Information Security Management System (ISO/IEC 17799)
For a Hosted SAP System

Bryant Carter

Submitted November 7, 2004

G7799 Version 1.1
Orlando, FL April 2004

Table of Contents

Define the System

Project Summary

This paper covers the development of an Information Security Management System (ISMS) for an SAP outsourcer (refer to here within as the Company) based in the US. The initial ISMS will cover the standard SAP hosted solution, which consist of the data center facilities, hardware, SAP software, Oracle database and networking within the data center.

The concept and vision of the Company is to provide a trusted system upon which a customer can leverage and host their SAP data in a secure and controlled manner. To this end, the Company strategy is to build a solid basic SAP solution that has been independently verified for security and control. This consists of conducting SAS 70 Type II Service Auditors Report, maintaining their ISO 9001 Quality Certification and obtaining their BS 7799 Certification.

Overview of the Company

The Company is an SAP outsourcer in the US. It has approximately 260 employees and three primary data centers serving many US and Canadian customers. The three data centers are located in the US South, US Northeast and US West Coast. The Company provides a wide range of reliable, secure, high-performance outsourced application solutions for SAP. The Company supports both fully hosted and remotely managed environments. Additional services include Security Administration and Disaster Recovery.

The Company's SAP service offerings are designed to provide customers flexibility to meet their availability, performance, security and risk management needs.

Full hosted and managed SAP solutions - A managed SAP environment including hardware, software, 24x7x365 help-desk support, networking services and application management.

Remotely Managed Operation - Remote management of a SAP application in customer's data center by our experience staff.

Security Administration Services - Administration of customer level SAP security activities, including User Administration and Profile Administration.

Disaster Recovery – Several disaster recovery options are available, from standard business continuity service to customized solutions for individual application environments.

Hosted Environment History and Future

The hosted environment has been in existence for several years serving many companies. Customers have been demanding more security and controls of their environment over the last five years. This is due to a general concern for security and more recent years, privacy and Sarbanes-Oxley. As a result, management has decided to pursue 7799 certification as well as maintain the annual SAS 70 reports and ISO 9001 Quality Certification. In the future, approximately in CY 2006, BS 15000 (IT Service Management) certification will be pursued. This overall plan will provide the Company and their customers with the proper confidence, security and control they demand and expect.

Phased Approach to Complete Certification

Phase I

In the first phase, within the fully hosted and managed SAP service at the US South, the physical environment, facilities, hardware, software (OS, Middleware and Application software), and help desk support will be within the scope of the ISMS.

Phase II

In the second phase, add the other two data centers (US Northwest and US West Coast) to the ISMS scope. This will require that the differences at the policy, standards and work instructions level be understood and resolved. Additionally, enhance the contract language to cover BS 7799 certification.

Phase III

In the third phase, full networking services (Data Center to Customers), application management and Remotely Managed Operation will be added to the ISMS scope.

Phase IV

In the fourth phase, Disaster Recovery and Security Administrative Services will be added to the ISMS scope.

Phase V

In the fifth phase, the Company will leverage from their work from ISO 9001 and BS 7799 to pursue and obtain BS 15000 (IT Service Management) Certification.

System Description

The US South Data Center is owned and managed by the Company. Facilities management is controlled by the Company, however, some facility task are outsourced to a 3rd party vendor. Physical security is outsourced to a 3rd party security firm. The Company sets the policies and standards for physical security, and is carried out by the 3rd party security firm. The Data Center consists of 200,000 sq ft of floor space, and is separated into a staging area for the receiving and setup of new equipment, a production environment and a development environment. There is also customer demo area that is separated from all other areas. Customer can request a caged area to separate their systems from other customers. The data center is separate into two security zones. The first is a customer zone in which screened customers can access. This is limited to the customer demo area and escorted access to the customers systems. The other zone is referred to as the protected zone, and consists of all non customer zone area. The protected zone is further protected via access control and access is only granted with a need to know or access. Access is controlled by the Physical Security Manager.

The Standard SAP environment consists of standard SAP build on both UNIX and Windows with Oracle as the database. The operating systems, database and SAP Basis are only access on a need to know bases with unique identification and authentication.

Current State of Security

Through the years, the company has created several documents that support the security of the environment. These documents are:

- Ethics and privacy training documents which describe the ethical behavior that is expected when dealing with fellow colleagues, customers, vendors and business partners. Additionally, it describes the privacy policy for company personal data and customer data.

- Service and system security architecture and design documents that describe the security that must be designed into all services and systems.

- Information security policies, standards and requirements that describe the baseline security requirements that must be implemented to obtain company and/or customer acceptable levels of risk.

- Operating procedures and work instructions that describe the procedures and instructions that must be followed so that assets (company and customers) are protected according to security policy.

- Business continuity plans that describe the steps to be followed to minimize the impact of disruptions to company and customer assets.

Although these documents are very good content wise, they could be organized better, and deployed in a consistent and uniform manner.

The ISMS will be used to identify gaps, as well as to organize and strengthen the above documents, and help to ensure they are deployed and implemented in a consistent, uniform and predictable manner.

There are a number of staff members that perform security related work, but very few have security as part of there job title. There is a IS Security Manager, but no formal security organization. Currently, the IS Security Manager uses his influence to get a majority of the security related work done.

ISMS Project Plan (PDCA – Plan)

Project Objectives

The main objectives in the development of the ISMS are the following:

1. Formalize the security organization and security practices into an Information Security Management System by using ISO 17799 as the framework.
2. Leverage the work completed from previous SAS 70 and ISO 9001 work.
3. Start small by implementing ISMS for Full Hosted and Managed SAP Solutions; providing protection for the critical assets.
4. Integrated other SAP services into ISMS over the next two years.
5. Once all services are integrated into the ISMS, leverage SAS 70, ISO 9001 and 7799 work for BS 15000 (IT Service Management) Certification.

Steps used for the ISMS development

Before the ISMS can be developed, a presentation to management for support, sponsorship and funding took place. The team was formulated and a team charter and roles and responsibilities (RACI chart) were developed.

The high level phases of the plan were developed with a focus on internal and external (customer) requirements. An ISO 17799 consultant was selected, ground rules for the consultant established, RACI chart was updated and project plans discussed with the team and consultant.

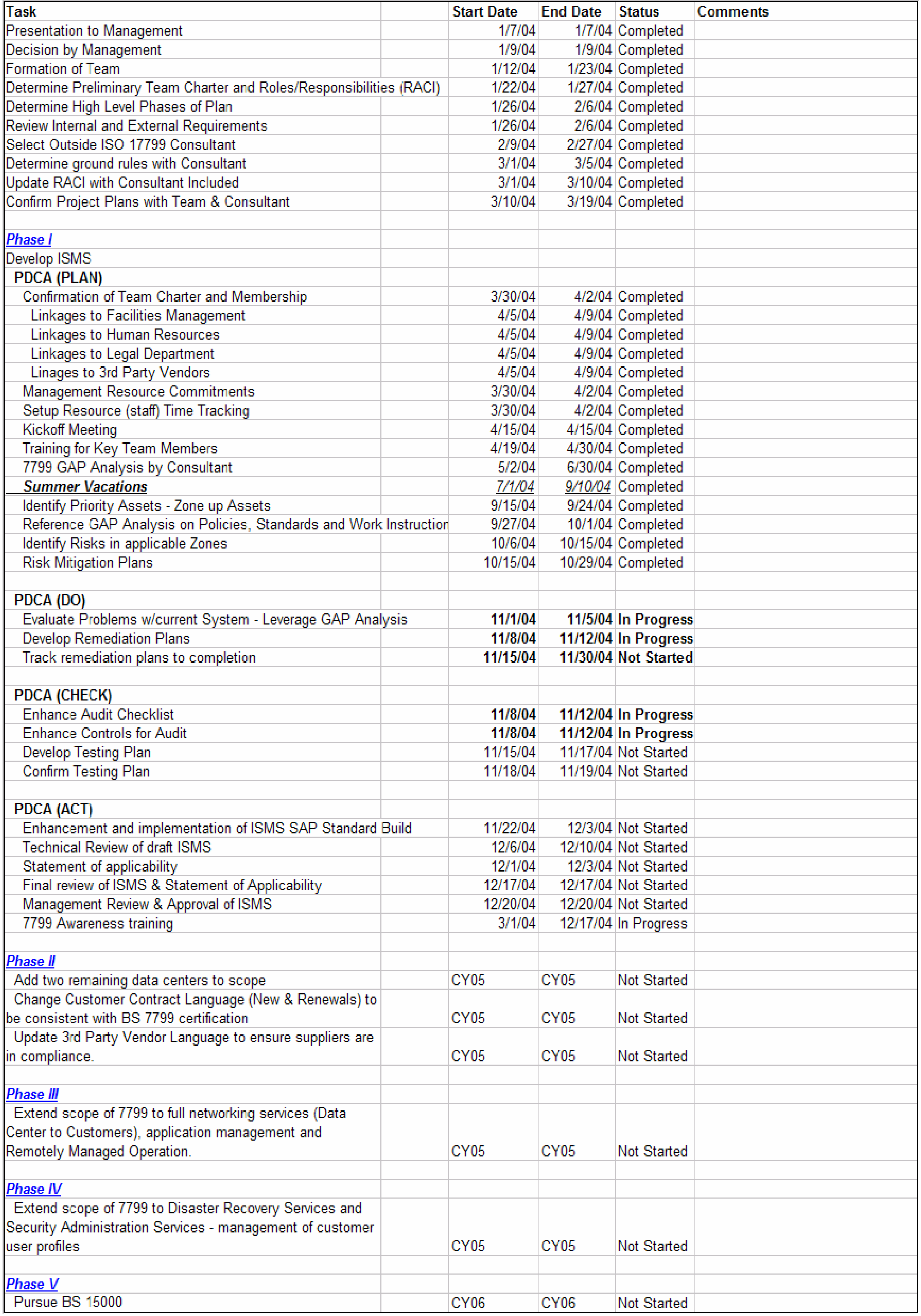
The ISMS development process is driven by the identification of assets and a risk assessment. The identification of assets identified the critical assets to consider for the ISMS. This is a process that has occurred in the past for the Company, but it has been done in an informal manner. The identification of assets has been formalized.

