Global Information Assurance Certification Paper

Access to SAP Service Information Security Management System

GIAC G7799 Certification Practical
Version 1.0
Vladislav Hadzivukovic

June 25, 2004

I Define the system

The company is an information and communications technology (ICT) service provider with approximately 600 employees located across the country. It also manages two high security data centres at two different locations.

Our product offerings include infrastructure management, applications management, information brokerage, business process outsourcing and associated ICT professional services.

The company's mission is to provide quality bundled information and communications technology (ICT) services and solutions, based upon world class infrastructure and technology, which support our clients' business processes.

The company's business objective is that services to clients are delivered in accordance with the security requirements specified in Service Level Agreements (SLA).

The company's Application Access Service hosts business applications in secure data centres and delivers them to clients via private network or over the Internet.

More and more clients ask for < COMPANY NAME> services to be compliant with ISO17799. So the management, Executive Management Team, has asked for risk analysis to be carried out to find out which services have the biggest impact on the loss of revenue. SAP R/3 was among the top ones. The management has then decided to develop and implement an ISMS using ISO 17799 methodology.

Access for SAP R/3 provides clients with a complete service, from basis support and network services through to server management and disaster recovery. We support approximately 100 SAP R/3 systems across many platforms.

The intended scenario covers implementation of dedicated host for any or all IT solutions available from SAP. We install and manage the OS, we install and manage SAP kernel and we install and manage the databases. We also host the server. Client is responsible for the SAP application on the server as well as for SAP GUI on its workstations. This scenario covers the majority of our clients' circumstances.

The objective of the Access to SAP Service Information Security Management System (SAP ISMS) is to ensure that the *confidentiality*, *integrity*, and *availability* of information systems are adequately protected as stated in the SLA so the correct information is available when required by authorized users. Information security supports the business processes that achieve <COMPANY NAME> goals.

Compromised information has a number of consequences, such as encountering considerable penalties, loss of clients and damaged reputation. Access to SAP is a service with significant revenue and as such it is important to accept and deliver contractual obligations for protecting client's information. The request in the market for this service is growing and management has decided that the best way of retaining existing clients and get new ones is to develop and implement a security system for this service that would follow the ISO 17799.

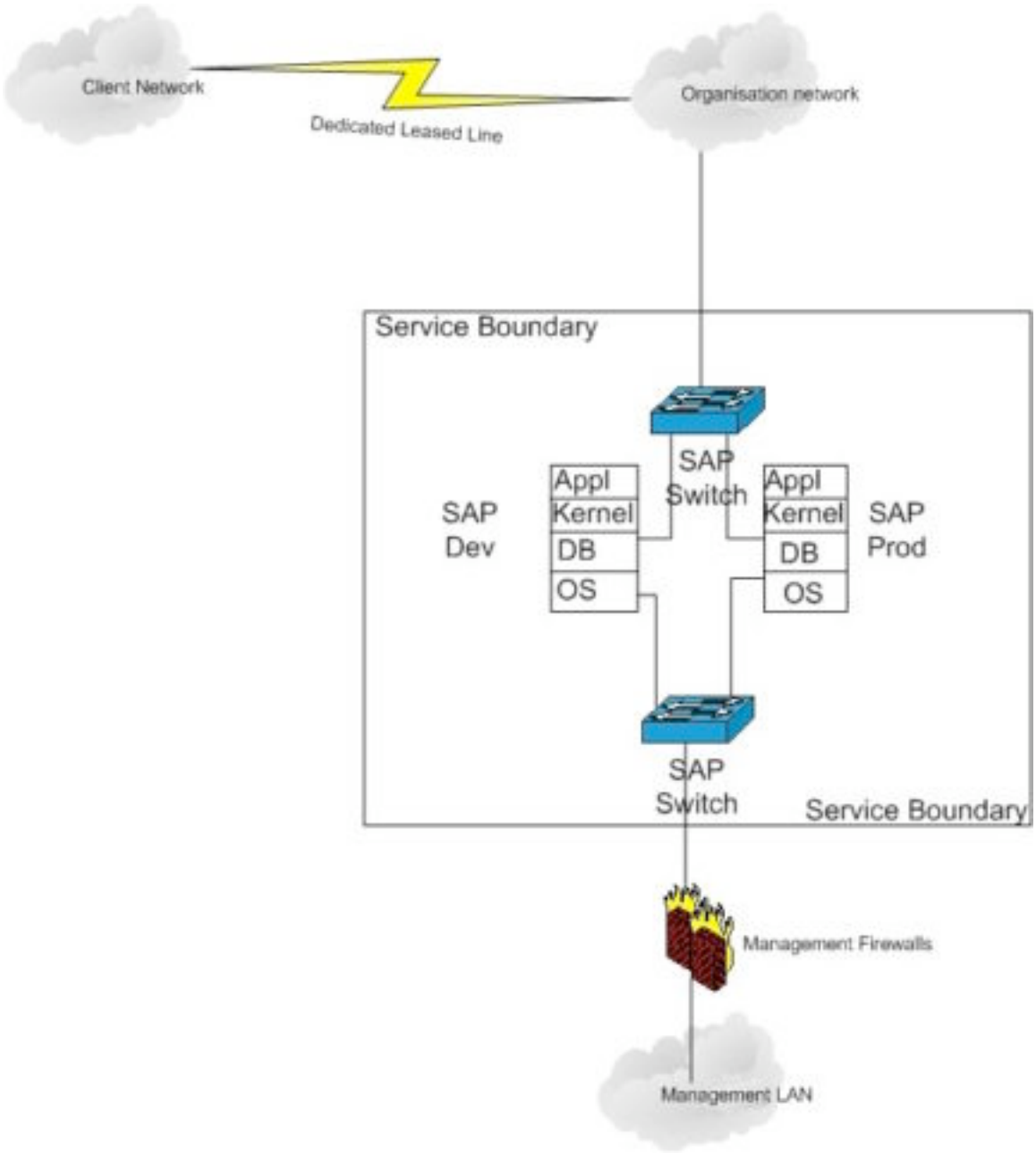
The SAP ISMS covers the information systems supporting <COMPANY NAME>'s key business process, Access to SAP Service. The scope of the SAP ISMS is defined as being those information systems within the domain of the <COMPANY NAME> Internal Advisory Board. Those information systems and their information assets are listed in the SAP Information Asset Register.

All Information Systems covered by the SAP ISMS are physically within the <COMPANY NAME> facilities. These systems are accessed by authorised <COMPANY NAME> staff within <COMPANY NAME> premises.

All Access to SAP Service information systems are managed in-house. There is no outsourcing of management or control of information systems, servers, desktops, data storage, or networks.

The Access to SAP Service Information Security Management System covers the service that is made up of a number of critical information systems provisioned by information assets. The scope covers the implementation of dedicated host for any IT solution available from SAP.

To be able to precisely define SAP ISMS, it is very important to define exact boundaries of the service. The boundaries are presented in the following diagram:



The Hardware included in this service is:

- A switch that connects the SAP hosts to <COMPANY NAME> network
- A switch that connects the SAP hosts to <COMPANY NAME> Management Firewall
- One host for Production
- One host for Development and Testing
- Cables that connect those item

Everything outside of those boundaries is not covered by SAP ISMS.

The Software included in this service is:

- OS running on hosts
- OS running on Switches
- Database
- SAP Kernel
- SAP Application

The <COMPANY NAME> provides full support for the OS, Database and SAP Kernel on the hosts. It also fully supports the switches and the OS running on them and provides the secure physical location for the hardware in the Data Centre.

Through the assignment I will develop and implement ISMS around this system that is in line with <COMPANY NAME>'s Quality Management System and ISMS as well as in accordance with the principles of ISO 17799.

<COMPANY NAME> complies with the requirements of ISO 9001:2000, Quality Management System, and has the registration of the certification. The development and implementation of <COMPANY NAME>'s ISMS is well underway and will be requesting a registration of the certification under AS/NZS 7799.2 within next couple of weeks. A number of security policies and procedures are in place and implemented and they will be used or referenced in the development and implementation of Access to SAP Information Security Management System.

The operation of the SAP Information Security Management System is supported by the following documentation:

- *System architecture and design documents* that describe the security designed into Access to SAP Service
- *Operating procedures and authorities* that describe the procedures to be followed so that systems are operated in accordance with security policy and all changes are properly authorised
- *Information security policies , guidelines, and standards* that describe the minimum rules to be applied so that Access to SAP Service information security risks are mitigated to acceptable levels
- *Business continuity plans* that describe the procedures to be followed to minimise the impact of disruptions to Access to SAP Service

This assignment should show how ISMS for a service should be developed and implemented as well as provide information to <COMPANY NAME> where

discrepancies, weak points, in the overall ISMS are. It will also review existing policies and procedure and provide feedback to <COMPANY NAME> Information Security Management Forum and individual teams.

