

CRAMM 5 Case Study



RISK ANALYSIS IS A SIGNIFICANT PART OF PREPARATION FOR ISMS CERTIFICATION

Top management of a large Czech company decided to establish and operate an Information Security Management System. Risk analysis, carried out with CRAMM, was an integral part of the project which concluded with system certification in compliance with ISO/IEC 27001 (BS 7799). CRAMM is the most widely used methodology in Europe for risk analysis and management. Its quality has been proven by many successful certifications and satisfied clients. Mainly, the countermeasures library and security documentation templates are very useful for establishing and operating ISMS.

Security department specialists did not see a need to buy the methodology and other supporting tools and, therefore, they asked a leading consultancy firm for assistance. A Partnership Approach was chosen and all company specialists and external consultants worked together in close cooperation. This way of work effectively utilized all resources and ensured the transfer of know-how to internal specialists.

“We had limited resources, but once we used a partnership approach and CRAMM, we utilized them in more effective ways.”

Jan Nowak, Security Manager

Project Initiation

The project team consisted of two internal specialists and two consultants, of which one led the project. PRINCE2 methodology was used for project management and all activities necessary for proper initiation were carried out accordingly. The project goal, approach, quality assurance plan, time schedule, team and description of activities, including resources, were summarized in the first project output - Project Initiation Document.

Gathering information about the systems and revision of current security documentation was performed during the initiation stage.

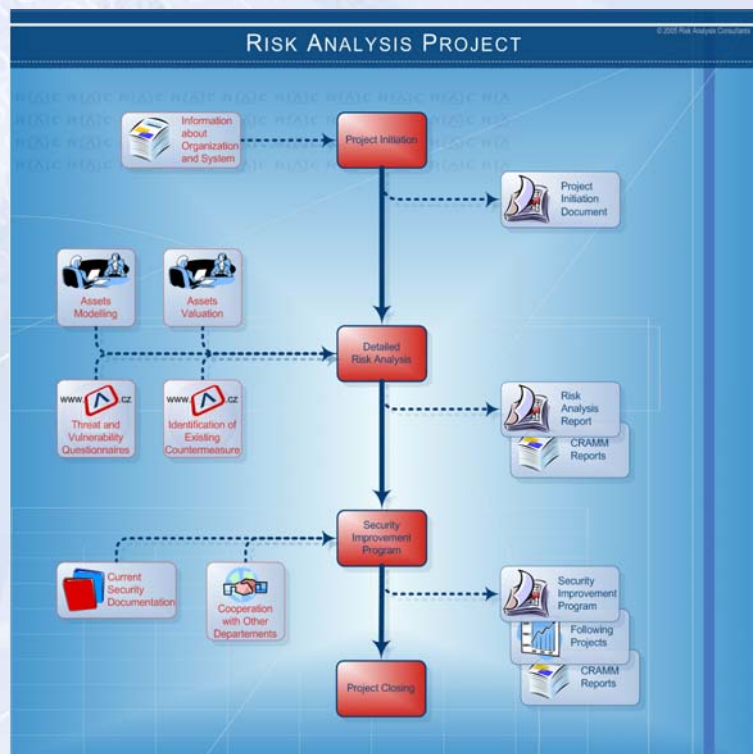
Detailed Risk Analysis

Risk analysis was divided into two parts:

- ◆ Identifying and Modelling Assets
- ◆ Risk Evaluation

Assets are practically everything in an organization related to information processing. The most significant are Data Assets whose identification is not always easy. The company processed huge amounts of information about production, customers, suppliers, their personnel, as well as strategic management information such as accounting, etc.

The data groups had been specified and within the analysis the subgroups were defined e.g. according to content, category, department, or data sensitivity. 10 groups and 54 subgroups were identified in total.



Many interviews with previously chosen respondents took place during the data evaluation process. The respondents (usually users of the data groups or subgroups) described potential breaches that could harm the company's reputation, bring about financial losses or cause other damage. All possibilities of unavailability of data, its disclosure and modification were investigated.