The risk assessment identified the main risks to the identified assets involved in the standard SAP system. Controls were identified to mitigate the risks. The security policy and standards, as well as the management structure for the ISMS was improved and enhanced.

Once the baseline ISMS for Fully Hosted and Managed SAP Solutions is in place, the other phases can be integrated into the ISMS.

Project Plans

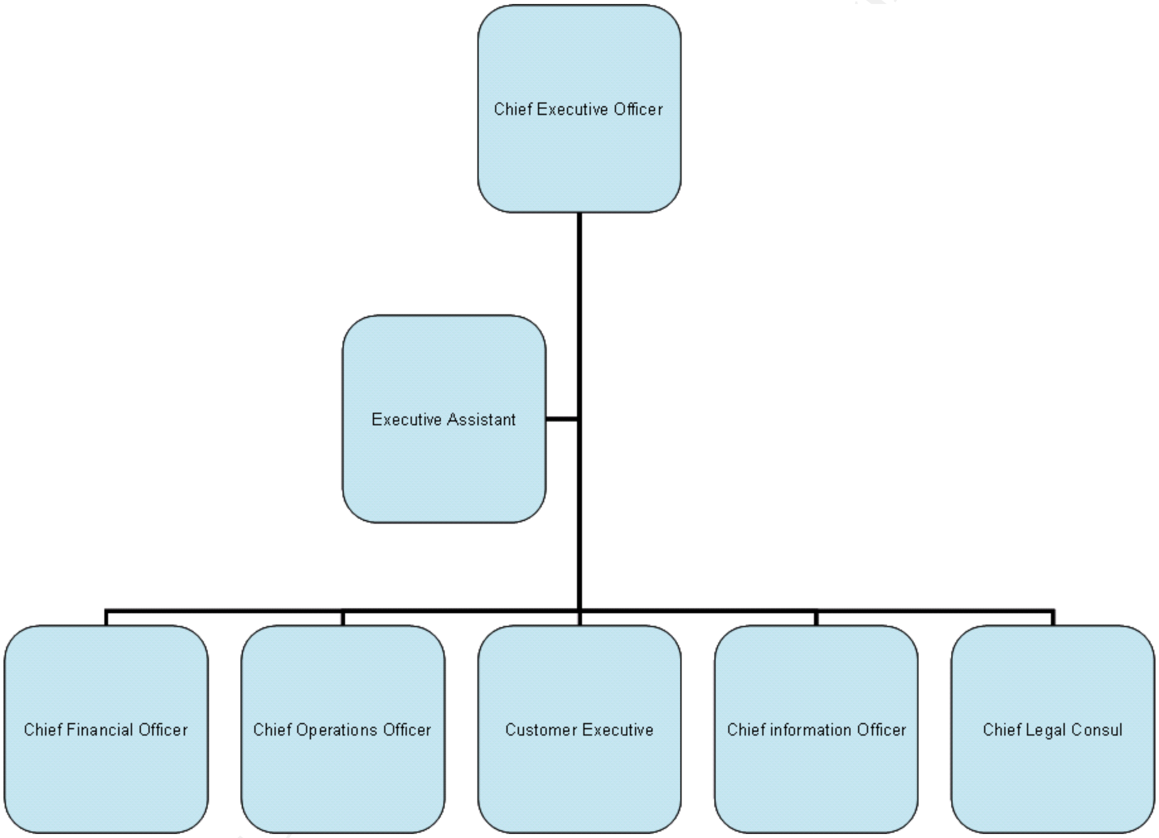
The details of the project plans follow:



Task	Start Date	End Date	Status	Comments
Presentation to Management	1/7/04	1/7/04	Completed	
Decision by Management	1/9/04	1/9/04	Completed	
Formation of Team	1/12/04	1/23/04	Completed	
Determine Preliminary Team Charter and Roles/Responsibilities (RACI)	1/22/04	1/27/04	Completed	
Determine High Level Phases of Plan	1/26/04	2/6/04	Completed	
Review Internal and External Requirements	1/26/04	2/6/04	Completed	
Select Outside ISO 17799 Consultant	2/9/04	2/27/04	Completed	
Determine ground rules with Consultant	3/1/04	3/5/04	Completed	
Update RACI with Consultant Included	3/1/04	3/10/04	Completed	
Confirm Project Plans with Team & Consultant	3/10/04	3/19/04	Completed	
Phase I				
Develop ISMS				
PDCA (PLAN)				
Confirmation of Team Charter and Membership	3/30/04	4/2/04	Completed	
Linkages to Facilities Management	4/5/04	4/9/04	Completed	
Linkages to Human Resources	4/5/04	4/9/04	Completed	
Linkages to Legal Department	4/5/04	4/9/04	Completed	
Linages to 3rd Party Vendors	4/5/04	4/9/04	Completed	
Management Resource Commitments	3/30/04	4/2/04	Completed	
Setup Resource (staff) Time Tracking	3/30/04	4/2/04	Completed	
Kickoff Meeting	4/15/04	4/15/04	Completed	
Training for Key Team Members	4/19/04	4/30/04	Completed	
7799 GAP Analysis by Consultant	5/2/04	6/30/04	Completed	
Summer Vacations	*7/1/04*	*9/10/04*	Completed	
Identify Priority Assets - Zone up Assets	9/15/04	9/24/04	Completed	
Reference GAP Analysis on Policies, Standards and Work Instructior	9/27/04	10/1/04	Completed	
Identify Risks in applicable Zones	10/6/04	10/15/04	Completed	
Risk Mitigation Plans	10/15/04	10/29/04	Completed	
PDCA (DO)				
Evaluate Problems w/current System - Leverage GAP Analysis	**11/1/04**	**11/5/04**	**In Progress**	
Develop Remediation Plans	**11/8/04**	**11/12/04**	**In Progress**	
Track remediation plans to completion	**11/15/04**	**11/30/04**	**Not Started**	
PDCA (CHECK)				
Enhance Audit Checklist	**11/8/04**	**11/12/04**	**In Progress**	
Enhance Controls for Audit	**11/8/04**	**11/12/04**	**In Progress**	
Develop Testing Plan	11/15/04	11/17/04	Not Started	
Confirm Testing Plan	11/18/04	11/19/04	Not Started	
PDCA (ACT)				
Enhancement and implementation of ISMS SAP Standard Build	11/22/04	12/3/04	Not Started	
Technical Review of draft ISMS	12/6/04	12/10/04	Not Started	
Statement of applicability	12/1/04	12/3/04	Not Started	
Final review of ISMS & Statement of Applicability	12/17/04	12/17/04	Not Started	
Management Review & Approval of ISMS	12/20/04	12/20/04	Not Started	
7799 Awareness training	3/1/04	12/17/04	In Progress	
Phase II				
Add two remaining data centers to scope	CY05	CY05	Not Started	
Change Customer Contract Language (New & Renewals) to be consistent with BS 7799 certification	CY05	CY05	Not Started	
Update 3rd Party Vendor Language to ensure suppliers are in compliance.	CY05	CY05	Not Started	
Phase III				
Extend scope of 7799 to full networking services (Data Center to Customers), application management and Remotely Managed Operation.	CY05	CY05	Not Started	
Phase IV				
Extend scope of 7799 to Disaster Recovery Services and Security Administration Services - management of customer user profiles	CY05	CY05	Not Started	
Phase V				
Pursue BS 15000	CY06	CY06	Not Started	

Organizational Structure and Responsibilities

The Company organization structure and responsibilities (in relationship to the Company ISMS) follow:



Chief Executive Officer (CEO) - The CEO is responsible for the operation, management and execution-to-plan for the entire company. The CEO reports to the Company's Board of Directors. The CEO along with the IT Security Manager and CIO will have final approval authority of all security related purchases and new employee hires.

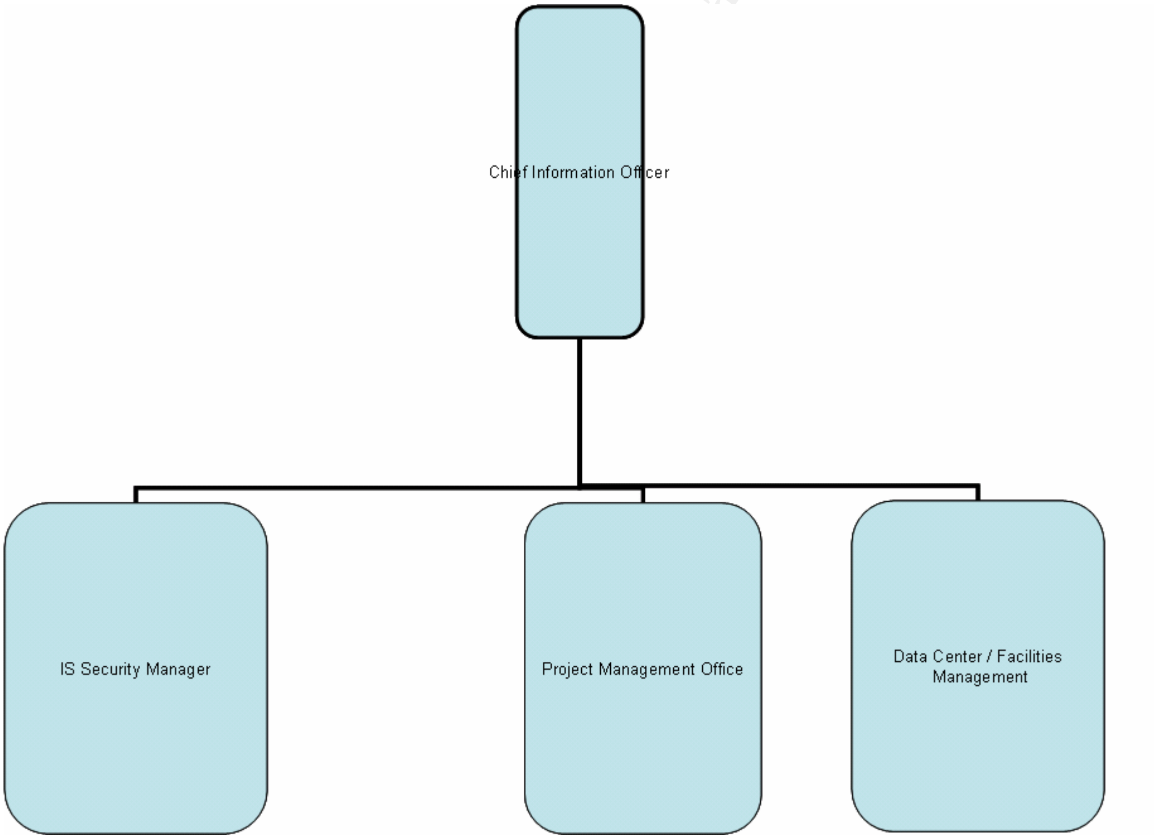
Chief Financial Officer (CFO) - The CFO will be responsible for insuring that all security related expenditures are made in compliance with company policies and the Security Forum. The CFO's staff member participating on the Security Management Team (the Financial Analyst) will provide the CFO with all financial material on security related projects in order for the CFO to ensure compliance.