II Plan

To describe what the real issues are it is necessary to perform a risk analysis on the service. The issues are closely associated with business objectives. Here are presented only three of the major risks:

Business Objective	Provide a reliable service at all times by managing information security within <COMPANY NAME>
Risk	The risk that by not having clear directions from management and its full support could cause a breach of SLA.
Control	Create and publish the security policy. Introduce and document a comprehensive information security infrastructure for Access to SAP Service.

Business Objective	Access to SAP service should ensures that confidentiality, integrity and availability of information systems are adequately protected
Risk	Information systems are made of information assets. The risk not having assets identified is that there is a possibility that the system is not completely protected. That would leave a number of security vulnerabilities to the system.
Control	Create an information asset register.

Business Objective	To provide a long lasting reliable service
Risk	Inadequate architectural design could cause loss, modification or misuse of data. This could damage <COMPANY NAME>'s reputation, <COMPANY NAME> could lose client confidence and encounter financial losses.
Control	Ensure that specific managing capacity planning procedure is in place

As the risks have been acknowledged and not having service ISMS in place some estimates have been produced:

- loss of a number new businesses to competitors, approximately 30% of total of lost businesses
- penalties encountered due to unreliable service and breach of SLA, approximately $25,000.00 per month
- increased costs as planning not appropriate, approximately $15,000.00 per quarter

Overall success of Access to SAP Service ISMS would be measured:

- winning new businesses, the target is to decrease losses to competitors to less than 20% of total fail of wining tenders
- reduce financial losses to less then $10,000.00 per month
- reduce costs due to inappropriate planning, decrease monitoring and staff hours in resolving the issues to less than $10,000.00 per quarter

The implementation of Access to SAP ISMS would require strong management support and cooperation of a number of people throughout <COMPANY NAME>. The timeline for the project has been set at 6 months. The reason for such a short timeframe is that a lot of policies and procedures are already in place. A simple project plan follows SANS '7799 twelve steps of overall ISMS implementation.

Month 1:

- Establish Importance: prepare and present the case of necessity of having Access to SAP Service ISMS to senior management
- Define the Scope: Document Access to SAP ISMS, define boundaries
- Establish Security Organization: create the charter and have the charter and the scope approved at the first inaugural meeting
- High level policy: write the policy, circulate it internally for comments, have the management to accept it, publish it and have it internally announced

Months 2 to 5:

- Identify and classify assets: identify assets used in the service, update the <COMPANY NAME>'s asset register
- Identify and classify risks: perform risk analysis on identified assets by following standard <COMPANY NAME>'s risk assessment process
- Plan for risk management: review the residual risks and review existing policies and procedures, initiate creation of new ones if needed, update the risk register once the controls have been accepted by the committee
- Implement the Risk Mitigation strategy: organize the documentation and have content for training prepared
- Create Statement of Applicability: use Annex A of the BS 7799.2:2002 to document what controls do apply to Access to SAP ISMS
- Training and Security Awareness: check if <COMPANY NAME>'s formal training and awareness program satisfy the requirements of the SAP ISMS

Month 6:

- Monitor and Review: initiate few internal audits
- Maintain and Improve: Review audit results as well as security incidents reports and recommend for either corrective or preventative actions to resolve the issues

- Evaluate ISMS: organize for an external organization to come and evaluate/audit implemented ISMS

The plan will have to be submitted to Project Office for approval and registration as it requires involvement of a number of different teams and staff.

Establish Access to SAP Information Security Management System

As the project plan stated, the first step is to establish comprehensive information security infrastructure for the Access to SAP service.

It is absolutely necessary to obtain full management support and one way of doing it is to establish a management forum, SAP Management Information Security Forum (SAP MISF) with its role clearly defined. It should be a cross-departmental governance forum.

The SAP Management Information Security Forum (SAP MISF) ensures that there is clear direction and visible executive management support for security initiatives within Access to SAP Service. Its charter should be produced and accepted at the first meeting.

High Level Policy

The next task of the SAP Information Management Security Forum (its role is given in the III Do section) is to establish and endorse a high level policy statement. The policy is very similar to <COMPANY NAME>'s Information Security Management Policy Statement and it supports it entirely. It should also be reviewed by <COMPANY NAME>'s Management Information System Forum. It should be signed and dated by the <COMPANY NAME>'s Managing Director. The policy is published on the <COMPANY NAME>'s Intranet and is included in the Service Level Agreements (SLAs).

Establish Committee

The next step is to establish a number of subcommittees with very similar charter of drafting security policies and procedures for their area of responsibilities. Each subcommittee would include a manager/team leader from that area of responsibility, an information security officer, a delegate from legal and contractual department and a quality coordinator that looks after that area.

The responsibility charter for subcommittees would be specified and endorsed by SAP MISF or <COMPANY NAME> MISF.

There are a number of other committees within the <COMPANY NAME> that report directly to <COMPANY NAME> MISF and they, if requested, have significant input to SAP MISF. The following committees are already in place:

Operating System
Database
Physical Security
Personnel Security
Network Management
Data Centre

As stated previously the SAP Information Security Management System (SAP ISMS) is controlled through a management framework that identifies roles and responsibilities for information security within Access to SAP Service.

The SAP Committee coordinates the implementation of security policy across the service and reviews the operational performance of security measures.

This was a management infrastructure but I believe it is also important to mention other teams and roles in the Access to SAP service.

A number of other teams offer various supports to SAP ISMS.

- The service Quality and Strategies Unit support the SAP ISMS through internal audits and process development.

- The Information Security Team (IST) supports the SAP ISMS through:

  - risk assessment
  - policy development
  - training and awareness
  - business continuity management
  - liaison with external agencies
  - advisory and consulting services

- The Security Operations Team supports the SAP ISMS through:

  - configuration validation
  - change review
  - technical audit
  - incident response
  - monitoring and forensics
  - management of critical security infrastructure

Teams, such as SAP Basis Team (supports for the SAP kernel), Database Team (supports database), OS Support Team (supports host Operating System), Network Engineering Services Unit (supports switches and OS running on them) and Data Centre Services Unit (supports hosting service) support SAP ISMS through:

- implementing security policies in their operating procedures
- following procedures
- facilitation of audit
- managing information systems to security policies
- investigating security incidents

There are also a number of other units and teams that have impact in Access to SAP Service such as Sales and Marketing, Business Services, Technology and Strategies Services as well as Finance and Corporate Services.

Identify and Classify Assets

Access to SAP Service is made of a number of different Information Systems. Information Systems are often common/shared (ex, Data Center), but there are also individual ones that are specific for this service. This is a reason why a number of controls, already in place, could be used (or if necessary with some modifications) in this service. Every Information System is made of Information Assets. There are assets that belong to different Information Systems (ex, air-con as an asset that belongs to Data Centre as well as to Network Management Information Systems). This can be portrayed with the following representation:

Service ← Information Systems ← Information Assets

Identifying and Classifying Assets is done during the Technical Architecture Design Process. As part of the development of the new SAP ISMS, it is necessary to recognize new critical Information Systems:

- SAP
- Host Management running SAP

Other Information Systems that have significant impact in Access to SAP Service are:

- Data Centre
- Network management
- Charging (invoice customer charging management)

- Register of suppliers (including contract staff)
- Sales tracking and reporting
- Network services job tracking
- Fault tracking and reporting
- HR

The next step is to recognize Information Assets that build new Information Systems:

- Physical (routers, hosts, switches, mass storage)
- Electronic (OS, Database, SAP Kernel, SAP Application, Data, logical access)
- Documentation
- User Registration Procedure
- Business Continuity
- Backup
- Archives

Other Information Assets that have impact on Information Systems that have bearing on the service:

- Physical (cables, UPS, air-conditioning, physical access)
- Operational Support (Personnel)

The Information Asset Register is generated as a spreadsheet with multiple worksheets. A single worksheet represents one information system and contains information assets that create that information system. It also contains information about the information system owner, information assets description, information assets classification, assets location and information about the change authority: The template is shown here:

Information Asset Register		**System:**		
		Owner:		
Information Asset	**Description**	**Change Authority**	**Location**	**Classification**

The classification is done according to <COMPANY NAME>'s classification levels:

- **PUBLIC**
  Information is intended for public disclosure in its current form and at the current time. Information integrity must be maintained.

- ***X*-IN-CONFIDENCE**
  The *X* in *X*-IN-CONFIDENCE designates the intended audience for the information. Typical examples include:

-

Intended audience	Classification
<COMPANY NAME> staff only	<COMPANY NAME>-IN-CONFIDENCE
Both <COMPANY NAME> and one (or more) business partner	COMMERCIAL-IN-CONFIDENCE
Client staff only (i.e. should not be disclosed within <COMPANY NAME>)	CLIENT-IN-CONFIDENCE

  Disclosure of the information outside the intended audience could have consequences up to the "Moderate" level

- **PROTECTED**
  Disclosure of information outside the intended audience could have consequences up to the "Major" level

- **HIGHLY PROTECTED**
  Disclosure of information outside the intended audience could have consequences up to the "Catastrophic" level

By default, <COMPANY NAME> information is considered <COMPANY NAME>-IN-CONFIDENCE.

