The risk assessment of information system security

Miroslav Bača, PhD
FOI Varaždin

Introduction

- Total risk = threats x vulnerability x asset value.

- Developing steps for risk assessment program:
  - Understand the organization and identify the people and assets at risk,
  - Specify loss risk events and/or vulnerabilities,
  - Establish the probability of loos risk and frequency of events,
  - Determine the impact of events,
  - Develop options to mitigate risk,
  - Study the feasibility of implementation of options, and
  - Perform a cost benefit analysis.

Complete risk assessment methods

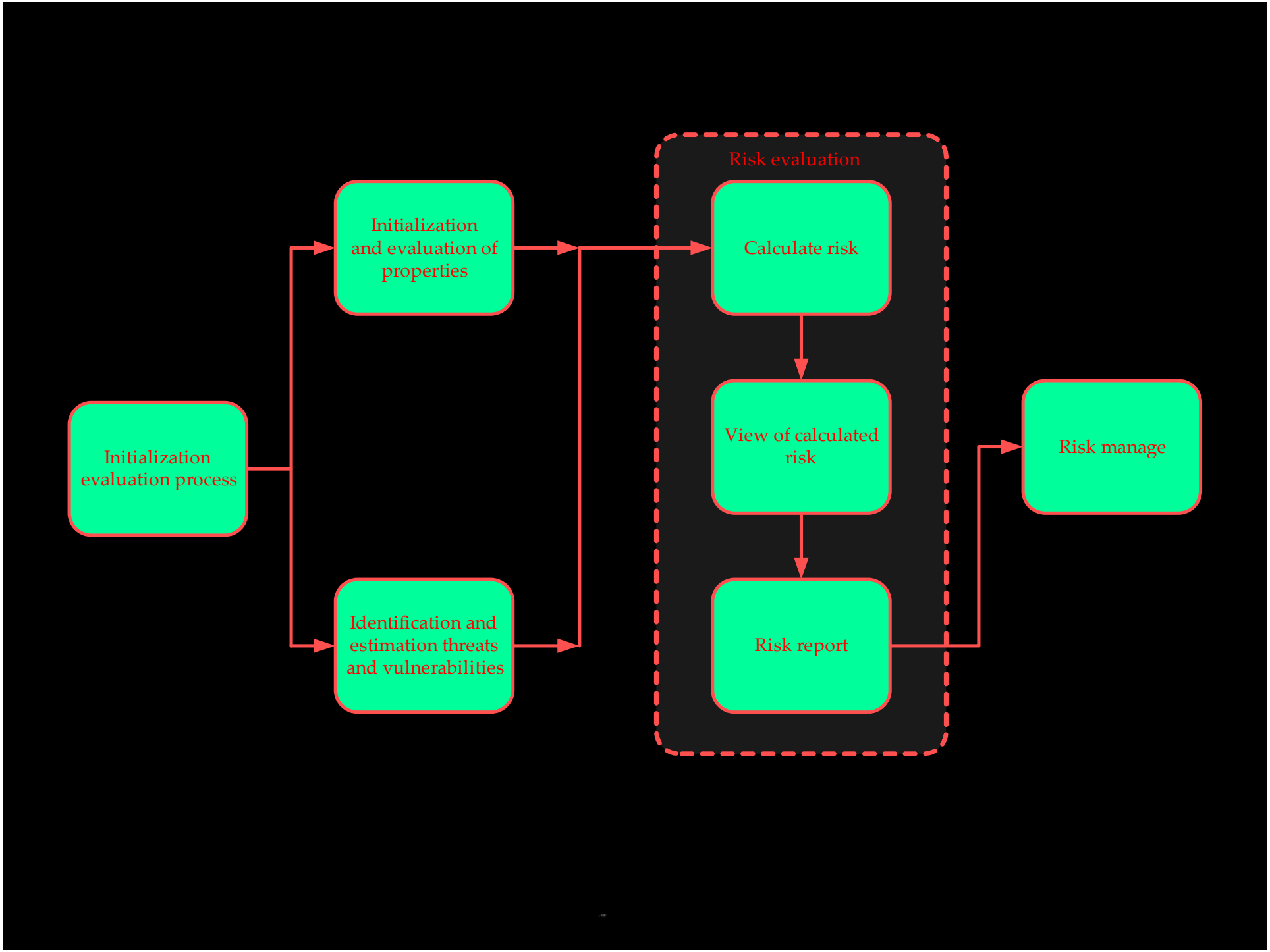
- Complete methods for risk assessment in information system security must give support in:
  - Detecting critical places and parts in organization,
  - Detecting risk factors,
  - Collecting data about risk factors,
  - Evaluation and estimation risk, and
  - Report and display result process of risk assessment.

