

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Table of Contents 1
Laufey_E_Johannesdottir_G7799.doc 2

© SANS Institute 2005, Author retains full rights.

Protecting a payroll system

GIAC Certified ISO-17799 Certification (G7799)

Practical Assignment
Version 1.1

Submitted by: Laufey E. Johannesdottir
Location: SANS 2004, London UK
Submitted Date: 9.2.2005

© SANS Institute 2005 Author retains full rights.

Table of Contents

Abstract 1
System Definition 2
- Introduction 2
- ISMS scope 2
- The organization 2
- Security culture and current state of security 2
- The system selected for this practical 3

Step 1: Plan 3
- Security organization for this ISMS 4
- The ISMS 4
- Planning the ISMS 5
- Project plan for the HR ISMS 5
- Policies in the ISMS 6
  - Access management and monitoring 6
  - Change management in operational environment 6
  - Operational procedures 7
  - Incident management 7
- Risk Assessment 8
- Risk management 12

Step 2: Do 13
- Risk 1 14
- Risk 2 15
- Risk 3 16
- The 7799 controls selected 16
  - Responding to security incidents and malfunctions 16
  - Operational Communications and operations management 16
  - Access control 17
  - Systems development and maintenance 17
  - Compliance 17
- Statements of applicability 18

Step 3: Check 18
- Control objectives and audit items 19
  - Control objective for – 19
  - Control objective for – 19
  - Control objective for – 20
  - Control objective for – 21
  - Control objective for – 21
  - Control objective for – 22
  - Control objective for – 22
  - Control objective for – 24
  - Control objective for – 25
- ISMS improvements 25

Step 4: Act 25
- Audit plan for the ISMS 26

© SANS Institute 2005 Author retains full rights.

Maintaining the ISMS 26
ISMS training 27
Conclusion 28

© SANS Institute 2005, Author retains full rights.

List of Figures

Figure 1 9
Figure 2 11

List of Tables

Table 1 10
Table 2 10
Table 3 12
Table 4 13

© SANS Institute 2005, Author retains full rights.

Abstract

The organization is a financial institution operating in three counties. Each country has its own center of IT operations.

The organization is currently replacing its payroll system with a new HR system that includes a new payroll system and other subsystems that are not available in the old system. The new system has far greater functionality than the old system. Self service functionality for the employees has been added in the new system. This allows employees to access selected data about themselves and data can be exported from the system to be included in on-line banking solutions. The new HR system will only be used for the employees in one location of operations.

The old payroll system was located at and run by the HR department. The system creates a salary payment file that contains bank and salary data for each employee.

The new system will be located in and operated by the company's IT department. The wage payment file created by the new system will contain more data than the old file, e.g. it contains an image and data for the pay slip.

The privacy of the employee's salary and finance data is of major importance within the company.
Employee accounts are therefore access protected so they can only be viewed by the employee himself / herself and a small group of trusted employees.

The HR department is concerned that the new system and the new operational environment might create some exploitable security weaknesses.

The purpose of this paper is to use the ISO -17799 Plan-Do-Check-Act methodologies to assess and control risks related to implementation of the new system.

This system was selected because there are concerns regarding its implementation and operation that must be addressed and acted upon. The best method to do so is to use a well defined methodology to assess and control the risk in a systematic manner.

© SANS Institute 2005 Author retains full rights.

System Definition

Introduction

The assignment is to develop a ISMS for an internal payroll system. The payroll system was selected because the security requirements for the system and its operational environment are different than those defined for applications used to service external customers. There where also concerns about its security that had to be addressed in an objective manner.

ISMS scope

The ISMS will cover the payroll application, the application server and the database for the application. The system applies to the operations staff within the IT department responsible for the operation of the server and database, the central access management group and the staff within the HR department that uses the application.
Data transferred out of this system to other systems is not covered by the ISMS.

The organization

The organization is a leading financial institution with a market share approximately 30% of domestic deposits and lending. The organization provides financial services both locally and internationally. The organization has distinct IT services in each country it operates. IT services for the domestic operation are centralized and the 50 branch offices are serviced from headquarters.
The system selected for this practical is only used for the 1100 domestic employees.

Security culture and current state of security

The organization is in the process of revising its IT security processes in order to make them more formal and more easily testable by internal and external parties.
In order to accomplish this an ISO 17799 compliant ISMS system is being implemented. It will apply to IT operations, system development and software procurement. The project is expected to be completed late in the year 2005.

A Security Organization has been established as part of the ISMS for the company. The Security organization is headed by the Security committee.
On the committee are the directors of Finance and Operations, Human Resources and IT.
Working for the committee are the Information Security Manager (ISM) and Manager for Physical Security.
The Security Committee is responsible for and supervises the implementation of the ISMS. It provides a link to executive management and has the appropriate authority to endorse decisions taken concerning the policies and procedures.

© SANS Institute 2005, Author retains full rights.

The Information Security Officer is commissioned by the Security committee to manage the operation and implementation of the ISMS.

A high level security policy approved by executive management is used by work groups creating detail policies and operational procedures as a frame of reference and a set of minimum requirements.

The system selected for this practical

The system selected for this practical is a new HR system that is currently under development. The system is being developed by a software developer outside the organization. The system will be implemented in phases.
The development and implementation project is controlled by a steering group that consists of the system owner, who is the group leader of the salary group within the HR division, a project manager appointed by the IT division and a project manager appointed by the software developer.

The new HR system is based on a payroll system that has been in use since 1999.
The design is based on three tier architecture, "fat" client, application server and a database server. The system is programmed in C++, Javascript and NET. The main technical changes in the new system are that the database is now Oracle, where the earlier version used Btrieve.

The HR system will be implemented in eight phases.

1. Payroll including web access to pay slips was implemented in January 2005.
2. The next seven parts will be delivered over the next nine months, as of January.
3. Figure 1, in chapter Step 1 is an overview of the system. The dotted line depicts the boundaries of the ISMS.