Identify and Classify Risks

There is a standard work procedure that describes the process of risk assessment in the <COMPANY NAME>. That has been followed and is explained here.

The risk assessment is undertaken when either a new information system is developed or a significant change is made to an information system or an important new threat is identified or when more than 2 years has elapsed since the previous assessment was completed.

The first step is "Where a risk assessment is identified, SAP MISF asks SAP Committee. Resource requirements are estimated and then are committed by the SAP Committee. <COMPANY NAME>'s Security Manager is given a task to perform the risk assessment by SAP Committee. The <COMPANY NAME> Security Manager initiates a service request, nominates an Action Officer within the Information Security Team and discusses the requirements with the Action Officer.

The second step is "Scoping a Risk Assessment". That is done by the Action Officer who documents the scope of the risk assessment, using <COMPANY NAME>'s template. If no suitable asset register exists, the Officer lists the information assets within the scope of the security risk assessment, or if a suitable asset register exists, notes the location of the register in the scoping document. Once the scope is defined the Action Officer obtains a signoff of the scope from both the System Owner (SAP Committee chairman) and the <COMPANY NAME> Security Manager as well as records the details of consultations, including issues that influenced the scope for the risk assessment and the location of the Security Risk Assessment Scope document.

The next step is "Identifying Risks and Assessing Risks". The Action Officer (in consultation with the System Owner) lists/identifies threats that may compromise the confidentiality, availability of any critical information assets using <COMPANY NAME>'s risk register spreadsheet template and <COMPANY NAME>'s generic risk register as a guide. By assessing the risks the Action Officer measures both (a) the Likelihood and (b) the Consequence, of each threat occurring using the following tables:

Consequence Scale

Measure	Description
Catastrophic (>$10 Million)	Complete disaster for <COMPANY NAME> - unrecoverable.
Major (>$250 000)	Major problems would occur and threaten the provision of important services resulting in significant loss.
Moderate (>$50 000)	Services would continue but would need to be reviewed or changed.
Minor (>$10 000)	Effectiveness of services would be threatened but dealt with.
Insignificant (<$10 000)	Dealt with as part of routine operations.

Likelihood Scale

Measure	Description

Almost certain	Is expected to occur in most conditions (1 or more times per year).
Likely	The event will probably happen in most conditions (2 years).
Possible	The event should happen at some time (5 years).
Unlikely	The event could happen at some time (10 years).
Rare	The event is highly unlikely to occur.

Risk Levels

Measure	Description
Extreme	Annualised exposure > $1,000,000.
High	Annualised exposure >$100,000.
Medium	Annualised exposure >$10,000.
Low	Annualised exposure <$10,000.

Level of Risk

Likelihood	Consequences				
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
Almost certain	**Low**	**Medium**	**High**	**Extreme**	**Extreme**
Likely	**Low**	**Medium**	**Medium**	**High**	**Extreme**
Possible	**Low**	**Low**	**Medium**	**High**	**Extreme**
Unlikely	**Low**	**Low**	**Medium**	**High**	**Extreme**
Rare	**Low**	**Low**	**Low**	**Medium**	**High**

Tthe Action Officer then enters the appropriate rating in the risk register spreadsheet and determines the level of risks. He updates the risk register spreadsheet.

The last step in this phase is "Reviewing Assessed Risks and Risk Mitigations". The Action Officer reviews the assessed risks with the Security Manager and System Owner. Then he consults, as necessary both within and external to <COMPANY NAME>, to determine appropriate mitigation strategies for each risk assessed to be unacceptable. Alternatives are evaluated and the selected risk mitigation strategies are documented in the risk register spreadsheet.

All consultation and all notes are documented in the service request log.

Plan for Risk Management

This stage is to review the residual risk and find out if the controls as mitigation strategies are acceptable and initiate creation of new procedures or policies if required.

"Reviewing Risk Mitigation Strategy" involves the Action Officer who reviews the mitigation strategy with the System Owner and the Security Manager, records the result of the review and reassigns the service request back to the Security Manager.

The Security Manager initiates the actions necessary to implement the risk mitigation strategy and presents it to SAP Committee. Once the committee has agreed that all the controls (risk mitigation strategies) are acceptable, the Security Manager updates the risk register, notes the implementation requests in the action log, files the completed risk register and notifies the System Owner. The last step is to close the service request.

An extract of the template for the risk register is shown here:

Information Security Risk Register				**System:**	***SAP***		
Information Asset	**Risk Description**	**Likelihood (untreated)**	**Consequence (untreated)**	**Controls**	**Likelihood (treated)**	**Consequence (treated)**	**Residual Risk**

One procedure that had to be produced is "Planning for Capacity Requirements" There is company wide policy named "System Planning Policy" but detailed and specific guidelines were necessary. (Appendix A is <COMPANY NAME>s "System Planning" policy). The procedure had to be expanded to cover the risk of loss of data due to inadequate testing or planning. It is also an answer to the control 10.1, Security requirements of systems.

Implement the Risk Mitigation Strategy

The implementation of the risk mitigation, as a first step, is to organize the documentation. System Owner signs off the risk register and organizes publication of the documentation, policies and procedures. The next stage would be to organize training, to educate all parties (implement policies and procedures). This task is given to HR to organize training in cooperation with SAP committee that would propose the content of the training. HR would keep the records of training attendees.

Statement of Applicability

Access to SAP Information Security Policy is largely implemented through <COMPANY NAME> Quality Management System (QMS). The QMS work procedures and instructions are developed to implement relevant security policies and standards. *Statement of Applicability* documents the link between controls defined in Annex A of BS 7799.2:2002 and SAP ISMS policies and procedures. The majority of relevant policies and procedures are <COMPANY NAME> wide ones that can be easily implemented to SAP ISMS. Only a few new procedures had to be separately developed.

The majority of controls defined in the ISO 17799 are applicable to Access to SAP Service. For example:

3.1.1 Access to SAP Service Information Security Management Policy Document, its creation and publication

3.1.2 Review and evaluation of the policy, evaluation of its effectiveness

4.1.1 Management Security Forum, a management body that gives strategic guidance

4.1.2 Information Security Coordination, operational part of the management infrastructure

8.2 Operational procedures and responsibilities that describes system planning

9.2 User Access Management that would ensure access to information only to those who are authorized

11.1.X Business Continuity Management that ensure continuation of the service in case of unforseen interruptions

12.1.X Compliance that would ensure that Federal and State laws are followed

Statement of Applicability is a document within the scope of the Quality Management System (QMS) and is maintained in accordance with <COMPANY NAME>'s Document and Data Control procedures

Training and Awareness

As previously mentioned, in Implement Risk Mitigation Strategies, training and awareness is coordinated through the HR department. Our <COMPANY NAME> ensures that all personnel defined in the ISMS are competent to perform what is required in regards to <COMPANY NAME> ISMS as well as in the SAP ISMS.

There are three levels of training:

1st level: a part of the induction. At this stage a new employee obtains general information about security in the organization. It covers Passwords, ID Cards, E-mail and Internet use. The new employees also sign a code of behavior sheet.

2nd level: new employees get the <COMPANY NAME> security training (within a month from the commencement of the employment). This session lasts two hours and introduces all security policies and practices to staff. At the end of this training there is a test/quiz to measure the effectiveness of the training. This is all recorded and kept with individual personal files. (Annual repetition/refresher of this training is performed).

3rd level: a specialist/technical training (ex, SAP technical or UNIX administration) is done or organized by adequate Team Leader/Manager. Every Team Leader records education and training as well as experience of team members.

This is all described in HR work procedures and it can be easily implemented in SAP ISMS. Individual Position Descriptions contain information of any security requirements. An example of a security requirement for an OS Administrator is a security clearance with State authorities and training on procedures to enter Data Centre.

Monitor and Review

As the <COMPANY NAME> complies with the requirements of ISO 9001:2000, Quality Management System, and has certification, the registration of the internal audit process is in place and implemented on SAP Information Security Management System. A separate audit schedule, frequency and audit checklists have to be generated for Access to SAP ISMS.