British Standard

- 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,
  - Proportionate for different situation,
  - Inaccurate is and it's very bed solution for cost analysis, and
  - Metrics is qualitative.

CRAMM

- Risk evaluation process with this method goes to three steps:
  - Identification and evaluation of properties,
  - Identification of threat and vulnerabilities,
  - Recommendation and selection of protection measures.
- The major advantages are:
  - Structural approach to risk evaluation,
  - Hierarchical base of protection measures,
  - Help in planning continued business,
  - Possibility to evaluate different information systems.

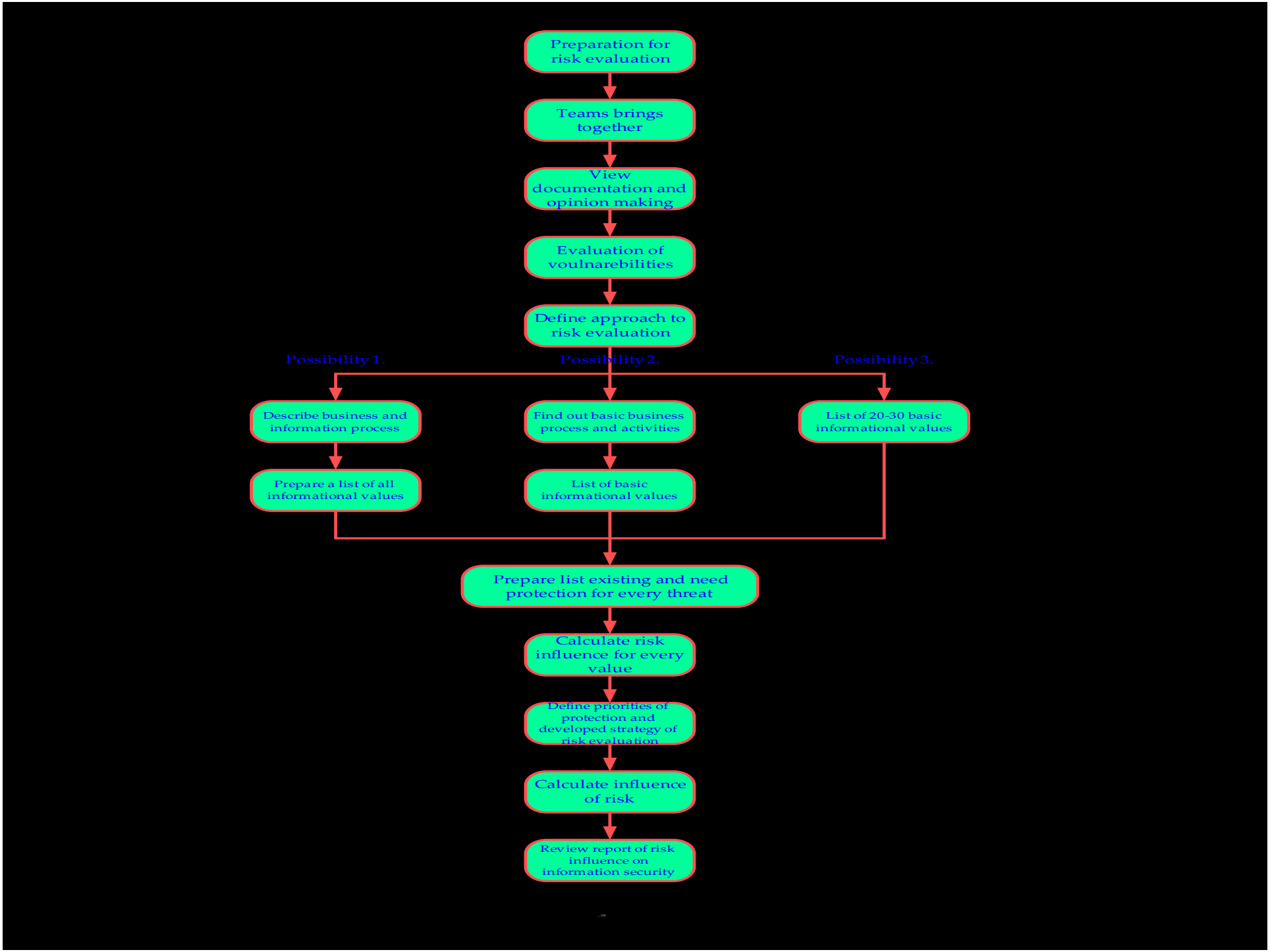

Initialization evaluation process
Initialization and evaluation of properties
Identification and estimation threats and vulnerabilities
Risk evaluation
Calculate risk
View of calculated risk
Risk report
Risk manage

COBRA

- This method uses standard forms of structured queries, and evaluation goes in three steps:
  - Building queries,
  - Risk evaluation, and
  - Reports construction.
- Major advantages of this method are:
  - Large base of threats,
  - Adaptable knowledge base,
  - Possibility of partly evaluation of single module, and
  - Simplicity of evaluation.

