An Overview of Risk Assessment Methods

Georgios Antoniou , Maria-Christina Saravanou, Vasilis Stavrou

{antonioug, saravanoum, stavrouv}@aueb.gr

Information Security and Critical Infrastructure Protection (INFOSEC) Laboratory

Dept. of Informatics, Athens University of Economics & Business, Greece

Introduction

- Security of Information Systems is a major issue for every organization.
- A security incident may result in loss of availability, confidentiality or integrity of assets for the organization.
- RA/RM is very important for organizations in order to protect their assets, maintain their continuity and their quality of services.
- There are several RA/RM methods to choose from.
- There are specific similarities and differences between the RA/RM methods.
- There are RA/RM methods that are more appropriate than others, in order to perform risk assessment in an organization according to its needs.
- There is no formal method to evaluate the various RA/RM methods.

Suggested Evaluation Criteria

Validity
- Phases
  - Preparation (1)
  - Risk Identification (2)
  - Risk Analysis (3)
  - Risk Assessment (4)
- Type of Analysis
  - Qualitative
  - Quantitative
- Accuracy
- Consistency
- Complexity
  - Statistical Model
  - Class

Acceptance
- Popularity
  - Geographical Coverage
- Compliance with standards
  - AS/NZS
  - ISO/IEC

Resources
- Cost
  - Money
  - People
- Time

Usefulness
- Usability
  - Focus
- Scope
  - Organization (type, size)
- Life Cycle
  - Release
  - Update
- Adaptability
- Software Support
- Ease of use
  - Interface
  - Documentation
  - Training

Evaluation Table

Criteria/Method		AS/NZS 4360	Canadian TRA	CORAS	CRAMM	EBIOS	FAIR	IT-Grundschutz	Magerit	MEHARI	NIST SP 800-30	OCTAVE	RISKIT	RiskSafe	SRA	TARA
Complexity (Class)		E	A	E	A	B	A	E	A	A	A	D	A	A	A	A
Type of Analysis	Qualitative	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓
	Quantitative	✓	✓	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✓	✓
Focus	RM/RA	RM	RM	RA	RA	RA	RA	RM	RA	RM	RM	RA/RM	RM	RA	RA	RA
Phases	1	✓	✓	✓	✓	✗	✗	✗	✓	✓	✗	✓	✗	✓	✗	✗
	2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Software Support		CCS Risk Manager, Countermeasures, Modulo Risk Manager, Proteus Enterprise, Resolver Ballot	N/A	CORAS Tool	CRAMM expert, CRAMM express	EBIOS tool	OpenPERT MS Excel Plugin	BSI - GSTOOl, HiScout SME, SAVe, IGSDoku, Secu-Max, Baseline-Tool, PCCheckheft	µPilar, Pilar Basic, Pilar (Trial Version)	MEHARI 2010 basic Tool, RISICARE	N/A	Resolver Ballot	CCS Risk Manager, Countermeasures, Modulo Risk Manager, Proteus Enterprise, Resolver Ballot	SaaS RiskSafe Tool	SRA Tool, MS Excel	N/A
Usability	Level															
Life Cycle	Released	1995	2007	2003	1985	1995	2001	1997	1997	1998	2002	1999	2009	2012	2002	2010
	Last Update	2004 (AS/NZS 4360:2004)	2007 (TRA-1)	2011 (V1.1)	2011 (V5.1)	2004 (V2..0)	2009	2005 (V2.0)	2013 (V3.0)	2010 (Mehari 2010)	2012 (Revision 1)	2005 (V2.0)	2009	2012 (V1.0)	2002	2010 (V1.0)
Compliance with Standards		AS/NZS 4360 (31000)	N/A	AS/NZS 4360 (31000)	ISO/IEC 27001	ISO/IEC 27001, 13335, 15408, 17799	ISO/IEC 27001 13335	ISO/IEC 27001 13335	ISO/IEC 13335 17799 15408 27001	ISO/IEC 27001 13335	N/A	N/A	ISO/ IEC 31000, FAIR	ISO/IEC 27001 13335	SRA	N/A
Flexibility																
Scope		Small & Big	Small & Big	Small & Big	Small & Big (mostly big & governmental)	Small & Big	Small & Big	Small & Big	Small & Big	Small & Big	Small & Big	Small & Big	Small & Big	Small & Big	Small & Big	Small & Big
Popularity		Australia and New Zealand	Canada	Unknown	Several countries, particularly EU	Several countries, particularly EU	USA and Canada	Several countries, particularly EU	Several countries, particularly EU	Several Countries	USA	USA	USA	Several countries, particularly EU	UK	USA
Cost of Software (€)		150 - 227.330	N/A	Free	1.900 - 3.730	Free	Free	860	1.500	Free	N/A	1.300	150 - 227.330	After contact	Free	N/A
Score & Overall Evaluation		43	37	55	46	43	46	42	56	46	36	43	36	49	45	36