The schedule and frequency of Access to SAP Service ISMS audits are established by the best practice in the <COMPANY NAME> and are documented. The audit schedule is endorsed by the SAP MISF. The document also provides information on different type of audits and who performs the audit. The template for the audit schedule:

Audit Type	Audit Target	Audit Benchmark	Auditing Body	Governance Body (review)	Audit Frequency

The audit process follows the PDCA cycle:

Plan: audit schedule, compliance requirements, resource
Do: define audit scope, establish audit team, create checklist
Check: conduct the audit, generate the report
Action: corrective and preventative actions are raised, management review

In the Plan phase Information Security Team establishes the audit schedule considering:

- the criticality of the system/service
- compliance requirements
- resource availability

The schedule is presented to SAP MISF who reviews and endorses the audit schedule.

The Do phase defines the audit scope by specifying:

- the audit target
- benchmark/standards
- tools and/or checklists
- takes in consideration previous audit reports, corrective and preventative actions

This phase also establishes the audit team. The criteria for the team members are the skills and competencies of the members as well as the availability to perform requested assignments.

During the Check phase, the audit is conducted. It starts with the entry meeting, with auditors and auditees, at which the audit is confirmed and scheduled. The next step is actual audit. The audit results are then evaluated against the benchmarks or standards. The report is produced and it contains all recommended corrective actions and opportunities for improvement. At the exit meeting with auditors and auditees, the report is presented and all corrective actions are agreed on.

In the last phase, Actions, all corrective actions are raised and implemented. At the end the audit report, corrective actions and opportunities for improvement are presented for the review to SAP MISF. The last step is initiation and implementation of preventative actions (opportunities for improvement) and once that is done, the audit register is updated.

Monitoring of the effectiveness of the Access to SAP ISMS is regularly done at individual team meetings as well as on SAP Committee and SAP MISF meetings.

Security breaches and security detected errors in the Access to SAP Service are recognized and promptly actions are carried out by following defined Change Management process within <COMPANY NAME>. The security incidents and

completed actions to resolve them are reported to SAP Committee for review. All significant incidents and actions are recorded in the minutes of the SAP Committee and reported to SAP MISF.

The review of the audits is done at the SAP Committee meetings. The reports are reviewed and the status of corrective and preventative actions is checked. If it is necessary, additional corrective or preventative actions are raised. SAP Committee also reviews and actions opportunities for improvement.

Maintain and Improve

The SAP ISMS is maintained through process. This is managed process applies at three levels:

- Operational review at a Unit level occurs within the Quality Management System (QMS) procedure
- Operational review of the whole Access to SAP Service occurs within the SAP Committee
- Strategic review occurs within the SAP Management Information Security Forum

Operational management review focuses on incidents and audit results, and resulting corrective and preventative actions.

Strategic management review focuses on the alignment of the SAP ISMS with <COMPANY NAME>'s business objective and strategy, risk management, policy and accreditation. Strategic review also evaluates the effectiveness of the SAP ISMS by reassessing training and awareness and audit programs, and reviewing trends in incidents and corrective and preventative actions. It also should review the success of the ISMS implementation in regards to winning new business and financial losses and costs.

Where management review identifies improvements, requests for change are initiated by the appropriate authority and submitted for action through <COMPANY NAME>'s Change Management Process.

For the SAP ISMS to stay effective, it is necessary to regularly review and improve on results obtained from different audits, to use and to review security policy and objectives as well as risk register, and to do analysis of security incidents and events. The emphasis of improvement is to address nonconformity through corrective (reactive) and preventive (proactive) actions. As the new technologies and business requirements emerge so do new threats and vulnerabilities and it all has effect on the Access to SAP Service and SAP ISMS.

In the document, Security audit frequency (Appendix B), the schedule and frequency are described. The audit schedule is endorsed by the SAP MISF. The document also provides information on different type of audits, who performs the

audits and how often the audits are carried out. If significant event occurs, such as change to business or organization that has security implications, an audit can be triggered earlier then scheduled.

Monitoring of the SAP ISMS is done through regular audit reviews on the SAP Committee meetings as well as on the SAP MISF meetings. At the meeting analysis of security incidents and trends is commented on. Also suggestions and feedback from all parties involved is taken into account.

It is essential to constantly improve efficiency of SAP ISMS. This is mainly done through corrective and preventative actions. The processes and procedures for corrective and preventative actions are well documented at <COMPANY NAME> through Change Management Process.

Corrective actions are taken to eliminate nonconformities associated with an event/incident and are reactive responses. Corrective actions are undertaken in order to prevent recurrence of the event/incident. The first steps in the process require identifying the nonconformities, then determine the cause and evaluate the need for action to prevent recurrence. The next steps are to define and implement the corrective actions and review them.

Preventative actions are undertaken to prevent nonconformities from future occurrence. The priority of actions is determined based on the results of the risk assessment. The preventative action process is very similar to the corrective action process. First the potential nonconformities are identified as well as their causes, than preventative actions are defined and implanted. The last step is the review or the actions taken. It is usually more cost-effective to prevent nonconformity than to correct it.

III Do

Using information developed in the previous part, Plan, the steps for the implementation are presented.

1 Create SAP Management Information Security Forum

Problem: The service needs full management support to guide and provide strategies for information security in the service.

Action: the problem is addressed by creating a forum

Steps:
-- Create a charter for the SAP Management Information Security Forum
-- Create an agenda for the first meeting and attach the charter
-- Organize inaugural meeting chaired by the Security Manager
-- Finalize the charter
-- Publish the charter

The charter is presented here and should be accepted at the first inaugural meeting:

SAP Management Information Security Forum

1 Context

To ensure that there is clear direction and visible management support for security initiatives for Access to SAP service and that such activities are consistent with <COMPANY NAME>'s business goals. The SAP Management Information Security Forum (SAP MISF) brings together a cross-departmental group of managers from across <COMPANY NAME>. The forum promotes security for Access to SAP service.

This reference document describes the role and membership of the SAP Management Information Security Forum within the Access to SAP Information Security Management System.

2 Role

SAP Management Information Security Forum:

- Advises <COMPANY NAME> Executive Management Team and <COMPANY NAME> Management Information Security Forum of the impact of information security issues on Access to SAP business objectives and strategy
- Consults with the ICT Steering Committee on the alignment of ICT and information security policies and directions

- Consults with the Project Governance Committee on major initiatives to enhance information security
- Reviews and endorses the information security risk register and mitigation controls (policies)
- Promotes the implementation of information security policies
- Monitors the effectiveness of the SAP Information Security Management System by:
  - Reviewing incident trends and corrective and preventative actions
  - Reviewing the audit program
  - Reviewing the training and awareness program.

3 Membership

The Management Information Security Forum comprises:

- <COMPANY NAME> Security Manager (Chair)
- Manager, Legal and Contractual Services
- A Service Operations Manager
- A Sales Director

4 Meetings

The Management Information Security Forum

- Meets at least two times a year, with additional meetings when required
- Keeps minutes of such meetings

2 High level policy

Problem: The Access to SAP service does not have a high level policy to which all elements of the service would abide by.

Action: Create and endorsed a high level policy.

Steps:
-- Draft a high level service policy
-- Circulate it amongst organizational Information Management Security Forum members
-- Adjust the policy
-- Put on the agenda for SAP Management Information Security Forum meeting to discuss the high level policy
-- Circulate the draft of the policy among all teams
-- Finalize the policy
-- SAP MISF to approve the policy
-- Organize for the policy to be published on the Intranet so it is accessible to all company employees

A copy of the Access to SAP Service policy statement follows:

Access to SAP Information Security Management Policy
Statement:

<COMPANY NAME> recognizes the importance of protecting the value of our client's information that is placed in our custodianship.

We manage logical and physical security risks through an Information Security Management System for Access to SAP (ISMSASAP). The ISMSASAP provides the framework through which our employees protect confidentiality, integrity and availability of our client's information according to its value specified in the Service Level Agreement (SLA).

The detailed policies, guidelines and standards of the ISMSASAP support best practice information security management and complies with legislative, regulatory and contractual obligations. Policies are implemented through the processes and controls of our ISO 9001 Quality Management System.

The objective of this policy is to ensure that:

- All logical and physical security related business risks are identified and managed to a level acceptable to <COMPANY NAME>
- Services to clients are delivered in accordance with the security requirements specified in SLAs.

This policy is endorsed by ICT Steering Committee and Managing Director.

Responsibility for the management of the ISMSASAP is delegated to organization Security Manager, supported by his team. He convenes SAP Management Information Security Forum (SAPMISF) as a cross-departmental governance forum. Under its charter SAPMISF reviews and approves security policies that directly affect Access to SAP and coordinates the implementation and review of information security according to Access to SAP SLAs.

This policy is signed and dated by Managing Director.

3 Create SAP Committee

Problem: There is no body in the organization that would support clearly directions for the security initiatives for the service.

Actions: Create the SAP committee with clearly defined chart that would represent operational part of the implementation of the security policy.