Step 1: Plan

The HR department was concerned that the project and the new system might incur some security risks and introduces exploitable security weaknesses in comparison to the old system.
The decision to let the IT department operate the new payroll system evoked concerns in the HR department about the confidentiality of the data, now that people outside the HR department would have direct access to the server.
They where also concerned that changes in the access control function of the new system could unintentionally make data in the system available to unauthorized users, e.g. that ordinary employees could get same access as super users.

© SANS Institute 2005, Author retains full rights.

It was considered important that implementation of the system would not proceed until these concerns had been addressed in a constructive manner.

The HR department and the ISM did an appraisal of the system to identify what risks the project and the new system might introduce.
The appraisal was done in an informal manner where the ISM reviewed the project documentation, the operational environment of the current system and the proposed operational environment for the new system.
The outcome of the appraisal was that a distinct ISMS was needed for the HR system as it needs a different level of protection compared to other systems operated by the IT department.

The ISMS for HR system will not cover areas that are already covered by the company-wide or general ISMS. It will instead be focused on areas where the controls defined by the general ISMS are either not ready or not sufficient.

Security organization for this ISMS

A sub-security committee was created for this project. This was mainly done to save time and to keep the work focused on this sole system. The principal Security Committee is more concerned with setting general outlines and defining minimum requirements that apply to the organization as whole.

On the Sub Security Committee for this ISMS are the ISM and the system owner; who is also the chairman. The system owner sets the security objectives for the ISMS and approves policies and controls selected for the system.

Workgroups are writing the policies and procedures. They contain employees from IT operations and HR department, depending on what area they are covering.

The ISMS

The ISMS implemented for the HR system may in no respect set weaker security controls than those defined by the general ISMS that applies to the whole organization. The ISM is responsible for controlling this and keeping the two ISMS's in harmony

There is one basic difference in the purpose of the distinct ISMS for the HR system and the general ISMS for the company.
The latter is mainly concerned with protecting information and systems from unauthorized use from users inside the company and attacks from the outside of the company. The IT operations staff is not considered a security threat and is considered "trusted" in that scenario.
However, the IT staff is not "trusted" in regards to the HR system which requires different approach in how the system is protected and how possible misusage

© SANS Institute 2005

Author retains full rights.

can be identified.
The term IT operation staff is used here as denominator for the system administrators, DBA's and network administrators. These are the people that have the authority to access any data they want. They can give themselves all the privileges they need and the can easily cover their tracks.

The main purpose of this ISMS is therefore to put into place controls that allow the HR department to monitor all access to the system by the IT staff.

This was the original objective of he ISMS before a risk assessment was made for the system and its operational environment.

Planning the ISMS

The time to create the ISMS was limited as the system was already in acceptance testing when concerns about its security were raised. It was important that the ISMS would be focused on areas that portrayed the biggest risk. In order to identify these areas a risk assessment was performed.
The outcome of the formal risk analysis of the system and its environment were used to reassess the purpose of the ISMS and create a project plan.

The results of the risk assessment showed that the vulnerabilities thought to pose the biggest risks where actually not the vulnerabilities that could cause the greatest harm.

The results of the analysis revealed that disclosure of salary information was not the biggest risk. The purpose of the ISMS was therefore redefined to take into account that the biggest risk is that the system is not ready, but is being developed.

The main purpose of the controls that need to be implemented is to protect the system from disruptions caused by installation of new software versions and unauthorized changes.

The lesson learned from this is that a risk assessment in the planning stage of a ISMS can be can be used to identify the real and most important areas of risk. This will help setting the scope and the focus of the ISMS and prevent emphasis on false risks and vulnerabilities. A formal methodology like FCMA can be used to identify risk areas in an objective manner and transform the discussion from "I think" to "I know".

Project plan for the HR ISMS

The project plan has the following main phases;

1. Preliminary definition of ISMS scope *(Finished)*

© SANS Institute 2005, Author retains full rights.

2. Risk assessment *(Finished)*
3. Revised definition of ISMS scope *(Finished)*
4. Implementation of separate test and production environments *(Finished)*
5. Creation of policies *(Finished)*
6. Writing and implementing procedures:
   a. System testing and system acceptance
   b. Change management in operational environment *(Finished)*
   c. Access management and monitoring
   d. Outsourced software development
7. Perform risk assessment for new parts of the application – this is a recurrent activity until all phases have been completed.

The HR ISMS project is planned to finish in March.

Policies in the ISMS

Policies that are needed in this ISMS to address the vulnerabilities identified in the risks assessment are:

- Access management and monitoring.
- Change management in operational environment.
- Operational procedures.
- Outsourced software development.
- Incident management.

This is not a complete list but serves as an example of the policies that needed to be written or extended.

Access management and monitoring

Purpose
The system owner must define who can access the system and what privileges each user group can have in the system. Access control must be based on "need to know" principle.
Audience
All employees.
Areas of 7799 addressed
9.1 Business requirement for access control.
9.2 User access management
9.3 User responsibilities.

Change management in operational environment

Purpose
To protect the operational environment from changes that could disrupt operation (availability or integrity) of the application.
All changes in the operational environment must be authorized by the system owner.

© SANS Institute 2005, Author retains full rights.

