auditor observations:**		
12.- There are documented procedures for virus pattern update. *Objective: Identify which is the procedure for actualization of virus pattern, whether it is manual or automatic.* **Auditor observations:**		
13.- There are documented procedures that addresses the potential risk of infections *Objective: Identify procedures that indicate which are the steps to perform in case of an infection by malicius software.* **Auditor observations:**		
14.- Policy for information backup is aligned with business operational continuity and contingency recovery. *Objective:Identify wether back ups are performed according to policy for contingency and operational continuity planning.* **Auditor observations:**		
15.- The back up procedure indicates how backup should be labeled and where should back ups be stored. *Objective: Verify that there is a documented procedure that indicates how backups should be labeled , and where should them be contained.* **Auditor observations::**		
16.- Back ups are stored in a physical place away from the site. *Objective: Verify that back ups exists on site and off site to maintain availability of these in case of emergency or contingency of systems on site.* **Auditor observations:**		
17.- Back up inventory is frequently updated *Objective: Verify the existence of a backup inventory that identifies backup type, date and operator that performed the data.* **Auditor observations:**		

18.- There are documented procedures for the destruction of backups that are no longer needed. *Objetive: Verify the existence of procedures that allow a reliable destrucction of backups that are no longer neccesary.* **Auditor observations:**		
19.- Audit registers of operations are kept for the diferent systems and SOC assets. *Objective: Verify that working systems within the SOC are generating audit records.* **Auditor observations:**		
20.- There are procedures that ensure that remote conections are confidential (VPN) *Objective: Verify that methotds are used in order to protect confidenciality of remote conections.* **Auditor observations:**		
21.- There are procedures that include apropiate controls for conections through public networks, telefony, or others where there is no control. *Objective:Verify that there is controls that watch over the integrity of confidenciality of the information que goes through public networks.* **Auditor observations:**		
22.- Among the different processes are included devices such as Firewalls, IDS, IPS in case they are needed. *Objective: Verify the existence of security devices in the enterprise network.* **Auditor observations:**		

To check the level of patches in the SOC's workstations, a Windows Security Scoring Tool will be used. This tool is based in the analysis of four categories: Service packs and hotfixes, Policies, Security Settings and available services, User Rights, File and Registry permissions, and other systems requirements. Each of these 4 categories has a score of 2.5 and add a total score of 10. This tool is used with templates that match each version of Microsoft Operative System and is included in the auditory report.

Below is shown the report which contains the results of applying the checklist and the obsevations made by the auditor.

Report

The checklist was applied to the SOC's Chief as well as to the security analist. Below is given a set of observations of each of the sections outlined in the checklist that guided the audit process.

From the section of security policies, is concluded that it exists a document of security policies, that has sections concerning Policies, Access Control, Classification and Assets Control, Organizational Security, Personal Security, Physical Security, communications and operations management. This document was delivered to the

SOC personnel at the beginning of their job labours, but it is not entirely applied because of lack of procedures associated with the policies and lack of control over the compliance to policies. This document has not been updated since its creation and is not signed by the unit's manager which would allow to give support in demostration of the organization commitment to this set of policies.

From the section Asset Control and Classification, it is concluded that there is no existance of any type of documentation regarding the identification of the SOC's assets (Inventory), nor exists any classification of security for them. However it is important to mention that exists a policy that indicates how the control and classification of the assets should be handled, besides it exists a guide of security clasification of information, that is not applied due to a lack of knowledge of its existance by the operators and the SOC's Chief.

From the section of physical and enviromental security it is concluded that exists a group of controls oriented to protect leaks of information, control prevention of unathorized access, control protection of assets within the SOC's perimeter, existance of a biometric access control and defined procedures for visitors to the site. The only weakness in the defined policies is that there is no physical means for the destruction of documentation and reports. No papers are used within the SOC, thus it is not neccessary any equipment that allows the secure destruction of this.