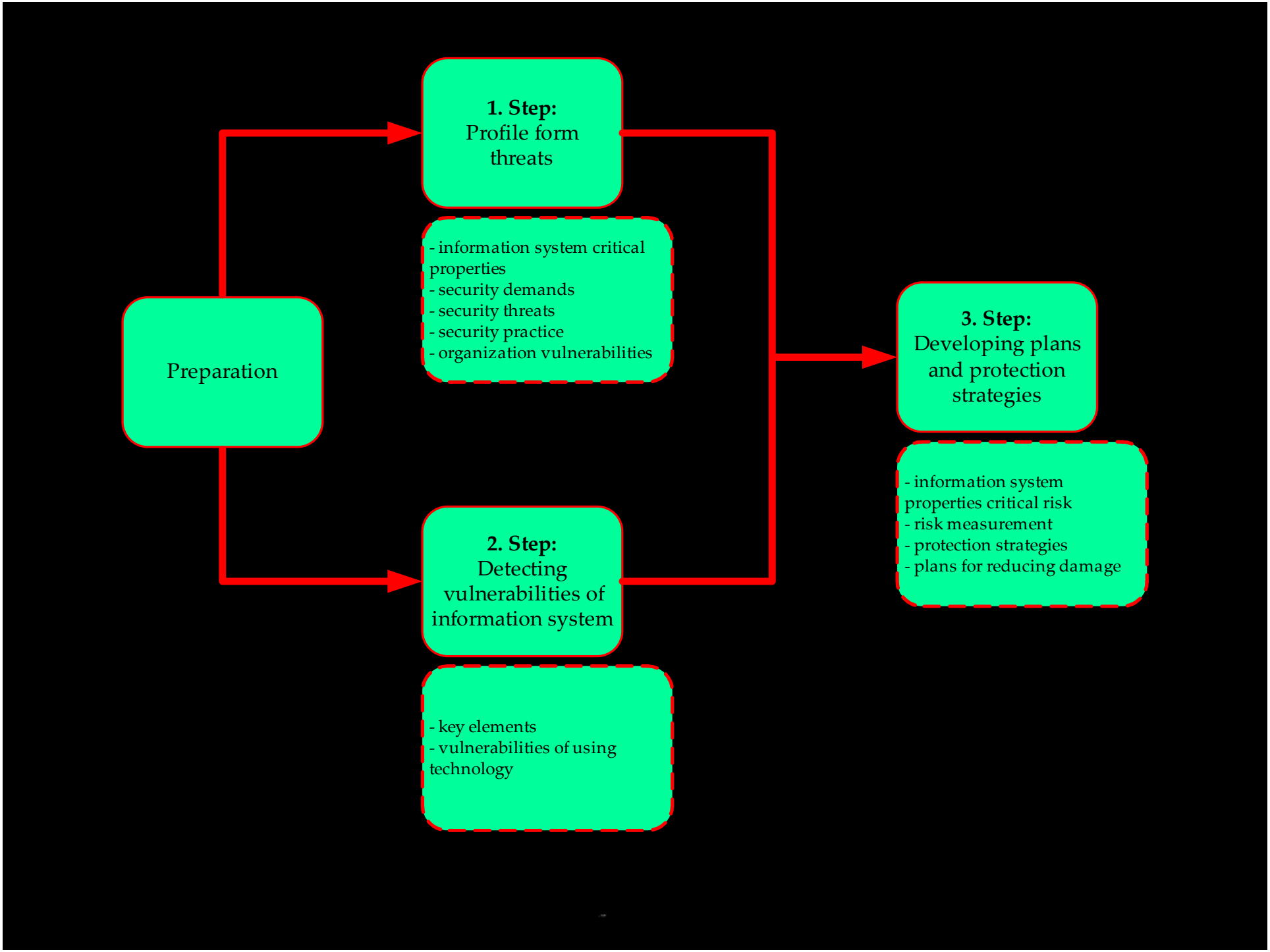
RuSecure

- Based on BS 7799 standard
- Contains manuals *Information Security Policies* and *Glossary and Reference Manual*
- Major advantages of this method are:
  - Good layout of steps and simplified leading thru process and presentation of evaluation which can be understand by inexperienced user,
  - Good layout and structured criteria,
  - Simplicity, and
  - Short time of execution.


Preparation for risk evaluation
Teams brings together
View documentation and opinion making
Evaluation of voulnarebilities
Define approach to risk evaluation
Possibility 1.
Possibility 2.
Possibility 3.
Describe business and information process
Find out basic business process and activities
List of 20-30 basic informational values
Prepare a list of all informational values
List of basic informational values
Prepare list existing and need protection for every threat
Calculate risk influence for every value
Define priorities of protection and developed strategy of risk evaluation
Calculate influence of risk
Review report of risk influence on information security

OCTAVE

- This method threat risk like function of:
  - Information system and his valuse,
  - Threats, and
  - Vulnerabilities.
- Implementation of this method have next steps:
  - Determine critical means and threats,
  - Determine organization and technological threats,
  - Develop strategies for protection and aviod risk.


Preparation
1. Step:
Profile form threats
- information system critical properties
- security demands
- security threats
- security practice
- organization vulnerabilities
2. Step:
Detecting vulnerabilities of information system
- key elements
- vulnerabilities of using technology
3. Step:
Developing plans and protection strategies
- information system properties critical risk
- risk measurement
- protection strategies
- plans for reducing damage

- First purpose of OCTAVE method was implementation in large information systems.

- Major advantages of that method are:
  - Detalied instruction and manuals,
  - Large financial and human resources are need,
  - Flexible and adaptable,
  - Modulate and qualitative, and
  - Universal and integral approach.

NASA (FMEA)

- The FMEA method is very suitable for erroe understanding, analyse of error effect and preventing errors.