Audience
IT staff responsible for operating the application server and database. (Developers have no access in production environment).
Areas of 7799 addressed
10.5.1 Change control procedures
8.1.2 Operational change control
8.1.4 Segregation of duties
8.1.5 Separation of development and operational

Operational procedures

Purpose
The maker of the application has defined how it must be operated and the system owner / users have documented their demands for availability. Operational procedures must be documented in order to meet these requirements.
Audience
IT staff responsible for operating the application server and database.
Areas of 7799 addressed
8.1.1 Documented operating procedures

Outsourced software development
Purpose
To state what demands the organization makes of the developer regarding change management, version control, quality of the work and licensing.
Audience
The buyer of the application (HR department) and the seller (developer).
Areas of 7799 addressed
10.5.5 Outsourced software development

Incident management

Purpose
To define how the organization will respond to security incidents to minimize damage and how similar events can be preventive.
Audience
All employees.
Areas of 7799 addressed
6.3 Responding to security incidents and malfunctions
6.3.1 Reporting security incidents
6.3.2 Reporting security weaknesses
6.3.4 Reporting software malfunctions
6.3.4 Learning from incidents
6.3.5 Disciplinary process
12.1.7 Collection of evidence
8.1.3 Incident management procedures

© SANS Institute 2005 Author retains full rights.

Procedures that describe what must be done to obtain the objectives set in the policies are written and implemented by the work groups. The effectiveness and compliance to the procedures is audited by the ISM.

Risk Assessment

The risk assessment was performed by the system owner, the salary group, the project manager from IT and the ISM. The work was done in a number of brainstorm sessions where the ISM documented the results and acted as a catalyst for ideas and kept the work within the scope of the FMECA methodology.
FMECA was chosen mainly because it includes steps where controls to detect, prevent and limit the damage are defined during the risk assessment stage, not afterwards.

The assessment was performed in two main phases. First the focus was on defining what could possibly go wrong and if it did, what where the consequences. The likelihood of each event was briefly discussed. If the group found that this type of event would probably not happen within the next 18 months or only happen every 5 years or more it was not included in the assessment.

It was helpful not only to concentrate on worst case scenarios, but to discuss all possibilities and identify what elevates a minor incident to a critical problem. The most frequent cause in our case was timing, either at what time in the month the incident occurred (this is a monthly based salary system) or how long the problem persisted. We put the outcome from this into our results and found it helpful information when it came to revising the availability requirements for the HR system.

The group worked with following severity definitions:

I. **Catastrophic** The system fails at the worst possible time and the effect is felt by all employees as well as parties outside the organization. The company is fined in the aftermath.

II. **Critical** The failure is felt by all employees. It takes much effort to remedy the effects of the failure and / or there are big expenses involved.

III. **Marginal** The failure is felt by one to five employees. It takes small effort to remedy the effects of the failure (less than day).

IV. **Minor** The failure is felt by one to five employees. It takes almost no effort to remedy the effects of the failure (less than 1 hour).

© SANS Institute 2005

Author retains full rights.

Figure 1 is a simplified version of one of the diagrams created in step 2 in FMECA and used for the risk assessment.

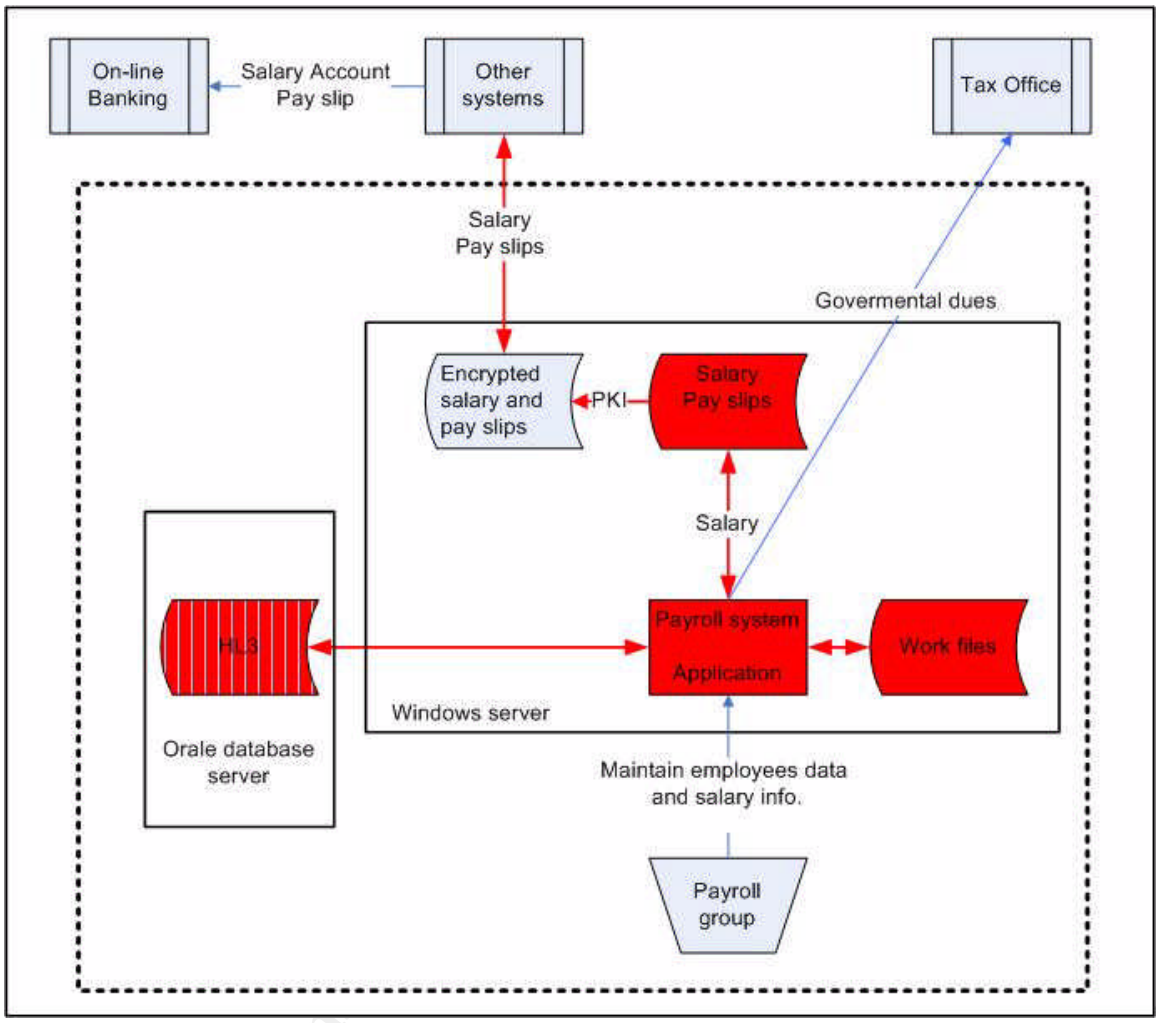


Figure 1

The read parts of the system indicate where data is stored in a text format.

