universität wien

DISSERTATION

Titel der Dissertation

"An Approach to Continuous Information Security Risk Assessment focused on Security Measurements"

Verfasser

Stefan Schiebeck, MSc

Angestrebter akademischer Grad

Doktor der Sozial- und Wirtschaftswissenschaften (Dr.rer.soc.oec)

Wien, 2014

Studienkennzahl lt. Studienblatt:	A 084 175
Dissertationsgebiet lt. Studienblatt:	Wirtschaftsinformatik
Betreuer:	Univ.Prof.DI.DDr. Gerald Quirchmayr

This thesis is dedicated to my parents, Karl and Gertrude, who emphasized the importance of education and lovingly steered me in the right direction, to my girlfriend Isabella, whose compassion and support helped me to accomplish this thesis, and to the staff of supporting organizations, who made this research possible.

This thesis was supported by the program line “Trust in IT Systems” by the Austrian Research Promotion Agency (FFG) [819952].

Contents

Acknowledgements

First of all, I would like to express my deepest appreciation to Professor Gerald Quirchmayr for being my supervisor over the past years. He provided excellent guidance, challenged and enriched my ideas and kept me motivated throughout the research and development process. This dissertation would not have been possible without his support, understanding and encouragement. I am very thankful for the opportunity to hold guest lectures at universities in Thailand and Malaysia and collaborate with scientists from all over the world in multiple national and international research projects.

I would also like to show my gratitude to my master thesis advisor Professor Ingrid Schaumüller-Bichl, who – in addition to being a great teacher at the University of Applied Sciences Upper Austria, Campus Hagenberg – provided the spark for my interest in Information Security Management and Risk Management and helped me to establish the preceding research of this thesis.

I am very grateful for the chance to establish my doctorate while working for SEC Consult, which allowed me to lead and participate in a multitude of cutting-edge information security consulting projects, pushing me forward to learn about diverse domains and view similar topics from different perspectives. I would like to especially thank my coworkers and friends Andreas Nusser, Avi Kravitz, Daniel Fabian, Isabella Kreyci, Johannes Greil, Sebastian Petz, Thomas Kerbl, Ulrich Fleck, and our managers Clemens Foisner, Jürgen Kraupa, Markus Robin and Martin Eiszner for their help and encouragement. Thanks to our top management, this thesis and all future work has been made possible in the first place.

Special thanks goes to the Department of Defense (BMLVS), who provided me with insights, suggestions and references as well as the methodical evaluation and testing of the prototype. Regrettably, I cannot acknowledge them by name.

I am very much obliged to the Austrian Research Promotion Agency (FFG), who provided the funding necessary to conduct the foundational research and development project.

Furthermore, I would like to thank my family and closest friends, especially Sergiu Ardelean for creative- and moral support, Florian Reiterer for countless controversial discussions about the newest technologies and Jörg Eibl for invaluable assistance during the long hours of software design and development.

Finally, I would like to express my gratefulness to my girlfriend Isabella Fetty, who was always there for me, fed me, cheered me up and motivated me to accomplish this thesis.

Page intentionally left blank.

Glossary

AHP	Analytical Hierarchy Process
ANN	Artificial Neural Network
BBN	Bayesian Belief Network
Aggregation	Process of estimating the total effect of multiple independent effects
Accumulation	see Aggregation
ALE	Annual Loss Expectancy
Asset	Organizational value
Attack vector	Definition of a single or multiple consecutive events needed to exploit a vulnerability or circumvent a safeguard
Base measure	Measure defined in terms of an attribute and the method for quantifying it [34; p. 7]
BIA	Business Impact Analysis
Consequence	Outcome of an event affecting objectives [1; p. 1]
Control	Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature [34; p. 7]
CMM	Capability Maturity Model
CPT	Conditional Probability Table
Dashboard	Adaptable set of high-level visualizations to support decision making
Defuzzification	Process of estimating a crisp value out of a geometric result used in fuzzy logic
Dependency scenario	Set of logically/functionally dependent assets

Derived measure	Measure that is defined as a function of two or more values of base measures [34; p. 8]
Energetic sum	Function to estimate the aggregated sound pressure/risk resulting of multiple independent sources [cp. 63; p. 48f]. The proposed method recommends its usage to provide a risk-averse aggregation function for incoherent risks (see 3.1).
Exposure	Variable used to describe the combined effect on protection criteria based on underlying threat likelihoods and vulnerability weaknesses/safeguard immaturities (potential residual attack vector)
Flex	Apache Flex (formerly Adobe Flex) is a framework for the development of rich Internet applications based on the Adobe Flash platform
Functional relationship	Mathematical function used to aggregate effects
Fault Tree Analysis	Top-down, deductive failure analysis in which multiple undesired effects on a system can be analyzed
Fuzzy logic	A discipline that deals with approximate reasoning using fuzzy terms and fuzzy rules
Fuzzy rule	Conditional IF-THEN statement using fuzzy terms
Fuzzy term	Linguistic term defined with many-valued logic
HTTP(S)	Hypertext Transfer Protocol (Secure), a widely deployed communications protocol for communication over a computer network
IT-Grundschutz	Set of documents proposed by the German Federal Office for Security in Information Technology (BSI) describing methods, processes, procedures, approaches and measures related to information security

Impact	see Consequence
Joint analysis	Process of estimating the aggregated effects on assets based on their dependency scenarios
Likelihood	Chance of something happening [1; p. 3]
Maturity target	Desired level of safeguard process maturity based on CMM
Measure	Combination of a measurement with its metric
Measurement	Process of obtaining information about the effectiveness of ISMS and controls, the achievement of control objectives and performance of ISMS processes, using a measurement method, a measurement function, an analytical model, and decision criteria [34; p. 8]
Metric	Unit of measurement
Membership degree	Degree to which a fuzzy term is accomplished
Module	Set of information describing information security threats, safeguards, roles, responsibilities and methods to ensure baseline protection of a specific scope
Protection criteria	see Risk criteria
Protection criteria risk	Risk estimated for specific protection criteria
Qualification target	Desired set of safeguards in scope according to ISO/IEC 27001 certification based on IT-Grundschutz
Risk	Effect of uncertainty on objectives [1; p. 3]
Risk criteria	Terms of reference against which the significance of a risk is evaluated [1; p. 4]
Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether

	the risk and/or its magnitude is acceptable or tolerable [1; p. 4]
Risk factors	Set of variables (e.g. impact, threat likelihood, safeguard maturity) having an effect on risk
Risk factor target	Risk factor instantiation within a risk model that is being influenced by an expert rule
Risk identification	Process of finding, recognizing and describing risks [1; p. 4]
Risk model	Total set of objects describing an organizational environment in regards to risk assessment and management
Risk treatment	Process to modify risk [1; p. 5]
Risk management	Coordinated activities to direct and control an organization with regard to risk [1; p. 5]
RoR	see Ruby on Rails
Ruby on Rails	An open-source rapid prototyping web application framework based on the general-purpose programming language Ruby
Safeguard	see Control
SIEM	Security Incident- and Event-Monitoring
Threat protection criteria influence	Estimated level of effect of a threat on specific protection criteria

1 Motivation for a Measure driven Risk Evaluation Framework

Today's information security risk assessment and management methods and supporting tools still rely primarily on subjectively estimated risk factors, providing no framework to incorporate measurements or expert knowledge in an analytical model.

Previous research in [3; p. 47ff] and [55; p. 69ff] on information security risk assessment methods and tools conducted in cooperation with the Austrian Federal Ministry of Defense has shown the need for a simple, adaptable modeling framework based on standards and best practices that can be easily extended, as well as an integrated framework for metrics and knowledge management, that allows for the exchange of formalized metrics and expert knowledge.

Based on these requirements, the research underlying this thesis was aiming to:

- identify a generically usable risk assessment approach for information security risks and a supporting library,
- define metrics management and calculation framework,
- evaluate and implement knowledge management approaches for continuous inference and reassessment,
- define an overall framework and methodology, modeling options and aggregation functions,
- design and implement a prototype and supporting system architecture, and
- evaluate and interpret the conclusiveness of assessment results.

Because complex risk models usually include reasonable and justified, yet scientifically unprovable assumptions that capture the occurrence and relations of risks, the full validation of the assessment and inference functions remains impossible from a scientific point of view. As shown in [9; p. 12f], even a model describing risks solely based on scientifically validated measurements would still be unprovable, even though the effort to capture all measurements would be enormous, because the relation between measures and risk factors is still influenced by subjective judgment of modelers.

Therefore, the objective of this research was the definition of a framework, model and supporting architecture to provide a balanced, manageable way of gaining insight to risks and trends based on a comprehensive role based estimation and assessment framework that is automatically influenced by an expert knowledge system using a small set of selected security metrics that have a high impact on the overall model.

The proposed model consequently provides a framework for extendable technical and organizational sensors that continuously gather various security relevant attributes, derives security metrics and indicators based on ISO/IEC 27004 and uses adaptable knowledge management approaches to continuously infer risk factors of an assessment model based on ISO/IEC 27005, using IT-Grundschutz as an extendable modeling framework.

The core part of this doctoral thesis is structured as follows:

- Chapter 1 outlines the motivation for this work,
- Chapter 2 describes the foundations of the disciplines to integrate,
- Chapter 3 introduces the proposed integrated process and model,
- Chapter 4 illustrates an integrated assessment,
- Chapter 5 demonstrates the proposed framework and prototype,
- Chapter 6 describes evaluation & validation techniques,
- Chapter 7 gives a final conclusion, summarizes scientific contributions and limitations and gives a brief outlook on future work, building on the results of this thesis.

2 Foundations

2.1 Risk Assessment and Management

Besides ISO 31000, which is the most widespread international standards on risk management, covering a generic view on risk management, ISO/IEC 27005 [1] is a core driver for this research, because it provides detailed guidance for information security risk assessment and management and is applicable to all types of organizations. Being compliant with ISO/IEC 27001 [71], most complete in comparison with other existing standards and internationally recognized, the process below is the assumed state of the art for information security risk assessment and management (see Figure 1).

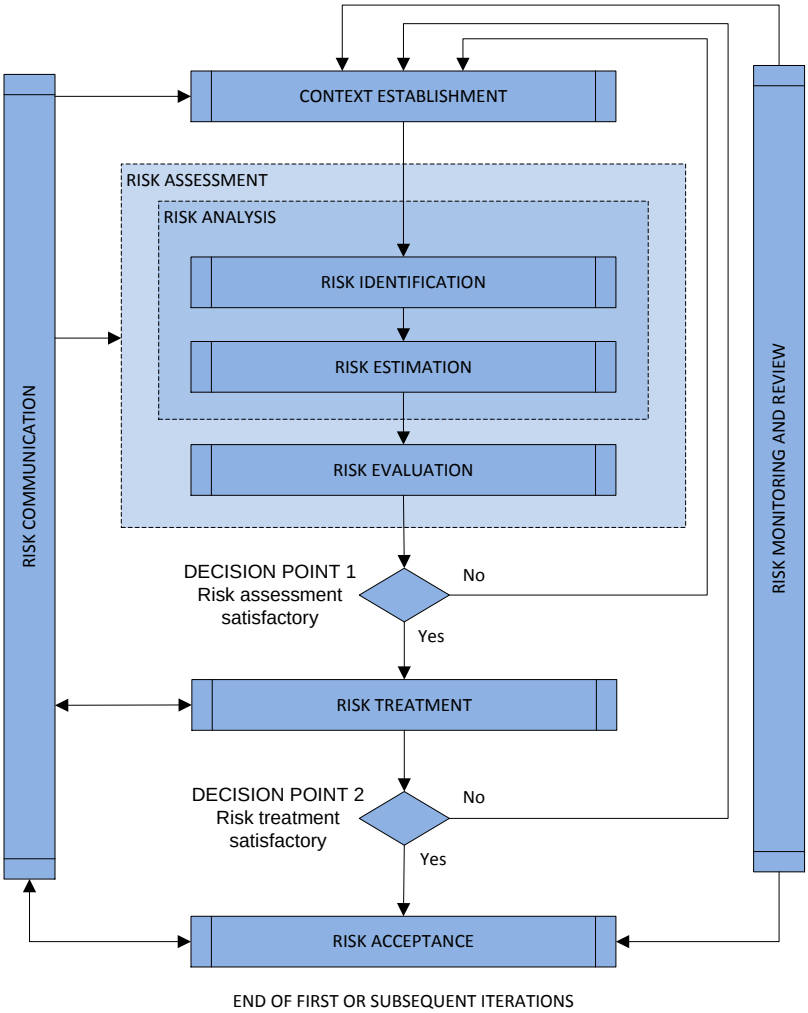


Figure 1: High level risk assessment and management process according to ISO/IEC 27005 [cp. 1; p. 8]

"...the risk management process can be iterative for risk assessment and/or risk treatment activities. An iterative approach to conducting risk assessment increases depth and detail of the assessment at each iteration. The iterative approach provides a good balance between minimizing the time and effort spent in identifying controls, while still ensuring that the high risks are appropriately assessed." [1; p. 8]

ISO/IEC 27005 defines risk generically as

"...a function of the consequences that would follow from the occurrence of an unwanted event and the likelihood of the occurrence of the event." [1; p. 13]

$$R := f(consequence, likelihood) \tag{1}$$

In order to allow more detailed assessments for the information security context, the methodology in [1] extends the generic definition of (1): *Consequence* incorporates a multitude of impacts (e.g. financial, reputational, etc.) on each affected protection (e.g. availability) and *likelihood* is diversified to cover the likelihood of the threat occurring as well as the likely level of weakness of an exposed vulnerability [1; p. 14ff]. An organizational asset is threatened by a threat source, which uses a vulnerability of the asset to cause an impact due to the loss of the affected protection criteria, as outlined in Figure 2.

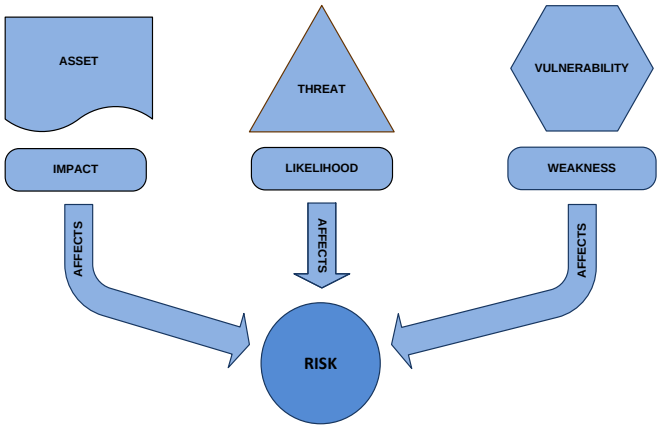


Figure 2: Risk factors according to ISO/IEC 27005. An asset risk is affected by its associated impact, threat likelihood and likely level of vulnerability weakness.

Especially for the analysis of specific types of threats (e.g. deliberate acts), it may be reasonable to further diversify these variables (e.g. attacker-capabilities, -motivation and -resources, ease to identify/exploit vulnerabilities, etc.) in order to provide a greater assessment depth and detail if required.

Having this model in mind, the risk *R* of an asset is a function of the consequences that would result from the losses of its protection criteria (e.g. confidentiality *C*, integ-

rity *I* and/or availability *A*), the threat likelihood *T* and the likely level of weakness of the vulnerability *V* exposed (2) [1; p. 14ff]. The vector *CIA* can of course be extended according to the needs of the application domain, e.g. following the PIAAA[1] extension described in [58; p. 7f].

$$R := f(f_{impact}\begin{pmatrix} C \\ I \\ A \end{pmatrix}, T_{likelihood}, V_{weakness}) \tag{2}$$

Because most risk modeling frameworks, especially those focusing on establishing compliance, rely on safeguard requirements to compensate for likelihood, it has been shown in [41; p. 140f] that the estimation of a vulnerability weakness can be substituted based on the safeguards *S* maturity gap (3), which is designed to mitigate the respective threat and the exposed vulnerability to a desired level.

$$R := f(f_{impact}\begin{pmatrix} C \\ I \\ A \end{pmatrix}, T_{likelihood}, S_{maturity\ gap}) \tag{3}$$

Designing a model using (3) has the advantage of a greater pool of pre-defined risk factors and the disadvantage that information on residual threat likelihoods and vulnerability weaknesses is not available due to the safeguard-centric design. Therefore, future work should incorporate the assessment of residual risks for critical assets during detailed risk analysis (outlined in 7.2).

Annex B of [1] defines the basic structure of primary and supporting assets to achieve a view of dependencies and hence, business impact and risk inheritance relations between assets. The annex gives examples of primary and supporting assets but does not define separate risk assessment techniques that go beyond the assessment of a singular asset. Therefore, the proposed model established asset dependency relations using a suitable knowledge management discipline, evaluated in chapter 2.3.1 and described in chapter 3.1.

[1] Privacy, Identification, Authentication, Authorization, Accountability

Having established the basic risk factors and estimation function, the base pool of risk factors has to be identified in order to give the user a comprehensive working environment. In order to meet general scientific and economic requirements, the risk factor catalog should:

- be maintained either by a governmental agency or a well-known, reliable, vendor independent company specialized in information security
- be regularly updated
- cover a comprehensive set of assets, threats and safeguards or vulnerabilities to be used as risk factors
- ideally predefine a risk factor structure based on generic assets and their general threats and vulnerabilities for ease of modeling
- be available in multiple languages, at least in English and German

In [45] a preliminary reference source for threats, vulnerabilities, impacts and controls has been compiled by members of the ENISA ad-hoc working group on risk-assessment and -management. During initial research of this thesis, those standards, best-practices and well known de-facto standards of information security management and risk management have been compared according to their approximate amount of asset-, threat-, vulnerability- and control-definitions. The results of this evaluation are outlined in Figure 3, followed by a short description of each referenced standard.