Customer Operations Officer (COO) - The COO is responsible for all operations. The COO will be responsible to ensure that all operations are executed according to company and customer policies.

Customer Executive (CE) - The CE is responsible for communications, marketing and performance reporting to customers. The CE will be responsible to ensure the objectives of BS 7799 are communicated to the customer and ensure customer expectations are understood and communicated to Security Forum.

Chief Information Officer (CIO) –The CIO is responsible for the operations, management and execution of the IT infrastructure, as well as the operations and management of all Data Center Facilities.

Chief Legal Counsel (CLC) – The CLC is responsible for legal matters including contract management, patents and licenses, litigation and regulatory compliance.


Chief Information Officer
IS Security Manager
Project Management Office
Data Center / Facilities Management

IS Security Manager (IS Sec. Mgr.) - The IS Security Manager is responsible for all Logical Security; this includes security governance, operations and management. Currently, the IS Security Manager has four individuals covering System, Network, SAP and Oracle security responsibilities. They develop policies and standards, as well as the overall security architecture. The IS Security Manager will be promoted to Chief Information Security Officer in 2005.

Project Management Office (PMO) – The Project Management Office is responsible for managing and ensuring the timely and cost effective completion of all IT related projects.

Facilities / Data Center Manager - The Facilities / Data Center Manager is responsible for the environmental, health, safety and security (EHS&S) programs for the company.

Other functions with a dotted line to the CIO:

IT Quality Consultant (ITQ) – The IT Quality Consultant is responsible for the quality, reliability, consistency and integration of products, services, processes and practices within the IT infrastructure.

Privacy Consultant **(PC)** – The Privacy consultant is responsible for employee and customer privacy development and compliance. The PC also has responsibility to create a business advantage for privacy and support company values.

Legal Consultant (LC) – The Legal Consultant identifies legal solutions and recommends courses of action that help resolve the client organization's business issues and requirements. The LC acts as legal advisor and advocate for the company in litigation, regulatory and governmental administrative matters. The LC acts as a legal advisor to the contracting group.

Finance Analyst (FA) –The Finance Analyst is responsible for the financial analysis of trends and business opportunities for the CIO and his staff. Primary focus is Profit & Loss and balance sheet responsibilities, reporting and analysis. This would include research work on subjects such as rate of return, depreciation, working capital, account reconciliations, investment and financial and expense performance comparisons, as well as recording revenues, product costs, operating expenses and general accruals.

Human Resources Representative -The HR representative is responsible for developing, implementing, and/or maintaining employment programs. The HR rep. assists managers with defining clear job skill specifications to ensure appropriate identification of candidates and selection of highest quality hires. The HR rep. interviews and screens candidates; conducts reference checks either personally or through a third party; manages staffing forecasts and headcount; and manages internal selection process. Coordinates succession planning with management to ensure development plans are in place for key internal employees/positions.

Committee Status

The gap analysis showed that not all departments were linked into the overall ISMS. All departments and job functions mentioned above have been integrated into the ISMS and will have a solid or dotted line into the CIO for accountability purposes.

During the gap analysis the following group and/or committees were identified:

- Service and system architecture committee which developed the architecture for services and systems
- Facilities and physical security which developed the architecture and security controls for the facilities
- Customer relationship committee which developed the governance model for working and interacting with existing and potential customers
- Information security policy committee which developed the security policies, standards and requirements
- Quality forum which shared quality best practices
- Internal assessment group which share best practices for conducting internal quality assessments
- SAP working group committee which researched and analyzed existing and new SAP services; information was feed into the Service and system architecture teams

As noted above, these groups and/or committees were not well integrated with each other and did not always take security into consideration. To correct this for the ISMS, the following groups and/or committees were created:

- Security Operations group
- Information Security Management Forum
- Information Security Working Forum

The Security Operations group represents the IT Security operations team and to bring experience and knowledge for how security policy and standards have and can be implemented.

The Information Security Management Forum (ISMF) was the biggest change to the organization. This forum is co-chaired by the CEO and CIO and includes the following key executive managers: CFO, COC, CE, and CLC. The IS Sec. Mgr., which will become the Chief Information Security Officer (CISO) at the beginning of 2005, and is also a member of this team. This team meets quarterly, sooner if determined necessary by the co-chairs, and will ensure there is clear direction and support for security activities. The team ratifies security policies, set dates for compliance and ultimately has responsibility for the compliance to security policies. They also play an active role in promoting security internally and externally to customers, and ensuring adequate and knowledge resources are in place to carry out the security activities.

The Information Security Working Forum (ISWF) is lead by the CISO and has representatives from all departments (quality, finance, legal including outside legal consul for legislation, PMO, operations, customer team) of the company. The ISWF will meet on bi-monthly bases (weekly during phase I) to ensure input and co-ordination of the information security policies across all functions and locations, security awareness, and proper resource execution. Additionally, this forum is the trigger for regulatory and legislative awareness into the company and when necessary, sponsor and support working groups to investigate and determine the impact of legislation on the company.

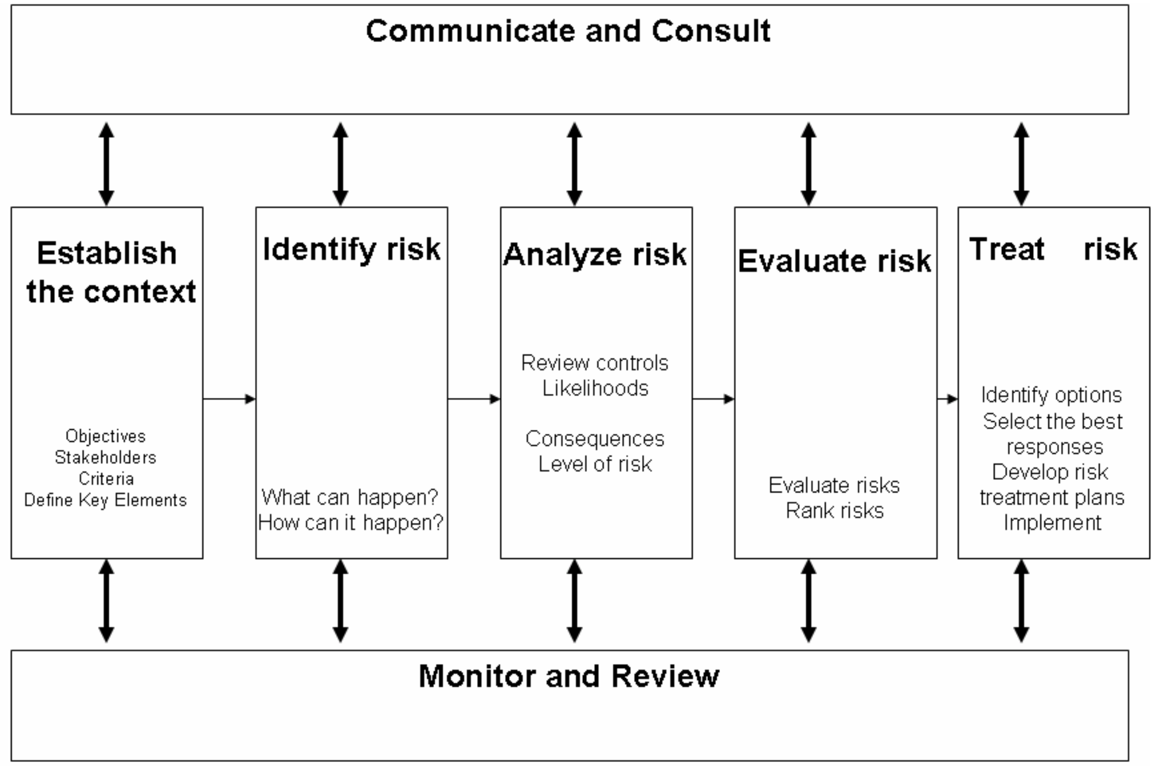
For both the ISMF and ISWF, the PMO team is responsible for managing the agenda, documenting the meetings, including materials presented, decisions made and owners assigned to projects and tasks.

Customers have and will continue to be made aware of the ISMS efforts through the Customer Executive Team. They are being educated on the changes to the overall security and how the development of the ISMS will impact them in the short and long term.

The total size of the company is 260 employees, however, for the first phase, only approximately 35 employees will be affected. These employees come from various departments within the company at the US South location, but most report into the CIO. As the Company progresses to full ISMS, all employees will be included.

