The risk assessment of information system security

Miroslav Bača, PhD
University of Zagreb, Faculty of Organization and Informatics, Varaždin, Croatia,
miroslav.baca@foi.hr

Abstract

Every organisation today which are use information technology have problem with information system security. The first step in process of protection of an information system is identification and classification of information resources or assets, which need protection, because they are vulnerabilities to threats. The major purpose of the classification is to prioritize further investigation and identify appropriate protection. The typical assets associated with information and information technology includes: information, hardware, software, people, services and documents. Risk assessment is process of assessing security-related from internal and external threats to an entity, its assets, or personnel. Also, we can say that the risk assessment is process of identifying vulnerabilities and threats to an organization's information resources (difference in terminology between the risk analysis and the risk assessment brings a new vague in the risk management process). Generally, risk can be transferred, rejected, reduced or accepted, but risk never eliminated, and they can be describing in the follow mathematical equation: Total risk = threats x vulnerability x asset value. When we develop risk management and assessment program, we must follow next steps: 1. Understand the organization and identify the people and assets at risk, 2. Specify loss risk events and/or vulnerabilities, 3. Establish the probability of loss risk and frequency of events, 4. Determine the impact of events, 5. Develop options to mitigate risk, 6. Study the feasibility of implementation of options and 7. Perform a cost benefit analysis. For developing a risk management and assessment program we must use some of the various methods and techniques for risk assessment, which can be complete or incomplete. Differences between these two approaches in process of risk assessment determine which approach will be implemented in particular organization. The risk assessment process is about creation decisions. The impact of a successful attack and the level of suitable risk for any given situation is a basic strategy decision. A primary problem of risk management is to accomplish a cost-effective balance between design characteristic and the related countermeasures to threats and impact. This paper describes an analysis and comparison of complete methods for risk assessment major representative like British Standard (BS); CCTA[1] Risk Analysis and Management Method (CRAMM); Consultative, Objective and Bi-functional Risk Analysis (COBRA); RuSecure; Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) and Failure Mode and

[1] *Central Computer and Telecomunications Agency*

Effects Analysis (FMEA), which is the first step in process of develop a new method for risk assessment for the particular organisation.

Keywords: risk, assessment, evaluation, method

1. Introduction

In the purpose of information system risk assessment process approach it is necessary to consider some of the most complete methods for risk assessment in information system security. These methods must give support in:

- Detecting critical places and parts in organisation,
- Detecting risk factors,
- Collecting data about risk factors,
- Evaluation and estimation risk, opposite to chosen risk methodology, and
- Report and display result process of risk assessment.

These five steps are used in selection of effective protection control. The major representative, complete methods for risk assessment are British Standard (BS), CCTA Risk Analysis and Management Method (CRAMM); Consultative, Objective and Bi-functional Risk Analysis (COBRA); RuSecure; Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), and Failure Mode and Effects Analysis (FMEA). When we talk about risk assessment methods, generally we can watch these methods through prism of complete security risk assessment methods and methods and techniques which have been used for complete risk assessment method support (or for a solving a specific types of problems).

2. British Standard

This method distinct three basic approach for information system security risk assessment: basic, detailed and mixed. Basic steps in BS method are depicted on Figure 1.

Basic approach has next characteristic:

- Simplified evaluation and identification of mean values, threats, vulnerabilities, existing and scheduled protection measurements,
- Probability is not involving,
- Minimal request for financial resources, human resources and time resources,
- Proportional for different situation,

- ☞ Inaccurate because the solution for coast analysis is below standard,
- ☞ Metrics is qualitative.

Detailed approach has next characteristics:

- ☞ Simply but detailed assessment and identification of mean values, threats, vulnerabilities, existing and scheduled protection measurements,
- ☞ Assessment of emergence incidents probability,
- ☞ Methods have more financial, time and information request,
- ☞ More precisely then basic, and
- ☞ Metrics have quantitative values.

Mixed approach has next characteristics:

- ☞ Using both basic and detailed approach, or using parts of basic approach and parts of detailed approach according to needs,
- ☞ This method give four techniques for risk security measure:
  - o *Matrix with Predefined Values*
  - o *Ranking of Threats by Measures of Risk*
  - o *Assessing Value for the Frequency and the Possible damage of Risks*
  - o *Distinction between Tolerable and Intolerable Risks.*

3. CRAMM

CRAMM method vas developed and modulated in Great Brittan police. Strategy of avoiding the risk was replaced with strategy of manages risk. Basic steps of this method are depicted on Figure 2. CRAMM method is use for support in:

- ☞ Information system risk assessment,
- ☞ Identification of security request according to BS ISO/IEC 1799, and
- ☞ Identification request of continued business and possibility solution for advance of information system security.