From the section Administration of communications and operations, there is existance of procedures for the maintenance of equipments, for the restauration and restart of these. However there are no procedures for the administration of databases, or procedures that indicate when, how and where should back ups be made and stored and for which devices should be made; this is a SOC main weakness regarding the administration of communications and operations. Other important subject is capacity planning that actually is not carried out, even if there is a specified policy that indicates that these must be fullfilled for the diferent systems.

From what has been revised in the SOC, it is recommended to perform a better spreading and capacitation of the security policies, and the implementation of procedures for the effective application of these, incorporating senior administration approval. Besides it is important to make an inventory of assets with its respective classification of security, identifying its levels of importance for its operation, so as to the implement adequate controls for its protection. Besides it is recomended to fulfil the procedures regarding to capacity planning, back up, operation and administration of the data base systems and others that do not have this.

Regarding the patches and hot fixes of the Workstation, it is concluded that the workstations have a score of 2.5 in 80% of the machines, which means that they are updated with its patches and only 20% has a score of 1.25 which indicates a lack of updates and hotfixes, The scoring tool evaluates other items apart from patches and hotfixes which were delivered to Silicon technology so as to make improvements towards the other items and raise the level of security of the workstations. It was recomended to execute the scoring tool in a periodic way so as to detect possible risks of security due to the no aplication of patches and hotfixes.

In the Appendix A, the checklist is included with the global result got from the audit process.

References

- 2003, "The Audit Process, Customer Surveys", http://www.auditnet.org/survey.htm
- 2004, Windows Security Scoring tool, http://www.cisecurity.org/bench_win2000.html
- Sans, 2003, "Security Auditing: A Continuous Process", http://www.sans.org/rr/papers/index.php?id=1150
- BSI, 2002, BS 7799-2, “Specification for information security Management Systems”
- ISO/IEC 17799, 2000, “Information Technology: Code of Pratice for information security management”
- 2003, Internet Security Forum, “The Standard of Good Practice for Information Security”, http://www.isfsecuritystandard.com/index_ie.htm

Appendix A

Ítem: Security Policies The objective of this section is to identify the existance of security policies, documentation, maintenance and applicability of these.	Yes	No
The security policy is documented and updated. *Objective: To verify the existance of a document that describes the security policies that must be applied.* **Auditor Observations: It's documented but not updated.**	X	
The policy is signed by the enterprise's administration (or equivalent) to indicate administration approval. *Objective:To verify administration support to policy.* **Auditor Observations:**		X
The policy is written in a clear way and summarized. **Objective:To verify that the policy is clear to be understood by the final user.** **Auditor Observations: The policy is clear but not summarized.**		X
All the envolved personnel (staff) knows the exitence of the document referring to policies. *Objective:If it has existed internal difusión of the document referring o security policies.* **Auditor Observations:**	X	
The policy indicates the use and administration of accounts and passwords ***Objective:*** **Identify if there are policies associated to the use and management of passwords.** **Auditor Observations:**		X
The policy indicates how incidents of security will be reported and the channels for that. **Objective: Identify if there is a structure in the organization with identified responsable to inform security incidents and if these are known.** **Auditor Observations:**		X
The policy indicates how should control access to facilities be handled *Objetive: To verify that exists a policy that controls access to by authorized personnel to facilities within the organization.* **Auditor References:**	X	
The policy indicates that the personnel will receive training according to the job they perform. *Objective: To verify the existence and compliance with a policy that indicates security training for the personnel.* **Auditor observation: There is no knowledge of its existence**		X