Steps:
-- Create a charter for SAP committee and have it discussed and approved by SAP MISF
-- Organize first meeting for the committee and have the roles of the committee explained and commented on
-- Finalize the committee's charter
-- Publish on the Intranet the charter and make it available to all company's employees

The following new subcommittee charter is presented here:

SAP Committee

1 Context

To ensure that there is clear direction and visible support for security initiatives for SAP and that such activity is consistent with <COMPANY NAME>'s business goals and SLA. SAP Committee is a cross-functional, representative group of operational managers or their representatives who coordinates and reviews the implementation of information security controls within SAP.

This reference document describes the role and membership of the SAP Committee within the Access to SAP Information Security Management System.

2 Role

SAP Committee:

- Agrees specific roles and responsibilities for the implementation of security policy
- Ensures that security training needs are recognised and incorporated into training program
- Ensures that security is addressed within the Change Management Process , including the design of new systems or services and the implementation of projects
- Reviews security incidents and resulting corrective and preventative actions
- Reviews internal audit reports and initiates additional corrective or preventative actions as required
- Monitors the progress of corrective and preventative actions resulting from security incidents or audits
- Advises SAP Management Information Security Forum of trends in security incidents and emerging threats
- Promotes the continual improvement of SAP Information Security Management System

3 Membership

The SAP Committee comprises:

- SAP Team Leader (Chair)
- A representative from Information Security Team
- A representative from Legal and Contractual Services
- A representative from Quality Management Unit
- Access to SAP Product Manager
- Service Operations Team Leader responsible database
- Service Operations Team Leader responsible for operating systems
- Service Operations Team Leader responsible for network management

4 Meetings

The SAP Committee

- Meets at least four times a year, with additional meetings when

required

- Keeps minutes of such meetings

4 Identify and Classify Assets

Problem: For an effective service all service assets need to be identified and classified. Assets need to be identified during the technical design phase, and the asset register for the service has to be created. There is no asset register for this service.

Action: Generate the asset register.

Steps:
-- Raise a request to service owner for establishment of the asset register for Access to SAP service
-- Follow up with the request

The pull out from the asset register for SAP system is presented here:

Information Asset Register		**System:**	***SAP***	
		Owner:	***JOE BLOGGS***	
Information Asset	**Description**	**Change Authority**	**Location**	**Classification**
Data	*Billing information, Customer master, Vendor master, Financial data, Project data, Purchasing information, Financial Asset data*	*Systems Accountant*	*SAP production box*	*<COMPANY NAME>-IN-CONFIDENCE*
	Test and development data	*Systems Accountant*	*SAP development box*	*<COMPANY NAME>-IN-CONFIDENCE*
Documentation	*Self documenting code*	*Client's Request*	*SAP Developing host, Intranet*	*<COMPANY NAME>-IN-CONFIDENCE*

	Requirements Specifications	*senior ABAP Programmer*	*Signed hardcopy in cabinet*	*Commercial-IN-CONFIDENCE*
	Requirements Specifications variations	*senior ABAP Programmer*	*soft copies (<COMPANY NAME> internal file server) Signed hard copies in cabinet*	*Commercial-IN-CONFIDENCE*
	technical specifications	*senior ABAP Programmer*	*SAP Dev and SAP Prod Boxes*	*Commercial-IN-CONFIDENCE*
	technical specification variations	*senior ABAP Programmer*	*SAP Dev and SAP Prod Boxes*	*Commercial-IN-CONFIDENCE*
	test scripts	*Systems Analyst*	*SAP Dev Boxes*	*Commercial-IN-CONFIDENCE*
User Guide(s)	*DDS On-demand procedures*	*Systems Accountant*	<COMPANY NAME> internal file server	*<COMPANY NAME>-IN-CONFIDENCE*
	SAP Online help	*Systems Accountant*	<COMPANY NAME> internal file server	*COMMERCIAL-IN-CONFIDENCE*
	Desktop procedure manuals	*Systems Accountant*	<COMPANY NAME> internal file server	*COMMERCIAL-IN-CONFIDENCE*
User Registration procedures	*<COMPANY NAME> work procedures and forms*	*Systems Accountant*	*<COMPANY NAME> Quality Management System*	*<COMPANY NAME>-IN-CONFIDENCE*
Operational Support procedures	*application procedures*	*Systems Accountant*	*<COMPANY NAME> Intranet server*	*<COMPANY NAME>-IN-CONFIDENCE*
	programming standards	*Senior ABAP Programmer*	*<COMPANY NAME> internal file server*	*<COMPANY NAME>-IN-CONFIDENCE*
	naming standards	*Senior ABAP Programmer*	*<COMPANY NAME> internal file server*	*<COMPANY NAME>-IN-CONFIDENCE*
	systems procedures	*Systems Accountant*	*<COMPANY NAME> Quality Management System*	*<COMPANY NAME>-IN-CONFIDENCE*
	work procedures	*Systems Accountant*	*<COMPANY NAME> Quality Management System*	*<COMPANY NAME>-IN-CONFIDENCE*
	DDS On-demand	*Systems Accountant*	*<COMPANY NAME> internal file*	*<COMPANY NAME>-IN-CONFIDENCE*

	procedures		*server*	
Business Continuity Plan(s)	*SAP based plan*	*Systems Accountant*	*<COMPANY NAME> internal file server Hard copies in cabinet*	*<COMPANY NAME>-IN-CONFIDENCE*
Backups	*<COMPANY NAME> silo back-up service*	*Systems Accountant (recovery)*	*Off-site storage (Recall)*	*<COMPANY NAME>-IN-CONFIDENCE*
Archives	*Included in current system*	*Systems Accountant (recovery)*		*Commercial-IN-CONFIDENCE*
	Last updated:	***21-Apr-04***		

And the extract from the asset register for Host Management system is given here:

Information Asset Register		**System:**	***Host Management***	
		Owner:	***Mo Bloggs1***	
Information Asset	**Description**	**Change Authority**	**Location**	**Classification**
Data	*Information required for Host Management. E.G. Host Diagrams, Clients, Host Devices, System Admin,OS Version.*	*Manager, SAP Basis*	*Internal Host Management Server*	*<COMPANY NAME>-IN-CONFIDENCE*
Documentation	*Document Management System*	*Manager, SAP BASIS*	*Internal Host Management Server*	*<COMPANY NAME>-IN-CONFIDENCE*
User Guide(s)	*Server and Application Support*	*Manager, SAP BASIS*	*Internal Host Management Server and Hard Copies.*	*<COMPANY NAME>-IN-CONFIDENCE*
User Registration procedures	*Procedures described in the <COMPANY NAME> Quality*	*Manager, SAP BASIS*	*Internal Host Management Server*	*<COMPANY NAME>-IN-CONFIDENCE*

	Management System			
Operational Support procedures	*SAP BASIS Procedures*	*Manager, SAP BASIS*	*Internal Host Management Servers*	*<COMPANY NAME>-IN-CONFIDENCE*
Business Continuity Plan(s)	*Host Management BCP*		*Internal Host Management Servers and hard copies*	
Backups	*Silo Backup System Redundancy: 3 host management servers*	*Manager, SAP BASIS*	*Off-site storage (recall)*	*<COMPANY NAME>-IN-CONFIDENCE*
Archives	*Host Diagram, System Document Management, Hosts Configuration, Availability Data*	*Manager, SAP BASIS*	*Host Management server 2 and 3*	*<COMPANY NAME>-IN-CONFIDENCE*
	Last updated:	***22-Apr-04***		

5&6 Identify and Classify Risks and Plan for Risk Management

Problem: This can only be performed once the asset register is created. There is no risk register for this service

Action: Produce a risk register

Steps:
-- Raise a request to Security Manager to put on the agenda of the SAP MISF meeting a need for the risk register for Access to SAP Service
-- Follow up with request
-- Organize a meeting with Security Manager and Service Owner to review the risk register

Information Security Risk Register				**System:**	***SAP***		

Information Asset	Risk Description	Likelihood (untreated)	Consequence (untreated)	Controls	Likelihood (treated)	Consequence (treated)	Residual Risk
Data	*Loss , modification or misuse of data;*	*Likely*	*Moderate*	*ORGPOLS 631: Authorized Software; ORGPOLS 321:Asset Classification; ORGPOLS 671: E-commerce; ORGPOLS 672: Electronic mail;* SBTWP03: Communication between Teams	*Unlikely*	*Moderate*	*Medium*
	Uncontrolled access	Likely	Major	ORGPOLS 711: Access Control;SBTWP001: SAP Administration; ORGPOLS 721: User Access Management; ORGPOLS 722: Passwords ; SBTWP03: Communication between Teams	Unlikely	Moderate	Medium
	Loss of data in networks, or loss of protection of supporting infrastructure	Major	Almost certain	ORGPOLS 651: Network Security; ORGPOLS 911 Business Continuity	Unlikely	Minor	Low