Risk evaluation with this method has three steps:

- ☞ Identification and evaluation of properties,
- ☞ Identification of threat and vulnerabilities,
- ☞ Recommendation and selection of protection measures.

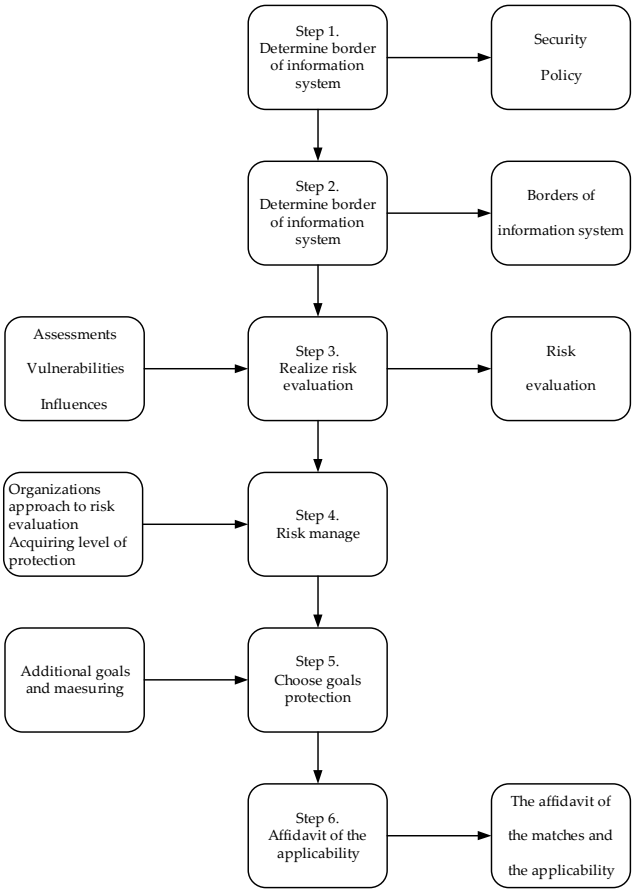

Figure 1 BS Risk management

CRAMM method is mostly qualitative but it has possibility of quantitative evaluation. In phase of determine the threats it's possible to modulate and determine interdependence threats and influences on business. Data processing is automated, but person who lead estimation process can change input values and watch the final result, this way it can give insight about risk component influence. CRAMM method creates various numbers of clear reports in result cheeking purpose. These reports have big influences on person who estimate risk in phase of recognition critical components. The CEAMM method can be used on all information system and in all information system living phases. The major advantages of this method are: structural approach to risk evaluation, has got hierarchical base of protection measures, gives help in planning continued business, it is possible to evaluate different information systems (small or big). The major imperfections of this method are: it can be used only by expert with big experience, complete revision lasts for months, it produces too long reports, it is not flexible enough, it is not appropriate for physical protection and procedural countermeasures, and it requires accurate data.

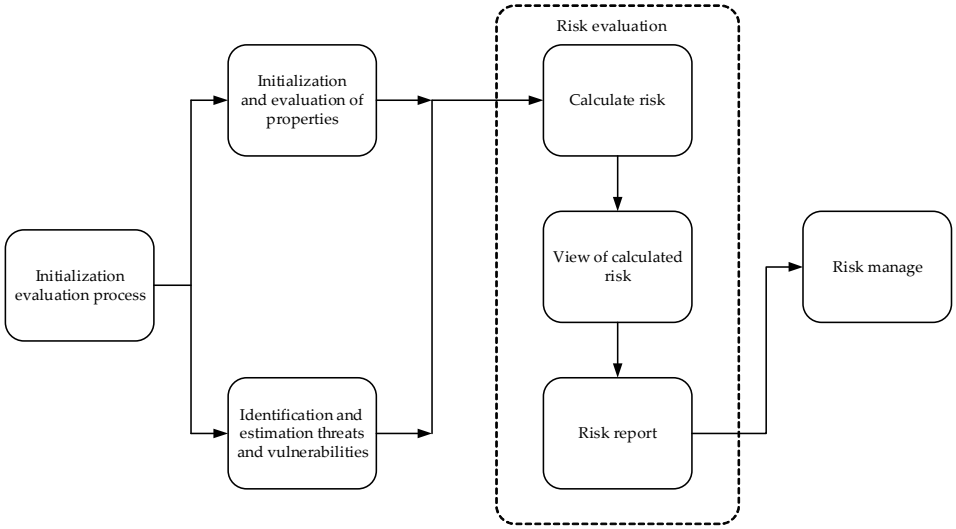

Figure 2 CRAMM method basic steps

4. COBRA

The first purpose of this method is helping and giving support to organisation which is introducing criteria from BS ISO/IEC 17799. This method has two basic program modules, *COBRA Risk Consultant* and *ISO Compliance Analyst*[2]*. COBRA Risk Consultant* gives support to process of evaluation risk security by: identification system threat, vulnerabilities, measurement degrees of risk and connecting with business influences, giving detailed solutions and recommendations for decrease of risk. This method uses standard forms of structured queries, and evaluation goes in three steps:

- Building queries,
- Risk evaluation, and
- Reports construction.