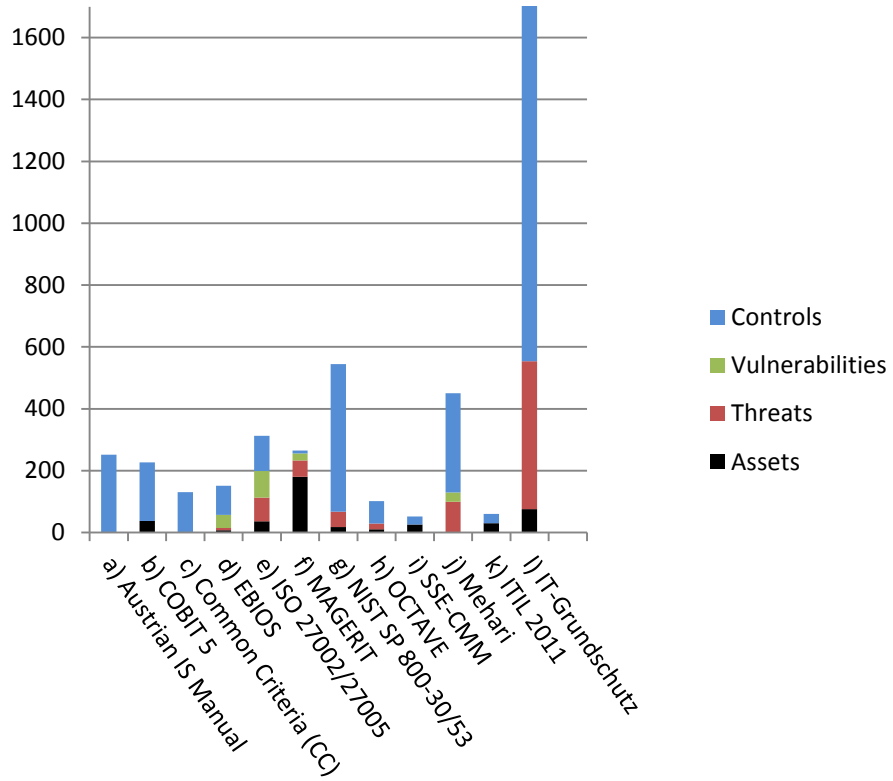


Figure 3: Comparison of the approximate amount of asset-, threat-, vulnerability- and control-definitions of sources defined in [45]

a) The Austrian Information Security Manual [68] gives guidelines for the establishment of an information security management process as well as a compact summary of technical and organizational security controls. The handbook is only available in German and does not cover assets, threats or any pre-established relations.

b) COBIT (Control Objectives for Information and Related Technology) 5 [73] is an international IT governance framework supporting business alignment of IT and IT auditing. It defines 17 generic enterprise goals and relates them with 17 IT-related goals, which in turn are related to 37 IT-Processes, providing control practices as well as value- and risk-drivers. There are a lot of interesting new mappings defined within COBIT 5, ranging from strategic goals to operational key goal- and key performance-metrics. While these mappings as well as mappings to the controls of many other standards are available in [6], [7], [8], no threats or prioritization of controls are defined.

c) The Common Criteria for Information Technology Security Evaluation (CC) [76] is intended to be used for the formal definition and certification of security requirements for a given product. Because the standard focuses on technical security aspects and their formal validation, it is not designed to be compatible to risk assessment and management methods.

d) EBIOS [77] is a French software product with its own methodology using a risk factor base recompiled from major ISO standards and best practices. While the risk assessment methodology is complex, the underlying risk factor base is not pre-estimated and only covers a relatively small number of high level aspects.

e) The ISO/IEC 27002 [72] catalog covers controls, while the ISO/IEC 27005 [1] adds examples of threats and vulnerabilities. While these standards are common, the list of threats and vulnerabilities are only a very high level subset. However, the controls of ISO/IEC 27002 are a fundamental part of today's information security management systems and risk management methodologies and will therefore be included as a cross-reference [57].

f) MAGERIT [78] is a Spanish risk assessment and management method with a supporting tool based on a large set of example asset classes but only a small number of non-related threats, vulnerabilities and safeguards.

g) The NIST SP 800-30 [74] gives some examples of assets and threats, while SP 800-53 [75] covers quite a lot of controls that are recommended for Federal Information Systems and Organizations. In annex H there are control

mappings to and from ISO/IEC 27002 which poses a practical add-on for another possible cross-reference.

h) Octave [79] is a method and a supporting tool strictly focused on a comprehensive risk assessment, providing a small set of generic security controls to build asset-based threat-profiles. The method and tool does not provide a risk management framework or any pre-established risk factor model.

i) The Systems Security Engineering – Capability Maturity Model (SSE-CMM) [80] is a process reference model designed for the IT Security domain and describes the essential characteristics of an organization's security engineering process that should exist. It provides process-, control- and goal-definitions but does not reference threats or any pre-established estimations.

j) Mehari [81] is a French risk-assessment and –management method that allows highly detailed scenario evaluation. The available catalog of controls, threats and vulnerability scenarios is quite extensive, but due to the method's complexity and the supporting Excel-workbook, it is not feasible for larger risk models from a maintenance point of view.

k) ITIL [82], the IT Infrastructure Library, is a comprehensive collection of best-practices for IT Service Management, developed by the UK Government. Currently published in version 3, it contains five core publications, each focusing on a separate service lifecycle stage (strategy, design, transition, operation, continual improvement). The de-facto standard defines recommended processes and procedures, focusing on the planning, provision and implementation of IT services, but does not provide detailed information regarding threats.

l) The most comprehensive catalog available that covers assets, threats and controls is IT-Grundschutz [5]. The relations of the risk factors are pre-established, controls are prioritized and their descriptions and additional control questions give details on evaluation aspects. The BSI has published a control-mapping from IT-Grundschutz to ISO/IEC 27002 [57], which eases the incorporation of both ISO/IEC 27002 as well as NIST SP 800-53 [74]. Therefore IT-Grundschutz can be used to model asset-threat-safeguard relations, allowing the interchange of IT-Grundschutz controls with ISO/IEC 27002 controls and NIST SP 800-53 controls. Furthermore almost all asset, threat and safeguard descriptions are available in German and English and updated regularly.

2.1.1 *Selected Modeling Framework*

Based on the high granularity of risk factors, international acceptance, simple but comprehensive modeling framework and governmental support, IT-Grundschutz [5], [64], [46-49] has been chosen as a predefined and pre-evaluated framework of risk factors to support asset modeling. Some textual descriptions which were not yet available in the English version [64] of the IT-Grundschutz catalogs have been translated by the author. IT-Grundschutz catalogs and cross-references are implemented using an additional cross-reference with ISO/IEC 27002 [57] and can later be extended with a mapping to NIST SP 800-53 and SANS 20 critical security controls [69]. Using the IT-Grundschutz catalogs has several advantages:

- it gives the end-user the most comprehensive risk factor base, compared to other existing sources,
- establishing a predefined asset structure and pre-evaluated risk factor relations,
- being commonly known and accepted,
- allowing a parallel view on ISO/IEC 27001/2 controls and other major standards for compliance audits and certifications, and
- needing less continuous maintenance.

The proposed model described in 3 follows all standards defined by IT-Grundschutz [46-49], including a technique used to model asset dependencies (see Figure 29) and a detailed risk analysis method [48] to support the extension of the model.

The first important difference to the risk model of ISO/IEC 27005 is that IT-Grundschutz substitutes the vulnerability risk factor using predefined safeguards to mitigate the substituted vulnerability. Due to the detailed safeguard definitions of IT-Grundschutz, the assessment of the "likely level of weakness" of those vulnerabilities is compensated by prioritized safeguards, mitigating the vulnerability to a general acceptable baseline (Grundschutz). Practice has shown that humans achieve more consistent results when defining safeguard priorities in their working environment than evaluating vulnerabilities. Figure 4 shows the risk factor relationships defined by IT-Grundschutz.

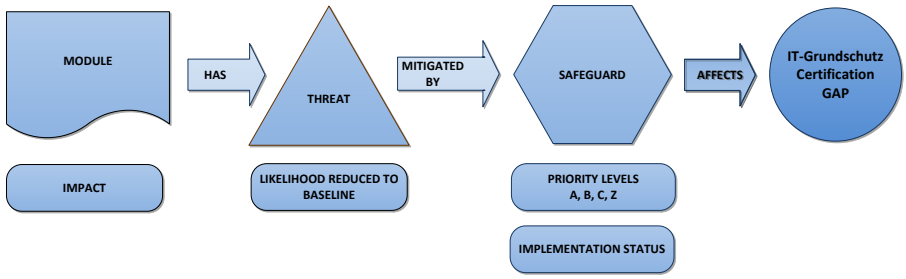


Figure 4: IT-Grundschutz GAP assessment model

IT-Grundschutz methodology is solely based on the evaluation of safeguard implementation states to estimate an IT-Grundschutz certification gap, but does not estimate the associated threat reduction or module protection.

The IT-Grundschutz catalogs are currently released in version 13 [5] and are comprised of ~80 modules, describing generalized aspects of information security (see Figure 5) by cross-referencing ~600 threats, mitigated to baseline levels by ~1200 prioritized controls. Figure 5 gives an overview of available IT-Grundschutz modules/types as well as threat- and safeguard-types.

Modules/types
Generic aspects of Information Security
Information Security Management, Organization, Personnel, Contingency Planning, Data Backup Policy, Data Privacy Policy, Concept of computer virus protection, Crypto-concept, Handling of security incidents, Hard- and Software-Management, Standard software, Outsourcing, Archiving, Information Security awareness and training, Patch- and Change-Management, Secure Deletion/Destruction of Data, Requirements Management
Security of the infrastructure
Building, Cabling, Office, Server Room, Data Media Archive, Technical Infrastructure Room, Protective Cabinets (room), Working place at home, Computer Centers, Mobile Workplace, Meeting, event and training rooms, IT cabling
Security of IT systems
General Server, Server under Unix, Server under Novell Netware 4.x, Windows 2000 Server. S/390 and zSeries mainframes, Windows Server 2003, Windows Server 2008, General client, General standalone IT system, Laptop, Unix client, Windows 2000 client, Internet PCs, Windows XP client, Windows Vista client, Mac OS X client, Windows 7 client, Security gateway (firewall), Routers and switches, Storage systems and –networks, Virtualization, Terminal server, Telecommunication system, Fax machine, Mobile Telephones, PDA, Printer, Copier and Multi-Function-Devices
Security in the network
Heterogeneous Network, Network and System Management, Modem, Remote Access Service, LAN connection of an IT system via ISDN, Wireless LAN, Voice-over-IP, Bluetooth
Security of applications
Peer-to-Peer services, Exchange of Data Media, E-Mail, Web server, Lotus Notes, Fax servers, Databases, Telecommuting, Novell eDirectory, Internet Information Server, Apache Webserver, Exchange 2000/Outlook 2000, SAP System, Mobile Devices, Generic directory service, Active Directory, Samba, DNS-Server, Internet usage, OpenLDAP, Web Applications, Logging

Threat types	**Safeguard types**
Force majeure	*Infrastructure*
Organizational shortcomings	*Organization*
Human failure	*Personnel*
Technical failure	*Hardware & Software*
Deliberate acts	*Communications*
	Contingency planning

Figure 5: Overview of pre-defined IT-Grundschutz modules/types, threat- and safeguard-types [cp. 5]

For every module outlined in Figure 5, a cross-reference table as shown in Figure 6 is defined and published [2] by the German Federal Office for Security in Information Technology (German BSI), but is not yet used throughout the methodology to assess risks.

Module 1.0 Security Management						
Controls	Cycle	Priority	T 2.66	T 2.105	T 2.106	T 2.107
S 2.192 Drawing up an information security policy	Planning and design	A	X	X	X	
S 2.193 Establishing a suitable organizational structure for information security	Implementation	A	X			X
S 2.195 Drawing up an information security concept	Implementation	A	X			
S 2.197 Drawing up an training concept for information security	Implementation	A	X			
S 2.199 Maintenance of information security	Operation	A	X	X		X
S 2.200 Preparation of management reports on information security	Operation	C	X			
S 2.201 Documentation of the information security process	Operation	C	X			
S 2.335 Defining the information security objectives and strategy	Planning and design	A	X		X	X
S 2.336 Acceptance of overall responsibility for information security at the management level	Planning and design	A	X	X	X	X
S 2.337 Integration of information security in organization-wide workflows and processes	Operation	A	X			
S 2.338 Creating target group oriented information security policies	Operation	Z	X			
S 2.339 Cost-effective use of resources for information security	Operation	Z		X		X
S 6.16 Taking out insurance	Contingency planning	Z		X	X	

Threats
T 2.66 Lack of or inadequate information security management
T 2.105 Violation of statutory regulations and contractual agreements
T 2.106 Disturbance to business processes as a result of information security incidents
T 2.107 Uneconomic use of resources as a result of an inadequate information security management

Figure 6: Cross-reference table of module “1.0 Security Management” [cp. 2]

Figure 6 shows the cross-reference between prioritized safeguards and the threats they are mitigating. The German Federal Office for Security in Information Technology has defined a staged certification process, requiring the implementation of increasing groups of safeguards:

- Level 1 “entry level”: All relevant “A” safeguards have to be implemented.
- Level 2 “higher level”: All relevant “A” and “B” safeguards have to be implemented.
- Level 3 “ISO/IEC 27001 certification based on IT-Grundschutz”: All relevant “A”, “B” and “C” safeguards have to be implemented. “Z” safeguards are additional recommendations for high security environments.

The certification levels follow a prioritized treatment of risks, meaning that high risks have to be mitigated first, followed by medium risks and at last low risks, so IT-Grundschutz safeguards can be grouped into the corresponding levels:

- “A” safeguards are mitigating threats that are very likely to happen, mitigation is very important
- “B” safeguards are mitigating threats that are likely to happen, mitigation is important
- “C” safeguards are mitigating threats that are somewhat likely to happen, mitigation is recommended
- “Z” safeguards are additional recommendations, their implementation may be suitable for environments with high security requirements

Using the presented approach, threats and related protection criteria exposures can be estimated based on IT-Grundschutz [2] using approximately 8000 prioritized cross-references in order to provide a generic, pre-estimated environment that can be adapted to the organizational context.

Another significant aspect that can be used to establish the risk assessment requirements is the pre-established asset dependency structure (see Figure 7) of IT-Grundschutz to establish a managed and reasonable way of performing BIA and document requirements throughout the organization.

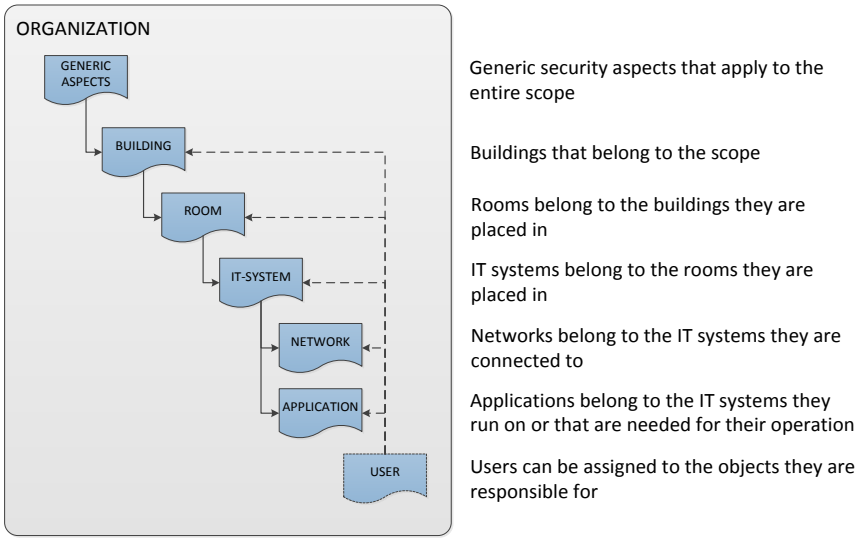


Figure 7: Pre-defined modeling structure of IT-Grundschutz [cp. 47; p. 62]

The proposed model uses and extends the safeguard-/threat-/impact-factor model of IT-Grundschutz as well as the modeling structure, to allow assessments on protection criteria and a more comprehensive assessment of dependencies (see Figure 29).

To establish the requirements for risk assessment based on IT-Grundschutz, further assumptions have to be made, which are outlined in 3.1.

The knowledge management technique used to achieve the risk assessment requirements is evaluated in 2.3.1 and described in 3.1.

2.2 Security Measurement

Based on ISO/IEC 27005 as a reference to risk assessment and management, the related ISO/IEC 27004 [34] is perfectly suited to provide guidance on the development and use of security measures in the context of information security.

> *"Measurement will verify how well selected security requirements, which are based on risk assessment and applicable legal and regulatory requirements, have been met."* [34; p. 5]

The standard provides a measurement model (see Figure 8) describing a generic measurement and how the results are fed back into the ISMS.