Ítem: Asset Control and Classification Determine the existance of an assets inventory (Software, Hardware, Information, among others) where it is identified the owner, location, security classification and an identifier. *Objective: To identify the existance of an inventory of assets where its recorded its owner, security classification, location and verification of the information.* *Auditor observations:*		
1.- Manteinance for the inventory is contemplated for all information assets. *Objective: To verify that the inventory is updated verifiying the information of the assets present in the inventory.* **Auditor observations:**		X
2.- There is a classification for the security of information *Objective: To verify the existance of a security classification, written and approved.* **Auditor observations:**		X
3.- Information assets have been assigned a security classification *Objective: To verify that information assets have a security classification that is known and applied.* **Auditor Observation:**		X
4.-This security classifications are reviewed with the security senior manager or equivalent. *Objetive: To verify that security classifications are known and approved by the security senior manager or equivalent.* **Auditor observations: 90% are labeled approximately**		X
5.- Information is labeled according to their security level. *Objetive: To verify that information is labeled according to their classification level of existing information.* **Auditor observations:**		X
Item: Physical and Enviromental Security Identify the eficiency of implemented controls regarding physical and enviromental security, identifying access controls, location, doors security, fire controls.		
1.- Information assets are located in an enviroment that has a security perimeter. *Objective: To verify that information assets are located and protected by a security perimeter, according to their level of security.* **Auditor observations:**	X	
2.- The security perimeter is in compliance with the objective of preventing unathorized access. *Objective: To verify the existance of controls mechanisms in the security perimeter that prevents unathorized access to facilities.* **Auditor observations:**	X	
3.- The security perimeter is consistent with the risks associated to the assets. *Objective: To verify that the security perimeter has apropiate controls according to the assets that secures.*	X	

Auditor observations:		
4.- Access to activities within the security perimeter is restricted in a need to have basis. *Objective: To verify that only authorized personnel has access within the perimeter* **Auditor observations:**	X	
5.- A physical device (Example: key, card) is required at the access control besides something he knows (PIN, Password). *Objective: To verify the existance of an access control that protects the entrance within the security perimeter to prevent unauthorized access.* **Auditor observations:**	X	
6.- There are procedures to control unauthorized access to facilites *Objective: To verify the existance of procedures that indicate how should personnel colaborate to prevent or detect unauthorized access.* **Auditor observations:**		X
7.- SOC personnel is aware of this access control procedures *Objective: Verify that SOC personnel knows and uses these existing access control procedures.* **Auditor observations:**	X	
8.- SOC visitors are supervised within the perimeter at all times. *Objective: Verify that SOC visitors within the perimeter are supervised at all times by a person belonging to the enterprise and proper authorization has been issued.* **Auditor observations:**	X	
9.- Information servers are located away from public access places and/or roadways *Objective: Verify that the processing center is located away from public access places or roadways that represent a risk to instalation security.* **Auditor observations:**	X	
10.- Dangerous materials or fuels are kept outside the data center or servers room. *Objective: Verify that there is no flammable material either within or outside the data center, such as paper, or any other flammable material.* **Auditor observations.:**		X
11.- It is forbidden to smoke, eat or drink in locations that possess technology equipment. *Objective: Verify that activities that can damage or affect equipment inside locations that contain tecnology equipment are not carried out. Example smoking, drinking, eating.* **Auditor observations:**	X	
12.- If the equipments performs critical business process, is it protected by a uninterrumped power suply (UPS)? *Objetive: To verify that in case of power supply interruption there are power sources available that ensures operational continuity.* **Auditor observations.:**	X	
13.- UPS are available to workstations for operators or end users	X	

Objective: Verify that if there are UPS in the system, this is available to workstations. **Auditor observations:**		
14.- Communication and electricity wires are installed in separated panels. *Objective:To verify that there is proper separation of communication wires and electricity.* **Auditor observations::**	X	
15.- All storage media is wiped before being reused. *Objective: Verify thatstorage media, such as CDRW, Hard Disks, Diskettes are wiped by reliable procedures before they are reused.* **Auditor observations: Media are not used**		
16.- Information chosen for deletion is destroyed by reliable means. (paper grinder, media destruction). *Objective:Verify that media and disposed information is destroyed by reliable means to ensure that it cannot be reassembled.* **Auditor observations: There is no equipment to grind the documents that must be eliminated**		X
17.- It exists a policy of clean desktop and screen. *Objetive: Verify that confidential documents are not left on operators desktops and workstations are locked when left unattended.* **Auditor observations::**	X	
Item: Communication and Operations Management Corresponds to verify the existence of procedures that watch over proper operational enviroment, including operational changes, incident report, capacity planning, information back up and system maintenance.		
1.- There is existence of procedures for the operation of all systems and procesess. *Objective: Identify procedures that indicate the workings and operation for the existing systems.* **Auditor observations: There are Procedures for 50% of the systems approximately**	X	
2.- There is existence of procedures for databases administration. *Objective: Verify the existence of procedures for the administration of databases.* **Auditor observations::**		X
3.- It exists procedures of restoration and restart of systems *Objective: Verify the existence of processes that indicate the steps required to restore the systems and its restart.* **Auditor observations: They exist but must be improved, because some systems lack important steps to complete the procedure.**	X	
4.- It exists procedures for equipment maintenance *Objective: Verify the existence of procedures that indicate how equipment maintenance should be done for the different equipments.* **Auditor observations::**		X
5.- There are documented procedures for change control. *Objective:Verify the existence of a change control procedure, that watches over changes,*		X