© SANS Institute 2005

Author retains full rights.

Example from phase 1, step 3 and 4 in FMECA.

Table 1

Possible failures and effects				
Point of failure	**Failure**	**Effect of failure**	**Severity**	**ID**
Payroll software	Faulty software	Employees are not paid -> turmoil and discontent	Critical	1
Payroll software	Faulty software	Governmental dues are not paid -> can lead to big fines	Catastrophic	2
Payroll software	Incorrect access control – incorrect access profile -	Disclosure of personal information – unauthorized changes lead to wrong salary calculations – errors hard to find	Critical	3
Payroll Database	Incorrect access control	Disclosure of personal information	Critical	4
Payroll Database	Can't connect to database - Can't run batch jobs	Work can not be done -	Critical - if problem persist for more than 2 hours	5
.... and more				

Table 2

Probability of failure		
Point of failure	**Failure**	**Probability / Frequency**
Payroll software	Faulty software	New versions and bug fixes can contain errors – very likely / 1 pr. month minimum
Payroll software	Incorrect access control – incorrect access profile -	Changes to the access control architecture in the system – adding or updating new profiles / 1 every 3 months
Payroll Database	Incorrect access control	Adding / updating database users / 1 every 2 months

© SANS Institute 2005

Author retains full rights.

Payroll Database	Can't connect to database - Can't run batch jobs	In current environment / 3 – 5 times every week
.... and more		

In the second phase controls that could be implemented to detect, prevent or limit the damage caused by the fault where identified.
In order to find the appropriate controls a fault tree analysis was done for events with Catastrophic and Critical severity.

Figure 2 is an example of the results from a fault tree analysis. The example here is an analysis of why faulty software has reached production environment.

© SANS Institute 2005, Author retains full rights.

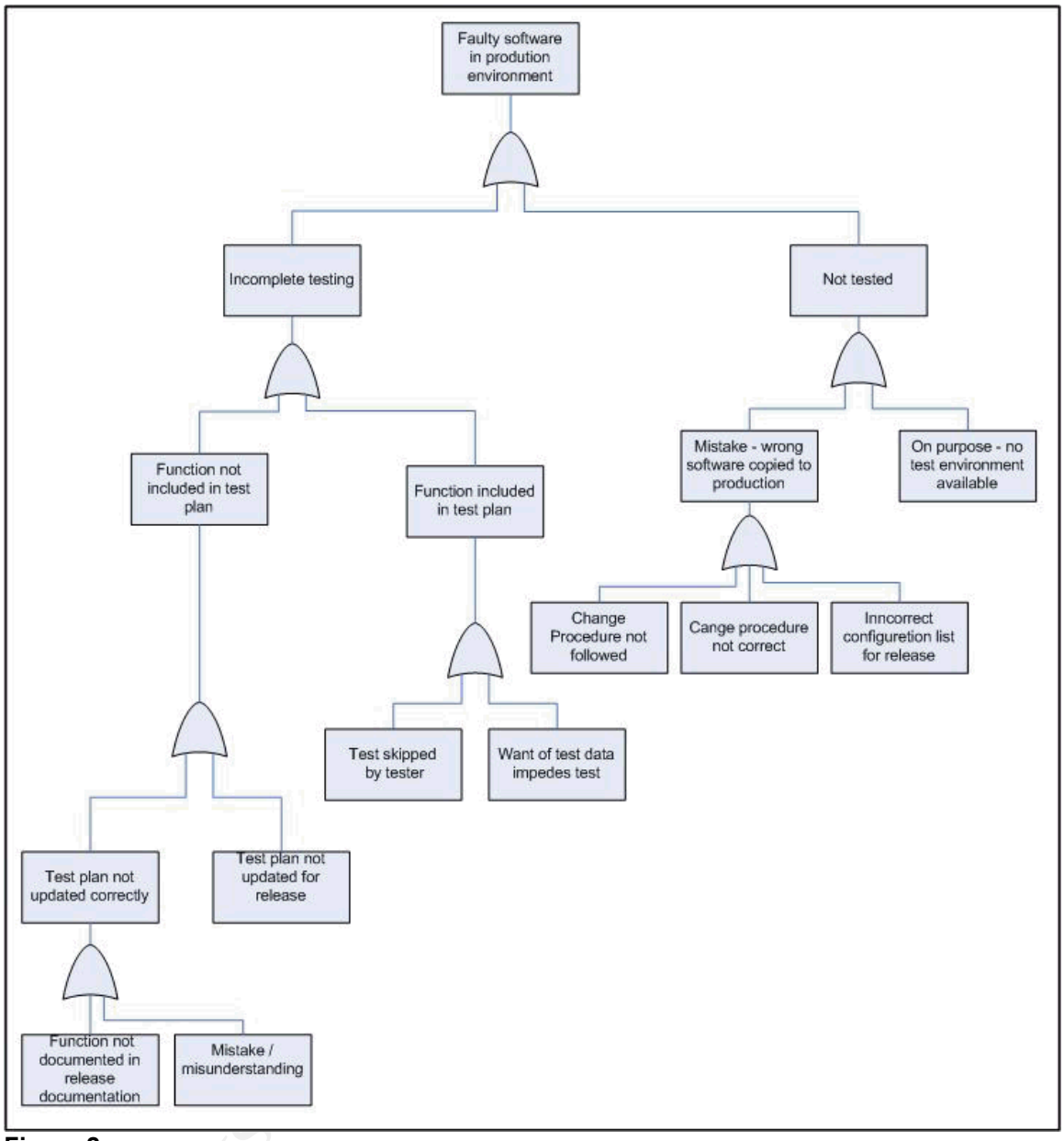


Figure 2

© SANS

The system is under development and this risk analysis covers only the first part. It is therefore necessary to update the risk assessment as new parts are added. This will be done by the same group that did the original analysis. The system owner is responsible for scheduling group meetings. The ISM will verify if the assessment has been updated to reflect changes in the system.