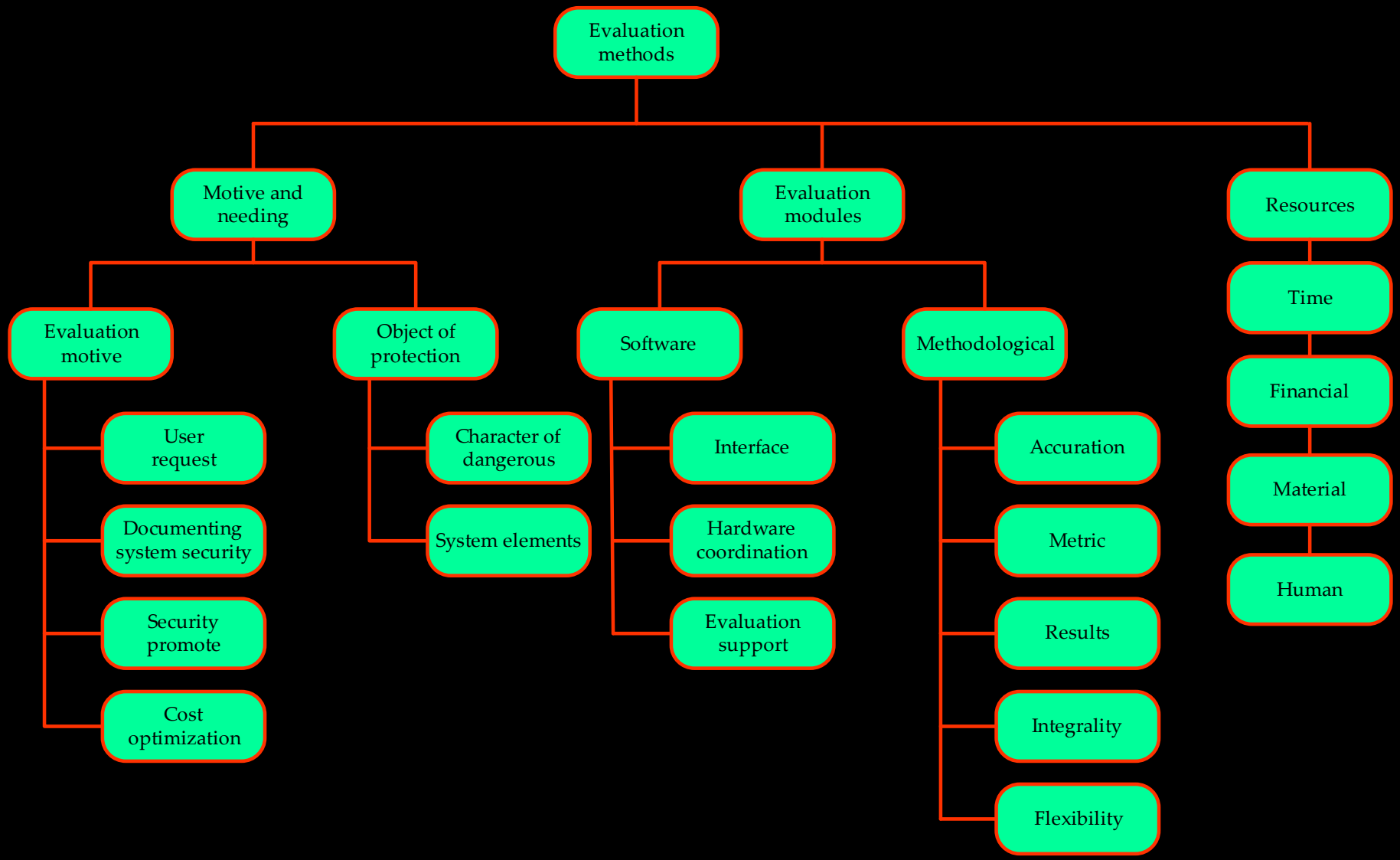
- This method make possible:
  - Specify possible error causes,
  - Checking and evaluating all possible errors and consider possible consequence for user,
  - Re-establish control measurement, and
  - Evaluate specifications for supervising.

- Major advantages of this method are:
  - Simplicity,
  - Clear and documented procedure,
  - Possibility of individual usage,
  - Very short time of assessment, and
  - Price.

Conclusion

- For qualitative determination of risk assessmet methods it is necessary to analysing methods possibilities,
- Only with selection and synthesis major characteristic of risk assessment methods it can be possible to determine real criteria for comparison and evaluation of specific method,
- The best way to solute a problem of methods choosing is by using a multi criterion choosing method which is very best in fill different choice criteria of risk assessment method.

- Example of decomposition which can be used like basic step in process of selection complete solution for risk assessment information system security.



The end

Thank you for your attention !