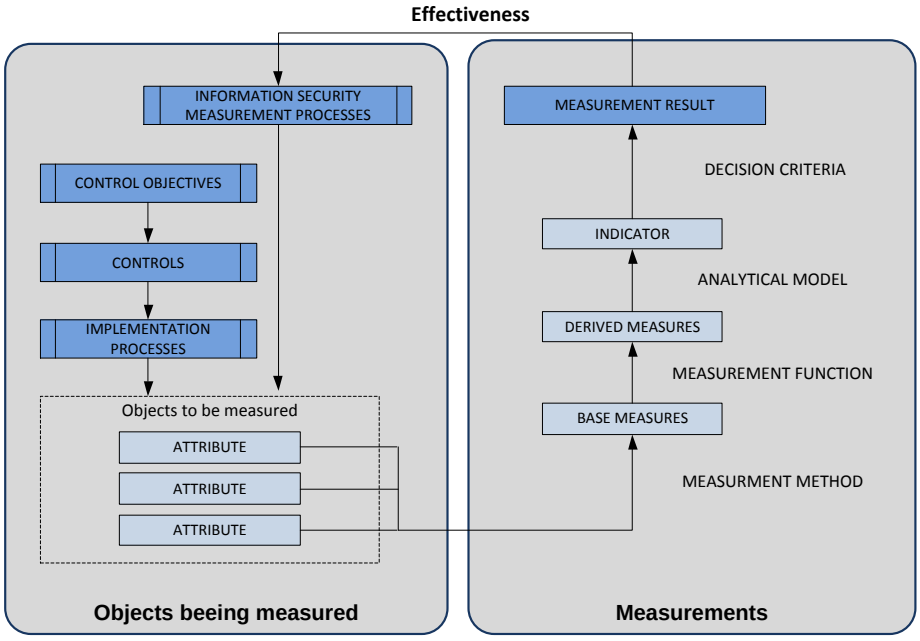


Figure 8: Measurement model according to ISO/IEC 27004 [cp. 34; p. 13]

Measures and measurement development starts by identifying the activities, products and services with the highest priorities to achieve an iterative implementation approach like ISO/IEC 27005. Then, security relevant attributes of those objects (resulting from the measurement process, control objectives, etc.) are identified, consolidated using base and derived measures and evaluated using indicators, as shown in Figure 9. To get final measurement results, decision criteria regarding target expectations and thresholds for initiating improvement actions have to be defined.

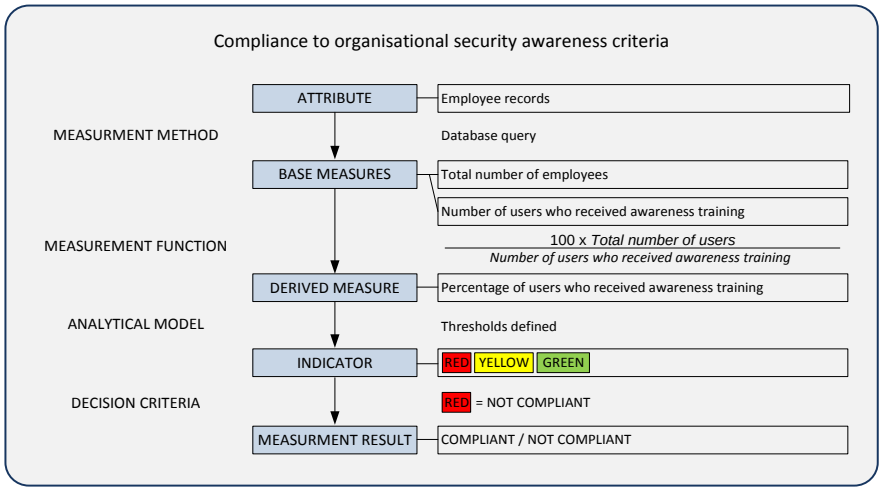


Figure 9: Measurement example for compliance to organizational security awareness criteria

While the measurement model of ISO/IEC 27004 is suitable to derive security measures and indicators, it defines no further technique to assist in the estimation of implications to the risk model based on the measurement results. Instead, the standard refers to a requirement of ISO/IEC 27001:2005.

> *"Assess the realistic likelihood of security failures occurring in the light of prevailing threats and vulnerabilities, and impacts associated with these assets, and the controls currently implemented."* [34; p. 5]

During the latest update of ISO/IEC 27001 in 2013 the explicit requirement for assessing threats as well as vulnerabilities has been adapted (amongst other changes) and now only reflects the requirement for assessing the realistic likelihood of the occurrence of risks. The latest version of ISO/IEC 27001 also extends and consolidates measurement-related requirements in clause 9.1 "*Evidence of the monitoring and measurement of information security"* in order to facilitate security monitoring. To achieve an integrated process between risk assessment and security measurement, a knowledge management technique has been used that is evaluated in 2.3.4 and described in 3.3.

It is very important to distinguish between metrics and measurements at this point – metrics are definitions of units (e.g. meter, dB, Number of viruses detected in user files) while measurements are the quantities of the unit (e.g. 2 meters, 80 dB, 312 viruses detected in user files). Security metrics (also referred to as measures when combined with measurements) have become valuable components of Information Security Management Systems over the last few years, but unfortunately they don't yet earn as much attention as they should. A successfully implemented and managed security metrics program can benefit any organization in various ways:

- It serves as a measurement model for effectiveness of security controls. This is especially relevant during an ISO/IEC 27001 compliance audit.
- It helps to identify areas that require improvement (e.g. key performance indicators, key goal indicators).

- It helps to track and justify budgetary decisions by measuring how much money is spent in different areas with different success rates (e.g. using Return-On(-Security)-Investment models).

Because most security attributes and related measures can be generalized and exchanged between organizations, a huge pool of selectable measures is available through standards and best practices, as shown in Figure 10.

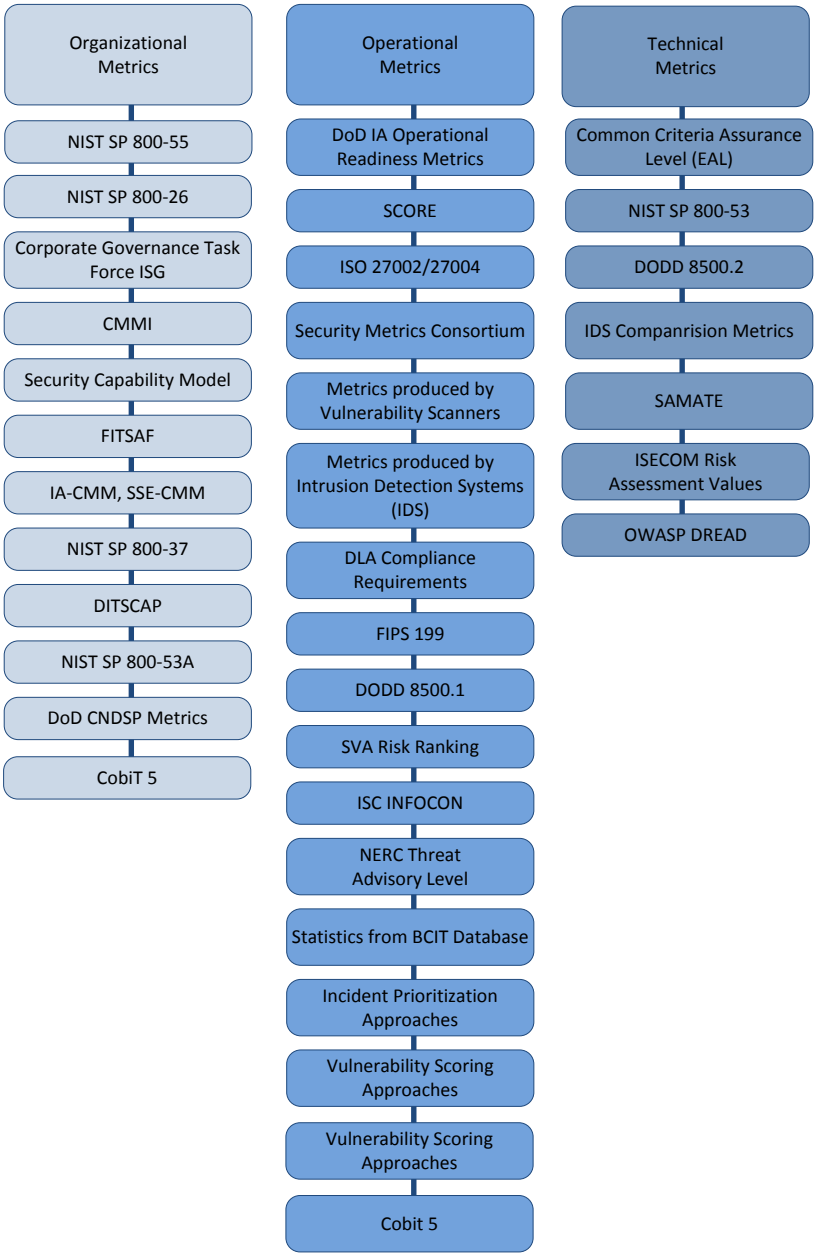


Figure 10: Metrics categorization and resources [cp. 50; p. 16]

Additionally to the metric sources outlined in Figure 10, the Metrics Catalog Project was launched on April 2008. The online metrics catalog [54] is a tool for the security metrics community to organize and share metric definitions. The metrics catalog is comprised of ~350 metrics and categorizes them depending on their relation to defined contexts, as shown in Figure 11.

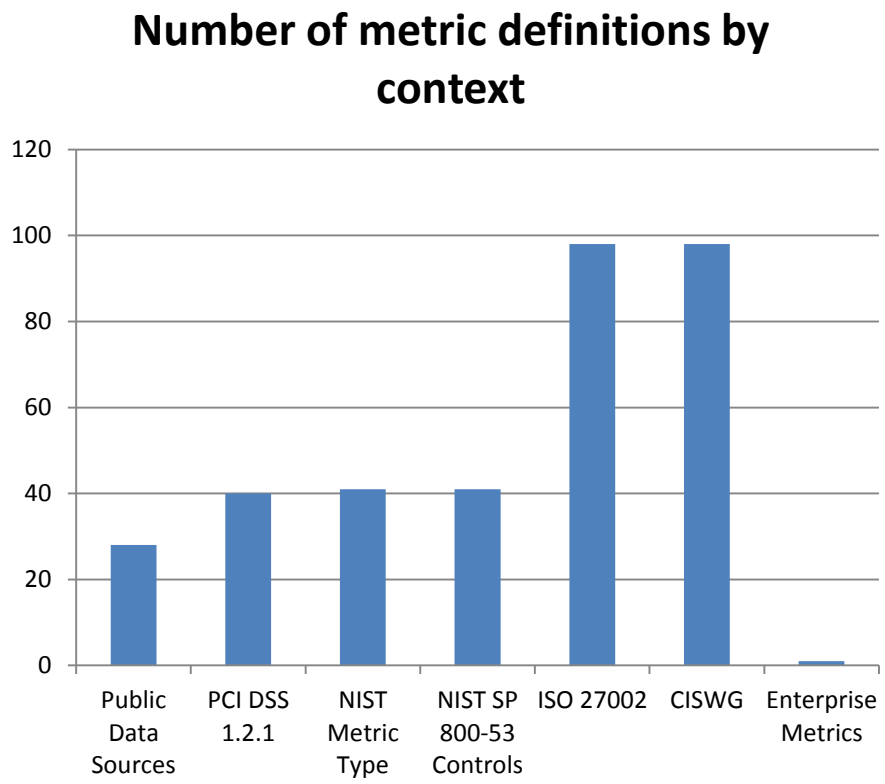


Figure 11: Number of metric definitions by context [cp. 54]

When selecting security metrics for an organization, certain criteria should be considered to ensure usefulness and cost-effectiveness [cp. 34; p. 20]:

- Strategic: Measure is aligned with the organization's business objectives and stakeholder needs
- Quantitative: Measure provides objective and empirical data
- Interpretive: Measure accommodates subjective inputs that assist with the interpretation of data
- Cost-effective: The cost of measurement collection is balanced against the potential losses to which the measure relates
- Verifiable: Third-party reviewers are able to assess data and concur with the results

- Meaningful: Measure provides meaningful information about applicable risk factors over time to enable assessment of the impact of changes or consistency of results
- Useful: Measure results should support mission, financial and operational decision making
- Indivisible: Measure collects data at the most discrete, unanalyzed level possible
- Well-defined: Measure documented using a defined template
- Repeatable: Measurements produce comparable and reproducible results

2.2.1 *Security Measurement Integration*

While most standards and best practices merely use internal measures that relate to safeguard effectiveness, the proposed model also incorporates internal and external measures that relate to threat likelihoods and asset impacts. Figure 12 shows a comparison of recent surveys and statistics in the context of information security and their approximate number of available measures, in the context of

- vulnerability measures, relating to vulnerability weakness trends (which in turn relate to safeguard priority, e.g. which vulnerability is used how often to cause an incident/number of incidents per vulnerability)
- threat measures, relating to threat likelihood trends (e.g. how many incidents happened, number of incidents per threat source)
- impact measures, relating to asset impact trends (e.g. how much did an incident cost, how long did it take to remediate an incident)

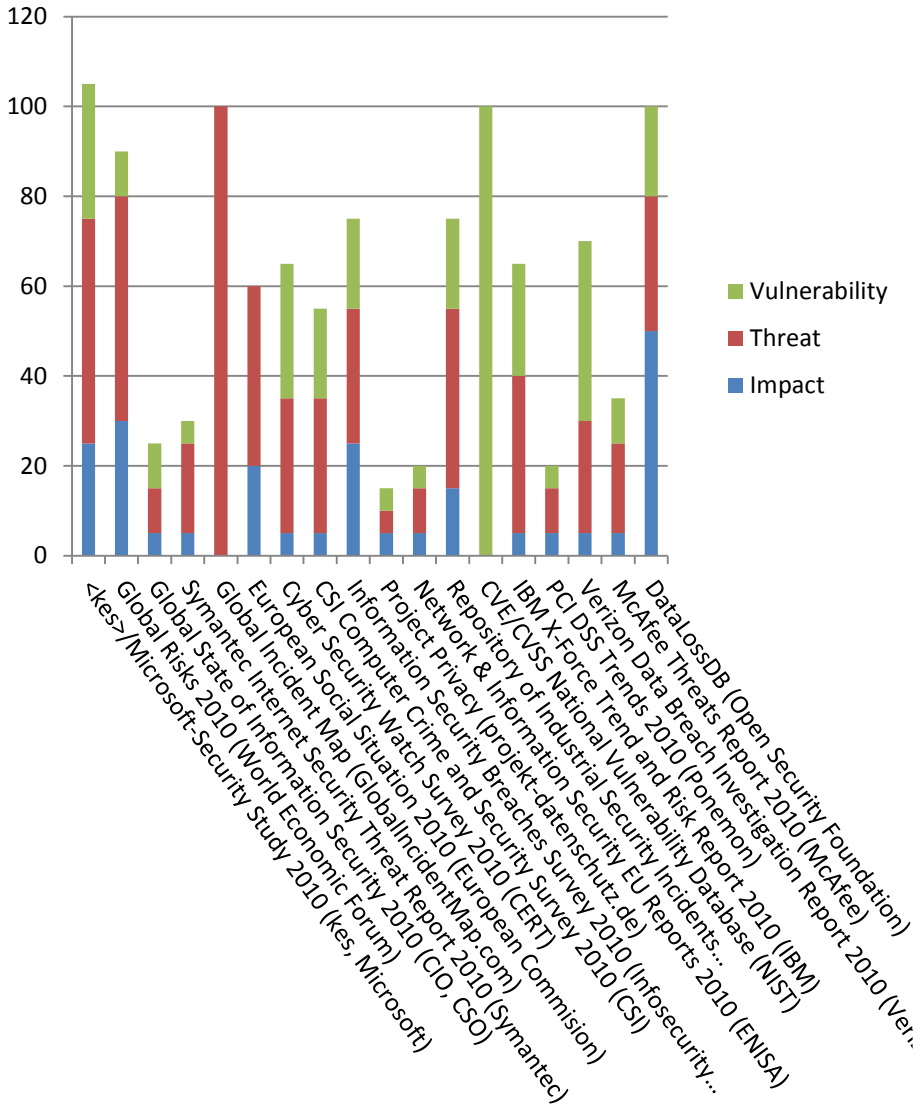


Figure 12: Approximate number of measures by related risk factor

Because not only measure definitions or external measures can be exchanged between organizations, also the generalized definition of estimated influence of those measures on risk factors can be formally defined and exchanged.

The proposed method uses a specific knowledge management technique to integrate the analytical model, indicator, decision criteria and measurement result into the estimation of impact on evaluated safeguard-, threat- and impact-indicators of the risk assessment model. The approach is evaluated in 2.3.4 and described in 3.3.

2.3 Knowledge Management

Knowledge management comprises a set of different methods to identify, relate and exchange knowledge that can be used to gain insights into specific topics. The evaluation of applicable knowledge management techniques focused on simulation models and expert systems that allow a machine interpretation of the documented knowledge to express a result. In a broader sense, knowledge management also covers relational database, document management, e-learning and collaboration systems in general.

The following evaluation of knowledge management approaches aims to identify suitable solutions to:

- support the risk assessment by enabling the knowledge based aggregation of risk factors as well as the definition and aggregation of asset dependencies, and to
- support the integration of security measures, by enabling knowledge management to define analytical models, indicators, decision criteria and measurement results as well as to express exchangeable relations with the risk factors of the assessment model.