	Hardware loss, or comprise or damage	Moderate	Likely	ORGPOLS 521: Data Centre; ORGPOLS 522: Equipment maintenance; ORGPOLS 911: Business Continuity; ORGPOLS 523: Disposal of media and equipment	Unlikely	Minor	Low
	Loss of data due to inadequate testing or planning	Major	Possible	ORGPOLS 621: System Planning; SBTWP04: Planning for Capacity Requirements; SBTWP01: SAP Administration	Unlikely	Minor	low

Documentation	*Loss or damage of requirements specification through human error, theft or ,fraud*	Major	Likely	ORGPOLS221: Service level Agreement; ORGPOLS411: Personnel security; ORGPOLS431: Management of security incidents;ORGPOLS911: Business Continuity plan; ORGPOLS511: Secure area (physical access)	Possible	Minor	Low
User Guide(s)	*Loss or damage of operating procedures*	Moderate	Likely	ORGPOLS611: Documented Operating Procedures; SBTWP001: SAP Administration; ORGPOLS911: Business Continuity Plan	Rare	Minor	Low

User Registration procedure	*Uncontrolled access to information systems (system & application)*	Moderate	Likely	ORGPOLS711: Access Control; SBTWP001: SAP Administration; ORGPOLS722: Passwords; ORGPOLS221: Service Level Agreement	Unlikely	Moderate	Medium
Operational support procedure	*Unauthorized user access to SAP Basis procedures*	Moderate	Likely	ORGPOLS611: Documented Operating Procedures; SBTRF002: Hardware Configuration; ORGPOLS711: Access Control; SBTWP001: SAP Administration; ORGPOLS722: Passwords; ORGPOLS911: Business Continuity Plan	Unlikely	Moderate	Medium
	Loss of security of application system software	Major	Likely	ORGPOLS612: Change Control;ORGPOLS614: External Service Providers;	Unlikely	Minor	Low

Business Continuity Plan	*Interruption to business activities*	Major	Likely	ORGPOLS 911: Business Continuity Plan; ORGPOLS 221: Service Level Agreement ;	Unlikely	Moderate	Medium
Backup	*Uncontrolled access to media or damage to media*	Moderate	Likely	ORGPOLS 221: Service Level Agreement ; ORGPOLS 821: Protection of Sensitive Information ; ORGPOLS 1001: Compliance; SBTWP001: SAP Administration; ORGPOLS 523: Disposal of Media and Equipment	Rare	Moderate	Low
	Loss of tape in transport	Moderate	Likely	ORGPOLS 221: Service Level Agreement ; ORGPOLS 614: External Service ORGPOLS 821: Protection of Sensitive Information Providers;	Rare	Minor	Low

Archives	*Breaches of <COMPANY NAME> Information Security Policy*	Major	Likely	ORGPOLS 1001: Compliance; ORGPOLS 431: Responding to Security incidents	Unlikely	Moderate	Medium

7 Implement Risk Mitigation Strategies

Problem: There are risks that company does not have mitigation strategies in place. One control that does not have the mitigation strategy is for System Planning Policy. There is a company wide policy that covers the risk on a high level, but there is a specific need for a procedure for this service. It is to cover the risk of loss of data due to insufficient capacity.

Action: Create procedure "Planning for Capacity Requirements"

Steps:
-- Draft a policy
-- Submit the policy to Sap Committee for review
-- Organize for the procedure to be published on the Intranet and make it available to those who require it
-- Follow up with the System Owner to sign off the risk register as the new procedure is now included

The new procedure is presented here:

Planning for Capacity Requirements

1 PURPOSE

The purpose of this procedure is to document the process for managing capacity requirements and it fully supports ORGPOLS621System Planning.

2 DEFINITIONS

Nil

3 RESPONSIBILITIES AND AUTHORITIES

- SAP Practice Manager

- SAP Product Manager
- SAP Basis Team (SBT) Group Manager
- Unix/SAP Basis Team
- Service Manager

4 PROCEDURE

Regular communication is required between <COMPANY NAME> SAP Basis Team and the UNIX group to ensure that client capacity requirements are supplied within the Service Level Agreement (SLA) timeframe. This communication process is outlined below:

a) Notification of Capacity Requirements by Client

- When an initial Service Level Agreement (SLA) is signed, initial capacity requirements are specified.
- The SAP Group Manager is kept informed of client requirements via regular minuted client meetings, via the Service Manager and via pro-active monitoring by the SAP Basis Team staff as recorded in the monthly client report.

b) Request for/Variation of Capacity Requirements

- A SBTFM004 is completed and a copy is supplied to all relevant staff as stated on form. This is the primary interface to the <COMPANY NAME> billing system.
- At the SAP Committee meetings any future proposed capacity requirements are also discussed.

c) SAP UNIX operational Meeting

- Capacity requirements are discussed at the weekly SAP UNIX Operational Meeting. If UNIX advises that capacity is available for allocation, the SAP team proceeds with the required work.
- If capacity is not available, the SAP Group Manager informs the SAP Product Manager to initiate the process to procure more capacity, and relevant branch personnel (account Manager) to obtain client authorisation for increased charges.

d) Procurement of Capacity

- Determine if the responsibility is <COMPANY NAME>'s or the clients.
- If capacity is the client's responsibility, then the account manager is

advised so that marketing and client acceptance of costs can occur.

- If capacity is <COMPANY NAME>'s responsibility, then the SAP Product Manager prepares a Business Case and ORGFM060 for approval. Once procurement of additional capacity has occurred, the SAP team proceeds with the required work.

5 REFERENCE MATERIAL

Nil

6 REFERENCES

System Procedure

7 RECORDS

Completed SAP R/3 Request for Variation in System Configuration
SAP UNIX Operational Meeting Minutes

8 Statement of Applicability

Problem: The Statement of Applicability does not exist

Action: Create and publish a Statement of Applicability

Steps:
-- Draft a Statement of Applicability
-- Organize a meeting with the System Owner for comments
-- Submit the draft to SAP Committee
-- Committee approves and System Owner sign it off
-- Publish it on the Intranet

Extract of the Statement of the Applicability follows:

Statement of Applicability for Access to SAP Service		
Date: 20 May 2004		
Control	**Control objective**	**Policy/Document**
3 Security Policy		

3.1 Information Security Policy	To provide management direction and support for information security	Access to SAP Information Security Management Policy Statement
3.1.1 Information Security Policy Document		Access to SAP Information Security Management Policy Statement - published on the Intranet
3.1.2 Review and Evaluation		SAP MISF charter
4 Organizational security		
4.1 Information Security infrastructure	To manage information security within the Access to SAP Service	SAPMISF001 - SAP Management Information Security Forum, SAPRF001 - SAP Committee, <COMPANY NAME> charter, Individual Position Description
4.1.1 Management information security forum		SAPMISF001 - SAP Management Information Security Forum
4.1.2 Information security co-ordination		SAPRF001 - SAP Committee
4.1.3 Allocation of information security responsibilities		SAPMISF001 - SAP Management Information Security Forum, SAPRF001 - SAP Committee, Individual Position Description for Database Administrator, System Administrator and SAP Team Leader
4.1.4 Authorization process for information processing facilities		ORGSP012 - Change Management Process, ORGPOLS612 - Change Control Policy
4.1.5 Specialist information security advice		Communication with external security <COMPANY NAME> is in the Information Security team's charter, Position Descriptions of certain employees describe them as contact points to application and database suppliers
4.1.6 Co-operation between <COMPANY NAME>s		Legal & Contractual team charter, SLA, ORGSP013 - Incident Management Process
4.1.7 Independent review of information security		ORGPOLS213: Security Reviews, Quality Management Charter includes information in regards to internal audits, SLA
4.3 Outsourcing	To maintain the security of information when the responsibility for information processing has been outsourced to another <COMPANY NAME>	
4.3.1 Security requirements in outsourcing contracts		Not applicable: Access to SAP Service does not have requirements for outsourcing.