Risk assessment and management

What is Risk? Webster's New College Dictionary, 1995, defines risk as the possibility of suffering harm or loss. The definition shows that there are two parts to risk: the possibility that a risk event will occur, and the harm or loss that results from occurrences of risk Events. **[1]**



Risk Management Overview (AS/NZS 4360:1999), Dr. Dale F Cooper, www.Broadleaf.com.au

The Risk Assessment is a process to identify the risks and assess the damage or loss it could cause. The end result of a risk assessment is justification of any control or safeguards that need to be implemented to mitigate the risk to an acceptable level as defined by management. Selecting controls or countermeasures will complete the Risk Management process. For the development of the ISMS, because of the IS Security Managers familiarity with the risk management methodology based upon the Australian and New Zealand Standard (AS/NZS 4360), it will be used. The above diagram shows the risk management overview and is quoted from Dr. Dale F. Cooper from http://www.broadleaf.com.au/tutorials/Tut_Standard.pdf .

Establish the Context

Per Dr. Cooper, to be able to recognize a risk, it is necessary to know what is at risk. The first step in the standard process is to define the context of the risk assessment, which falls into two parts, one description and the other creative.

To ensure that all significant risks are captured, it is necessary to know the objectives of the enterprise within which risks are to be managed; this is know as the descriptive part of the context analysis.

Objectives lie at the heart of the context definition, and they are linked into the risk management process via criteria for measuring success. Success criteria are the basis for measuring the achievement of objectives, and so are the used to measure the impact of anything which might jeopardize (loss or harm) those objectives, the consequences of risks.
[2]

The Company has set expectations for its risk evaluation criteria for what is acceptable risk and what is not.

For identified assets or an asset zone (an asset zone is a common set of assets such as network devices), the CIA model (confidentiality, integrity and availability) will be considered. Additionally, utility, authenticity and possession as defined by Donn B. Parker in the Computer Security Handbook will be used. [3] Management has decided that all risk considered to be "High" or higher will require a risk treatment plan to mitigate to an acceptable level. Once all "High" or higher risk are mitigate, all "Medium" risk will be mitigated.

Risk Identification

Risk identification is the determination of threats and vulnerabilities that could lead to loss or harm. Per the diagram above, the key questions are:

- What can happen?
- How can it happen?

The risks identified are linked to the risk register later in the Risk Assessment and Management.

Risk Analysis

Likelihood of risk and consequences of risk are considered for each asset or asset zone per the Company's expectations. The Company Management wants to keep the initial risk analysis simple and to the point. The reason behind this is that several types of risk assessment and management approaches have been used in the past, but most if not all have been very labor intensive and bogs down the entire process. Management does not want to spend six plus months doing a risk analysis. The management directive is to get the risk analysis done within two weeks. As a result, the ISMS steering committee has decided on the following tables:

Likelihood Criteria (Qualitative)	
Risk Level	**Description**
TRIVIAL	Not likely to occur.
LOW	Likely to occur once every 18 months or less
MEDIUM	Likely to occur once every 12 months or less
HIGH	Likely to occur once every 06 months or less
CRITICAL	Likely to occur once every 01 months or less

Consequences Criteria (Qualitative)	
Risk Level	**Description**
INSIGNIFICANT	Nil or no impact
SIGNIFICANT	Compromise of data, loss of integrity or availability of asset(s).
CRITICAL	Extended outage, damage to brand, loss of utility or possession of data. Disclosure of private company data.

To guide the risk analysis team, the risk evaluation criteria table below is used to enable decisions to be made by on the risk treatment options.

Risk Evaluation Criteria

		Consequences		
		INSIGNIFICANT	**SIGNIFICANT**	**CRITICAL**
Likelihood	**TRIVIAL**	NIL	NIL	NIL
	LOW	NIL	MEDIUM	**HIGH**
	MEDIUM	NIL	**HIGH**	**CRITICAL**
	HIGH	NIL	**CRITICAL**	**CRITICAL**
	CRITICAL	NIL	**CRITICAL**	**CRITICAL**

Risk Evaluation and Treatment

Results from the risk analysis will be a list of risks from "NIL" to "CRITICAL" to the Company hosted SAP environment. Risk at a **"HIGH" or more risk level** are considered unacceptable and must implement controls to mitigate the risk to an acceptable level.

Risks that are **"CRITICAL"** should be addressed first, and then **"HIGH"** risk should be addressed.

Policies and Standards Current Status

The Company has created several policies, standards, requirements, guidelines and procedures through the years; however, they are not organized and deployed in a consistent and uniform manner. The table below captures the documents in place:

- Documents highlighted in **orange** need to be updated and or implemented in a consistent manner.
- Documents highlighted in **green** are ok.
- Documents highlighted in **red** need to be developed.

Name of Document	***Purpose***	***Audience***	***BS ISO/IEC 17799:2000 Ref.***
7799 Security Awareness & Training Policies	*Specific 7799 awareness & training policy*	*Management and Individual Contributors included in the first phase of the ISMS. To be extended to all employees in the remaining phases.*	*Sub-set of A.6.2 A.6.3*
Access Controls for Customers and Vendors Standards	*How to setup access for customers and vendors*	*Customers and Vendors.*	*A.4.2 A.9.1 to A.9.6*
Administrator Security Policies	***How to protect administrator access. Dos and Don'ts of an admin.***	***All administrators.***	***A.9.2***
Configuration Management Policies	*When and how to use configuration mgmt. system with respect to assets*	*All administrators*	*A.5.1.1*
Facilities and Physical Security Controls for Data Center and General Office Space	*Secure access to physical assets, equipment and environment Portables and Workstations*	*Facilities and Physical security staff Employees of company*	*A.7.1 A.7.2 A.7.3*
Operational Procedures	*Secure operations of processing environment*	*Operations Staff*	*A.8.1 A.8.2 A.8.3 A.8.4 A.8.6 A.8.7*
Disposal of Hardware & Software	*Proper disposal and/or destruction of hardware, media and software.*	*Data center staff, administrators, privacy officer, and management.*	*A.7.2.6 A.8.6.2*

General Security Awareness and Training Policies	General security awareness and training.	All employees on annual bases.	High level A.6.2 A.6.3
Incident Management Policies	All incidents including security	All employees	A.6.3
Network Security Policies and Standards	How to setup and secure network.	Security and network personnel.	A.4.3.1 A.8.5 A.9.4
Oracle System Security Policies & Standards	How to setup and secure Oracle.	System and Oracle administrators	A.10.1 A.10.5
Patch Management Standards	**Requirements for patch management with linkages to change management.**	**Management, customer and administrator.**	**A.10.5.1 to A.10.5.3**
Personal Conduct Standards	**Company and professional conduct expected of employees.**	**All employees Some parts share with Vendors**	**A.6.1.1**
Personnel Security Policies	Personnel policies including background checks.	All employees	A.6.1.2
Physical Security Policies	How to setup and secure buildings, data centers and office space.	Primarily facilities and data center staff. Office space for all employees	A.7.1 A.7.2 A.7.3
Privacy Policies	How to protect and handle personal identifiable information.	All employees and vendors.	A.12.1.4
UNIX System Security Policies & Standards	**How to setup and secure UNIX.**	**System Administrators**	**High level covered lower level not consistent.**
Virus Management Standards	How to setup and secure platforms from Viruses.	System and Network Administrators	A.8.3 A.10.5.4
Business Contingency Planning and Disaster Recovery Planning	Business Resumption and Disaster Recovery	Management Staff System, Network and Operations Staff	A.11
Windows System Security Policies & Standards	**How to setup and secure Windows.**	**System Administrators**	**High level covered lower level not consistent.**
SAP Standards			
• SAP Access Management and	Access Management	System Administrators	A.10.1

Security Standards	*and Security Standards for SAP*		*A.10.2* *A.10.4* *A.10.5*
• *SAP Basis Administration Standards*	*Basis administrative standards*	*Basis Administrators*	*A.9.1* *A.9.2* *A.9.3* *A.9.6* *A.9.7* *A.10.1*

Key Risk to the System

Below are four main risks to the system. There are other risks to the system, but management has determined that these are the most critical risk for the successful implementation and on-going management of the ISMS.

1. The IS Security Manager has overall responsibility for security, however, in the past, this function has been more operational focused, than a governance role with the proper representative and oversight.
2. General security awareness training is in place and given to employees on annual bases, however, specific training on the ISMS is not in place and management feels this is critical to ensure a successful start for the ISMS.
3. During the gap analysis, it was determine that there were no policies or procedures in place for the proper disposal and/or destruction of hardware and data, or the proper management of licenses.
4. Also during the gap analysis, it was determine that privacy legislative was well understood and addressed, however, other applicable legislative was not well known and understood and it's impact to the Company and its customers.

Plans for Addressing the Risks

To minimize the risk to the Company and its Customers, a set of controls must be put in place. The following controls were put in place to address the risk:

1. A formal Security Forum where the IS Security Manager will provide leadership and governance and have representatives for all critical departments.
2. Create a 7799 specific security awareness program with the support of the Security Forum to educate employees, vendors and customers on the overall intent and purpose of the ISMS, how they play a role and how they can contribute and provide feedback. In the short term, management wants this to be a specific training so as to highlight its importance.   Over time, the 7799 awareness and training will be integrated into the standard security awareness and training program.

3. Develop, approve and communicate a policy of the disposal and destruction of hardware and data. Develop, approve and communicate a policy on management of software license.
4. Develop a formal plan sponsored by the Legal department and supported by Information Security Working Forum to understand all applicable legislative and its impact to the Company and its Customers. Management supports the idea of brining in an outside legal firm and/or accounting firm for consulting on this topic.

Risk ID	Asset Identification	Threat to Asset	Likelihood	Consequences	Resultant Risk	Controls
1	Policy	Policy and Security Strategy not approve or understood by key management personnel and employees	**HIGH**	**SIGNIFICANT**	**CRITICAL**	ISO 17799 Section 4.1.1
2	Policy	Security continues in ad hoc manner w/o employees, customers and vendors understanding their roles	**HIGH**	**SIGNIFICANT**	**CRITICAL**	ISO 17799 Section 6.2.1
3	Policy / CIA	Lost and or compromise of hw and data. Non compliance to software license agreement.	**HIGH**	**CRITICAL**	**CRITICAL**	ISO 17799 Section 7.2.6, 8.6.2, 12.1.2.2
4	Policy / Brand	Penalties and/or fines per legislative, brand damage.	**HIGH**	**SIGNIFICANT**	**CRITICAL**	ISO 17799 Section 12.1.1

ISMS Implementation Plan (PDCA – DO)

In this section, I will describe steps to be taken to address the problems identified in the gap analysis for the hosted SAP environment so that the Company is positioned to move forward with their 7799 certification.