2.3.1 Functional Relationships

Functional relationships use mathematical functions to estimate risks within a decomposed system model. The first step in using functional relationships is to define the system structure based on a functional decomposition of the analyzed system into its contributing factors, creating the structure of component relationships (dependencies). This decomposition is performed until the desired analysis depth is reached.

2.3.1.1 System Decomposition

Figure 13 shows the simplified decomposition of an asset based on the IT-Grundschutz module “1.0 Security Management” into its threats, safeguards and measures.

Based on this dependency structure, mathematical functions describing the logical behavior among the components and their associated factors are selected to represent the estimated overall system behavior. The modes of influence among components are in reality far more complex than classical logical relationships as used in fault tree analysis [53] can represent, creating the need for more sophisticated relationships. To indicate the degrees of influence on parent components, weightings can be assigned to every factor to represent the relative importance among components.

Examples of functional relationships in the context of risk assessment are estimation functions used to express behavior between risk factors as well as asset dependency models used to aggregate/inherit exposures and business impacts.

The decomposition of the asset in Figure 13 is based on the cross-references of the module down to the safeguard layer, creating a functional decomposition of the asset using its threat-, safeguard- and measure-components. These components are evaluated by the risk assessment, using a consistent structure and similar properties, which allows the usage of a uniform aggregation function for every layer.

The related security measures at the bottom layer are designed to potentially influence every layer of the model (see 2.2.1) and need individual evaluation to establish similar properties between measures (ISO/IEC 27004 analytical model [34; p. 15], e.g. using thresholds). Because the derived measures outlined in Figure 13 are based on individual scales, their relations have to be represented in a non-uniform manner. To represent different degrees of influence between measures, weightings have to be defined additionally.

The integration of measures into the other layers is designed to be an overlaying influence (value ± influence), rather than a uniform relation, because the proposed model is designed to use subjectively estimated values for the safeguard-, threat- and impact-layers (risk assessment) that are influenced by objectively measured attributes. Because the amount of relevant security measures needed to express all factors of the model would be too extensive to be manageable, the proposed model is designed to be influenced by high-impact security measures rather than based on all related attributes. Using high-impact measures adds the benefit of easing the recognition of subjectively wrong risk estimations – controls that are estimated to meet the target effectiveness but are influenced based on objective measures by the expert system.

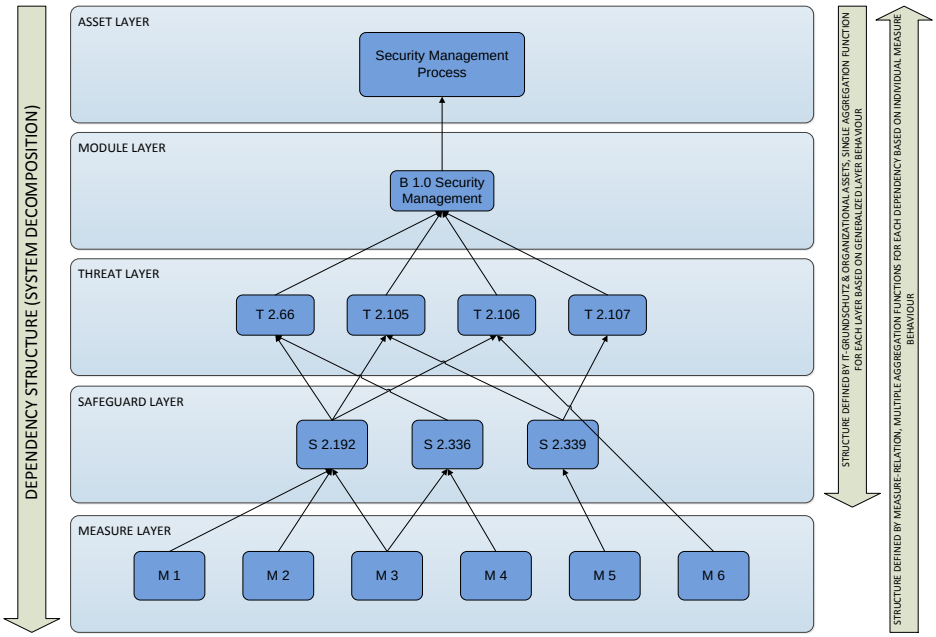
Based on these circumstances, the functional relationships needed to express the generalized behavior of the simplified model (and all models following the same structure and properties) in Figure 13 are:

- one function to aggregate module exposure to the asset risk layer,
- one function to aggregate threat likelihoods to the module exposure layer,
- one function to aggregate safeguard risks (expressing the immaturity/ineffectiveness of the safeguard) to the threat layer, and
- *n* functions to express the influence of *n* relations between the measure (expressing indicator/result) and its related components.

The usage of functional relationships in the example in Figure 13 requires the definition/selection of 3 generalized functions down to the safeguard level and 7 specific functions to describe the measure influence. This is because risk factor components down to this level follow a structurally and parametrically uniform standard (IT-Grundschutz), which therefore allows the usage of generalized functions. Security measures, on the other hand, are unique in their definition (although most derived measures will tell a percentage) and have specific indicators depending on the context, which requires a more adaptable way of establishing relations.

This could be circumvented by establishing a generalized scale for measures (e.g. 1…low, 2…medium, 3…high) and a single aggregation function to estimate their influences, but this leaves the user with the establishment of 18 thresholds for 6 measures. Using thresholds would also lead to leaping increases in influence prediction whenever a threshold level is reached.

The proposed model circumvents this problem by using functional relationships for the risk assessment model and a separate discipline to establish relationships with selected, high-impact measurements. These relationships are defined using fuzzy logic and fuzzy control, allowing the definition of smooth measure indicators and specific expert rules on correlating risk factors.



Security measures (M)	Scale
M 1 Percentage of employees trained regarding the Information Security Policy during the last year	0…100
M 2 Maturity level of Information Security Policy according to the COBIT Security Policy Maturity Model	1…6
M 3 Is the current Information Security Policy approved by Management?	0…1
M 4 Percentage of management staff sensitized on IT security during the last year	0…100
M 5 Time since the last IT security check was conducted	0…infinite
M 6 Percentage of DatalossDB-registered companies with major security incidents during the last month	0…100

Figure 13: Simplified functional decomposition of a security management process, outlined by the IT-Grundschutz module *B 1.0 Security Management* and applicable security measures

2.3.1.2 Establishment of Relationship Functions

Most risk assessment methods available for the information security market use very basic functions or matrices to estimate risks which do not take concurrent effect of risks into account. Especially when using comprehensive models that provide greater risk factor insight, it is extremely important to take concurrency of assets, threats and vulnerabilities/safeguards into consideration.
The proposed model therefore uses a more risk-averse approach to express parallel risks, originally used to calculate the sum of the sound pressure levels of multiple incoherent radiating sources, described in chapter 3.1.

The following functions, along with their bounded and normalized variants to suit specific models and parameters, should therefore only be used under specific circumstances, where the behavior of underlying components is expressed accordingly.

a) Maximum aggregation

The aggregation method in (4) should be used if the parent component behavior *P* is only dependent on the single maximum of its factors C_i. This should only be used if all *n* input factors C_i are mutually exclusive. Although this is not the case in most risk environments (e.g. components are usually threatened by multiple independent factors in parallel), this aggregation method is very common among risk assessment methods.

$$P := \underset{1 \leq i \leq n}{max}(C_i) \tag{4}$$

A valid usage of maximum aggregation within the proposed model is applied within joint analysis, where the total (master) asset protection criterion impact $Asset_{\ impact}$ is estimated based on the maximum protection criteria impacts of *n* scenarios (slaves) the asset is required in.

$$Asset_{pc\ impact} := \max_{1 \leq i \leq n}\left(Asset\ Scenario_{pc\ impact_i}\right) \tag{5}$$

b) Sum aggregation

This method should be used if the component behavior *P* is dependent on all factors C_i and none of the *n* factors are correlated. As soon as any correlation exists, the estimation falsely includes values representing shared properties.

$$P := \sum_{1 \leq i \leq n} C_i \tag{6}$$

An appropriate usage of this aggregation function in the context of the proposed model would be the summarization of multiple isolated module risks R_{module} (describing self-contained parts of the system, e.g. summing up baseline module risks with additional risks identified during detailed risk analysis) into a single asset risk R_{asset}. However, the proposed model favors the extension of modules rather than the separate modeling of baseline and detailed aspects, in order to support comparability between modules and ease harmonization of detailed aspects with the pre-defined baseline risk factor environment.

$$R_{asset} := \sum_{1 \leq i \leq n} (R_{module_i}) \tag{7}$$

c) Product aggregation

The product aggregation should be used under circumstances where the component behavior is dependent on all n factors and the individual factors are not correlated. If any correlation exists, the estimation falsely includes values representing shared properties. In comparison to maximum aggregation, this method results in an outcome scale that is quite larger than the input scale and should therefore be selected with caution, when used with other functional relationships, to avoid inconsistent results based on scaling. This aggregation function should only be used in conjunction with lower scales, if the relationship differs in a way that justifies the scaling difference, e.g. if the fact, that multiple incoherent factors influence the component, leads to an increased output value that is relative to each input value.

$$R_{asset} := \prod_{1 \leq i \leq n} (R_{asset\ risk\ factor_i}) \tag{8}$$

An example for the usage of the product aggregation when used in conjunction with lower-scale aggregation methods is the calculation of asset risk, based on its non-correlated risk factors impact and exposure:

$$Risk_{asset} := Impact_{asset} \times Exposure_{asset} \tag{9}$$

d) Minimum aggregation (redundancy)

The minimum aggregation should be used in environments where the component risk can be distributed among multiple redundant systems. This is generally true for fail-safe or load-balancing systems where multiple components are used to compensate for (temporary) protection criteria failures. In (10), the generalized risk *C* is aggregated using the minimum risk *R* of its *n* redundant components, mitigated by the number of components *m* that can fail simultaneously without disrupting the function of the overall system.

$$C := \min_{1 \leq i \leq n} (R_i) \times \frac{1}{1+m} \tag{10}$$

In the context of information security risk assessments, this is applicable for e.g. the risks of an IT system cluster based on the risks of its redundant IT systems (11). Depending on the cluster architecture concerning the preservation of the systems protection criteria, some protection criteria may not share this functional relationship, because the cluster technologies may allow e.g. differing subsystem configurations that allow targeted attacks on the confidentiality or integrity of exposed subsystems, which increases their exposure.

$$R_{cluster\ availability} := \min_{1 \leq i \leq n} (R_{subsystem\ availability_i}) \times \frac{1}{1+m} \tag{11}$$

Because most redundancy configurations itself may be prone to error, the proposed model assumes the simplified formula in (12) for estimation of redundant system components, in order to provide a risk-averse estimation.

$$R_{cluster\ availability} := \min_{1 \leq i \leq n} (R_{subsystem\ availability_i}) \tag{12}$$

Because these functions describe the behavior of concurrent risk factors of an asset as well as the behavior of risks between dependent assets, specifically tailored aggregation functions should be selected throughout the model to best express the contextually estimated behavior of risks.

In order to assist in the definition of weightings among system components, Delphi Analysis [4] or the Analytical Hierarchy Process (AHP) [10] can be used.

2.3.1.3 Usage of Functional Relationships

Based on risk assessment recommendations in [1; p. 54], previous research and evaluation of risk assessment methods and tools in [3], [45], and [55], the usage of functional relationships in the context of information security risk assessment is assumed practicable. Because the underlying risk assessment method and model can become subject of evaluation, if confronted with major incidents, the proposed model prioritizes the implementation of a highly transparent risk assessment model using functional relationships.

In [9], functional relationships are used to describe risk models solely based on measurements, which is assumed to be only feasible for the assessment of small systems, due to the effort needed to identify and gather respective measures. Therefore, the proposed model focuses on the incorporation of a small set of critical security measurements that are used to influence risk factors of a comprehensive risk model.

High level relationships based on IT-Grundschutz and generic aggregation functions (e.g. safeguard-threat-module) provide the basic estimation foundation. Functional relationships can be used immediately upon definition and require no further derivation of data.

2.3.2 Artificial Neural Networks

An Artificial Neural Network (ANN) is a system based on the operation of biological neural networks. ANNs are composed of artificial neurons or nodes, which are connected to each other in layers to represent the abstract model of a specific system. This approach is used when the system is too complex to be modeled or if there is not enough knowledge about the system. Neural networks are often used for solving artificial intelligence problems without creating a model of the real system at hand.
An artificial neural network is a weighted network of nodes with activation thresholds that trigger output functions which produce a specific output state. An example model is shown in Figure 14:

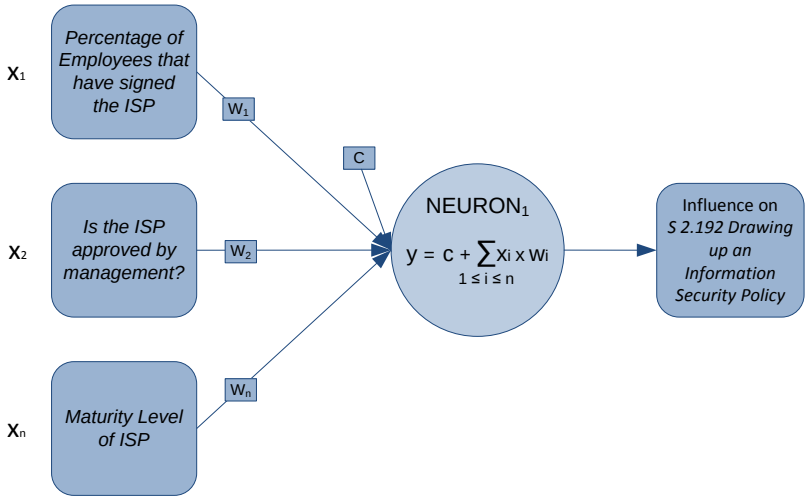


Figure 14: Simplified single-layer ANN model describing the relation between security measures and safeguard influence

The neuron has an activation function *y*, which calculates the output on a scale of [-1, +1]. The weighted connections w_i between the output of the nodes x_i and the constant *c* are activated (summed up) and define the quantitative effect of the related neuron. The abstract definition for a simple single-layer network (ANN consisting of a single neuron layer between input and output nodes) is shown in (13) [cp. 16; p. 33]:

$$y := c + \sum_{1 \le i \le n} x_i \times w_i \tag{13}$$

where *n* is the number of factors for neurons on this layer. In multilayer networks needed to express complex system component interactions, the output node *Y* can be used as an input node in different layers. The design of the topology has to be planned according to its purpose using one or more input-neurons, one or more different hidden layers with neurons and one or more output neurons as outlined in Figure 15.

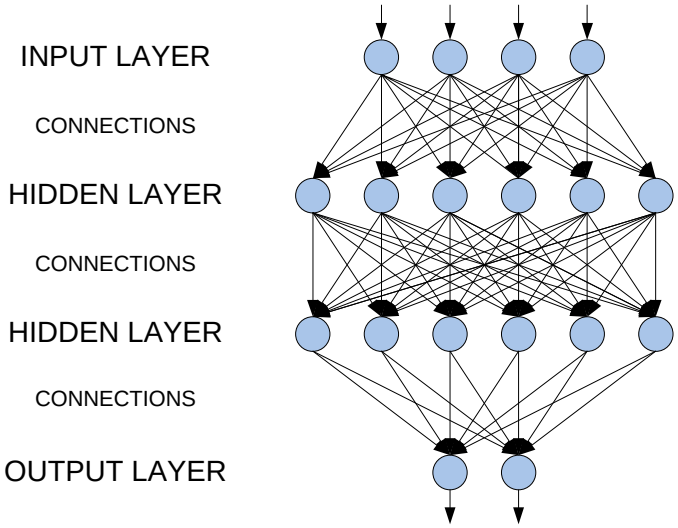


Figure 15: Multi-layer ANN topology using two hidden neuron layers

Small networks are usually Feed-Forward-Networks, meaning that the connection of nodes is only possible to the next layer neurons, but there are other topologies without this restriction available for use in more complex scenarios (Recurrent-Networks). The selection of the best topology is usually trial-and-error, but can be supported using back-propagation [14] and genetic algorithms [15].

The possible states of the output neurons are determined by their output-functions. Commonly used output-functions are visualized in Fig. 7.

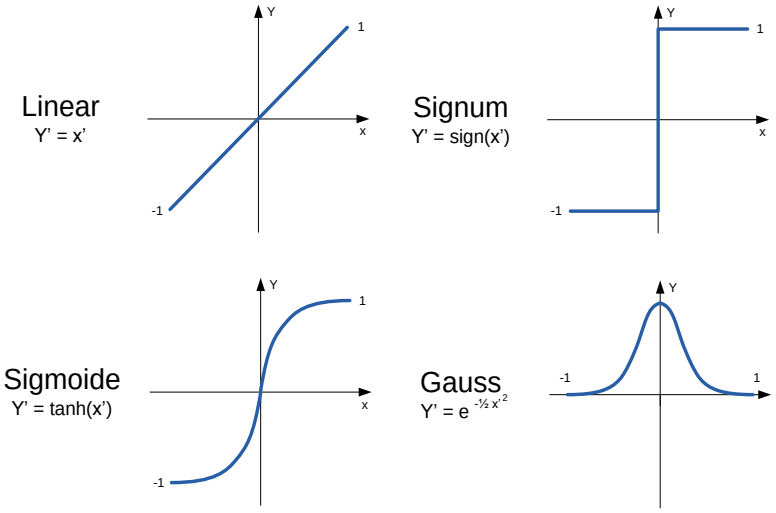


Figure 16: Sample ANN node output- functions

Once the basic topology is established, different learning algorithms are available to train the ANN. This is essentially done by creating a set of input values, calculating the ANN and deciding whether the output values show the desired correlation. If the ANN comes to a wrong conclusion, it can adapt its decision using various methods. Learning can be done by adapting the weightings of the node connections, adaption of node activation thresholds, adaption of the topology or by learning with genetic algorithms [16]. These methods can also be distinguished by being online or offline, meaning that learning takes place after every input (online) or only when all training steps are completed (offline).