5 Asset classification and control		
5.1 Accountability for assets	To maintain appropriate protection of organizational assets	
5.1.1 Inventory of assets		Asset register for Access to SAP Service
5.2 Information Classification	To ensure that information assets receive an appropriate level of protection	
5.2.1 Classification guidelines		<COMPANY NAME> classification level published document
5.2.2 Information labeling and handling		<COMPANY NAME> procedures and instruction for labeling according to classification
8 Communications and operations management		
8.1 Operational procedures and responsibilities	To ensure the correct and secure operation of information processing facilities	
8.1.1 Documented operating procedures		ORGPOLS611: Documented operating procedures, SBTRF007: Service Flow
8.1.2 Operational change control		ORGSPS612: Change Management Process, ORGWPS012: Change Management Procedure
8.1.3 Incident management procedures		ORGWPS05: Reporting Security Incidents, ORGSP013: Incident Management Process, ORGWPS013: Incident Management Procedure, SLA, UNXWP051: User ID, Security Monitoring and Reporting
8.1.4 Segregation of duties		SBTWP003: Communication Between and Within Teams, Position Description for Database Administrator, OS Administrator, SAP Basis Team and Network Administrator
8.1.5 Separation of development and operational facilities		ORGPOLS613: Separation of development and production, SBTRF007: Service Flow, SBTWP001: SAP Administration
8.2 System planning and acceptance	To minimize the risk of system failure	
8.2.1 Capacity planning		ORGRFS621 – System Planning, SBTWP004: Planning for Capacity requirements

8.2.2 System Acceptance		SBTWP001: SAP Admin; ORGRFS613: Separation of Development, Production and Acceptance
8.7 Exchanges of information and software	To prevent loss, modification or misuse of information exchanged between <COMPANY NAME>s	
8.7.4 Security of electronic mail		Not applicable: no e-mail agent run on the hosts

As it can bee seen from this extract, a number of controls are implemented and have policies and procedures in place. For example control 3.1.1, Information security policy document, has reference to Access to SAP Information Security Management Policy Statement. Control 5.1.1 has reference to the Asset register for Access to SAP service. Control 8.2.1 capacity planning, has reference to <COMPANY NAME>'s policy System Planning, ORGRFS621, and a procedure Planning for Capacity Requirements, SBTWP004. SBTWP004 is the new procedure that has been created during Implement Risk Mitigation Strategies step.

Examples of controls that are **NOT** implemented are control 4.3.1, Security requirements in outsourcing contracts, and control 8.7.4, Security of electronic mail. Control 4.3.1 is not implemented as there are no elements of this service that are outsourced, and the control 8.7.4 is not implemented because e-mail software, agent, is not installed and so e-mail is not used on hosts.

9 Training and Awareness

Problem: Is HR covering all training requirements for this service.

Action: Ensure that HR is covering and recording all training for all positions that are required to provide this service, specifically to cover new procedures.

Steps:
-- Organize a meeting with HR representative to check Position Description (PD) for all staff involved in providing the service
-- Inform of the outcome SAP Management Information Security Forum, write a report
-- Follow up with HR if there is a need to update any position description or organize or update any of the security trainings
-- Organize a meeting with team leaders to check if new procedures have been implemented and find out if new training is required.

10 Monitor and Review

Problem: There is no audit schedule for this service.

Action: develop an audit schedule, have MISF to approve it and publish it.

Steps:
-- Use <COMPANY NAME> Security Audit schedule to create Access to SAP Service specific one
-- Submit it to Access to SAP Information Management Security Forum for approval
-- Organize for the audit schedule to be published

The developed audit schedule is included in the Appendix B.

IV Check

Now as SAP ISMS is implemented the review of the system is mandatory to check its effectiveness. I will check compliance to ISO 1799. All the auditing checklists for this assignment are using information form the ISO 17799 checklist.

Security Policy checklist

The Access to SAP Information Management Security Policy has been written and published. The copy of the policy is illustrated earlier (under the High Level Policy subtitle in the III Do section). Also SAP Management Information Security Forum and SAP Committee charters are presented in the Do section (under the headings Create SAP Management Information Security Forum and Create SAP Committee respectively). Interview with senior management would provide answer to the checklists' questions.

Control: A 3.1.1	**Section**: Information Security Policy Document	
Audit Question		
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		
Reason		
The existence of the policy provides the proof of management direction and commitment to information security for Access to SAP Service		
Audit steps	**Findings**	**Compliance**
Find out if the policy exist	Policy exists, and it is sighted	Yes
Find out if it has been approved and signed by senior management	It has been approved by SAP MISF, minutes of the meeting seen. It is signed and dated by Managing Director	Yes
Is the policy published	It is published on the Intranet and available to all staff.	Yes
Is policy clear	It has been circulated amongst management and staff	Yes

Control: A 3.1.2	**Section**: Review and Evaluation
Audit Question	
Whether the Security policy has an owner, who is responsible for its maintenance and review according to a defined review process. Whether the process ensures that a review takes place in response to any change affecting the basis of the original assessment, example: significant security incidents, new vulnerabilities or changes to organizational or technical infrastructures	
Reason	
The regular review of the policy is necessary to reflect any changes in or Access to SAP Service or any organizational changes	

Audit steps	**Findings**	**Compliance**
Does the policy has its owner	The owner of the policy is Security Manager	Yes
Is the owner responsible for its maintenance	Yes Security Manager maintain it	Yes
Is the policy regularly reviewed	The Security manager reviews it regularly. The process of policy reviewing can be improved. It is suggested that this be done in line with the risk assessment	Partial compliance

Organizational security checklist

The charter for Access to SAP Information Security Management Forum and SAP committee are presented earlier in the Do section of this assignment. Individual position description and different team system procedures are not included here. Interview with members of the forum and members of the committee should provide answers to the checklists' questions.

Control: A 4.1.1	**Section**: Management information security forum
Audit Question	
Whether there is a management forum to ensure there is a clear direction and visible management support for security initiatives within the organization	

Reason		
It is important to have management commitment and clear directions in providing information security for Access to SAP service		
Audit steps	**Findings**	**Compliance**
Does the forum exist	Yes, forum exist	Yes
Is the role of the forum clearly defined	Yes, it is described as in the charter of the forum	Yes
Are the roles available to employees	Yes, the charter i published on the Intranet. It has been sighted	Yes
Does the forum regularly meet	Yes, it meets regularly. Recently there has been more meeting as the forum tries to implement ISMS for this service. The minutes of the meetings have been sighted	Yes
Check the minutes	The minutes are on the Intranet and available to all forum members	Yes

Control: A 4.1.2	**Section**: Information security coordination	
Audit Question		
Whether there is a cross-functional forum of management representatives from relevant parts of the organisation to coordinate the implementation of information security controls.		
Reason		
It is important to have involvement from different parts of the company to have different views as well as dissemination of information in regards to information security for Access to SAP service. It also coordinates the implementation of information security controls in all parts of the company that have some involvement in providing service.		
Audit steps	**Findings**	**Compliance**
Does the service has a nominated person or body responsible for maintaining appropriate security measures	The Access to SAP Information Management Security Forum as a strategic body and Sap Committee as an	Yes

	operational body	
Are the members of the forum from different parts of the organization	Yes, there is a cross functional representation described in the charter	Yes

Control: A 4.1.3	**Section**: Allocation of information security responsibilities	
Audit Question		
Whether responsibilities for the protection of individual assets and for carrying out specific security processes were clearly defined.		
Reason		
It is important to have an asset owner as a person responsible for the protection of those assets		
Audit steps	**Findings**	**Compliance**
Are the responsibilities for security issues clearly defined for Access to SAP service	Access to SAP Information Management Security Forum, SAP Committee, Information Security Team	Yes
Check any other relevant roles from the scope of the system	Individual team system procedures, Position Description of database admin, OS system admin and SAP team leader	Yes
Do all the assets in this service have owners	Yes, the asset register contains information about the owner. The register has been seen	Yes
Is the owner aware of the ownership of the assets	Yes, individual interview with the asset owner has been conducted and he has confirmed the ownership	Yes
Check the position description	The ownership is mentioned in the PD	Yes

Control: A 4.1.4	**Section**: Authorization process for information processing

Audit Question
Whether there is a management authorisation process in place for any new information processing facility. This should include all new facilities such as hardware and software.
Reason
It is important that any changes to either service or system are only done with management approval.

Audit steps	**Findings**	**Compliance**
Does the formal change management process exist	There is a company wide Change Management Process in place.	Yes
Does it mention Access to SAP service specifically	No, but all services and systems are included	Yes
Who is responsible for the information system security changes for the Access to SAP service	The responsible person is the System Owner	Yes
Are there procedures for testing hardware and software	Test procedures and instructions have been sighted for both hardware and software	Yes

Control: A 4.1.5	**Section**: Specialist information security advise
Audit Question	
Whether specialist information security advice is obtained where appropriate. A specific individual may be identified to co-ordinate in-house knowledge and experiences to ensure consistency, and provide help in security decision making.	
Reason	
It is absolutely vital for the service to be in contact with different specialist security organizations or agencies. It is a way to obtain latest information about security issues.	