This section contains the problems, and the action and steps required to implement the actions.

Problem Description- Creation of Security Management and Working Forum / Steering Committee

The IS Security Manager has overall responsibility for security, both operational and governance. In the past this has been focused more on the operational aspects of security and not on the overall governance of security for the Company. Security was viewed as a necessary evil and not a business enabler. The CEO wants security and controls to become enablers for the Company. The CEO believes this will be a vehicle to build the confidence of the staff, management and the customers. To that end, the CEO is sponsoring the 7799 certification efforts.

Action Plan

Early in the process, the CEO and CIO made a presentation to management and the board of directors to get their approval to proceed with the 7799 certification efforts. The proposal has been approved and is moving according to the project plan managed by the PMO. The specific steps taken were:

Steps

1. CEO and CIO present proposal to Executive Management and Board of Directors.
2. Executive Management and Board of Directors approved proposal.
3. CEO and CIO named Co-Chairperson of Information Security Management Forum
4. IS Security Manager named Chairperson of Information Security Working Forum
5. Security Forum Charter and Roles and Responsibilities developed and approved.
6. Quarterly executive management meetings established.
7. Weekly security forum meetings established. This will continue on this schedule until the first phase is complete.
8. Formal job tiles and positions to be changed at the start of FY05.

Problem Description- Specific 7799 Security Awareness and Training

During the gap analysis, it was determined that the general security awareness training was in place and given to employees on annual bases. However, specific training on the ISMS is not in place and management feels this is critical to ensure a successful start for the ISMS. Several employees were not aware of ISO 17799, what it was or how it would help the Company and/or its Customers.

Action Plan
To ensure employees, vendors and customers understand ISO 17799, the outside consultant was tasked by the Security Forum to develop, publish and train all applicable employees, vendors and customers on ISO 17799 and how it will apply to them. The consultant was also tasked with providing "real" industry examples of the benefits of ISO 17799 and how it can become an enabler for the Company and its Customers. The specific steps taken were:

Steps

1. Obtain approval from Security Forum for security training material (includes "real" industry examples), method of communication, budget and timeline.
2. Provide training per schedule.
3. Work with HR representative to track the delivery of the 7799 training using the existing tracking system.

Problem Description- Gaps in Security Policies

During the gap analysis, it was determine that there were no policies or procedures in place for the proper disposal and/or destruction of hardware and data, or the proper management of licenses. All types of hardware devices were being disposed using various insecure methods and vendors. Additionally, management of software licenses was in need of more structure and organization, especially as it related to software managed for customers.

Action Plan
In order to address the gaps in the security policies, the Security Forum assigned the task of drafting the new security policies to the ISO 17799 consultant. The consultant was responsible for researching industry policies and best practices, reviewing existing customer contracts and using this information to develop and present the policies to the Security Forum for ratification.

Steps

1. Security Forum assign consultant to develop policies.
2. Consultant to perform research on industry policies and best practices.
3. Consultant to review existing contracts for software licensing requirements to include in policy and transition plan to new policy.
4. Consultant to develop test cases for next policies and how the various situations will be addressed by the new policies.
5. Security Forum to ratified new policies.

Problem Description- Applicable Legislation

During the gap analysis, it was determine that privacy legislative was well understood and addressed, however, other applicable legislative such as Sarbanes-Oxley was not well known and understood and it's impact to the Company and its customers. In several situations, it was determine through customer meeting minutes that customers had repeatedly ask about Sarbanes-Oxley and the Company did not adequately address the questions. In one case, one customer threatened to break the contract.

Action Plan

The Security Forum with support from ISMF and the Board of Directors approved the hiring of an outside legal consultant to help understand the top critical legislations affecting the company that has not already been addressed. As expected, Sarbanes-Oxley is the top priority for the foreseeable future. The specific actions to integrate Sarbanes-Oxley are as follows:

Steps

1. Security Forum hire legal consultant with support from Executive Management and the Board of Directors.
2. Consultant to perform research on legislative most applicable for the Company.
3. Consultant to work with executive management to determine top legislative priority. Sarbanes-Oxley was the top priority.
4. Consultant to analyze impact on the Company, its customers and the roles and responsibilities for each party.
5. Consultant to help structure a strategy to handle Sarbanes-Oxley request and update current contracts to the future.
6. Consultant to provide educational material and training to Sales and Account Teams, Customer Executive and consultant with Customers as needed.
7. Develop a more rigorous Policy for the on-going effort to maintain compliance with all applicable local, state and federal regulations.

Statement of Applicability

A majority of controls as defined in ISO 17799 are applicable to our system for phase I. The areas covering application security controls (10.2), some cryptographic controls (10.3) and some system security files controls (10.4) are not applicable. The following table provides a quick summary of which ISO 17799 controls are applicable and which ones are not.

ISO/IEC Control Nr.	Label	Applicable
3	Security Policy	Yes
3.1	INFORMATION SECURITY POLICY	yes
3.1.1	Information security policy document	yes
3.1.2	Review and evaluation	yes

4	Organizational Security	yes
4.1	INFORMATION SECURITY INFRASTRUCTURE	yes
4.1.1	Management information Security forum	yes
4.1.2	Information security co-ordination	yes
4.1.3	Allocation of information security responsibilities	yes
4.1.4	Authorization process for information processing facilities	yes
4.1.5	Specialist information security advice	yes
4.1.6	Co-operation between organizations	yes
4.1.7	Independent review of information security	yes
4.2	SECURITY OF THIRD PARTY ACCESS	yes
4.2.1	Identification of risks from third party access	yes
4.2.1.1	Types of access	yes
4.2.1.2	Reasons for access	yes
4.2.1.3	On-site contractors	yes
4.2.2	Security requirements in third party contracts	yes
4.3	OUTSOURCING	yes
4.3.1	Security requirements in outsourcing contracts	yes
5	ASSET CLASSIFICATION	yes
5.1	ACCOUNTABILITY FOR ASSETS	yes
5.1.1	Inventory of assets	yes
5.2	INFORMATION CLASSIFICATION	yes
5.2.1	Classification guidelines	yes
5.2.2	Information labeling and handling	yes
6	PERSONNEL SECURITY	yes
6.1	SECURITY IN JOB DEFINITION AND RESOURCING	yes
6.1.1	Including security in job responsibilities	yes
6.1.2	Personnel screening and policy	yes
6.1.3	Confidentiality agreements	yes
6.1.4	Terms and conditions of employment	yes
6.2	USER TRAINING	yes
6.2.1	Information security education and training	yes
6.3	RESPONDING TO (SECURITY) INCIDENTS AND MALFUNCTIONS	yes
6.3.1	Reporting security incidents	yes
6.3.2	Reporting security weaknesses	yes
6.3.3	Reporting software malfunctions	yes
6.3.4	Learning from incidents	yes
6.3.5	Disciplinary process	yes
7	PHYSICAL AND ENVIRONMENTAL SECURITY	yes
7.1	SECURE AREAS	yes
7.1.1	Physical security perimeter	yes
7.1.2	Physical entry controls	yes
7.1.3	Securing offices, rooms and facilities	yes
7.1.4	Working in secure areas	yes
7.1.5	Isolated delivery and loading areas	yes
7.2	EQUIPMENT SECURITY	yes
7.2.1	Equipment siting and protection	yes
7.2.2	Power supplies	yes
7.2.3	Cabling security	yes
7.2.4	Equipment maintenance	yes
7.2.5	Security of equipment off-premises	no
7.2.6	Secure disposal or re-use of equipment	yes
7.3	General Controls	yes
7.3.1	Clear desk and clear screen policy*	yes

7.3.2	Removal of property*	yes
8	Communications and operations management	yes
8.1	Operational procedures and responsibilities	yes
8.1.1	Documented operating procedures	yes
8.1.2	Operational change control*	yes
8.1.3	Incident management procedures	yes
8.1.4	Segregation of duties	yes
8.1.5	Separation of development and operational	yes
8.1.6	External facilities management	yes
8.2	System planning and acceptance	yes
8.2.1	Capacity planning	yes
8.2.2	System acceptance	yes
8.3	Protection against malicious software	yes
8.3.1	Controls against malicious software	yes
8.4	Housekeeping	yes
8.4.1	Information back-up	yes
8.4.2	Operator logs	yes
8.4.3	Fault logging	yes
8.5	Network management	yes
8.5.1	Network controls	yes
8.6	Media handling and security	yes
8.6.1	Management of removable computer media	yes
8.6.2	Disposal of media*	yes
8.6.3	Information handling procedures	yes
8.6.4	Security of system documentation	yes
8.7	Exchanges of information and software	yes
8.7.1	Information and software exchange agreements	no
8.7.2	Security of media in transit	yes
8.7.3	Electronic commerce security	no
8.7.4	Security of electronic mail	yes
8.7.4.1	Security risks of electronic mail	yes
8.7.4.2	Policy on electronic mail	yes
8.7.5	Security of electronic office systems	yes
8.7.6	Publicly available systems	yes
8.7.7	Other forms of information exchange	yes
9	Access control	yes
9.1	Business requirement for access control	yes
9.1.1	Access control policy	yes
9.1.1.1	Policy and business requirements	yes
9.1.1.2	Access control rules	yes
9.2	User access management	yes
9.2.1	User registration	yes
9.2.2	Privilege management	yes
9.2.3	User password management	yes
9.2.4	Review of user access rights	yes
9.3	User responsibilities	yes
9.3.1	Password use	yes
9.3.2	Unattended user equipment	yes
9.4	Network access control	yes
9.4.1	Policy on use of network services	yes
9.4.2	Enforced path	yes
9.4.3	User authentication for external connections	yes
9.4.4	Node authentication	yes