This technique provides the benefit that the underlying function must not be known before learning can begin. At the same time, this has the drawback that the underlying function also cannot be derived, even after learning is finished. Because of the concept of ANNs, it cannot be retraced why inputs give certain outputs, because the information about the behavior of the network is coded into its topology, the weighting of its nodes, their activation thresholds and their output-functions.

2.3.2.1 Usage of Artificial Neural Networks

Artificial Neural Networks are easy to work with and results are – depending on the simplicity of the topology design - easy to interpret. Using ANNs to represent complex models as needed for the establishment of assets and asset dependency models is possible, but yields multiple problems.

ANNs need a lot of training and supervision in order to be correct, which leads to a delayed usability of the outcomes and a high workload for supervisors (unless other training algorithms are used). Additionally, a training effectiveness cannot be guaranteed and can lead to over-fitting for specific scenarios.

Using simple single-layer ANNs to represent the relation between measures and their respective safeguard influence (see Figure 13) seems to be more realistic approach, but yields the same scaling problems regarding training and supervision.

Based on these drawbacks and the fact that the actual aggregation function cannot be derived (black box model), the usage of ANNs for the proposed model is not reasonable.

2.3.3 Bayesian Belief Networks

Bayesian Belief Networks (BBNs) are probabilistic models that represent a set of variables (nodes) and their conditional dependencies using directed acyclic graphs (DAG).

BBNs are made of nodes which represent (usually Boolean) variables and arcs to connect with other nodes, representing a causal relationship between them. Each node has a Conditional Probability Table (CPT, or NPT for Node Probability Table) which defines the probability of the node having a specific state (true/false) in relation to the conditions of its affecting nodes states. The key feature of BBNs is that they enable its user to model and reason about uncertainty using a visual conception of the system.
Hybrid BBNs can make use of continuous node variables, allowing its user to approximately model variables with continuous values (e.g. 0 – infinity) using distribution functions instead of CPTs. However, since this approach substantially complicates the mathematical background of inference and learning, most implementations can only handle discrete variables, forcing the user to calculate with discretized variable sets. Highly sophisticated frameworks [40] use dynamic discretion to simulate continuous variables - e.g. 0-10, 11-20, 21-30, etc.), which leads to performance issues when dealing with larger models.

Figure 18 outlines a simplified example of the IT-Grundschutz module *1.0 Security Management* and some example measures *M1*, *M2* and *M3*. Because the proposed model is designed to estimate risk factors (*S1*, *T1*) rather than derive them completely from measures, the example includes estimation nodes (*E1*, *E2*) that are used to define the risk factors based on manual estimation. The measures are designed to influence the estimated nodes in a negative way (increasing risk), depending on their state (e.g. using thresholds as analytical models) and the defined CPTs.

When the actual state of one or more nodes is known, the BBN can calculate the probability of the state of the other nodes using the Bayes theorem (14).

The theorem defines how to calculate conditional probabilities for two nodes *A* and *B* with *P(B)* > 0:

$$P(A|B) = \frac{P(B|A) \times P(A)}{P(B)} \tag{14}$$

where *P(A)* is the a priori probability for *A* being true, *P(B|A)* is the probability of *B* being true under the condition that *A* is true and *P(B)* is the a priori probability for *B* being true. In addition to this inference algorithm, various efficient learning algorithms for topology- and probability-adaption are available [21].

The main advantage of BBNs lies in their inference types, which can also be mixed:

- Diagnostic: from effects to causes
- Causal: from causes to effects
- Inter-causal: between causes of a common effect

In the context of risk assessment and measure integration, only causal inference produces useful results, because there is no point in estimating e.g. the probability of a measure state based on estimated safeguard risk (diagnostic). Also, the inference between measures based on their common safeguard risk provides no useful insight

(inter-causal). Some forms of diagnostic and inter-causal inference may be used at a higher level of the risk assessment model (e.g. when integrated with Return-On-Security-Investment models).

Because a nodes CPT includes all possible state combinations of its immediate parents, the size of the table can become quite large when using multiple states as needed for the context of risk assessments (opposed to using Boolean states).

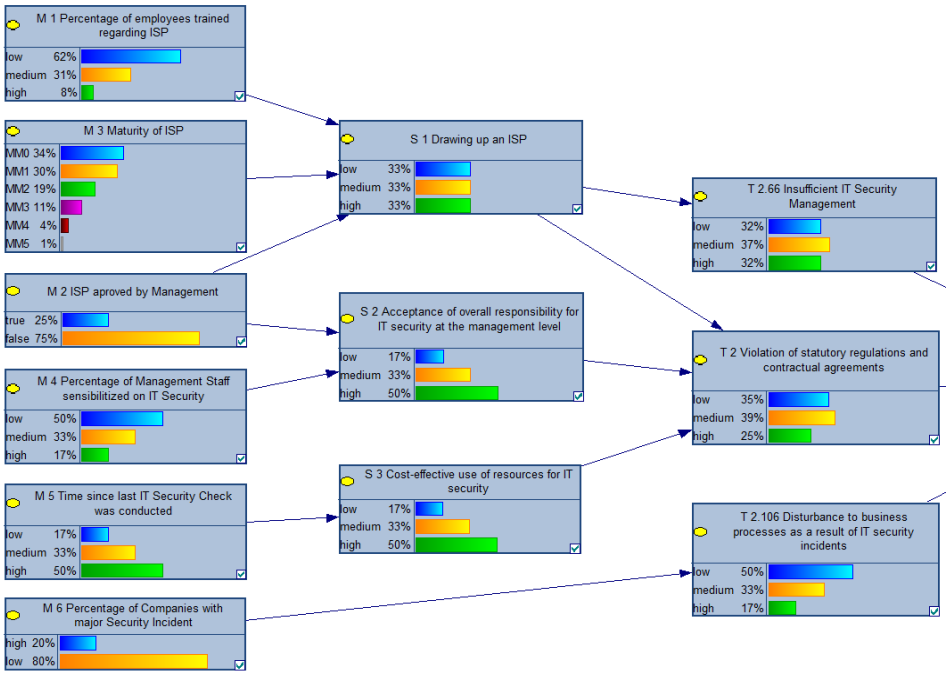


Figure 17: Example BBN subset of the IT-Grundschutz module *B 1.0 Security Management* using the GeNIe 2.0 tool

In [11; p. 6] the problem of conditional probability is approximated using linear regression, a common method to predict the outcome of a variable based on the information of other variables [12], [13; p. 239ff]. This principle could be used to generate CPT entries for a given node, incorporating the desired behavior as shown in Figure 19.

Based on IT-Grundschutz safeguard priorities and safeguard maturity gap, the basic linear risk function can be estimated. Using the safeguard priority, a maturity target and the subjective evaluation of safeguard maturity of the user, appropriate risk levels can be estimated. Negative measure influence can be represented by incorporating probabilistic variance into the CPT to increase the probability of elevated risk. The identification of influence of each measure, as well as their conditional influences can be derived by referencing their expressiveness (regarding safeguard influence) against each other using AHP.

The following example describes the principle based on the BBN subset shown in Figure 18.

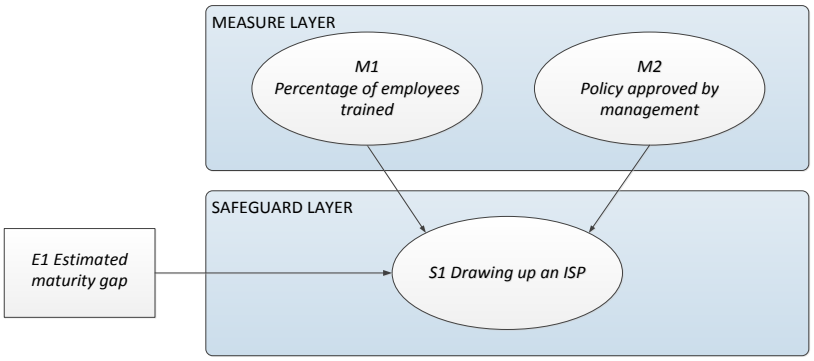
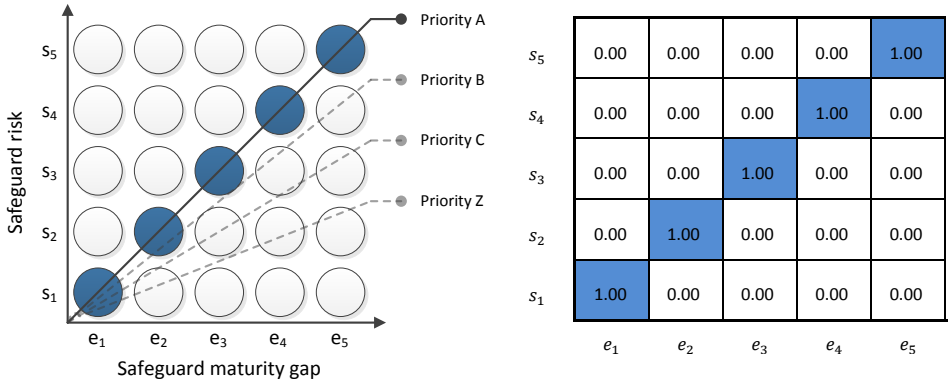


Figure 18: Simplified BBN subset

The safeguard risk level S_i is assumed to increase linear with the safeguard maturity gap e_i (example priority *A*), safeguards with lower priorities *B*, *C*, and *Z* respectively lead to lower risks. Other functions (e.g. sigmoid, trapezoidal), can be used to describe desired risk functions.



	e_1	e_2	e_3	e_4	e_5
s_5	0.00	0.00	0.00	0.00	1.00
s_4	0.00	0.00	0.00	1.00	0.00
s_3	0.00	0.00	1.00	0.00	0.00
s_2	0.00	1.00	0.00	0.00	0.00
s_1	1.00	0.00	0.00	0.00	0.00

Figure 19: CPT generation base layout

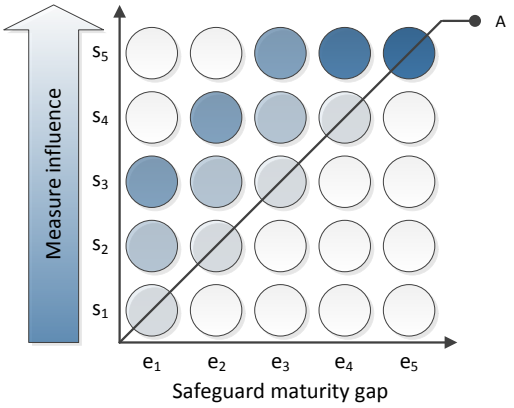
The measures *M1* and *M2* are secondarily used to provide negative influence on the maturity estimation (showing increased risk for *S1*).

Depending on the worst-case correlation of measures states, which in this example are a low level of trained employees with an unapproved policy, the estimated level of influence on *S1* can be estimated in the interval [0, 1]. The maximum influence level is used to describe a total safeguard failure, leading to maximum risk regardless of the subjectively estimated maturity gap. This level of influence should only be used if the available measures fully describe all aspects of the safeguard (e.g. including actuality/review cycle, clearness of scope, etc.).

In a next step, all other correlations between possible measure thresholds or states have to be estimated with an influence level relative to the previously defined maximum. If all required conditional influence levels are estimated, the probability masses of the CPT could be generated based on the schema shown in Figure 20. This approach has similarities to the Linear Conditional Probability Matrix Generator

(LCPMG) presented in [11], but differs in the way that probabilities showing decreased risk should not be included, in order to only provide risk-averse influence on the subjective risk estimation.

By distributing the probability masses upwards, estimated influence levels could be used to provide probabilistic variance in safeguard risk estimation as indicated by the colored transition in Figure 20.



	e_1	e_2	e_3	e_4	e_5
s_5	0.00	0.00	0.60	0.90	1.00
s_4	0.00	0.60	0.30	0.10	0.00
s_3	0.60	0.30	0.10	0.00	0.00
s_2	0.30	0.10	0.00	0.00	0.00
s_1	0.10	0.00	0.00	0.00	0.00

Figure 20: Example CPT-generation schema with approximated values for risk estimation using measurement influence in Bayesian Belief Networks

To minimize the effort for identifying conditional dependencies between risk factors, their aggregated maximum can be estimated using the noisy-OR model [17]. This allows to model causal independence[2], limiting the number of NPTs to be linear in *m*, as shown in Figure 21.

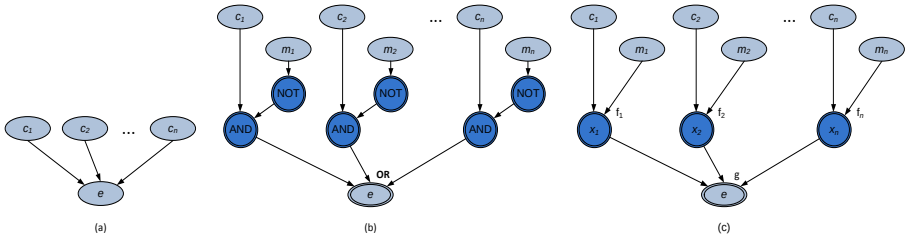


Figure 21: (a) BBN with multiple causes and a single effect (b) BBN with multiple causes with inhibitory interaction (c) BBN using the noisy-MAX operator [cp. 19; p. 827f]

[2] Causal independence is used in practice to simplify the problem of otherwise exponentially increasing NPTs, although it is known that in reality causes are never fully independent

In Figure 21, the nodes m_i represent inhibitory causal mechanisms (a special mechanism to inhibit the effect *e* of the cause c_i under specific circumstances) and the nodes with bold borders represent deterministic functions. Because the mechanisms are independent (hence the name causal independence or CI) in the noisy-OR model, its usage leads to a significant reduction in the number of probabilities required to quantify the cause-effect relationship.

A CI distribution reduces the number of assessments needed for any node from *n*m* of the unrestricted model to *m*, where *n* is the number of states of the parent nodes and *m* the number of states of the child node [cp. 18, p. 135]. It also speeds up inference substantially if there are many parent states.

Unfortunately, the noisy-OR model is primarily used to model causes that are sufficient to produce the effect in the absence of all other causes [18; p. 135] (no possibility to model correlations between measures) and can only handle causes with Boolean states by design [21; p.486f], which reduces its applicability in the context of risk assessment.

The extension to handle multi-valued variables, the noisy-MAX model, was introduced by [21; p. 486]. In noisy-MAX models, multi-valued variables influence the effect, and their combination is specified by the MAX-operator. In [21; p. 487], leak probabilities are introduced, to allow the definition of "incompleteness" of the BBN representation. In the proposed model, this could be used to explicitly assign the probability that the effect (e.g. safeguard risk) will occur in the absence of any of the modeled causes (security measurements).

The third widely used CI model is the noisy-AND, which uses the SUM function.
These different CI models could be used in the proposed model to represent different estimation functions. A BBN built using the noisy-OR or the noisy-MAX model is not a BBN per se, due to the presence of the AND-, OR-, NOT- or MAX-operators. The inference engine has to convert this network into a network it can handle, or the engine must be extended to handle the required operators directly.

Despite of the described problems, the noisy-OR and the noisy-MAX models are the primary applied CI distributions in many real-life applications [20], [22].

BBNs are applicable to the problem proposed, as likewise work has shown [11], [24], [25] and [26]. Applied to the proposed model using conditional independence, inhibitory nodes would be based on measurements, while the cause nodes would represent the subjective safeguard maturity evaluation, affecting the safeguard risk using the noisy-MAX operator. Further causal relationships representing threats, modules, assets and asset dependencies would need conditional probabilities to represent the desired risk assessment functionality.

The development of larger models based on conditional dependence is hindered mostly because of the vast number of CPTs to describe.

The scalability of the computational complexity may be adapted by using different inference algorithms. The most common exact[3] inference methods are variable elimi-

[3] Exact inference has a complexity that is exponential in the network's tree width

nation [28], clique tree propagation [29] and recursive conditioning [30]. The most common approximate inference algorithms are stochastic Markov Chain Monte Carlo simulation [31], mini-bucket elimination [32] and variation methods like the expectation-maximization algorithm [27].

2.3.3.1 Usage of Bayesian Belief Networks

When using a BBN in the context of proposed risk assessment framework, the results of reassessing probabilities are only meaningful for causal inference, because each parent node is a generalization of its child. For example, safeguards relate to a certain threat, whose likelihood becomes a generalization of the safeguard risks. Therefore, one of the main advantages and reasons for the use of BBNs is not fully utilizable using the proposed model.

Similar research done in the context of information security, regarding ontology based generation of BBNs [54], has come to the conclusion, that specific mathematical functions used to derive the CPTs cannot be provided by the ontology and have to be modeled externally.

Because the underlying functions have to be estimated (using functional relationships) to deduce CPTs (if not simplifying the problem using CI) and the usage of BBNs in the context of risk assessment is mainly limited to causal inference, the integration of BBNs into the proposed model is assumed to be valuable at a later stage, when real life risk assessment data is available to help deduce CPTs using linear regression, as outlined in [11].