Risk management

Table 4 describes what controls can be implemented to lower the risk defined in table 1 and 2. These controls can not completely eliminate the vulnerabilities but the probability that they will happen after implementation of the controls is considerably lower. The estimated results are documented in table 3. These results have been endorsed by the system owner as acceptable risk.

Table 3

Probability of failure – after complete implementation of controls		
Point of failure	**Failure**	**Probability / Frequency**
Payroll software	Faulty software in production	New versions and bug fixes can contain errors – not likely / every 6 months maximum
Payroll software	Incorrect access control – in production incorrect access profile – in productio	Changes to the access control architecture in the system – adding or updating new profiles / once every 2 years
Payroll Database	Incorrect access control	Adding / updating database users / 1 every 12 months
Payroll Database	Can't connect to database - Can't run batch jobs	In new environment / 2 – 3 times a year
.... and more		

A detailed description for some of the controls from phase 2 of the FMECA is in the following chapter.

© SANS Institute 2005

Author retains full rights.

Step 2: Do

Results from risk analysis phase 2.

Table 4

Controls (Detect / Prevent / Eliminate)				
Point of failure	**Failure**	**Controls**	**Severity**	**ID**
Payroll software	Faulty software	a. Implement separate test and production environment. b. Create and improve test plans and test data. c. Inspect proposed changes and new version. d. Set rules for change management.	Critical	1
Payroll software	Faulty software		Catastrophic	2
Payroll software	Incorrect access control – incorrect access profile -	a. Define what is correct access define what job functions may access what data and use what features, set up profiles for each type of user. b. Test all new access profiles. c. Keep track of who has been given each profile.	Critical	3
Payroll Database	Incorrect access control	a. Define what is correct access – b. Set up monitoring and reporting for the database	Critical	4

© SANS Institute 2005

Author retains full rights.

Payroll Database	Can't connect to database - Can't run batch jobs	a. Implement separate test and production environment – put production database on more efficient hw – b. monitor performance	Critical - if problem persist for more than 2 hours	5
... and more				

This table is an example of the outcome from the risk analysis phase 2. The difference in severity for incidents ID 1 and 2 is due to the fines that the organization can get if is does not pay the governmental dues on time, see also table 1. Next is a details description of what actions need to be taken to implement improvements and controls.

Risk 1

Problem: There is no test environment available so new releases are put directly into production.

Description: A new version (new functionality or bug fix) is put into production and it affects the operation of the system. Employee data is not accessible or salary is not paid on time. The database or files can become corrupt.

Action: It is important to ensure that untested software is not put into production and the testing is as complete as possible. It is also important that testing does not influence the production environment and only the versions that have been tested are put into production. An effective roll-back procedure must be set up and tested to be able to recover quickly, should a defect version be accepted into production.

Steps:

1. Implement separate test and production environment.
    a. Database, all files and program libraries must be completely separate.
    b. An inventory of system parts must be created and maintained.
2. Inspect proposed changes and new version.
    a. Write a procedure for inspection and acceptance of new versions.
    b. Implement 2.a.
3. Create and improve test plans and test data.
    a. Write a procedure for testing that covers how testing is to be

© SANS Institute 2005, Author retains full rights.

prepared and performed, how test plans and test data are kept up to date with the version to be tested.
   b. Write test plans and update for new versions.
   c. Write guidelines for manual checking of calculations.
   d. Create test data and update for new versions.
   e. Implement 3.a to 3.d.
4. Set rules for change management.
   a. Write a procedure for how new versions are put into production. The procedure must cover what is an acceptable outcome from testing, who approves the update and how the production environment is backed up before the new version is implemented. The procedure must also document who can authorize a rollback.

Risk 2

Problem: The access control model for the system is complicated and it is extremely important that users only get the access they are authorized to have based on their job.

Description: The payroll system has an "all disallowed if not explicitly allowed" access control architecture which is good. The granularity is great, almost too much, it is possible in detail to control who has access to what feature and what data. This is both good and bad. When new features and data are being added to the system it is possible to lose track of who has access to what. It is too easy to make mistakes and give too much access to an unauthorized user. It was a concern that new version of the software might modify the rights of and features and thereby invalidate a profile.

Action: An access management procedure that compiles to 7799 has already been implemented within the organization. All applications for access are handled by a central access management group that validates and processes the application. The validation process includes -among other- the following checks: a) is the application authorized by the applicants' supervisor, b) is the application in conformance with the applicants' job functions, c) is the application in accordance with the access rules set by the system owner. A record is kept of all applications and how they where handled.

Documentation must be created by the system owner to be used by the access management group when they validate and process access applications.

Steps:

1. The system owner must validate and document each access profile in the application. The system owner sets rules for what job functions may use each profile.
2. The system owner documents which user groups may get access to the system and what profiles they are allowed to have. All other user groups

© SANS Institute 2005

Author retains full rights.

are not allowed to access to the system.
The documentation must be handed over to the central access management.

3. Verify that update of test plan includes an update of the documentation used in steps 1 and 2.
4. Set up a validation process for access profiles that checks if the documentation of the access profile is in accordance with the current version of the application or have software updates modified the profile.