9.4.5	Remote diagnostic port protection	yes
9.4.6	Segregation in networks	yes
9.4.7	Network connection policy	yes
9.4.8	Network routing control	yes
9.4.9	Security of network services	yes
9.5	Operating system access control	yes
9.5.1	Automated terminal identification	no
9.5.2	Terminal logon procedures	yes
9.5.3	User identification and authentication	yes
9.5.4	Password management system	yes
9.5.5	Use of system utilities (Administrative Access)	yes
9.5.6	Duress alarm to safeguard users	yes
9.5.7	Terminal time-out	yes
9.5.8	Limitation of connection time	no
9.6	Application access control	yes
9.6.1	Information access restriction	yes
9.6.2	Sensitive system isolation	yes
9.7	Monitoring system access and use	yes
9.7.1	Event logging	yes
9.7.2	Monitoring system use	yes
9.7.2.1	Procedures and areas of risk	yes
9.7.2.2	Risk factors	yes
9.7.2.3	Logging and Reviewing events	yes
9.7.3	Clock synchronization	yes
9.8	Mobile computing and teleworking	yes
9.8.1	Mobile computing	yes
9.8.2	Teleworking	yes
10	Systems development and maintenance	yes
10.1	Security requirements of systems	yes
10.1.1	Security requirements analysis and specification <production engineering>	yes
10.2	Security in application systems	no
10.2.1	Input data validation	no
10.2.2	Control of internal processing	no
10.2.2.1	Areas of Risk	no
10.2.2.2	Checks and Controls	no
10.2.3	Message authentication	no
10.2.4	Output data validation	no
10.3	Cryptographic controls	yes
10.3.1	Policy on the use of cryptographic controls	yes
10.3.2	Encryption	yes
10.3.3	Digital signatures	no
10.3.4	Non-repudiation services	no
10.3.5	Key management	no
10.4	Security of system files	no
10.4.1	Control of operational software	no
10.4.2	Protection of system test data	no
10.4.3	Access control to program source library	no
10.5	Security in development and support processes	yes
10.5.1	Change control procedures	yes
10.5.2	Technical review of operating system changes	yes
10.5.3	Restrictions on changes to software packages	yes
10.5.4	Covert channels and Trojan code	yes
10.5.5	Outsourced software development	yes

11	Business continuity management	yes
11.1	Aspects of business continuity management	yes
11.1.1	Business continuity management process	yes
11.1.2	Business continuity and impact analysis*	yes
11.1.3	Writing and implementing continuity plans*	yes
11.1.4	Business continuity planning framework	yes
11.1.5	Testing, maintaining and re-assessing BCP	yes
11.1.5.1	Testing the plans	yes
11.1.5.2	Maintaining and re-assessing the plans	yes
12	Compliance	yes
12.1	Compliance with legal requirements	yes
12.1.1	Identification of applicable legislation	yes
12.1.2	Intellectual property rights	yes
12.1.2.1	Copyright	yes
12.1.2.2	Software copyright	yes
12.1.3	Safeguarding of organizational records	yes
12.1.4	Data protection and privacy of personal information	yes
12.1.5	Prevention of misuse of information processing	yes
12.1.6	Regulation of cryptographic controls	yes
12.1.7	Collection of evidence	yes
12.1.7.1	Rules for evidence	yes
12.1.7.2	Admissibility of evidence	yes
12.1.7.3	Quality and completeness of evidence	yes
12.2	Reviews of security policy and technical compliance	yes
12.2.1	Compliance with security policy	yes
12.2.2	Technical compliance checking	yes
12.3	System audit considerations	yes
12.3.1	System audit controls	yes
12.3.2	Protection of system audit tools	yes

ISMS Audit Plan (PDCA – CHECK)

Several controls were check during the gap analysis conducted in June 2004. Of the controls checked, four were identified as being critical for the successful implementation of the ISMS. Below is a list of the critical controls and the auditing of these controls. Compliance status is current as of August 2004.

ISO 17799 Section 4.1.1 … Management Information Security Forum

Audit Questions –
Whether there is a management forum to ensure there is a clear direction and visible management support for security initiatives within the organization.

Importance –
Security and controls is critical to the Company. This has become evident at the highest levels of the company. It is critical to ensure security and controls are

visible within the Company and that the appropriate departments are represented.

Expectations for Compliance –
Departmental compliance in the Security Forum is mandatory and the PMO and Compliance teams will report any and all exceptions to the Executive Management and the Board of Directors.

Audit Steps / Findings / Compliance Status

Audit Steps	Findings	Compliance
1. Does a Security Forum exist?	In place and working as expected.	YES
2. Does the Security Forum have the proper representation?	Yes. One exception was reported to Executive Management and it was promptly addressed.	YES
3. Does the Security Forum have a charter and defined RACI that has been approved by Executive Management?	Initial charter and RACI created. Will be revisited by the end of CY04.	YES
4. Does the charter provide for ratifying policies, monitoring the organization for changes in people, technologies and processes?		YES
5. Does the Security Forum identify an accountable Executive Member for all security (physical and logical) activities?	IS Security Manager	YES
6. Does the Security Forum support security within the organization, with vendors and customers?	Vendors via procurement team and customers via Customer Executive	YES

ISO 17799 Section 12.1.1 … Identification of Applicable Legislation

Audit Questions –

- Whether all relevant statutory, regulatory and contractual requirements were explicitly defined and documented for each information system.
- Whether specific controls and individual responsibilities to meet these requirements were defined and documented.

Importance –
This control has become critical due to a customer threatening to exit their contract. It has also played an increasing role in acquiring new business, so management has stressed the importance as it relates to understanding and creating a strategy for Sarbanes-Oxley and other applicable legislative in the future.

Expectations for Compliance –
Compliance with this control is mandatory. All customer facing employees as well as the contracts team must understand and comply.

Audit Steps / Findings / Compliance Status

Audit Steps	Findings	Compliance
1. Has the Company identified all critical legislative and regulatory exposures?	Outside consultant identified most critical legislation.	YES
2. Has the company obtained copies of applicable legislative?	Outside consultant completed.	YES
3. Has the company created a position or strategy for dealing with the legislation?	Outside consultant is currently doing is.	NO Partial Completion
4. Has the compliance deadlines been determined?		YES
5. Has compliance checklist been developed?	Will be done after strategy is completed by consultant	NO
6. Has legislative collateral been created for customer meetings?	Will be done after strategy is completed by consultant	NO
7. Have an assessment program been developed?	Will be done after strategy is completed by consultant	NO
8. Have appropriate staff members	Partial training has been provide to key staff	Partial, no to be trained.

been educated and trained?	members	

ISO 17799 Section 3.1.1 … Information Security Policy Document

Audit Questions –

- Whether there exists an Information security policy, which is approved by the management, published and communicated as appropriate to all employees.
- Whether it states the management commitment and set out the organizational approach to managing information security.

Importance –

This is at the heart of providing proper security and controls that enable the business. The gaps in policies will be filled and communicated to employees, vendors and customers where applicable to ensure a clear understanding of the expectations of the Company.

Expectations for Compliance –

Only a few policies need to be created and a handful of others need to be updated. Management has set the expectations that all new policies and modified policies must be ratified by end of CY04.

Audit Steps / Findings / Compliance Status

Audit Steps	Findings	Compliance
1. Does the Security Forum have an inventory of security policies and standards in place for the Company?	YES, but some policies were missing based on the gap analysis.	YES
2. Are international standards checks against the inventory to ensure complete coverage?	YES, but some policies were missing based on the gap analysis against ISO 17799.	YES
3. Does a standard template exist for policies and standards?		YES
4. Has a process been created for the distribution of	Covers employees, vendors and customers as applicable.	YES

policies and standards to the proper personnel?		
5. Has a communication methodology been established for the security policies that addresses all audiences?	Covers employees and vendors.	NO – Customer's communication methodology is not in place. Will be addressed by Customer Executive.
6. Has the security awareness education and training check knowledge of the Security policies?	Security awareness education and training owner is part of the Security Forum and updates are required to be included before ratification.	YES

ISO 17799 Section 6.2.1 … Information Security Education and Training

Audit Questions –

- Whether all employees of the organization, third party users and customers receive appropriate Information Security training and regular updates in organizational policies and procedures.

Importance –
To ensure everyone is on the same page, including employees, vendors and customers, all personnel who have the responsibility for their execution must the policies, understand what their roles are in executing the policies, and what consequences are in place for failure to comply.

Expectations for Compliance –
All applicable employees, vendors and customers must acknowledge security education and awareness has been received.

Audit Steps / Findings / Compliance Status

Audit Steps	Findings	Compliance
1. Does a tracking method exist to ensure appropriate personnel have been trained?	Employees via employee record. Vendors via procurement contract. Customer via Customer Executive staff.	YES
2. Does a process	Part of Security Forum	YES

exist to ensure changes to security awareness material are known?		
3. Does a process exist to provide the Security Forum with enhancements to the training material?	Feedback system in place. Feedback double copied to Security Awareness Owner and Security Forum	YES

As noted above, these four checks were critical to the success of the ISMS. On on-going bases, a more detail and comprehensive audit checklist will be utilized to cover all controls and risk associated with the ISMS. In appendix A is a sample of the current audit checklist. Included in the audit checklist are general audit steps and more technical steps.