For each steps COBRA method gives a modification of query which are measure and examination after the filling, thanks to adaptable data base which ensures re-establishing a new criteria so that every area can be adaptable to users needs. The COBRA method contains library of countermeasures and protection recommendations. Major advantages of this method are: large base of threats, adaptable knowledge base, possibility of partly evaluation of single module and simplicity of evaluation. Major imperfections of this method are: weak software, lengthily evaluation, bad structure and muddled process evaluation.

5. RuSecure

[2] ***COBRA***, Continuity Consultant, Release:3.1.6b, C&A System Security Ltd. 2003.

The RuSecure method is based on BS 7799 standard, and it contains manuals *Information Security Policies* i *Glossary and Reference Manual*[3]. The Figure 3 depicted basic steps in process of risk evaluation by this method. This manual contains practical suggestions about execution of single part in process of evaluation risk. Major advantage of that method is good layout of steps and simplified leading thru process and presentation of evaluation which can be understand by inexperienced user. Other advantages are: good layout and structured criteria, simplicity, short time of execution. Imperfections are: complete hand made method, no software, there is no adaptability to organisation.

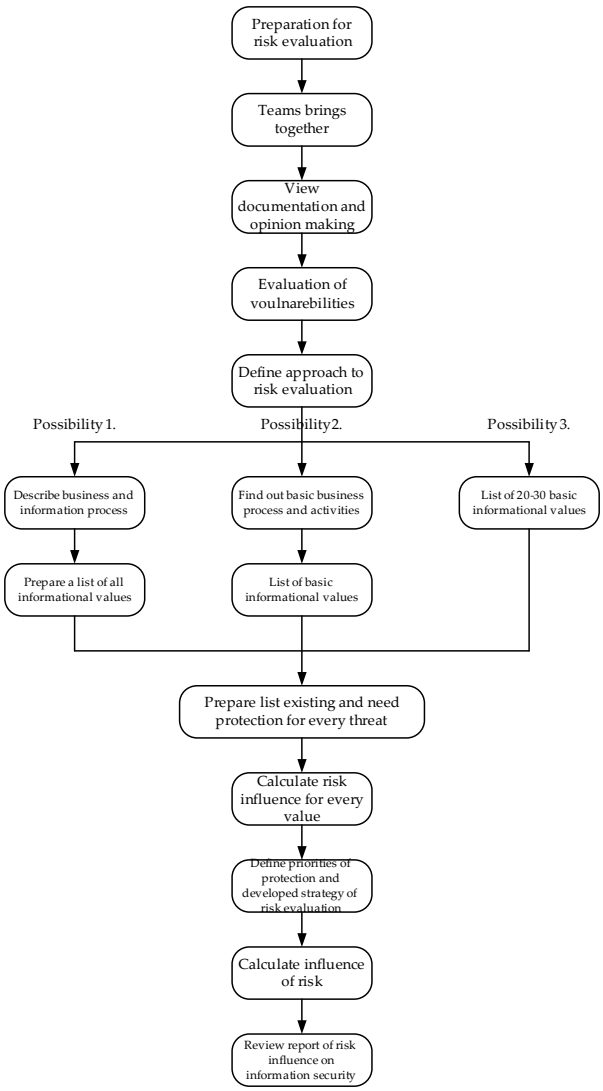

Figure 3 Steps of risk evaluation in RuSecure method

6. OCTAVE

[3] ***OMB Circular No. A-130***

The *OCTAVE*[4] method observe risk like function of properties, information systems and his value which is very important for business; threats which endangered properties of information system, and on the end vulnerabilities which expose to threats properties of information system. Implementation of this method has next steps:

- Determine critical means and threats to this means,
- Determine organisation and technological threats, and
- Develop strategies for protection and avoid risk.