2.3.4 Fuzzy Logic

The concept of Fuzzy Logic was introduced in 1965 in [35], [36], [37] and [38], to allow the modeling and calculation of vague terms and rules in order to apply a more human-like way of semantics.

Fuzzy logic differs from the classic set theory of Boolean algebra in allowing values to be more accurate than true and false. While Boolean logic allows only true or false, fuzzy logic allows intermediate values.

In mathematical terms, a value in classical set theory can be either a part of a set or not, while in fuzzy logic a single value can be part of multiple sets with multiple membership degrees (see Figure 23).

By definition, a fuzzy set is a membership function that defines the grade of membership of a value. The shape of the function should reflect human semantics in order to provide meaningful results.

As a result, vague linguistic terms like "*slow*", "*very high*", "*hot*", "*deep*", etc. can be described by fuzzy sets using membership functions. This first phase is called fuzzification. Inference uses a rule base to calculate fuzzy outputs, which are defuzzified into crisp values.

In the context of the proposed model, this approach allows a graphical representation of the analytical models and indicators used by security measures that can be related to risk factors using knowledge documented as expert rules. The expert rule set, describing relationships between measures and generalized risk factors using linguistic rules, can be easily understood and exchanged between organizations.

The three different phases and functional elements of fuzzy logic are outlined in Figure 22.

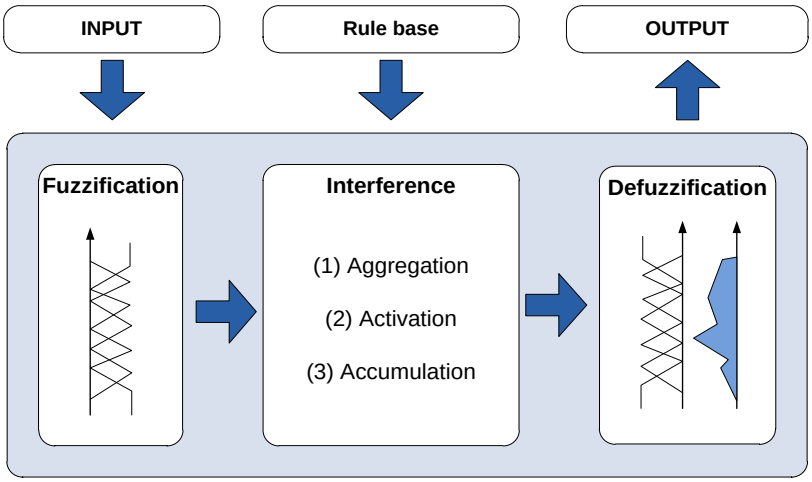


Figure 22: Structure and functional elements of fuzzy logic [cp. 39; p. 30]

2.3.4.1 Fuzzification

The definition of fuzzy sets is standardized in IEC 61131-7 [39], the Fuzzy Control Language (FCL) syntax specification.

The values of the input variables have to be converted into degrees of membership for the membership functions defined on the variable (see Figure 23).

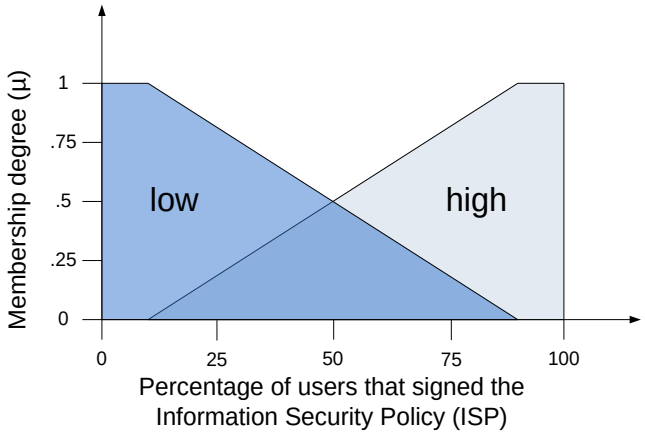


Figure 23: Simple fuzzy set to evaluate the fuzzy terms *low* and *high* for the fuzzy set *Percentage of users that signed the Information Security Policy (ISP)*

Piecewise linear membership functions are linear between the points defined, so the degree of membership is calculated from the crisp input value by the linear interpolation between the nearest function points. With this type of definition simple elements like ramps can be described. Other typical forms of membership functions include triangular, trapezoidal, gauss, generalized bell, sigmoidal and singleton (representing individual points). Also, rectangle functions can be used to describe classical set theory intervals.

2.3.4.2 Interference

This phase uses expert knowledge in form of multiple linguistic statements, called fuzzy rule (15). Empirical knowledge is documented as rules in the following form:

IF *condition* IS P_k THEN *conclusion* IS C_k (15)

In order to construct more complex rules, elementary operations like intersection (AND), union (OR) and complement (NOT) can be used to connect linguistic statements, enabling rules like:

IF *Months since last ISP revision* IS *high* AND *Percentage of users trained regarding the ISP* IS NOT *high* (16)
THEN (Negative influence on) *Drawing up an ISP* IS *High*

Because rules can incorporate multiple sub-conditions, specific attack vectors can be described explicitly by chaining multiple conditions using AND.

(1) Aggregation

Every rule is iterated and checked for the accomplishment of its conditions. If a condition consists of a single sub-condition, then the degree of accomplishment corresponds to this condition. However, if the condition consists of several sub-conditions, the total degree of the accomplishment a_k has to be determined by aggregation of the individual values a_{ki} (see Figure 24).

$$P_k = P_{k1} \text{ AND } P_{k2} \quad \text{OR} \quad (\text{NOT } P_{k3})$$

$$\underbrace{\underbrace{\text{Min}\{a_{k1}, a_{k2}\}}_{} \downarrow \underbrace{(1 - a_{k3})}_{}}_{}$$

$$a_k = \text{Max}[\text{Min}\{a_{k1}, a_{k2}\}, (1 - a_{k3})]$$

Figure 24: Principles of aggregation [cp. 39; p. 33]

In classical logic, these operators are defined using a traditional truth table, while fuzzy logic also allows all membership values in between (see Figure 25).

Classical logic				
x	y	x AND y	x OR y	NOT x
0	0	0	0	1
0	1	0	1	1
1	0	0	1	0
1	1	1	1	0

Fuzzy logic				
x	y	MIN (x, y)	MAX (x, y)	1 - x
0.2	0.6	0.2	0.6	0.8
0.5	0.1	0.1	0.5	0.5
0.9	0.3	0.3	0.9	0.1
0.7	0.7	0.7	0.7	0.3

Figure 25: Logical operators of classical and fuzzy logic

(2) Activation

If a rule is activated by accomplishing all conditions, then the degree of membership of the conclusion is determined on the basis of the degree of accomplishment of the aggregated conditions. For the context of risk assessment this is done using the minimum operator, in order to activate the conclusions only to the minimum of activated conditions.

The rule base can contain certainty functions or weighting factors, implemented by means of multiplication in the interval [0, 1]. The certainty function therefore reduces the membership degree of the conclusion and is expressed using the term "WITH" in a linguistic statement (17).

IF *Percentage of users that signed the ISP* IS *low*
THEN (Negative influence on) *Drawing up an ISP* IS *High* WITH 0.8 (17)

(3) Accumulation

If multiple rules activate, all conclusions are consolidated into an overall result using approximate reasoning. Usually, fuzzy logic uses the maximum operator (MAX) on all active conclusions to provide a balanced control system. In the context of risk assessment this should be done on the highest activated conclusion only, to estimate the worst case scenario. Otherwise, a higher activated conclusion for "low influence" could overrule a lower activated conclusion for "high influence" (see Figure 26).

The proposed model can circumvent this problem by using separate rule blocks to evaluate indicators (see Figure 26). Using this approach, the results are estimated separately for each rule block and can then be combined using the maximum operator (worst case estimation).

Because the correlation of indicators (using AND) can be used to describe significant higher estimations of influence, the influence levels should be designed to follow up on each other (see Figure 26).

2.3.4.3 Defuzzification

Interference supplies its accumulated membership functions as a geometric result. During defuzzification, the result is converted into a single crisp value using a defuzzification method. Commonly used methods are the Center of Area/Gravity, Center of Sums, Height and Left/Right Most Maximum [33], [39]. When using the approach outlined in Figure 26, the defuzzification method should return the value of the term at the Left-Most-Maximum (LM) [39; p. 12], in order to provide a worst-case influence. This allows an increasing level of estimated influence that is aligned with the membership function. Using this approach, measurement indicators can be easily mapped to their corresponding influence indicators.

The crisp output value of the defuzzification method serves as the output value of the fuzzy logic control program that is used to degrade the related risk factors of the risk model. If multiple rules providing multiple influences are activated, their conclusions are accumulated and defuzzified within separate rule blocks. If multiple influence estimations for a single risk factor exist, the maximum of all estimated influences is used.

2.3.4.4 Usage of Fuzzy Logic

This approach has the advantage that it provides a very easy way for end-users to define analytical models and indicators (membership functions, fuzzy terms) as well as expert knowledge on measure-risk factor relations in the form of expert rules. Unlike other disciplines like ANN or BBN, this approach does not require the definition of conditional dependence between measure influences, but allows the definition using chained sub-conditions. Because measures can be chained within rule conditions, correlating measures or attack vectors can be formulated using AND. This enables the definition of rules that are only activated if all measure sub-conditions show increased risk (e.g. IF *perimeter_1_breached* AND *perimeter_2_breached* THEN *perimeter_2_risk_factor_influence*).

The example in Figure 26 shows the inference and defuzzification of two rules. Depending on the interaction of measures, increasing influence levels (as well as rule weightings) can be assigned to adjust the desired estimated influence. Rules are estimated within separate rule blocks, in order to provide a worst-case-estimation of all activated rule influences using the Left-Most-Maximum (LM) operator.

The expert rules (containing knowledge regarding measure-risk factor relations) follow a formal, easily understandable syntax and can be easily exchanged between organizations, while sensitive information regarding measure indicators is documented separately using membership functions.

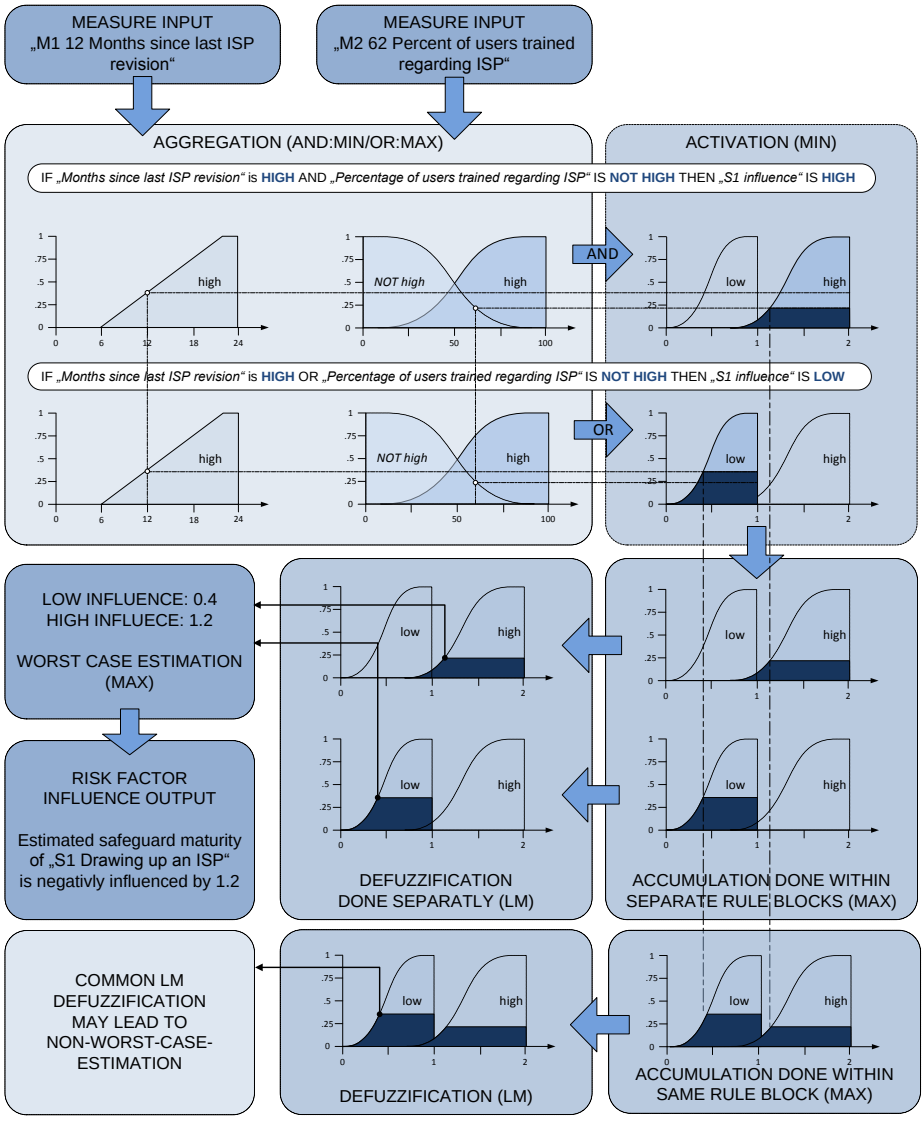


Figure 26: Example aggregation of two rules, activation, accumulation and defuzzification of safeguard influence.

3 Proposed integrated Model

In order to remain compliant with the risk assessment and management process defined by ISO/IEC 27005, the process is extended to visualize the integrated disciplines. The adjusted process in Figure 27 allows the continuous collection and interpretation of security measures, giving the organization a clearer sight on risk trends.

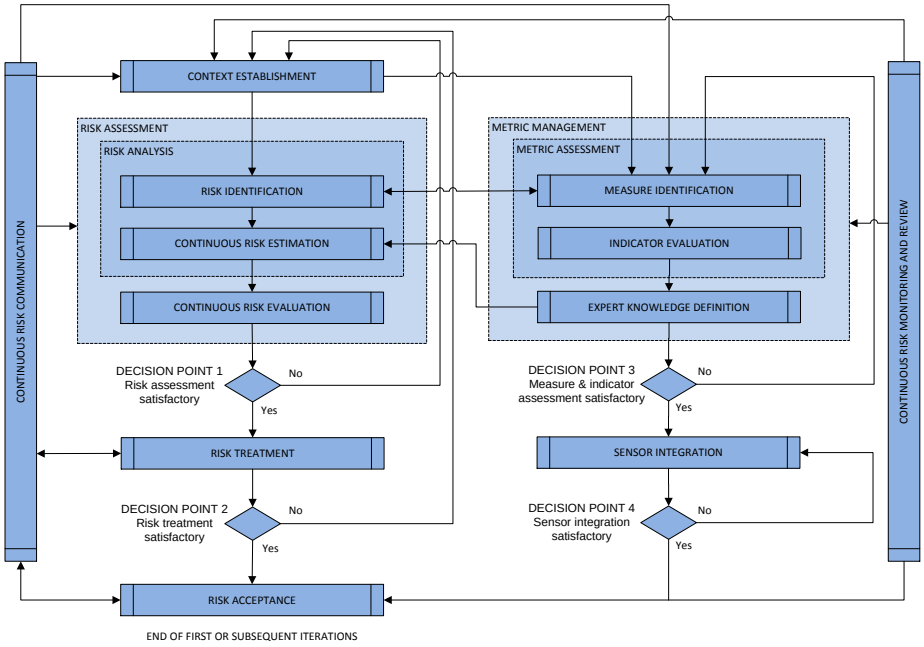


Figure 27: Extended risk management process for measurement integration, according to the requirements of ISO/IEC 27005 and ISO/IEC 27004

The proposed model uses the IT-Grundschutz-catalogs [5], -cross-references [2] and is compatible with all IT-Grundschutz standards [46-49]. Because the IT-Grundschutz methodology is not intended for risk assessment, the proposed model integrates a view on protection criteria (e.g. confidentiality, integrity, availability, etc.), defines a risk assessment framework and extends the method used for modeling dependencies between assets.

The information provided by IT-Grundschutz, along with its adaption to the organization specific environment (e.g. modification of risk factors, dependencies, etc.) is used to derive the exposure (potential residual attack vector) of each protection criterion at the asset level. In combination with estimated impacts on protection criteria, derived from a BIA of scenarios in which the assets are depending on each other, the proposed model is designed to estimate the risk associated with each asset within each scenario, as well as in total using multiple steps. A generalized risk estimation function is shown in (18).

$$Risk = Impact \times Exposure \tag{18}$$

The protection criteria impacts are identified using a BIA[4] and the exposure factor contains adjustable weightings for the module-, threat- and safeguard-layers and is used to estimate the potential attack vector that can be associated with the respective asset.