The following is a list of the various audit checklists that are available for use. The ones in bold are highlighted in Appendix A:

- **Data Center Infrastructure Checklist**
- Access Control of the Data Center Checklist
- **Data Center Access Controls Checklist**
- Monitoring Controls and Resources Checklist
- Fire Fighting Systems Checklist
- **Air Conditioning Systems Checklist**
- Power Generator Checklist
- Backup and Storage Checklist
- Maintenance and Cleaning Checklist
- Policies and Procedures Checklist
- SAP Basis Administration Checklist
- Windows Audit Checklist
- **General Patch Management Checklist**
- Virus Management Checklist
- Oracle Security Checklist
- Privilege Access Security Checklist
- 3rd Party Access Security Checklist
- **General Network Security Checklist**
- Cisco Security Checklist
- UNIX Security Checklist
- Customer Network Security Checklist
- Configuration Management Audit Checklist
- Security Incident Management Checklist

- Privacy Audit Checklist
- Personnel Background Checklist
- Security Awareness Checklist
- Administrator Security Checklist
-

The Information Security Working Forum will have responsibility to ensure that the audit checklist is carried out at least once per year for all major functions and services. Additionally, any time there is an organization change or people change, a process change or technology change, it will be the responsibility of management to understand the changes and the affect on the ISMS, the ISWF will need to ensure an audit takes place, results reported and the appropriate mitigation or remediation takes place.

You will note that the audit checklist varies in format and how the questions are asked. This is one of the process improvement projects that the ISWF will addressed in the coming year. As part of the process improvement project, all audit questions and steps will have a consistent format that will consist of the audit question, importance of the question, reference to the ISO 17799 standard, what test to perform and how to execute the test for compliance and whether or not compliance has been met. If any issues are noted, corrective action will be triggered and monitored until compliance is achieved.

ISMS Maintenance and Improvement (PDCA – ACT)

Since the BS 7799 Certification project started, several improvement projects have taken place. The following is a list of critical projects that have been completed to improve the overall ISMS:

- The Information Security Management Forum was created and put in place. This group has provided excellent support and has paved a way for success and will be critical to the on-going maintenance and improvement for the ISMS.
- The Information Security Working Forum was created and put in place. This team has done a good job providing tactical leadership and will continue to provide leadership and ensure continuous improvement.
- A gap analysis was conducted by an outside consultant. The process, tools and methodology used have been adopted by the Company and will be used to maintain the current certification, but will also be used to determine the gaps in the services to be brought into scope over the next couple of years.
- The process that was put in place by the PMO and Compliance team for remediation of issues identified in the gap analysis has been well received. This process clearly identifies issues, defines owners, defines project plans with reasonable completion dates, and the ISWF helps to eliminate and manage any roadblocks. This has lead to projects being completed on time. This process will be used for the other services when they are in scope and will be used when issues are identified for the current ISMS.

Other projects that will support process improvement

A project has been started to evaluate and improve the overall process for auditing the ISMS and for performing gap analysis.   For the existing ISMS, an inventory of all checklists has been completed. To improve the process, a standard template will be developed so that all checks and questions are structured the same way; basically, all questions will be asked the same way and will be asked so that we get the information needed to determine compliance and or make improvements. All audit questions and steps will have a consistent format that will consist of the audit question, importance of the question, relationship to the ISO 17799 standard, what and how to test for compliance and whether or not compliance has been met. If any issues are noted, corrective action will be triggered and monitored until compliance is achieved.

Efforts are being made to implement a formal risk assessment process to determine what areas should be audited and when they should be audited. The ISWF will initially provide approval for the plan and work out the tactical details, and then the ISMF will approve the plan and provide support and resources for its execution. The ISMF and ISWF will also approve the testing plan. It is important to note that the company strongly believes in having an adequate test strategy that leads to a good testing plan to validate the design of the controls. All audit results will be shared with the ISMF and ISWF and any issues will be managed by the PMO to ensure a quick and appropriate resolution.

Future Phases

The Company has made great strides in the first phase of the overall 7799 project and has created a solid foundation. In phases II through V, this foundation will be expanded. In phase II, the biggest efforts will be spent on including the other two data centers and enhancing the contract language with both customers and our vendors to be consistent with the Company's efforts around BS 7799. For new and existing customers up for renewal, it will clearly statement how services have been affected by the BS 7799 certification and how we have enhanced our services with the ISMS. For our vendors, we have existing contract language in place regarding security requirements, but the language and requirements will be tighten up to ensure consistency. The basic approached and lessons learned from our phase I will be used in phase II to bring into scope these other services.

For phase III, the scope of services will be expanded to include full networking services, application management and our remote managed services.

Similarly, in phase IV, the scope of services will be further expanded to included Disaster Recovery Services and Security Administration Services. These are typically add-on services for our major customers.

In the final phase, phase V, we will pursue BS 15000 certification. The organization has the quality management system, will have the information security management system and then will add in the IT service management system. A lot will be leveraged from our current management systems, quality and information security, for IT Service Management. The Company has been utilizing good IT Service Management for several years. As part of the auditing project, IT service management processes such as Incident, Problem, Change and Configuration management will be added to get ahead start on any potential weaknesses.

On-going Maintenance and Improvement

The ISWF has a maintenance and improvement plan that consists of the following:

- On a yearly base, have an external consultant evaluate the role of the Information Security Management Forum and Information Working Forum to ensure their stated charter is being carried out and determine the need for changes.
- Annually update policy. This is triggered by both the requirements of the policy and will be triggered by internal audits. As noted earlier, changes to the organization or people, processes or technologies will trigger a review of the policy.
- Annual review of the risk assessment methodology and asset inventory. As part of a yearly physical asset that is owned by the Quality team, an annual review of the asset inventory will be performed.
- Annual review of Statement of Applicability.
- Annual review and update of audit schedule, questions, methodology and tools. In addition to this, the certifier will also perform reviews during the year as appropriate.

Appendix A

The sample checklist in this section will all be converted into the new format where each question will have the same grammatical syntax, why the question is important, the reference to the ISO 17799 standard, what test to perform and how to perform those test, and a section to capture whether or not compliance has been met.

Data Center Infrastructure

- Is the Data Center sub-divided into distinct areas?
- Is this documented and defined in any process/procedure?
- Does the material employed in the partition and/or walls described in the previous item provide total insulation against violations and does it comply with the basic security needs of these rooms/areas? i.e.: Brick wall and/or dry wall are safer than a common chipboard wood panel wall).
- Do the partitions and/or walls, mentioned in the previous item for separating the Data Center and its areas, go all the way from floor to ceiling, completely separating the areas with no possibility of entrance/violations?
- Regarding the Data Center and its respective areas, are the partitions and/or walls mentioned in the previous item shared by other than Data Center Departments or another company or even any external area like streets, aisles, etc.?
- Is the material employed in the shared partitions and/or walls cited in the previous item adequate to provide the necessary protection level with no risks for violations in the area?
- Do the partitions and/or walls for the Data Center and its respective areas, cited in the previous item, have windows and/or any other similar feature?
- Are the structures of the windows and/or any other similar feature, described in the previous item, duly protected in order to prevent their violation in all areas of the Data Center? I.e.: glasses that withstand high impact, adequate sealing, protection bars, etc.
- Regarding the windows and/or similar features described in the previous item, are there those which allow total, partial or no visual access inside the area?
- Regarding the areas listed in the previous item that have total or partial visual access, is there any kind of confidential information and/or information that must not be known by other employees/departments?
- For the areas that have windows and/or similar features but do not allow visual access, please describe the resource used for visual protection like, for instance, drapes, films or even dark room concept.
- Is there a procedure and/or policy that warrants that no server is labeled with customers' names?
- Does the material that physically constitutes the Data Center areas – like partitions, walls, floor and ceiling – have an adequate composition to withstand occurrences of fire? I.e.: It withstands high temperature and is not flammable?

- Do the Data Center areas have an adequate raised floor, i.e.: one that complies with all security and infra-structure needs, providing for an adequate ventilation system, structured cabling, and space from the original floor, and, also, is it well maintained, organized and clean?
- Do the Data Center areas have an adequate suspended ceiling, i.e.: one that complies with all security and infra-structure needs, providing for an adequate ventilation system, structured cabling, and space from the original ceiling, and, also, is it well maintained, organized and clean?
- Are all hallways and passages in all Data Center areas totally free for employees' transit, i.e.: there are no physical barriers such as material, boxes, misplaced wiring, chairs, desks, hacks, etc.? In case there are, please describe and detail the location and the reason why such barriers exist.
- Where are all Data Center areas' wiring installed?
- Are all wires and cables in all Data Center areas properly protected by some feature that does not allow them to be violated? For example, still pipes, aluminum ducts, etc.
- Are all doors in all Data Center areas made of an adequate material that provides total security to the areas, without risk of violation?
- Are all doors cited in the previous item equipped with adequate features/devices for proper access control and security, such as locks, keys (common or magnetic), closing/opening coils, etc.?
- Is there any area in the Data Center that has an entrance and/or exit (access door) to an area out of the Data Center?
- Is the material used in the doors described in the previous item adequate to provide a proper protection level and no risk of violation in the area?

Data Center Access Control

- Does the Data Center have a defined owner?
- Is the Data Center classified as a restricted and controlled access area?
- Is the Data Center divided into restricted and controlled access areas?
- Are the access authorizations to all employees differentiated for each kind of area that forms the Data Center, i.e.: do all owners of each area approve access to their respective areas?
- Are all authorizations mentioned in the previous item obligatorily approved by the Data Center owner?
- Are there employees and/or departments that are granted access to all restricted and controlled access areas in the Data Center?
- Are the respective accesses reviewed and approved periodically?
- For the process/procedure mentioned in the previous item, do all area owners and, more importantly, does the Data Center owner participate of all revalidation and approvals?
- During the process/procedure described in the previous item, are the access cases that are not being used anymore identified?