teir impact and level of importance to the business operational continuity. **Auditor observations:**		
6.- There are documented procedures for configuration back up for the equipments. *Objective:Verify the existence of configuration backups for the SOC's equipments.* **Auditor observations: They exist but not for all the equipment, approximately are backuped 40% of the equipment**	X	
7.- There are documented procedures to handle malicius software *Objective:Identify the existence of procedures and tools that allow to control malicius software (computer virus, worm, troyans)* **Auditor observations:**	X	
8.- There are documented procedures to report security incidents *Objectives: Identify procedures that indicate which are the formal channels to report a security incident.* **Auditor observations::**		X
9.- Capacity planning is done for all information systems and assets. *Objetivo: Identify the existence of capacity planning focused on operational continuity.* **Auditor observations:**		X
10.- There are documented procedures that allow early detection of computer viruses, so as to prevent network infection. *Objective: Identify which are the procedures and/or tools that allow to detect viruses or to protect the network from malicius software.* **Auditor observations:**	X	
11.- There are controls to mitigate risks associated to files downloaded from internet or other external source. *Objective: Identify controls mechanisms for downloading and installation of files tools from Internet by the end users.* **Auditor observations:**		X
12.- There are documented procedures for virus pattern update. *Objective: Identify which is the procedure for actualization of virus pattern, whether it is manual or automatic.* **Auditor observations:**	X	
13.- There are documented procedures that addresses the potential risk of infections *Objective: Identify procedures that indicate which are the steps to perform in case of an infection by malicius software.* **Auditor observations: The procedure is automatic**		X
14.- Policy for information backup is aligned with business operational continuity and contingency recovery. *Objective:Identify wether back ups are performed according to policy for contingency and operational continuity planning.* **Auditor observations:**		X
15.- The back up procedure indicates how backup should be labeled and		X

where should back ups be stored. *Objective: Verify that there is a documented procedure that indicates how backups should be labeled , and where should them be contained.* **Auditor observations::**		
16.- Back ups are stored in a physical place away from the site. *Objective: Verify that back ups exists on site and off site to maintain availability of these in case of emergency or contingency of systems on site.* **Auditor observations:**		X
17.- Back up inventory is frequently updated *Objective: Verify the existence of a backup inventory that identifies backup type, date and operator that performed the data.* **Auditor observations:**		X
18.- There are documented procedures for the destruction of backups that are no longer needed. *Objetive: Verify the existence of procedures that allow a reliable destrucction of backups that are no longer neccesary.* **Auditor observations:**		X
19.- Audit registers of operations are kept for the diferent systems and SOC assets. *Objective: Verify that working systems within the SOC are generating audit records.* **Auditor observations:**	X	
20.- There are procedures that ensure that remote conections are confidential (VPN) *Objective: Verify that methotds are used in order to protect confidenciality of remote conections.* **Auditor observations:**	X	
21.- There are procedures that include apropiate controls for conections through public networks, telefony, or others where there is no control. *Objective:Verify that there is controls that watch over the integrity of confidenciality of the information que goes through public networks.* **Auditor observations:**	X	
22.- Among the different processes are included devices such as Firewalls, IDS, IPS in case they are needed. *Objective: Verify the existence of security devices in the enterprise network.* **Auditor observations:**	X	