Risk 3

Problem: Not enough workload capacity in database.

Description: One physical Oracle databases or instances can contain a number of logical databases. The logical databases look like independent databases seen from the user application. Heavy workload in one schema on an instance can have negative effect on the performance of other schemas on the same instance. This is the problem with the current environment. The payroll database is on the same instance as test applications. These tend to create unpredictable workloads that use up all available capacity. New users can not log on to the database and batch jobs can not run while the condition lasts.

Action: The payroll schema must be moved to a production instance where the hardware has more capacity and workload is more predictable.

Steps:

1. DBA must find a production database that has enough capacity for the payroll system.
2. DBA must create new schema and move all data and access definitions to the new database.
3. The payroll schema must be put into the monitoring routine for the instance.

The 7799 controls selected

ISO 7799 controls where not discussed at all until very late in the process. This was done on purpose because most of the participants have limited knowledge of the standard and it was likely that too much emphasis on the standards would cause distraction from the purpose of the work. The ISM did a mapping between the controls defined by the group to controls defined in the ISM 7799 as part of the last stage in this phase. This is a list of controls that apply in the HR ISMS.

Responding to security incidents and malfunctions

6.3 Responding to security incidents and malfunctions
6.3.1 Reporting security incidents
6.3.2 Reporting security weaknesses

© SANS Institute 2005, Author retains full rights.

6.3.3 Reporting software malfuctions
6.3.4 Learning from incidents
6.3.5 Disciplinary process

Operational Communications and operations management

8.1 Operational procedures and responsibilities.
8.1.1 Documented operating procedures.
8.1.2 Operational change control.
8.1.3 Incident management procedure.
8.1.4 Segregation of duties.
8.1.5 Separation of development and operational facilities.
8.2.1 Capacity planing
8.2.2 System acceptance
8.3.1 Controls against malicious software
8.4.2 Operator logs
8.4.3 Fault logging
8.6.3 Information handling procedures
8.7.1 Information and software exchange agreements
8.7.2 Security of media in transit

Access control

9.1 Business requirement for access control.
9.1.1 Access control policy.
9.2 User access management.
9.2.1 User registration.
9.2.2 Privilege management.
9.2.3 User password management.
9.3 User responsibilities.
9.3.1 Password use.
9.3.2 Unattended user equipment.

Systems development and maintenance

10.1 Security requirements of systems.
10.2 Security in application systems.
10.3 Cryptographic controls.
10.4 Security of system files.
10.4.1 Control of operational software
10.4.2 Protection of system test data
10.4.3 Access control to program source library
10.5. Security in development and support processes
10.5.1 Change control procedures
10.5.2 Technical review of operating system changes
10.5.3 Restrictions on changes to software packages
10.5.4 Covert channels and Trojan code
10.5.5 Outsourced software development

© SANS Institute 2005, Author retains full rights.

Compliance

12.1.7 Collection of evidence

© SANS Institute 2005, Author retains full rights.

Statements of applicability

Example of applicable controls.

8. Communications and operations management, the intention of this section of the standard is to ensure the correct and secure operation of the processing environment. Controls applicable for this are;

8.1.1 Documented operating procedures
8.1.2 Operational change control
8.1.3 Incident management procedure
8.1.4 Segregation of duties
8.1.5 Separation of development and operational facilities.

These controls are used in the context to set up separate environments for test and production and to ensure that possible incidents or problems will be effectively dealt with. It must also be documented how to operate the system in a correct and secure manner.

9. Access control, these controls are used to ensure that access to systems and data will by controlled on the basis of business and security requirements. Controls applicable for this are;

9.1 Business requirement for access control.
9.2 User access management
9.3 User responsibilities.

These controls are used in this ISMS to establish procedures for access management. Rules are set for access to the application where it is defined who can get access and what privileges are allowed for each type of user. It is established who can change the rules and when they must be reviewed.

Example of not applicable controls

9.8.1 Mobile computing, used to ensure secure access from mobile users is not applicable here as the only users allowed to connect to the system are users on the internal network. Mobile users are kept on a network separate from the internal workstations.

Step 3: Check

An ISMS is a system where people aim to secure the operation of information systems. They do so by creating documented policies, procedures and guidelines. The system is only effective if the rules are followed and the whole structure is adjusted to changes. Changes are unavoidable; the technological advancement seams to be unstoppable, new legislation puts more strain on information management competition is harder and malicious attacks on IT has become more frequent.

The ISMS must be under constant development. The effectiveness of the

© SANS Institute 2005, Author retains full rights.

system must be examined regularly. The term effectiveness is used here to define whether the system is being followed and whether it is protecting against the correct threats. Regular risk assessment of the ISMS must be performed to verify the latter. Internal audits is the method used to monitor compliance with policies and procedures.

Below are few checks that can be used to monitor compliance to some of the controls selected for this ISMS.

Control objectives and audit items

Control objective for –

Documented operating procedures
The objective of this control is to ensure that is documented how the system is to be operated. This documentation must be complete and available to the staff that is responsible for the operation.

Requirements and importance to this system
Some of the output from this system must be delivered to outside parties within strict time limits. It can lead to fines if the data is not delivered on time. It is therefore important that all jobs are run when scheduled and the output is delivered to the correct recipient within the correct time limits.

ISO reference	8.1.1 Documented operating procedures
Audit questions and checks	
1. Are there documented procedures for the operation of the system? 2. Do the procedures contain instructions on normal start? 3. Do the procedures contain instructions on restart / recovery after abnormal termination? 4. Are jobs defined in scheduler? 5. Is the documentation available to the staff that operates the system? 6. Are there instructions to take backup other than conventional backups?	

Control objective for –

Operational change control
Control of operational software
The objective of this control is to protect the payroll system and its operational environment from untested and unauthorized changes.