- Do all access doors to all areas have any kind of device for freeing access, in this case for opening the doors? For example, badge reader, biometrics reader, etc.
- Is there any area equipped with a door with a “one person only” access control system that does not allow the passage of people carrying equipment/material?
- For the doors cited in the previous item, is there an opening time control that blocks access if the defined time is surpassed? For example, in case the door is not closed in ten seconds, it will lock, interrupting access to the area and setting off an alarm.
- When equipment and/or material is taken inside or outside of the Data Center areas, i.e. when delivery or dispatching takes place, does this happen in an independent and/or intermediate area in relation to the Data Center?
- Is the area mentioned in the above item classified as of restricted and controlled access?
- Are all Data Center equipment dispatches and deliveries supervised by an employee and/or department in charge?
- Is there any door in the Data Center equipped with some feature/device that requires a code or password to be entered to free access/opening?
- Are the passwords and/or codes for the features/devices mentioned in the item above shared in any way?
- Are there badge controllers for opening doors to allow access in and also out of the Data Center areas?
- Regarding all badge controllers and/or biometrics readers used for door opening, do they record (Logs) main data of the employee, such as name, number, department, position as well as entrance and exit time?
- Is there a backup procedure for all Logs mentioned in the previous item, as well as an off-site backup?
- Is the area where the backup is stored, including the off-site backup area as well, classified as one of restricted and controlled access?
- Do the areas where the backup is stored, including the off-site backup, have systems of: 1- Access Control; 2- Fire Fighting; 3- Ventilation and Air Conditioning; 4- Monitoring?
- Are the Logs mentioned in the previous item being regularly sent to all area owners, including the Data Center Owner and the Security Officer so that they are able to review such logs regarding eventual identification of violations and/or failures?
- Is there an inventory control for all badges registered in the access control system, including those that are available but still not active in the access control system?
- Does the inventory control mentioned in the above item comprehend all badge numbers and respective holders as well as the people who approved each of them?
- Do all badges used by employees hold all the basic and necessary information to identify the employee, such as name, number, picture, department, id. Document, etc.?

- Do all badges have labels or warning texts containing information with the procedure to be followed in case the badge is lost or stolen?
- What happens when a badge is lost or gone astray?
- What employee and/or department is responsible for taking due actions when badges are lost?
- Is there an area where all available badges and the inventory control are stored?
- Is the area where the badges and inventory control are stored one of restricted and controlled access?
- Does the area where the badges and the inventory control are stored have systems of: 1- Access Control; 2- Fire Fighting; 3- Ventilation and Air Conditioning; 4- Monitoring?
- Do all Data Center areas' doors have any alarm device that shows when they are opened and/or violated, mainly those with access to the outside of the Data Center?
- Does the alarm system mentioned in the previous item have sound and visual features too?
- Is the employee and/or department in charge receiving the alarm warning automatically?
- How long does the employee/department take to reach the place when the alarm goes off?
- Does the employee and/or department in charge inform and record all details of the event with the responsible/involved departments, as well as all Data Center area owners, the Data Center owner and the Security Officer?
- Are all steps taken to close the event with all involved owners, including the Data Center owner and the Security Officer?
- Is there one or more systems that control the opening devices of all doors, as, for instance the badge or biometrics readers control systems, etc.?
- Is there one employee and/or one department that is responsible for controlling/managing all systems mentioned in the above item?
- Is there a backup procedure for the systems cited in the above item, as well as an off-site backup?
- Is the door opening control/management systems area, as well as the backup area and also the off-site backup area of restricted and controlled access?
- Does the door opening control/management systems area, as well as the backup area and the off-site backup area have systems of: 1- Access Control; 2- Fire Fighting; 3- Ventilation and Air Conditioning; 4- Monitoring?
- Do the Data Center door opening control/management systems, as well as all employed features/devices, have redundancy to handle cases like disasters, power black-outs, total badge loss, etc.?

Air Conditional Audit Checklist

- Do all Data Center areas have a ventilation and air conditioning system?

- Are the features/devices used by the ventilation and air conditioning system (machines and structures) shared through only one machine and structure or are there areas that have their independent features/devices?
- Where is the structure for ventilation and air conditioning installed in all Data Center areas? For example, above the suspended ceiling, below the raised floor or even in the equipment area.
- Is the ventilation structure in all Data Center areas duly protected by any feature that prevents its violation? For example, steel pipes, aluminum ducts, dampers, sealing, etc.
- Is the temperature for all Data Center areas in accordance with each area's facilities, material and installed equipment needs?
- Is there a central system/console to manage all ventilation and air conditioning features/devices, as well as an employee and/or department that is responsible for such management and control?
- Is the area where the central console for control and management of all ventilation and air conditioning features/devices is located an area of restricted and controlled access?
- Does the area where the central console for control and management of all ventilation and air conditioning features/devices is located have systems of: 1- Access Control; 2- Fire Fighting; 3- Ventilation and Air Conditioning; 4- Monitoring?
- Do all ventilation and air conditioning features/devices as well as its control and management system have any redundancy procedure to deal with cases of disasters, power blackouts, violation and/o defects/failures, etc.?

General Patch Management Checklist

Process Management

- Documented Patch Management Process in Place
- Manager/Owner responsible for Patch Management Process for each system, server and database
- Training for Patch Management Managers
- Specific Steps in Patch Management Process measured
- Patch Management Process Reviewed for Continuous Improvement

Patch Management planning

- Describe how notification of patches is obtained. This includes operation system, application, middleware, database and etc.
- Is the patch management process integrated into the Change Management Process?
- Describe the decision process for deciding what patches will be implemented
- Are there any patches that get installed by default such as security patches?
- Who has the authority to make these decisions? Ensure the authority has consulted with the owners or users of the system/application.
- Is there a back-out plan for patches that fail?
- Is the helpdesk and users notified when patch installation will cause service outage?

- Are patches installed during planned maintenance periods
- Is there a communication process for informing all patch managers about new patches?

Patch Installation procedures

- Does patch installation follow the Release to Production process? If not, describe release mgmt process followed.
- Are patches tested prior to going online? Is the testing environment comparable to the production environment?
- When changes occur, the systems should be reviewed and tested to ensure that there is no adverse impact on operation or security. This process should cover:
- Review of application control and integrity procedures to ensure that they have not been compromised by the operating system changes;
- Ensuring that the annual support plan and budget will cover reviews and system testing resulting from operating system changes;
- Ensuring that appropriate changes are made to the business continuity plans
- Is there a central point where newly released patches are kept?

Develop management reports

- Show management reports that indicate patch history
- How many emergency patches have been implemented?
- What is the process to do emergency patches? Who has the authority to approve and/or implement an emergency patch?
- Is there a list of patches released but not implemented? If yes, are the reasons explained?

Network Security Checklist

Network Configuration Management

- A risk assessment has been completed for each customer environment. This is periodically reviewed based on change to the customer environment.
- All network moves/adds/changes (configuration / physical) follow a "Change Management" process. Change Management requests are archived.
- A process exists for the archival and storage of all audit logs.
- There is no dial-in access to the Secure Infrastructure LAN.
- Risk analysis has been completed for any dial-in access from customer systems.
- Physical access to the network equipment (routers, firewalls, etc) and consoles is restricted to authorized users/operators.
- Backup and recovery procedures have been designed; backups are performed daily and compared to reference data.
- SNMP passwords are changed so they are neither PUBLIC, PRIVATE, SECRET nor blank. This is on both network equipment, and management stations.
- All administration commands for accessing and modifying configuration information are restricted to authorized users.

- All network components are identified and have been assigned an owner for management and administration.
- System topology, configurations and administration features are clearly documented, reviewed, and are auditable. A periodic review process exists to verify network integrity.
- Any change made to network equipment and/or customer environments has gone through the appropriate approval and review process.
- Service Level Agreements exist for any third party assigned to manage or administer any part or function of the network.
- The monitoring servers storing configuration and log data must follow the appropriate system security standard.
- When a network related application is running on a system platform, the latter must also follow the corresponding OS security standard.
- **Login Access Control**
- Sensitive configuration information such as type and firmware version is hidden until full user authentication.
- Appropriate banner information is displayed at login, indicating that system is to be used by authorized personnel only.
- All network equipment (routers, firewalls, etc), and network configuration files are securely password protected.
- All login attempts (successful and unsuccessful) are logged. Administration access restrictions based on IP address are implemented.
- All equipment ‘default’ passwords are changed.
- All logon accounts on both Company and Customer systems has an identifiable owner.
- There is a system login list maintained as part of the system documentation.
- Process in place to delete all terminated or transferred users who had access to and accounts on the system.
- A secure area exists for storage of written passwords.
- A process exists for 90 day change of passwords.
- A process exists to force a change of passwords, in the event of password disclosure or post system compromise.
- All passwords confirm to Company security guidelines. All staff are aware of these guidelines / standards.
- A regular check is made on appropriate network system passwords, with results logged and followed up.

Security Management

- Relevant host based or network security monitoring tools are installed and utilized. The monitoring of such tools is able to identify, classify, recover and report security incidents.
- Any connection from one customer cell to another is prohibited.
- Any end-user connection from a customer cell into Secured Infrastructure LAN is restricted, and controlled with strong authentication.
- Access between customer cells and Secured Infrastructure LAN are limited to approved (required) ports only.

- A systematic review process exists to resolve, validate and respond to log file exceptions.
- No access can be established from the Secured Infrastructure LAN back in to internal network.
- Access between internal network and the Secured Infrastructure LAN is limited through a secured server only (such as socks).
- A process exists to review all patches, Service Pack and Hot Fixes.
- Major System Patch bundles / Updates and Service Packs are reviewed and applied in a timely manner.
- Network engineers are alert to potential hardware/software security issues, and apply critical security patches, as they are made available.
- Network router access control lists have a control process to ensure validity, integrity and access rights.

Security Training and Development

- Management must allocate sufficient on-the-job time for employees to acquaint themselves with Data Center security policies, procedures and related ways of doing business.
- All network engineer staff have been provided with sufficient training and supporting reference materials to allow them to properly protect the Data Center and its customers information resources.
- Refresher courses and related materials are provided for network staff about their obligations with respect to information security.
- Every worker has completed a security awareness program within three months of starting employment with the Data Center.
-

Reference

[1] Jacobson, Robert V. Computer Security Handbook. ED. Seymour Bosworth, M.E. Kabay. Vol. 4. New York: Wiley, 2002.

[2] Cooper, Dr. Dale F, Tutorial Notes: The Australian and New Zealand Standard on Risk Management, AS/NZS 4360: 1999, http://www.broadleaf.com.au/tutorials/Tut_Standard.pdf

[3] Parker, Donn B. Computer Security Handbook. ED. Seymour Bosworth, M.E. Kabay. Vol. 4. New York: Wiley, 2002.