Evaluation Scale & Weight	
Very Poor	2
Poor	4
Fair	6
Good	8
Very Good	10

Usability Level Scale & Weight	
Non Satisfactory	3
Relatively satisfactory	6
Satisfactory	9

Flexibility Scale & Weight	
No Flexibility	3
Relatively Flexible	6
Flexible	9

Overall Evaluation Score (with ranges)	
Very Poor	35-39
Poor	40-44
Fair	45-49
Good	50-54
Very Good	55-59

Conclusions

- Standardized criteria for the evaluation of the RA/RM methods do not exist.
- Many researches suggest their own criteria based on previous work or experience.
- Usage of the suggested criteria is limited and the respective comparison includes only a few number of RA/RM methods (usually 2-4 methods).
- Most of the RA/RM methods use a qualitative model analysis and are supported by at least one software tool.
- Most RA/RM methods are technologically outdated (latest update more than five years ago).
- A framework for comparison and evaluation of the existing RA/RM methods is a necessity.
- Each organization should weight the evaluation criteria (using AHP) and choose the most appropriate RA/RM method which fits its needs.

References

1. Behnia, A., Rashid, R., Chaudhry, J., "A Survey of Information Security Risk Analysis Methods", *Smart CR*, vol. 2, no. 1, pp. 79-94, 2012.
2. Bornman, W., Labuschagne, L., "A comparative framework for evaluating information security risk management methods", in *Proc. of the Information Security South Africa Conference*, 2004.
3. ENISA, *Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises*, 2006.
4. Kotzanikolaou, P., Theoharidou, M., Gritzalis, D., "Risk assessment of multi-order interdependencies between critical information and communication infrastructures", *Critical Information Infrastructure Protection and Resilience in the ICT Sector*, pp. 151-170, IGI, 2013.
5. Lichtenstein, S., "Factors in the selection of a risk assessment method", *Information Management & Computer Security*, vol. 4, no. 4, pp. 20-25, 1996.
6. Mylonas, A., Theoharidou, M., Gritzalis, D., "Assessing privacy risks in Android: A user-centric approach", in *Proc. of the 1st Workshop on Risk Assessment and Risk-driven Testing*, pp. 21-37, Springer (LNCS 8418), Turkey, 2013.
7. Mylonas, A., Tsalis, N., Gritzalis, D., "Evaluating the manageability of web browsers controls", in *Proc. of the 9th International Workshop on Security and Trust Management*, pp. 82-98, Springer (LNCS 8203), United Kingdom, 2013.
8. Theoharidou, M., Tsalis, N., Gritzalis, D., "In Cloud we Trust: Risk-Assessment-as-a-Service", in *Proc. of the 7th IFIP International Conference on Trust Management*, pp. 100-110, Springer (AICT 401), Spain, 2013.
9. Theoharidou, M., Xidara, D., Gritzalis, D., "A Common Body of Knowledge for Information Security and Critical Information and Communication Infrastructure Protection", *International Journal of Critical Infrastructure Protection*, Vol. 1, No. 1, pp. 81-96, 2008.
10. Theoharidou, M., Kotzanikolaou, P., Gritzalis, D., "Risk-based Criticality Analysis", in *Proc. of the 3rd IFIP International Conference on Critical Infrastructure Protection*, pp. 35-49, Springer, USA, 2009.
11. Theoharidou, M., Kotzanikolaou, P., Gritzalis, D., "Risk assessment methodology for interdependent critical infrastructures", *International Journal of Risk Assessment and Management* (Special Issue on Risk Analysis of Critical Infrastructures), Vol. 15, Nos. 2/3, pp. 128-148, 2011.
12. Theoharidou, M., Tsalis, N., Gritzalis, D., "In Cloud we Trust: Risk-Assessment-as-a-Service", in *Proc. of the 7th IFIP International Conference on Trust Management*, pp. 100-110, Springer (AICT 401), Spain, 2013.
13. Theoharidou, M., Papanikolaou, N., Pearson, S., Gritzalis, D., "Privacy risks, security and accountability in the Cloud", in *Proc. of the 5th IEEE Conference on Cloud Computing Technology and Science*, pp.177-184, IEEE Press, United Kingdom, 2013.
14. Theoharidou, M., Mylonas, A., Gritzalis, D., "A risk assessment method for smartphones", in *Proc. of the 27th IFIP International Information Security and Privacy Conference*, pp. 443-456, Springer (AICT 267), Greece, June 2012.
15. Tsalis, N., Theoharidou, M., Gritzalis, D., "Return on security investment for Cloud platforms", in *Proc. of the Economics of Security in the Cloud Workshop*, pp.132-137, IEEE Press, United Kingdom, 2013.