1. During **context establishment**, specific risk models are defined that cover the desired qualification and maturity of the organization, protection criteria to be examined, definition of residual risk- and exposure-levels, role-based assignment of personnel and the definition of assessment schedules to facilitate a continuous process.
2. **Risk identification** follows the IT-Grundschutz procedure to identify risks as defined in [47]. During risk identification, organizational assets are identified based on a structured approach (applications, IT systems, networks, rooms and buildings), and related to each other to represent dependencies between assets. If no IT-Grundschutz modules are available to represent the asset in question, threats and safeguards can be modeled according to [48]. Because the IT-Grundschutz asset structure is not designed for risk assessments, the modeling structure is extended and reversed to allow the definition of asset scenarios. Assets can be related to each other by establishing scenario trees that are used to assess the inheritance of risks as well as the inheritance of protection requirements to facilitate BIA.
3. **Risk estimation** allows the analysis of business impacts based on each scenario (providing impact estimations) as well as the estimation of safeguard maturities (providing safeguard and baseline threat estimation). Depending on the results of the BIA, the threats and cross-referenced, prioritized safeguards provided by IT-Grundschutz modules have to be extended to enable a detailed risk assessment as defined in [48]. During this assessment, modules covering assets with high or very high protection requirements have to be assessed for additional threats and the need for further safeguards that are not covered within IT-Grundschutz. This process is facilitated by the possibility to increase pre-defined safeguard priorities as well as baseline threat levels. The estimation of safeguard maturities is supported by the detailed safeguard descriptions and additional control questions of IT-Grundschutz as well as the implemented cross-references, which enables the user to estimate different safeguard maturities regarding different threats. Estimation of asset risks as well as risk inheritance within asset scenarios is ac-

[4] While BIA is usually focused on availability requirements, the estimation of e.g. integrity and confidentiality requirements can be performed likewise by estimating the business impacts that would result from their loss.

complished using functional relationships (see 2.3.1). This approach has been used because of its wide-established usage within information security assessment methods and tools and the associated acceptance. Therefore, organization-specific risk calculation and aggregation functions and associated scales can be integrated very easily.

4. **Risk assessment** is compatible with ISO/IEC 27005 and can be conducted following an iterative approach, increasing the analysis- (assets, scenarios) and assessment-depth (general or threat-specific evaluation of safeguard maturities) over time. The evaluation of risks is supported by the visualization of asset- and scenario- risks as well as multiple sensitivity analyses.

5. The **treatment of risks** is aligned with IT-Grundschutz safeguards and follows a risk based approach. Based on the established asset scenarios, threats and respective safeguard maturities and -targets, a safeguard sensitivity analysis is performed to estimate the safeguards with the highest impacts to the overall risk model. To provide a relative view on risks, the proposed model estimates all current risks as well as all maximum risks (assuming total safeguard immaturity), depending on the context. Both estimations are based on an energetic aggregation [cp. 65; p. 50], creating a strictly monotonically increasing function, which allows a risk-averse estimation of relative risk exposure. This relative risk exposure does not merely express the relative amount of implemented safeguards, but the estimated relative exposure based on the estimation of multiple independent risk sources.

6. **Risk acceptance**, facilitated by context establishment (qualification/maturity targets) has to be performed formally for all assets showing risk exposure. Threat-specific risks may be accepted by a suitable role (e.g. top management).

7. **Risk communication** is supported by the framework through integration of users into the assessment-, management- and reporting-process.

8. **Measure identification** can begin at any stage after context establishment (the usage of measures is not required by the framework) and is ideally combined with risk identification to help identify appropriate security attributes. The metric assessment and management process is compatible with ISO/IEC 27004 and allows the definition or selection of pre-defined base measures and derived measures. Base measures can be assigned to users/roles, responsible for measure assessment or to external sensors that can be implemented to provide the required data automatically.

9. **Indicator evaluation**: The proposed model uses fuzzy logic and fuzzy control to allow detailed evaluation and graphical representation of the inference framework between measurements and risk factors. This approach is assumed to be suited best to the proposed problem, because it provides visually manageable indicator terms, as well as an expert rule base that can be used to influence associated risk factors based on indicators or specifically chosen correlations of indica-

tors. Indicators and measurement results as required by ISO/IEC 27004 are provided through fuzzy logic as indicator terms, membership functions and expert rules. Indicator terms are used to evaluate organizational-specific targets for measurements using adjustable membership functions and should therefore be re-evaluated in continuous intervals.

10. **Expert knowledge** can be defined as formal expert rules to relate these indicators with their respective risk factors (safeguards, threats and impacts), enabling influence of the risk model based on continuously supplied security measurements. Whenever a measure is provided by a user or an automated sensor, the derived measures are calculated and the expert system re-estimates the influences on the risk model. Measures and related expert rules to affect the risk model can be integrated until the desired assessment depth and level of details is reached. Measures can also be used without inference to the risk model in order to provide a framework for the collection and reporting of security measures.
11. **Sensor integration**: To support the continuous measurement process, the framework enables the registration of sensors that can be used to integrate other applications or specific sensors for automated data collection. Because the framework proposed is based on a web-service-backend, any application or script that is able to perform a simple HTTP(S) request can be used to gather security relevant data (from e.g. intrusion detection systems, firewalls, domain controllers, project management applications, etc.). The integration of sensors is continued until the currently desired level of automation is reached. Any measures that are not provided automatically through sensors can be assigned to specific roles to manage manual data acquisition.
12. The integrated framework is used as a whole to achieve **continuous risk monitoring and review**, in order to provide input for subsequent iterations of the process.

The further content of this chapter is structured as follows:

- 3.1 describes the process steps outlined in Figure 27 in more detail,
- 3.2 explains the underlying security measurement framework in detail, and
- 3.3 illustrates the integrated knowledge management framework and expert system configuration requirements.

3.1 Proposed Risk Assessment Approach

The proposed risk assessment approach uses three separate abstraction layers to estimate risks. Risks are assessed as individual protection criteria risks (e.g. confidentiality, integrity, availability risks) as well as overall for each organizational asset within the model.

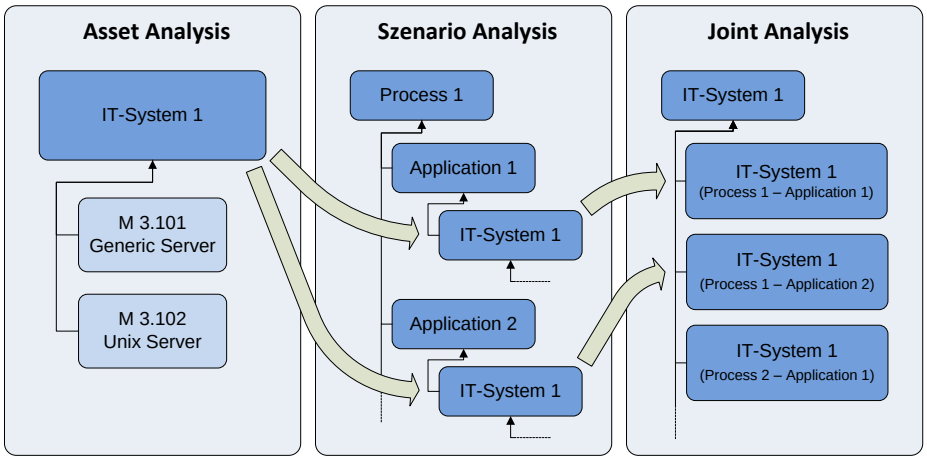


Figure 28: Separate assessment abstraction layers

The first layer provides organizational assets and their protection criteria based on IT-Grundschutz modules. If no IT-Grundschutz module is available for the asset in question, a detailed risk assessment according to [48] has to be performed. Multiple modules may be assigned to an asset to extend or specify its scope, e.g. the *Generic server* module provides generic server threats and safeguards, while the *Unix server* module extends those with Unix-specific risk factors.

The second layer allows the interrelation of those assets to assess risks using business impact analysis (BIA) and an extended fault-tree-analysis to incorporate their protection criteria dependencies amongst each other (e.g. IT system availability is dependent on the availability of the room and building it is located in, as well on organizational aspects).

The third layer provides an aggregated view of all assets, taking their different scenarios and dependencies into account. This allows a generalized view, as well as multiple scenario-specific views of any asset.

The proposed risk assessment process takes advantage of the IT-Grundschutz cross-references by allowing a threat-specific evaluation of a safeguard's maturities (e.g. a safeguard can be evaluated with different maturities against different threats scenarios), and by aiding the estimation of threat likelihoods, based on the aggregation of mitigating safeguard risks. This estimation is based on the number and importance of related immature safeguards for each threat, estimating a "baseline" threat likelihood (which can be in- or decreased depending on the organizational context) that can be minimized to zero when reaching the desired maturities.

Because the IT-Grundschutz framework does not (yet[5]) describe which protection criteria are targeted by a threat, a high-level evaluation has been carried out by a team of information security experts at SEC Consult.

Figure 29 shows a high-level overview on how information based on IT-Grundschutz cross-references and evaluated threat protection criteria influences is accumulated to estimate the amount of exposure for each of the module's protection criteria.

This exposure incorporates - amongst other factors - the safeguard maturity gaps, depending on the desired qualification target, as well as the related (and adjustable) baseline threat likelihoods (exposure ~ threat likelihood * safeguard maturity gap). Exposure is estimated for the asset and the underlying module layer, to provide an additional view that is separated from impacts. This allows viewing the level of exposures within the risk model without an interfering impact component (attack potential/compliance view). At the asset layer, the protection criteria exposures are multiplied with their respective protection criteria impacts (risk = impact * exposure) to provide the final risk estimation, as outlined in 2.1. This also substantially simplifies the generalized impact evaluation, as it has to be done only once for an asset's protection criterion loss, compared to all cross-references threats and safeguards that may be involved in that impact.

The estimation method is primary based on the assessment of safeguard maturities, incorporating the IT-Grundschutz catalogs and cross-references as well as protection criteria influence mappings. For the research prototype, these threat-protection criteria mappings have been established for the core criteria of information security (C, I, A).

Additional assessment variables are provided by weights influencing threats and their affected protection criteria as well as modules and assets and their inherited protection criteria (see Figure 42). The module-, threat- and safeguard types provided by IT-Grundschutz (see Figure 5) can also be used as anchor points to establish organization-specific weights.

[5] Some pre-releases of IT-Grundschutz modules (e.g. *MacOS X*) already contain detailed references regarding protection criteria.

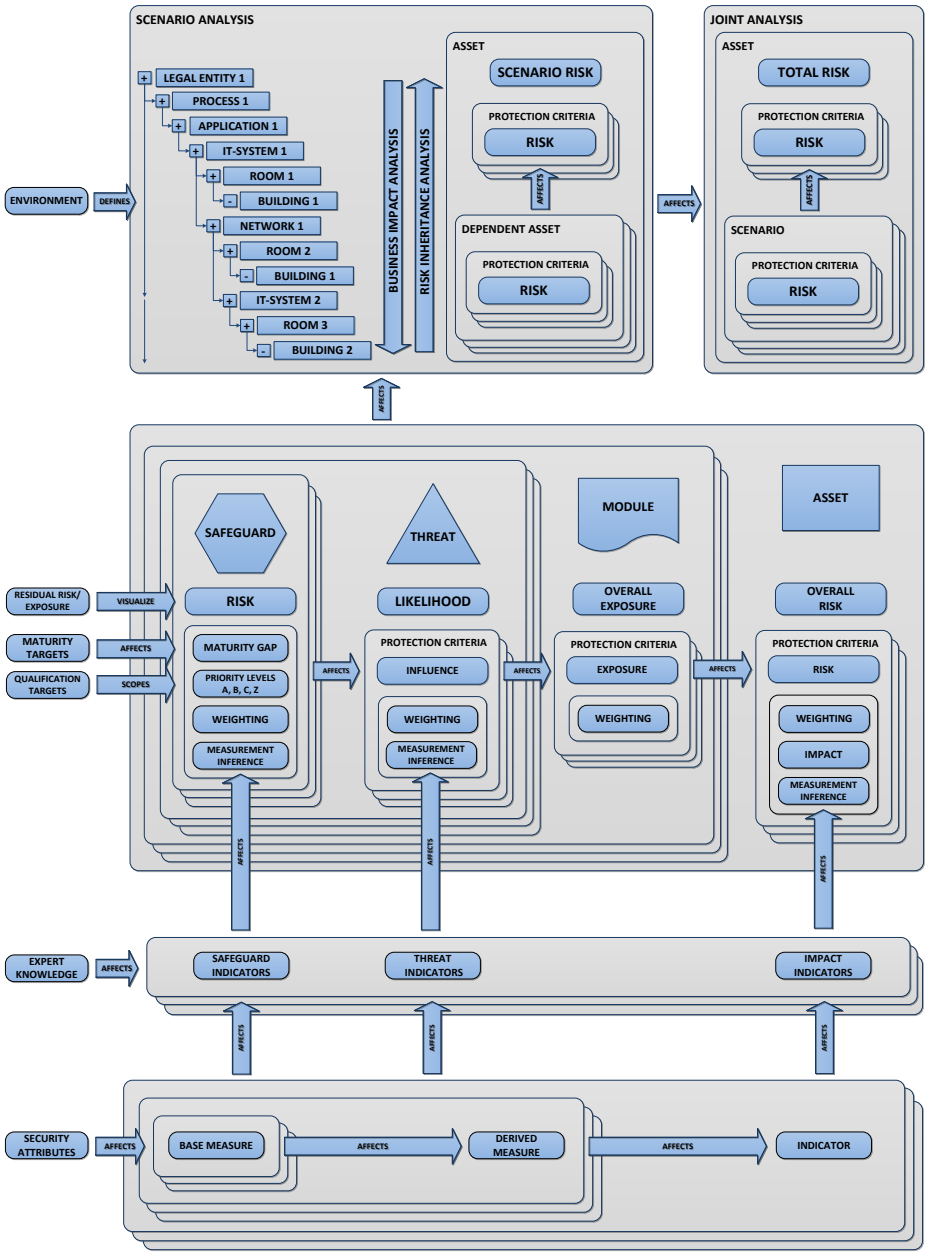


Figure 29: Overview of the proposed risk assessment-, expert knowledge- and security metric abstraction layers

The estimated safeguard risks lead to an increase in the likelihood of referenced threats, influencing several protection criteria. Those are aggregated at the module layer to provide a view on protection criteria exposures and overall exposure of the module. Multiple IT-Grundschutz modules can be assigned to an asset, which acts as another aggregation layer. At the asset layer, protection criteria have defined require-

ment (impact) levels, providing a view on protection criteria risks as well as an overall asset risk.

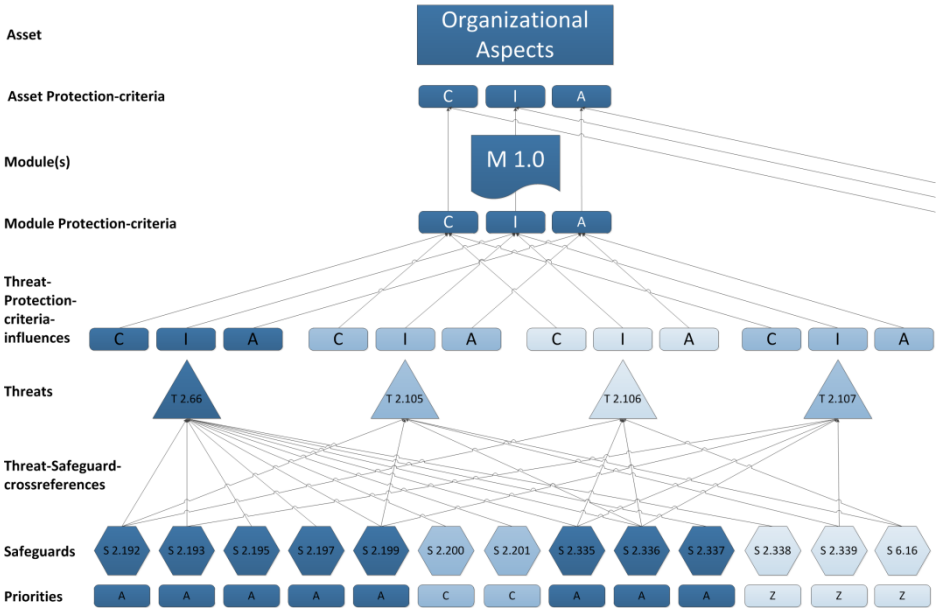


Figure 30: Asset analysis layer, based on IT-Grundschutz safeguards, threats and modules, extended with protection criteria exposures and assets that can be used as an additional aggregation layer.

The assessment variables can be adjusted to express different threat likelihoods and their influence on protection criteria, protection criteria exposures and protection criteria impacts. Additionally, safeguard maturities, threat likelihoods and impacts can be altered by an expert system built around safeguard-, threat- and impact-indicators that are monitoring security measures.

The second modeling layer establishes the relation between assets using scenario analysis, which is also used for BIA, providing protection criteria requirement (impact) levels for scenario assets. This dependency analysis is a great instrument for business continuity planning, which can be facilitated by the proposed model by e.g. using highly granular availability requirement levels for analysis. When designing the dependency model, the level of detail can be increased repeatedly over time, focusing on high risks while minimizing time and effort. This system-decomposition follows IT-Grundschutz best practices [48], but can be extended to model and assess detailed dependencies e.g. between IT systems and support applications, taking high-availability or load balancing aspects into account (see Figure 41).

As a last risk assessment abstraction layer, joint analysis provides a manageable way of estimating global asset risks based on the assets involvement in various scenarios. Because every asset is handled separately as a master and multiple slaves (scenarios), scenario assets can be adapted individually, allowing specific protection criteria-requirements or -exposures.

At the expert knowledge layer, influence indicators are defined and referenced with safeguard risks, threat protection criteria exposures or asset protection criteria im-

pacts, in order to establish correlations in the form of fuzzy rules between high-impact indicators and their appropriate risk factors.

The security metrics layer is used to provide organizational base- and derived metrics as well as metric indicators, describing "undesirable" states of the metrics using fuzzy terms.