Requirements and importance to this system
Changes in any part of the operational environment can disrupt the operation of the system. The environment includes:

- hardware
- network and system software

© SANS Institute 2005

Author retains full rights.

- database
- application software

An inventory of the system configuration must be created to clearly define what the system boundaries are and what parts belong to the operational system and the test system.
The change procedure must ensure that all changes are tracked (who, when, what, why) and that changes have been tested and approved before they are put into production.
Access to do updates in the production environment must be limited to authorized personnel only.
The procedure must cover how changes can be revoked and who authorizes such a back out.

ISO reference	8.1.2 Operational change control 10.4.1 Control of operational software
Audit questions and checks	
1. Is there a documented change procedure for this system? 2. Is there an inventory of the operational system and the test system? 3. Is there a change log? 4. Does the change log contain following info; a. Who requested the change b. Outcome from test c. Who authorized the update d. Who performed the update e. What were the results of the update, success / back out And timestamps for all above events 5. Compare inventory and the real live system. 6. Check who has access to do updates in the production environment.	

Control objective for –

Incident management procedure
The objective of this control is to establish a procedure where all incidents regarding the operation of the payroll system and ISMS are properly handled and documented.

Requirements and importance to this system
Incidents must be responded to in an effective and timely manner before they can escalate to into serious damage. It must be clear to all how to respond to incidents and the experience must be used to prevent similar incidents in the future. Data that can be used to investigate the incident must be protected and kept while incident is not closed.
An ISMS that is out of date with the real live processes and the systems it covers can do more damage than good. It is important that nonconformity and

© SANS Institute 2005

Author retains full rights.

inconsistency is used to develop and update the ISMS to make it more effective.

ISO reference	8.1.3 Incident management procedure
Audit questions and checks	
1. Is there a documented incident management procedure? 2. Is there a registration of all incidents? 3. Dose the registration allow for checking if the incidents been correctly classified and handled? 4. Does the process document time limits for responses ? 5. Have incidents been responded to in a timely manner? 6. Are there examples of incidents that have not been documented? This can only be verified by interviewing staff and reviewing documented incidents. 7. Are logs and other relevant data for open incidents available and protected from unauthorized access? 8. Dose the incident management procedure cover review of incidents by management?	

Control objective for –

Segregation of duties

The objective of this control is to reduce the risk of system being misused and unauthorized updates. .

Requirements and importance to this system

The operational environment for the salary system is sensitive to updates. The number of staff that can update any item in that environment must be kept to minimum. The person who authorized updates of the application software may not implement the version in the production environment.

ISO reference	8.1.4 Segregation of duties
Audit questions and checks	
1. Verify who has system admin rights on the production server, check both local and domain administrators. 2. Verify who has access to the database and what rights they have. 3. Verify logging settings on server and database. 4. Check logs for updates / access.	

Control objective for –

Separation of development and operational facilities

The objective of this control is to keep production environment separated from test so that tests can be performed without risk to the productions environment.

Requirements and importance to this system

The system is under development and each new version must be tested without any risk to the production environment. This can only be achieved if the two environments are completely separate. This check must ensure that no not

© SANS Institute 2005

Author retains full rights.

software or data is shared between the two environments.

ISO reference	8.1.5 Separation of development and operational facilities
Audit questions and checks	
1. Validate database setup and definitions, e.g. configuration files and startup procedures. 2. Validate software paths 3. Validate DDL used 4. Validate files used in each environment	

Control objective for –

Business requirement for access control

Access control policy

The objective of this control is to control access to the payroll system and its data. Access to data and functions is on "need to know" basis..

Requirements and importance to this system

Access to data and functions in the payroll application must be controlled so that each group of users can only access the data and functions that are necessary for them to their job. User groups must be defined based on job functions. Access control rules and privileges must be defined for each user group. The data each group has access to must be defined. These definitions must be mapped to the access profiles defined in the system.

ISO reference	9.1 Business requirement for access control 9.1.1. Access control policy
Audit questions and checks	
1. Has the system owner documented what job functions (user groups) may access the system? 2. Is it documented what data each user group can access / update? 3. Check if the access profiles in the system correlate to the documented user groups. 4. Check if each access profile is working as defined in item 2.	

Control objective for –

User access management

User registration

Privilege management

User password management

The objective of this control is to prevent unauthorized access to the application and its data.

Requirements and importance to this system

The system uses the Windows OS authorization to verify if the user is valid during log-on to the application. Users that have been de-activated in Active

© SANS Institute 2005

Author retains full rights.

Directory are therefore not able log on to the application. The application activates the access profile belonging to the user after checking his validity. Files belonging to and used by the system are stored on the payroll server. It must be verified that unauthorized users can not directly access (bypassing the system) the files and the database schema belonging to the system.
It must be verified that users that have changed jobs have been updated in the payroll application and if users that have left the organization have been removed. It must be verified that all users in the system have correct profile.

© SANS Institute 2005, Author retains full rights.

ISO reference	9.2 User access management 9.2.1 User registration 9.2.2 Privilege management 9.2.3 User password management
Audit questions and checks	
1. Is there a documented access management process? 2. Does access management process include deactivating users that quit? 3. Does access management process include updating user's access profiles when they change jobs internally? 4. Is there a documented password policy? 5. Is there a trace that proves that users have read the policy and agreed to it? 6. Compare users defined in the system and applications from the access management process. 7. Compare access profiles, users and their current job functions to verify that the profile is according to the job function. 8. Compare list of current employees and Active directory. 9. Check who has access to the payroll server, local and domain. 10. Check all grants to the database schema.	

Control objective for –

User responsibilities
Password use
Unattended user equipment
To prevent unauthorized access to the system and its data.