Audit steps	**Findings**	**Compliance**
Does the organization maintain contact with specialists security	Yes. It also has an account set up to receive security information from	Yes

agencies	different agencies	
Does the organization has a current list of contacts	Information Secu Team is the contact point in the organization. Security Manager is on the Access to SAP service Information Management Security Forum and SAP committee	Yes

Control: A 4.1.6	**Section**: Co-operation between organizations	
Audit Question		
Whether appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunication operators were maintained to ensure that appropriate action can be quickly taken and advice obtained, in the event of a security incident.		
Reason		
It is essential to stay in contact with those organization so any changes that can have impact to service are passed on in time to act accordingly		
Audit steps	**Findings**	**Compliance**
Does the Access to SAP service maintains the contact	There is a company wide process that maintains contact with those organizations	Yes
Is there a process to act on advice from those organizations	There are clearly defined two processes: Incident Management and Change management processes	Yes

Control: A 4.1.7	**Section**: Independent review of information security
Audit Question	
Whether the implementation of security policy is reviewed independently on regular basis. This is to provide assurance that organisational practices properly reflect the policy, and that it is feasible and effective.	

Reason		
It is essential to have an ISMS evaluated independently on regular basis to maintain an effective and feasible ISMS		
Audit steps	**Findings**	**Compliance**
Is the implementation of Access to SAP ISMS reviewed independently	Yes , there is a timeframe for those audit to take place	Yes
Is the review regular	Included in the organization's Audit Schedule	Yes

Asset classification and control

The extract from the Asset register for SAP and Hosts Management systems that are part of the Access to SAP service are presented in the Identify and Classify Asset header in the Do section of the assignment. Interview with service owner and asset owners would provide the feedback to the checklist.

Control: A 5.1.1	**Section** Inventory of assets	
Audit Question		
Whether an inventory or register is maintained with the important assets associated with each information system. Whether each asset identified has an owner, the security classification defined and agreed and the location identified.		
Reason		
It is essential to have an asset register to know what to protect. The assets have to be classified to know what and how the information about the asset can be disclosed outside the intended audience.		
Audit steps	**Findings**	**Compliance**
Check the asset register exists	Asset register seen as a published document on the Intranet with access to the document only to authorized people	Yes
Check the ownership	Ownership included in the asset register	Yes
Check the assets classification	Classification included in the asset register	Yes
Check the classification	<COMPANY NAME> has	Yes

levels	a document with the classification levels	
Check if the location of the asset is specified	Location included in the document	Yes
Check actual location	Access to data centre is limited, but accompanied assets have been sighted	Yes
Check that for all systems assets are in the registers	The scope defines two new systems and for both systems assets have been identified (SAP and Host Management)	Yes
Check that assets for all other systems mentioned in the scope are included in the register	There is a <COMPANY NAME> register with all the systems defined	Yes

Capacity planning

Company's System Policy is shown in the Appendix A. The specific procedure for this service has been presented under the header in Implement Risk Mitigation Strategies under the Plan section. Interview with Access to SAP service owner and Unix and Sap team leaders would provide the answers to the checklist questions.

Control: A 8.2.1	**Section** Capacity Planning	
Audit Question		
Whether the capacity demands are monitored and projections of future capacity requirements are made. This is to ensure that adequate processing power and storage are available. Example: Monitoring Hard disk space, RAM, CPU on critical servers.		
Reason		
It is important to provide reliable service and minimize systems failure		
Audit steps	**Findings**	**Compliance**
Is there a policy in regards to System Planning	Yes, there is a company's policy	Yes
Is the capacity monitored	The capacity is monitored. It is described in the UNXWP051: User	Yes

	ID, Security Monitoring and Reporting	
Are there any tools	Toolset and ISM are used	Yes
Are any reports produced and how often	System procedure for SAP Admin explains that monthly reports are made and sent to clients.	Yes
Check the existence of the report	Sighted.	Yes
Is there an alarm set to get activated once the capacity limit is reached	Alarm is raised once the set threshold is reached	Yes
Are initial capacity requirements specified	In the SLA	Yes
Are projection of future capacity requirements made	Technical design documentation and the SLA address this issue as well as procedure for planning for capacity requirements. It is also mentioned in the SLA with the client	Yes

V Act

There are a number of different ways to maintain and improve the Information Management Security System for Access to SAP Service given that it has been put in place. An audit schedule, included in the Appendix B, is in place and by just following it maintenance and improvement should be preserved. A number of internal as well as external audits and reviews would be carried out.

- Revise and update the policy. The audit schedule lists regular review of the High Level Policy every six months. It is done by the Information Security Team under the governance of SAP Management Information Security Forum. The review can also be done earlier if there are significant changes to Access to SAP service or if there are considerable organizational changes in structure or objectives or services. This would trigger a review of all procedures, standards and guidelines relevant to this service and policy. Incidents analysis and lessons learned from the incidents might also initiate a review of the policy. A security incident would mean that a security event has occurred and something in the service is compromised.

- Re-examine the charter of the SAP Management Information Security Forum and SAP Committee to see if all the relevant parties are involved and to see if roles has changed. Discuss if any new committee needs to be established or existing one abolished. This can be included in the standard meeting agenda.

- Regular review of asset inventory is performed as part of the completeness of mitigation strategies audit type. Assessment of the Statement of Applicability and the answer to controls would require existence of the asset register. This is normally done, according to the audit schedule annually.

- Evaluate and review tools that monitor hosts capacity. Currently Toolset and ISM are used to monitor CPU, disks, memory etc, and those tools produce a report and would raise alarms once the scoped limits are reached.

- Quality System team organizes regular audits for all organizational and teams' procedures and instructions. Any issues to service security would have been flagged to Security Manager. The issues would be resolved either through corrective or preventative action process.

- Annual audit of Completeness of mitigation strategies would invoke the review of all procedures and instructions related to the service.

- Any organizational improvement in regards to its Information Security Management System would have positive implications on the Access to SAP service. Any improvements in Change Management or Incident Handling processed would automatically improve this service as it is dependable on them. Lessons learned from security incidents could improve the whole security management process and should be discussed at committee meetings. This would increase the competency in the entire system.

- Organize external audit for the standard compliance with a recognized accredited auditor. From the report invoke corrective and preventative actions to improve the system. The frequency depends on the auditor's schedule.

References

1. AS/NZS ISO/IEC 17799:2001 Information technology - Code of practice for information security management
2. AS/NZS 7799.2:2003 Information security management Part 2: Specification for information security management systems
3. HB 248-2001: Organizational experiences in implementing information security management systems
4. <COMPANY NAME> Information Security Management System
5. <COMPANY NAME> Quality Management System
6. <COMPANY NAME> Risk Management System
7. SANS Institute Course Material for Track 11
8. BS 7799 Audit Checklist

Appendix A

Information Security Management - System Planning

1 CONTEXT

System Planning:

- Planning assumptions for capacity and processing planning have to be documented
- System usage and usage trends are monitored

2 GUIDELINE SECTIONS

- 621-1 Capacity and Processing Planning
- 621-2 System Usage and Trend Monitoring

3 GUIDELINES

621-1 Capacity and Processing Planning

Capacity planning is the prior assessment of the expected impacts from changes to computer systems and networks. The changed load on shared systems (e.g. communications equipment, electricity supply, air conditioning) must also be taken into consideration.

Potential problems include compromised disk, memory, bandwidth, and processor capacity, either at normal and peak processing times.

621-2 System Usage and Trend Monitoring

The usage of various components has to be monitored to recognise potential future problems. The trends give an indication when existing equipment will reach its limitations, and upgrades can be planned accordingly.

The degree of monitoring depends on the importance of the service, as determined by the service level agreement, or identified in the asset register as critical to the <COMPANY NAME>.

Appendix B

Security Audit Frequency

Audit Type	**Audit Target**	**Audit Benchmark**	**Auditing Body**	**Governance Body (Review)**	**Audit Frequency**
Threat assessment	Access to SAP Information Security Risk Register	Risk Register consistent with threat environment	Information Security Team	SAP MISF	Annually, or triggered by external event
Vulnerability assessment	Access to SAP infra-structure	Risk Register addresses identified vulnerabilities	SecOps, IST, external <COMPANY NAME>	SAP MISF	Annually, or triggered by external event
Completeness of mitigation strategies	Statement Of Applicability	Procedural implementation consistent with identified mitigation strategies	IST	SAP MISF	Annually, triggered by changes to SOA, or organizational change
Access to SAP Service Security policy	High Level Policy	Policy consistent with organizational policy and services	IST	SAP MISF	Every six months, or triggered by changes to the service
Configuration integrity	System configuration, Database configuration, Application configuration	Standard or best practice guidelines	SecOps, external <COMPANY NAME>	Security Manager/SAP MISF	As per SAP MISF approved schedule, or triggered by security incident, or by client request (can target all the system or individual components, defined in the scope)
Standards compliance	Relevant <COMPANY NAME> operations	Recognized standard (e.g. ISO 17799.2)	Accredited external auditor	Security Manager/SAP MISF	As per certifying <COMPANY NAME>'s schedule
SAP ISMS review	SAP ISMS	Effectiveness at adequately managing risks to Access to SAP information assets	SAP MISF, external <COMPANY NAME>	EMT	Biennially, if not triggered earlier by management review