ISI International Studies in Informatics HAGENBERG

fh OBERÖSTERREICH UNIVERSITY OF APPLIED SCIENCES

JOHANNES KEPLER UNIVERSITY LINZ

softwarepark hagenberg

Name

Dina Helmy
(Egypt)

Advisors

A. Univ.Prof. Dr.
Josef Küng

Company

voestalpine
EINEN SCHRITT VORAUS.

Evaluation of the Implementation Method of an Information Security Management System (ISMS)

The goal of this thesis is to help an internal IT service provider plan and implement an effective Information Security Management System (ISMS). A study of the initial situation at the company is carried out from which a best practice case is selected and examined to provide some guidance on how to establish a reliable basis for ISMS. Finally, a rollout concept is formulated to illustrate how to implement ISMS, as well as its scale of implementation. Certification may be regarded as an optional achievement when the ISMS is as well established as outlined. The company may gain the certification leads to become more trustworthy, reliable, credible, and increases its IT security level.

Service Provider
Security Level
ISO
Project Plan
ISMS

Establishing ISMS According to ISO/IEC 27001, 27002

As with all management processes, an ISMS must remain effective and efficient in the long term, adapting to changes in the internal organization and external environment. ISO/IEC 27001 therefore incorporates the typical "Plan-Do-Check-Act" (PDCA) deeming approach for continuous improvement: The Plan phase is about designing the ISMS, assessing information security risks and selecting appropriate controls. The Do phase involves implementing and operating the controls. The Check phase objective is to review and evaluate the performance (efficiency and effectiveness) of the ISMS. In the Act phase, changes are made where necessary to keep the ISMS as efficient as possible.

As for ISO/IEC 27002, which is also known as code of practice, it provides guidance for the organization to assess their own risks and apply suitable controls. It outlines 11 key controls with 39 security categories.

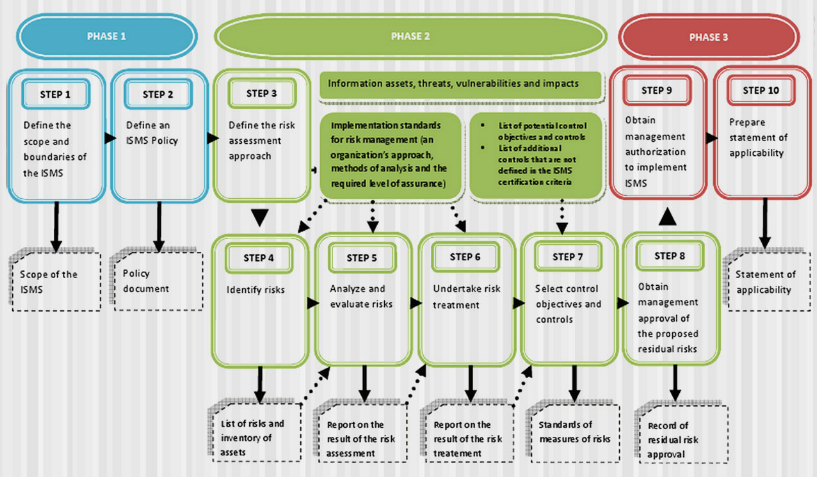
Current Situation at the Company

By examining the initial situation at the company it was found that it has a minimum IT security standards that it follows and a draft for an IT security policy. The initial situation at the company is summarized and compared to the ISO/IEC 27002, the comparison results are tabulated and studied in a gap analysis report. Statistics are done on the results which evoke that the company comply by about 81% with the ISO standards, assuming that the controls that are implemented partially, which constitute about 36.1%, are not a gap.

Best Practice Case

A research is carried out to find a best practice case for IT security guidelines. A good practice is found in the Federal Office for Information Security (BSI), as it has been offering assistance in IT security aspects for many years. It offers a BSI's IT-Grundschutz approach together with the IT-Grundschutz Catalogues, which is considered to be the most comprehensive standard work on IT security. This approach provides a methodology for establishing an ISMS and a comprehensive basis for assessing risk, monitoring the existing IT security level and implementing appropriate IT security safeguards.

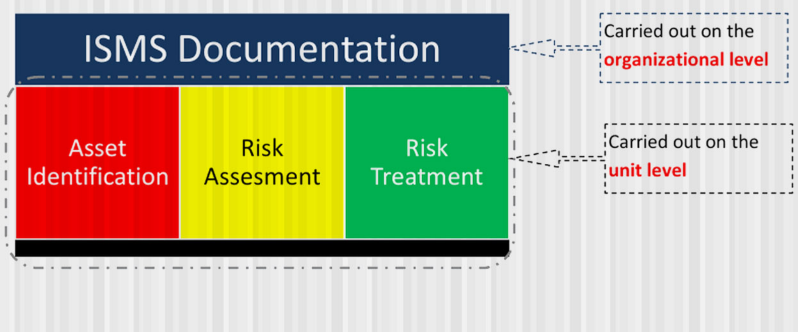
The IT-Grundschutz Catalogues have been used by many companies, to build their own safeguards catalogues in an easy, fast way and within budget. In the IT-Grundschutz Catalogues, 50 essential safeguards were presented together with the most common threats that might occur within an organization. Also, a set of summarized questions presented in 9 checklists, covering the 50 essential safeguards were provided. These checklists help an organization to detect its own vulnerabilities. Anyone that will implement these recommendations and follow the given guidelines will be building a solid foundation for a reliable level of IT security.



PHASE 1
PHASE 2
PHASE 3
STEP 1
Define the scope and boundaries of the ISMS
STEP 2
Define an ISMS Policy
STEP 3
Define the risk assessment approach
Information assets, threats, vulnerabilities and impacts
Implementation standards for risk management (an organization's approach, methods of analysis and the required level of assurance)
List of potential control objectives and controls
List of additional controls that are not defined in the ISMS certification criteria
STEP 9
Obtain management authorization to implement ISMS
STEP 10
Prepare statement of applicability
Scope of the ISMS
Policy document
STEP 4
Identify risks
STEP 5
Analyze and evaluate risks
STEP 6
Undertake risk treatment
STEP 7
Select control objectives and controls
STEP 8
Obtain management approval of the proposed residual risks
Statement of applicability
List of risks and inventory of assets
Report on the result of the risk assessment
Report on the result of the risk treatement
Standards of measures of risks
Record of residual risk approval

Rollout Concept Together with a Project Plan

A rollout concept is needed to be developed for the company in order to know how to carry out the ISMS implementation plan. Careful preparation will ensure that the project moves forward on the right track, therefore the project plan is composed of four tasks which are; asset identification, risk assessment and risk treatment, together with ISMS documentation that is carried out in parallel with all of the three tasks. The level of implementation of such tasks are determined (i.e., whether the task will be carried out in an organizational level or in unit level), and explicitly mentioned in the project plan. Finally, an audit (i.e., whether internal or external) is conducted to evaluate the current implemented ISMS and how much it complies with the ISO standards, and whether it deserves to gain certification or not yet.



ISMS Documentation
Asset Identification
Risk Assesment
Risk Treatment
Carried out on the organizational level
Carried out on the unit level