Requirements and importance to this system
Passwords are only effective if they are kept secret, changed regularly and created in a manner that makes them hard to break.
Workstations that are left unattended while logged on to the application can be used by unauthorized users to access the system. Users must be made aware of their responsibilities regarding creation and safekeeping of their passwords.

ISO reference	9.3 User responsibilities 9.3.1 Password use 9.3.2 Unattended user equipment
Audit questions and checks	

© SANS Institute 2005, Author retains full rights.

1. Check if there are there document rules for generation and safekeeping passwords. 2. Verify if the rules for creating passwords are correct in regard to e.g. length and letter combination. 3. Check if there are there document rules logging of or locking workstations when left unattended. 4. Check if the employees are aware of the rules; a. run test on the intranet b. interview employees 5. Check if the employees are following the rules by running a password cracker. 6. Verify that the Account Policies are set in accordance to the rules set in item 1. 7. Check if screen savers have been deactivated

Control objective for –

Protection of system test data
The objective of this control is to protect test data from unauthorized access.

Requirements and importance to this system
The salary system contains only information proprietary to the company. It was decided that a complete testing could only be accomplished by using copy of actual data from the production environment. The data in the test environment must therefore be protected in the same manner as the production data.

ISO reference	10.4.2 Protection of system test data
Audit questions and checks	
1. Compare access profiles in the test and production systems. 2. Compare database grants in the test and production system. 3. Compare who has access to the test server and production server both in Active Directory and locally on the server.	

ISMS improvements

The checklists are primarily used to test compliance to controls defined in the ISMS. They can be used to check if the staff follows the procedures or not. The level of compliance is an indication of how functional the ISMS is.
If the level of compliance is low then the reasons must be investigated to find out the root of the problem. It could be that the procedures are difficult to follow, the documentation is unclear, the staff lacks training or the staff lacks the motivation to follow procedures. It is important that the real reasons for low compliance are found before changes are made.

The results from these checks are reviewed by the ISM and the system owner in order to identify areas where changes must be made.
Results from audits of controls that belong to the general ISMS are reviewed by

© SANS Institute 2005

Author retains full rights.

the Security committee that will decide how the proceed.

Step 4: Act

The ISM is responsible for the operation of the ISMS. She monitors selected procedures e.g. change control in the production environment and takes part in acceptance testing of application systems.

The ISM performs audits on implemented procedures and tracks all incidents. Registered incidents are used to identify areas where improvements can be made. Many incidents originating in the same control, or area, of operation indicate that a control is inappropriate or missing.
The ISM keeps track of all incidents regarding each application system and works with the system owner to establish suitable controls.

The ISM reports to the Security Committee on the effectiveness of the system and proposes changes to the system based on results from audits and registered incidents.

The ISM and Security Committee meet regularly, at minimum once every 2 months to monitor the progress of the implementation and effectiveness of the ISMS for the company.

The Internal Audit function within the company gets a copy of all ISMS audits and incidents. They perform regular audit on the ISM and ISMS. They function as an external audit for the ISMS. The Internal Audit reports directly the Board.

Audit plan for the ISMS

The audit plan for the ISMS must cover all processes in the system during a two year period.
A process should be audited for the first time three to four months after implementation or rewrite. If it is done earlier there might not be enough data and if it is done later then you might have an ineffective procedure causing problems for too long.
A process that has many incidents linked to it should be audited after a shorter period than a process that has no or few incidents associated with it.

Maintaining the ISMS

The ISMS must be adjusted to changes and kept up to date with the business and its priorities.

The change process for the ISMS must be effective or the system can become obsolete and become an obstacle to the secure and effective operation of IT.

© SANS Institute 2005 Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Output from internal and external audit, the risk management process (both for single applications or the whole ISMS) and documented incidents are used by the ISM and the Security Committee to evaluate the correctness and effectiveness of the ISMS. It is important that these documents are reviewed on regular basis and used to control in what directions and how the ISMS developed.

The teams that are writing processes are supplied with management directives from the Security Committee and results from audits and incident management to assisted them in developing the ISMS in the correct direction.

The “Responding to incidents” procedure is used by employees to document when they can not comply with any procedure in the system. They document what procedure was involved and why they could not follow it. The same procedure is used to send improvement tips regarding the ISMS to the ISM. The ISM tracks all incidents and investigates what is the cause for the incident. If a procedure needs a minor adjustment then the ISM can change it and issue a new version. If the process needs major changes it is sent back to the work group that wrote for improvement and rewrite.

ISMS training

The employees that must comply to the ISMS need training in the appropriate parts of the system. The parts that apply to the whole organization are taught by the internal training team. More specific parts that apply only to a small group are taught by members of the group that wrote the process.
Brush up training and general security awareness is be available on the intranet.

.

© SANS Institute 2005, Author retains full rights.

Conclusion

Implementing an ISMS is a process with one main goal.

Protecting IT resources, where the objective it to preserve the confidentiality, integrity and availability.

The controls defined by the ISO 17799 standard can be used to realize this goal, but they must be selected carefully. The controls must be selected based on what resources must be protected and from what.

The experience from this practical has shown that a general ISMS that defines the same controls for all applications might not be sufficient in all cases. Some applications require different type and level of protection than other. The treats and acceptable security level must be identified pr. application.

All applications are not equally important to the business and the effort used to ensure acceptable security level must reflect that.

Effective ISMS must to allow various security levels for different applications. Using big effort to ensure the security in an application that does not contain confidential data and is of low importance to the business is a waste of resources. It is essential that the systems owners decide on acceptable levels of security for their applications after performing a risk assessment.

It is important to perform risk assessment for all systems that are used to support business processes important to the organization. This is a simple method to identify where to focus the effort. It also provides good documentation that can be used to document operational procedures and in business continuity planning.

The conclusion is that you have to differentiate between the applications in the ISMS. One size does not fit all. Each application must be measured to fit, using formal risk assessment methodology and its importance to the business.

© SANS Institute 2005, Author retains full rights.