Project Initiation Document

- ◆ Project objectives
- ◆ Approach to carry out the project, methodologies used
- ◆ Project team and roles
- ◆ Project stages, resources, outputs and responsibilities
- ◆ Time schedule
- ◆ Quality assurance plan, project risks



CRAMM 5 Case Study



RISK ANALYSIS DEFINES BASIC PARAMETERS FOR IMPROVING INFORMATION SECURITY

During the data evaluation, the financial losses, production disruption, loss of goodwill, and injuries to people were investigated. The real scenarios of these impacts were compared with valuation guidelines that are incorporated within CRAMM. These provided trustworthy support for determining the final value of data. First, the data subgroups were evaluated on a scale from 1 to 10 and then the highest values were assigned for each group of data representing one data asset in CRAMM.

The supporting information for asset modeling was summarized during the evaluation. Each server, workstation, network distribution component, application, connection etc. was subjected to simple analysis and the models were created to convey the relationships between data, software, processes, hardware and locations.

The value of physical assets was assigned based on costs of replacement and installation, in case of total damage.

Based on asset modeling and evaluation, the conclusions were summarized in the first part of the Risk Analysis Report. Data values, such as the most significant output from the first part of analysis, were presented in an easy to understand chart. The highest values were described in further detail in the report.

Risk Analysis Report

- ◆ Background, approach to carry out the analysis
- ◆ Identification and Asset Modelling
- ◆ Asset Evaluation
- ◆ Threat and Vulnerability Assessment, Risks
- ◆ Current Security Status, Existing Countermeasures

The goal of the second part of the analysis was calculating the measure of risks threatening the system. The specific threats and vulnerabilities were related to the assets and then assessed using questionnaires. Respondents, mainly system administrators and specialists from the physical security dept., answered the questions by way of CRAMM web interface reachable within the company intranet.

The measure of risk was calculated after all questionnaires had been completed. Afterwards, the security countermeasures managing the risks were generated by CRAMM.

CRAMM defined the recommended set of countermeasures for all security areas. The next task was to record the status of already existing countermeasures and choose those that will be assigned for implementation. At this point, the CRAMM web application stepped in again and the respondents chose countermeasures statuses or made decisions about countermeasure applicability.

The CRAMM template was used for the Risk Analysis Report. Besides assets modeling and evaluation, the report also summed up levels of threat and vulnerabilities and current status of security. It was estimated from the countermeasures status statistics what percent of recommended countermeasures were already installed and what part still needed to be implemented.

All conclusions were presented in a management (summarizing) style report. However, for their support, the set of countermeasure reports from CRAMM were created to provide detailed values for each asset, its measure of risk, relevant threat and specific countermeasure. The comprehensive reports were generated in many variations only in electronic form, due to their length.

Security Improvement Program

Detailed risk analysis showed weaknesses in the security of the system. For that reason, the scopes of the following projects defined the process of countermeasure implementations. The goal of each project was to improve the level of security for specific systems or areas. Based on CRAMM recommendations, projects such as development of security documentation, installation of new technologies and upgrading physical security etc. were initiated.

The projects, e.g for security documentation development, integration of new technologies or improvement of physical security, arose from CRAMM recommendations.

Security Improvement Program (scope of following projects)

- ◆ Security Documentation Development
- ◆ Organization Structure
- ◆ Physical Security Improvement
- ◆ Continual Security Awareness Program
- ◆ Incident Management Establishment
- ◆ Business Continuity Management
- ◆ eSecurity Infrastructure

The SIP, covering the projects, contained all activities including resources and responsibilities, project plans, outputs etc. Management Security Statement was also a part of SIP in order to support its realization.

Risk analysis was a basic step towards successful establishment of the ISMS. The audit, performed a couple of weeks ago, confirmed that all information risks are now properly managed. The newly acquired ISO 27001 certification became proof for customers and suppliers that the information about them is sufficiently and effectively secured.

Risk Analysis Consultants is a Czech based professional provider of information security services and solutions. We have assisted organizations from government and commercial sectors to protect their information since 1995. The company is owned by the main consultants, independently from any other company or group. We are the only firm exclusively specialized in the information security field in the Czech market, and one of the few in Europe and the world. Risk Analysis Consultants has been approved since 2003 by the Ministry of Justice of the Czech Republic as a private forensics institute which is qualified for the forensics services in cybernetics and computer technology area.