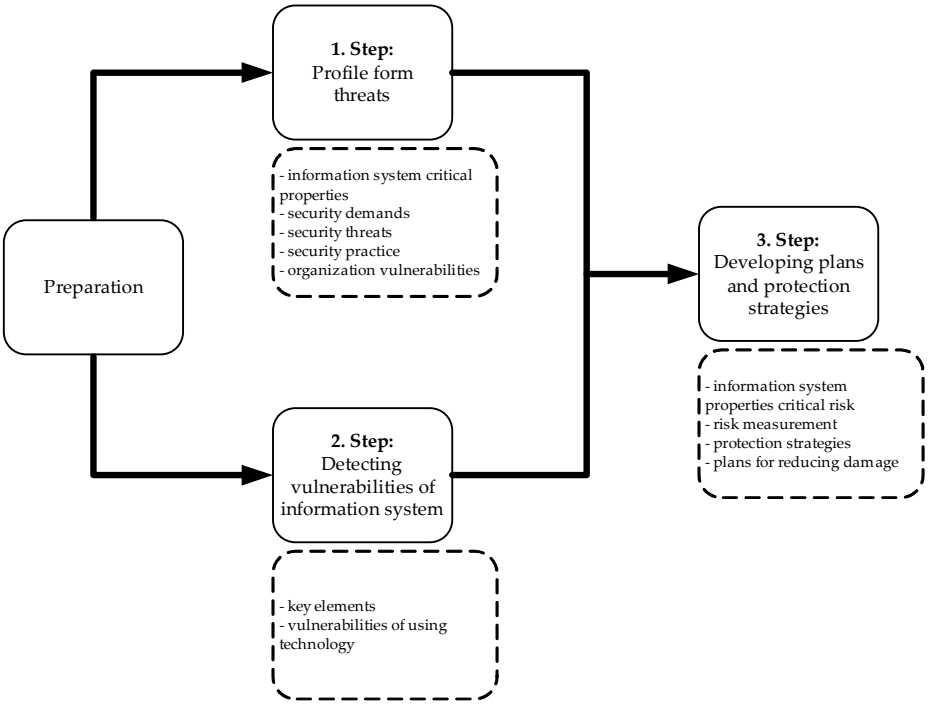

Figure 4 OCTAVE method

The planning scenario of this method is basic because that throws out all peddling assets which indirect evaluation of probability and introduces describing evaluation. The interpretation ways of this method is based on next opinions:

- Data about threat frequency are defective which result with bad probability analysis, Disburdening of probability insure better scenario understanding of threats and finding of solutions,
- Traditional techniques for probability determining are bad.

Success of OCTAVE method depends on experience of men who are evaluating and of quality team work. The first purpose of this method was implementation in large

[4] *Operationally Critical Threat, Asset, and Vulnerability Evaluation*

information system. This method can be adaptable for small organisation needings. Major imperfections of this method are: not containing secondary methods, protection measurement can be very expensive, no software, it's based for large business organisation and needs no expert help. Major advantages of this method are: detailed instruction and manuals, large financial and human resources are needed, flexible, adaptable, modulate, qualitative, universal and integral approach.

7. NASA[5]

The NASA approach use *FMEA*[6] method which is a risk evaluation basic method. The FMEA method is very suitable for error understanding, analyse of error effect and preventing errors. This method makes possible to:

- Specify possible error causes,
- Checking and evaluate all possible errors and consider possible consequence for user,
- Re-establish control measurement, and
- Evaluate specifications for supervising.

This method is very suitable for initial assessment because it is very easy for understanding. The component risk analysis is based on expert opinion which has been made on historical data[7]. Major advantages of this method are: simplicity, clear and documented procedure, possibility of individual usage, very short time of assessment and price. Major imperfections of this method are: absence of threat base, incompatibility with other criteria, the week possibilities of briefings and un-proportionate to large systems.

8. Conclusion

The balanced of individual method to characteristic of business organisation and right choice in determine the method is major question in process of risk assessment. For qualitative determination of methods for solving a problem of information system risk assessment it is necessary to analysing methods possibilities[8]. To determine real criteria for business organisation risk assessment it is necessary to find out which characteristic describe specific method for risk

[5] *National Aeronautic Space Exploration*
[6] *Failure Mode and Effects Analysis*
[7] That makes this method very subjective.
[8] Their structure, manners and application.

assessment, and on which way these methods can be connected with major characteristic. Only with selection and synthesis of major characteristics of these methods it can be possible to determine real criteria of comparison and evaluation of specific method. It can be possible to reduce a large number of risk assessment complete methods characteristic taking into consideration next criteria's: ways of data collecting, price, human resource, methodology, simplicity, manuals, need knowledge, accurate, documenting, software, interpretation rapidity and coordination possibility. Using secondary methods and techniques it can be alleviation to security risk assessment process. Secondary methods and techniques can be observed in few ways, but most frequent way is appropriateness to individual task.

