Verification, Validation, and Evaluation in Information Security Risk Management

Stefan Fenz and Andreas Ekelhart

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org

Motivation and Problem

- **Over the last four decades, various information security risk management (ISRM) approaches have emerged.**
- **A lack of sound verification, validation, and evaluation methods for these approaches exists.**
- **While restrictions, such as the impossibility of measuring exact values for probabilities and follow-up costs, obviously exist, verification, validation, and evaluation of research is essential in any field, and ISRM is no exception.**

Goals

- **Survey of verification, validation and evaluation methods referenced in ISRM literature**
- **Discussion and recommendation in which ISRM phases the methods should be applied**

Information Security Risk Management phases

Generic ISRM phase and its output	CRAMM phase	NIST SP 800-30 phase	OCTAVE phase	EBIOS phase	ISO 27005 phase
System Characterization **Output: inventory list of assets to be protected, including their acceptable risk level**	Asset Identification	System Characterization	Identification of Critical Assets and Corresponding Security Requirements Identification of Current Security Practices	Study of the Organization Study of the Target System Determination of the Security Study Target Expression of Security Needs	Identification of Assets
Threat and Vulnerability Assessment **Output: list of threats and corresponding vulnerabilities endangering the identified assets**	Threat Assessment Vulnerability Assessment	Threat Identification Vulnerability Identification Control Analysis	Identification of Threats and Organizational Vulnerabilities Identification of Current Technology Vulnerabilities	Study of Threat Sources Study of Vulnerabilities Formalization of Threats	Identification of Threats Identification of Vulnerabilities
Risk Determination **Output: quantitative or qualitative risk figures/levels for identified threats (input: threat probability and magnitude of impact)**	Asset Valuation Risk Assessment	Likelihood Determination Impact Analysis Risk Determination	Risk Determination for Critical Assets	Comparison of Threats with Needs (Risk Determination)	Identification of Impact Assessment of Threat Likelihood Assessment of Vulnerability Likelihood Risk Estimation
Control Identification **Output: list of potential controls that can mitigate the risks to an acceptable level**	Countermeasure Selection	Control Recommendations	Identification of Risk Measures	Formalization of Security Objectives	Evaluation of Existing and Planned Controls
Control Evaluation and Implementation **Output: list of cost-efficient controls that have to be implemented to reduce the risk to an acceptable level**	Countermeasure Recommendation	Control Evaluation Cost/Benefit Analysis Control Selection Safeguard Implementation Plan Development Control Implementation	Protection Strategy Development Risk Mitigation Plan Development	Determination of Security Levels Determination of Security Requirements Determination of Security Assurance Requirements	Information Security Risk Treatment (Risk Avoidance, Risk Transfer, Risk Reduction, or Risk Retention)

Results

How to verify, validate, and evaluate information security risk management phases?

	System Characterization	*Threat and Vulnerability Assessment*	*Risk Determination*	*Control Identification*	*Control Evaluation and Implementation*
Verification					
Sensitivity Analysis			•		•
Internal Result Comparison	•	•	•	•	•
Simulation			•		
Validation					
Experts	•	•	•	•	•
Alternate Decision Process	•	•	•	•	•
Statistical Evidence			•		•
Evaluation					
Management Decision Behavior Analysis	*Both methods evaluate the influence of the overall ISRM activities on the considered organization.*				
Control Quality Assessment					

Figure 1: ISRM verification, validation, and evaluation framework

Implications for Research and Practice

- **Our review of existing ISRM literature revealed that there are no standardized methods for verification, validation, and evaluation of ISRM-related research.**
- **Verification of ISRM approaches can be conducted objectively with the introduced methods, while validation turned out to be of a rather interpretive nature.**
- **The evaluation methods listed and the defined criteria allow organizations to survey effects of introduced ISRM approaches.**
- **Depending on the focus of the ISRM research, specific ISRM phases can be targeted and researchers can select suitable verification, validation and evaluation methods as described by our research results.**
- **Practitioners have to establish trust in potential or already implemented ISRM approaches. This usually requires the verification and validation of all ISRM phases. While verification and validation should be conducted at the beginning of the process, evaluation should be continuous so as to determine the benefit of the implemented approach.**

S. Fenz, A. Ekelhart: "Verification, Validation, and Evaluation in Information Security Risk Management," in IEEE Security and Privacy, Vol.8, 2010.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.