The best way to solve a problem choosing a methods choosing is by using a multi criteria choosing method[9] which is very best in filling different choice criteria of risk assessment method. Decomposition model of risk assessment factors may be described on the next way: suitability to motifs and needs of evaluation, suitability to evaluation objects, suitability to evaluation goal, fashions holding up to evaluation process, software, methodological, necessarily resource, material, finances, time and human. Figure 6 depicted the example of decomposition which can be used like basic step in process of selection complete solution for information system security risk assessment.

[9] One of possible solution can be and *AHP (Analytical Hierarchy Process)* method. AHP method supports decision making complex problem (few possibilities and criteria). This method is special in development a decomposition model of risk assessment factors.

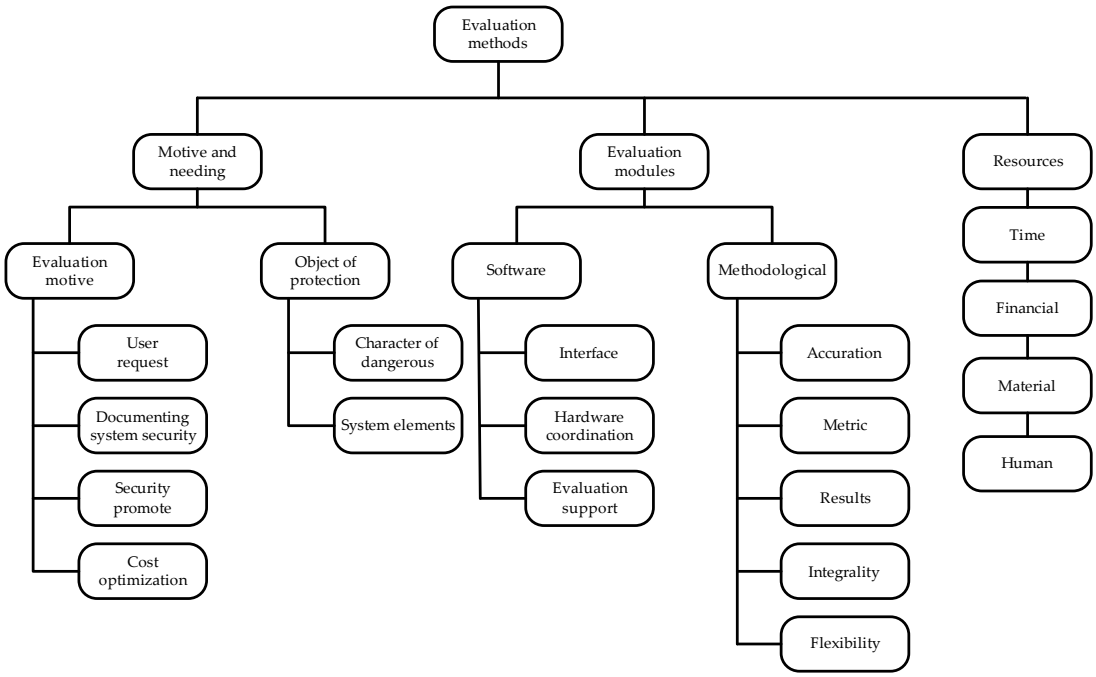

Figure 6 Hierarchical criteria model

9. Literatures

1. Bača, M. :Uvod u računalnu sigurnost, Narodne novine, Zagreb, 2004.
2. Borchgrave de Arnaue et al. :Cyber Threats and Information Security Meeting the 21st Chenzury Challenge, CSIS, http://www.csis.org/homeland/reports, 2000.
3. Cohen F. :Managing Network Security-Part 5:Risk Management or Risk Analysis, Network Security, http://www.sciencedirect.com, 1997.
4. ** BS 7799-2:1998, Information security management-Specification for information security management systems-Part 2, BSI, 1998.
5. ** COBRA, Continuity Consultant, Release:3.1.6b, C&A System Security Ltd. 2003.
6. ** CRAMM Management Guide, Crown, http://www.insight.co.uk/newsarchive.htm, 1996.
7. ** NASA Risk Management Tools, http://nodis3.gsfc.nasa.gov/library/mail_lib.html
8. ** OMB Circular No. A-130, http://www.whitehouse.gov/omb/circulars/a130/a130appendix_ii.html, 1996.

Biography

Miroslav Bača is an assistant professor at the Faculty of Organization and Informatics in Varaždin. His main areas of research and professional work are Information system security, biometics and computer related crimes