Model Assumptions and Limitations

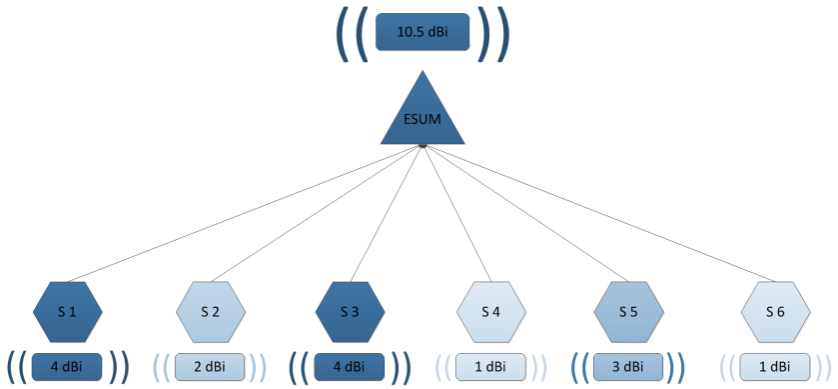
The proposed model is designed to estimate risks based on the residual attack vectors associated with organizational assets and their dependencies, using a role-based assessment approach.

In order to provide a cautious estimation of multiple parallel risks with overlapping aspects as provided by the IT-Grundschutz cross-references (see Figure 33), the proposed model suggests the usage of a function that not only increases with the level of vulnerability, but also with the number of parallel vulnerability sources[6]. A potential candidate for this is the energetic sum (19) [cp. 65; p. 50], which is used in physics to describe the resulting sound pressure level L_Σ from n incoherent radiating sources, emitting sounds with different pressure levels L_i.

$$L_\Sigma := 10 \times \log_{10}\left(\sum_{1 \le i \le n} 10^{\frac{L_i}{10}}\right) \tag{19}$$

Although this aggregation method has not yet been used for the estimation of risks by the scientific community, it has been successfully used by SEC Consult for over 10 years to estimate the total IT system risks based on multiple vulnerabilities identified during penetration tests. An example is shown in Figure 31.

[6] Within existing tools (e.g. OCTAVE, CRAMM, etc.), multiple threats are usually aggregated using the maximum operator as a worst-case-estimation. This, however, does not reflect the potential attack surface of multiple vulnerabilities in a risk-averse manner.



$$\mathrm{ESUM} = 10 \times \log_{10}\left(10^{\frac{S_1}{10}} + 10^{\frac{S_2}{10}} + \cdots + 10^{\frac{S_n}{10}}\right)$$

$$\mathrm{ESUM} = 10 \times \log_{10}\left(10^{\frac{4}{10}} + 10^{\frac{2}{10}} + 10^{\frac{4}{10}} + 10^{\frac{1}{10}} + 10^{\frac{3}{10}} + 10^{\frac{1}{10}}\right) = 10.5$$

Figure 31: Energetic sum example of multiple incoherent radiating sources with different sound pressure levels.

Applied to the proposed model, the energetic sum is used as outlined in Figure 31 to estimate the collective exposures of multiple risk factors, where a potential threat source has multiple parallel attack vectors.

The safeguard priority scale, in the interval of [1, 4], is assigned because the energetic sum provides an increase of ~3 for the first equal additional sound pressure source, decreasing to ~0.4 for the tenth equally high source (see Figure 32).

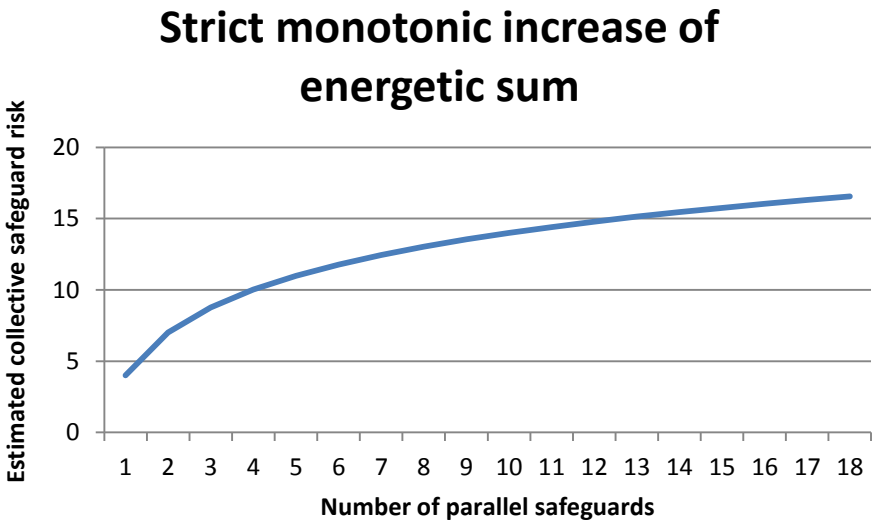


Figure 32: Energetic function based on an increasing number of parallel, maximum-priority safeguards

After some experimental calculations using the pre-defined cross-references provided by IT-Grundschutz, this scaling produced the most reasonable results to compare module complexity/exposure. In order to e.g. put more focus on safeguard priorities, the scale can be adapted for the risk model. Safeguard risks and respective maxima are calculated based on the illustrated example outlined in 4.2.1.1.

The proposed model requires organization-specific extensions to the predefined IT-Grundschutz modules to be comparable regarding their complexity/exposure. This can be achieved by either modeling extensions with the same level of detail, or by appropriately weighting extended threat- and/or module protection criteria to align them with similar components.

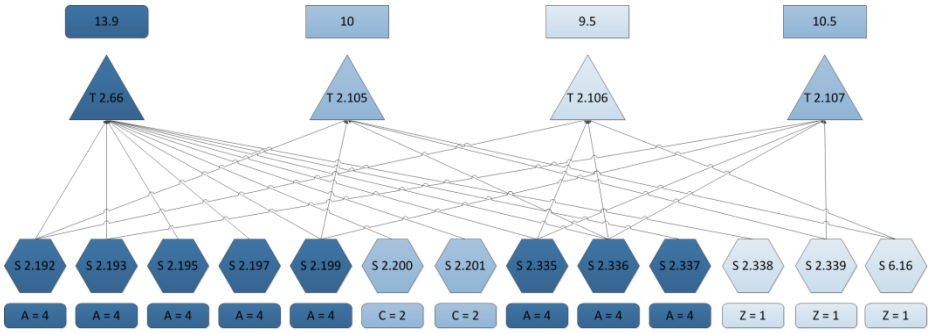
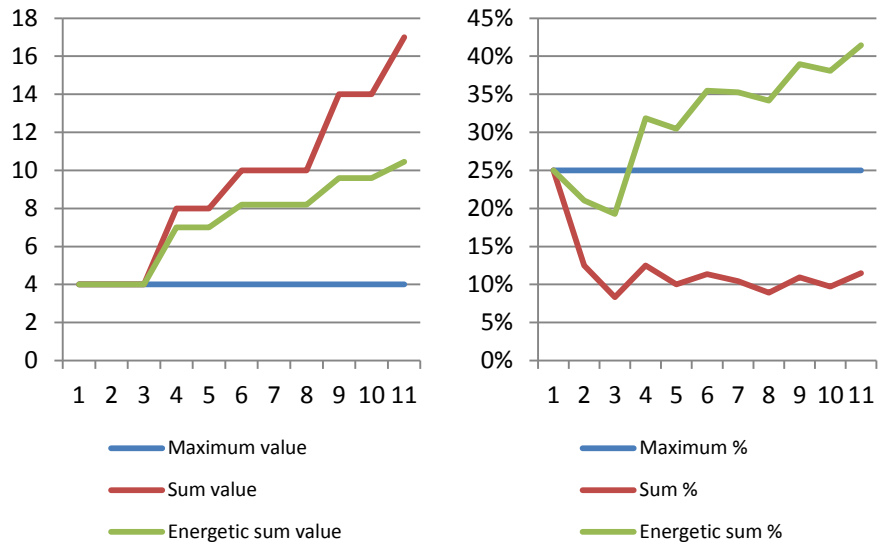


Figure 33: Simplified example of the energetic sum estimation for threats, using multiple safeguards with different priority levels, based on the IT-Grundschutz module “M 1.0 Security Management” in Figure 6.

In comparison to other functions usually used in the context of information security risk assessment (outlined in 2.3.1.2), the energetic sum has the advantage of taking the number of sources and their respective exposures into account, providing a risk-averse view of the residual attack vector.

In order for a threat to succeed, only a single of its vulnerabilities/safeguards needs to be exposed. However, in order to provide a risk-averse estimation as well as early-warning capabilities, the level and amount of exposed vulnerabilities should be taken into account. Opposed to the weakest link (maximum), the energetic sum provides an exposure estimation that increases with the number of potential attack vectors. In practice, aggregating risks based on the maximum operator (weakest link) usually has the disadvantage, that solely the weakest link is considered, neglecting other potential risk sources. Aggregation of risks based on the sum creates an increase that is directly proportional to the level and amount of attack vectors, which leads to a lowered estimation of single vulnerabilities. In reality, the amount of resources provided to treat risks usually does not increase proportionally with the number of potential vulnerabilities, but more in relation with the function shown in Figure 32.



	Safeguards			Maximum			Sum			Energetic sum		
	Risk	Max.	%	Value	Max.	%	Value	Max.	%	Value	Max.	%
S 2.192	4	16	25%	4	16	25%	4	16	25%	4.0	16.0	25%
S 2.193	0	16	0%	4	16	25%	4	32	13%	4.0	19.0	21%
S 2.195	0	16	0%	4	16	25%	4	48	8%	4.0	20.8	19%
S 2.197	4	16	25%	4	16	25%	8	64	13%	7.0	22.0	32%
S 2.199	0	16	0%	4	16	25%	8	80	10%	7.0	23.0	30%
S 2.200	2	8	25%	4	16	25%	10	88	11%	8.2	23.1	35%
S 2.201	0	8	0%	4	16	25%	10	96	10%	8.2	23.3	35%
S 2.335	0	16	0%	4	16	25%	10	112	9%	8.2	24.0	34%
S 2.336	4	16	25%	4	16	25%	14	128	11%	9.6	24.6	39%
S 2.337	0	16	0%	4	16	25%	14	144	10%	9.6	25.2	38%
S 2.338	3	4	75%	4	16	25%	17	148	11%	10.5	25.2	41%

Figure 34: Comparison of maximum, sum and energetic sum operators for estimation of total absolute and relative exposures, arising from an increasing number of immature safeguards

The charts in Figure 34 show the results of threat estimation based on maximum, sum and energetic sum, with an increasing number of safeguard risks *n* mitigating *T 2.66* in Figure 33. With every line in Figure 34, an additional safeguard with a respective current- and maximum risk is simulated and the absolute and relative collective risk estimation trend is given.

The left chart in Figure 34 shows a higher absolute value using the sum, which, however, can be compensated by normalizing each value with its potential maximum. When estimating the relative attack vector (%) shown in the right chart, the energetic sum shows a greater impact and is therefore more risk-averse. Because the energetic sum provides a strict monotonic increase as shown in Figure 32, opposed to the directly proportional increase provided by the sum, initial residual exposures create relatively higher estimations than subsequent ones.

While the maximum estimation offers the least insight into changes of the underlying factors, the usage of the sum operator provides more insight to the absolute risk but is only applicable if non-overlapping aspects are modeled. When compared to the estimation of relative risk, the energetic sum provides the most risk-averse increase in risk exposure if overlapping aspects (multiple safeguards/vulnerabilities affecting the same threat) are modeled. Risk exposure should be interpreted as the residual attack vector that results from gaps to the requirements defined within context establishment.

The energetic sum is used within the proposed model to estimate multiple parallel risk vectors where

- only a single vulnerability (immature safeguard) may exists in order for a threat to succeed (aggregation of threat exposure),
- only a single threat may succeed in order for a protection criterion to fail (aggregation of threat-, module- and asset protection criterion exposure), and
- only a single asset's protection criterion may fail in order for a dependent asset protection criterion to fail.

Because exposures are estimated using an energetic function in order to provide a cautious view on multiple parallel risks, the maximum exposures that are estimated for the risk model are dynamically dependent on the current

- desired level of detail used to perform risk analysis for each asset
- adjustments to the risk factor weightings to reflect the organizational context
- desired analysis depth used for the establishment of asset dependencies within scenario analysis
- desired functions used for the estimation of total asset exposure based on each scenario exposure

In order to provide a strategic alignment of exposure and impact scales, the current maximum exposure estimated for the risk model is used to normalize exposures to the desired scale-ratio between the impact- and exposure-factor used for risk estimation (see 3.1.1.3).

The risk factor framework provided by IT-Grundschutz is harmonized, meaning that modules are comparable regarding their threats and cross-referenced safeguards. Therefore, if modules are newly defined or extended, their resulting exposure should be related to those of pre-established modules, in order to compensate for different levels of detail when designing modules. This can be achieved using a variety of weighting variables, as shown in Figure 29.

The established risk model is self-contained, meaning that effects not expressed within the model are assumed to be negligible. As a result of this, as soon as all safeguards within the cross-references modules are estimated to be as effective as required by target definition, the modules show no residual exposures, hence no risks. However, residual likelihoods that remain, even with all targets reached, could be incorporated into the model easily using multiple levels of detail. This could be established by e.g. estimating the remaining likelihoods of each identified threat globally (once per risk model), specifically for each module's threat-reference (once per threat definition within each module), or highly detailed for each module-threat-reference (once per threat-safeguard reference within each module).

Due to the high level of detail of the IT-Grundschutz risk factor framework and the ability to relativize exposures between modules when using an energetic aggregation function, the current risk is shown both as an absolute value as well as relative to the potential maximum.

This adds the usability of showing absolute risks (the higher, the more complex the system) as well as relative risks equally (the higher, the more ineffective the required safeguards), supporting the identification of compliance issues and hence, the fulfillment of due diligence requirements.

In addition, the maximum exposure can be used to compare risk models regarding the level of detail and assessment depth incorporated into each model. This can be done by comparing

- the usage of modules and their respective maximum exposures, which increase strictly monotonically (due to the energetic sum) with the level of threat and safeguard assessment depth and detail (the more threats and safeguards defined and cross-referenced, the higher the maximum exposure)
- the root asset node(s) protection criteria exposures of the scenario tree, which increase strictly monotonically (due to the energetic sum) with the level of scenario/dependency assessment depth and detail (the higher the number of dependently modeled assets, the higher the inherited maximum exposures)

The dependencies between assets and the aggregation functions used to approximate the real-world behavior of risk-inheritance between dependent assets must reflect the characteristics of the modeled environment. In order to allow the selection of specific system behavior (e.g. identical components, redundancies, independent aspects), several aggregation functions besides the energetic sum have been incorporated as outlined in 2.3.1.2.

The integrated security measurement framework requires security metric indicators to be evaluated consistently with the maturity targets defined for the risk model, in order to correctly align measurement- and risk factor-indicators. The correctness of automatically gathered measurements can only be assured if sensors and related schema evolution is performed timely and accurately.

The definition of expert knowledge, used to integrate measure indicators with risk factor indicators, must reflect the real-world correlation between measurements and abstract risks.

During development of the prototype, the English version of the IT-Grundschutz catalogues has not been fully up to date, missing module-, threat- and safeguard definitions since 2005. Also, extensive evaluation has been done by the Austrian Federal Ministry of Defense, so the prototype's interfaces as well as the texts of the integrated IT-Grundschutz catalogues are based on the German language.

The English texts shown in examples throughout this thesis have been translated by the author.

3.1.1 Context Establishment

The following variables can be defined for specific risk models that can be created and adjusted dynamically over time.

3.1.1.1 Target Qualification

The target qualification defines the currently desired level of trustworthiness and can be specified globally or specifically for module-, threat- and safeguard-types outlined in Figure 5. The appropriate safeguards can be filtered based on the available IT-Grundschutz cross-references with threats and modules.

Qualification levels are aligned with the IT-Grundschutz priority/certification levels A, B, C, Z (see Figure 35) and define the scope of safeguards that are considered for implementation. Safeguards having higher qualification levels than the currently selected level are neglected during risk assessment, enabling a managed, iterative implementation approach. The values describing the desired qualification target in the interval [1,4] are reversed, in order to express the increase of risks that would result from a safeguard's immaturity at that level (an entry level safeguard renders higher risks if immature than a e.g. certification level safeguard).

It is assumed that a Z-level qualification target extends the trustworthiness of an ISO/IEC 27001 certification based on IT-Grundschutz (C-level), because they further increase the assessment scope. In order to support a quick-start approach, safeguards have to be evaluated initially before they are included within risk estimation, so if Z-level safeguards are provided within the risk assessment environment, they can be included, re-prioritized or marked "non-applicable" for the organizational environment during initial assessment. The inclusion of Z-level safeguards provides visualization of risks that go beyond certification requirements and are therefore marked as having the lowest impact value, compared to certification-relevant safeguard levels (see Figure 35).

Although IT-Grundschutz Z-level safeguards are basically not considered to be required in order to achieve a certification, the officially released mapping between ISO27001/27002 and IT-Grundschutz in [57] does reference Z-level IT-Grundschutz safeguards, indicating their inclusion within the scope of a risk-based assessment.

Qualification level	Safeguard scope	Number of safeguards	Value	Trustworthiness
Entry level	A	~ 600	4	Low
Higher level	A, B	~ 800	3	Medium
Certification level	A, B, C	~ 1000	2	High
Additional level	A, B, C, Z	~ 1200	1	Very high

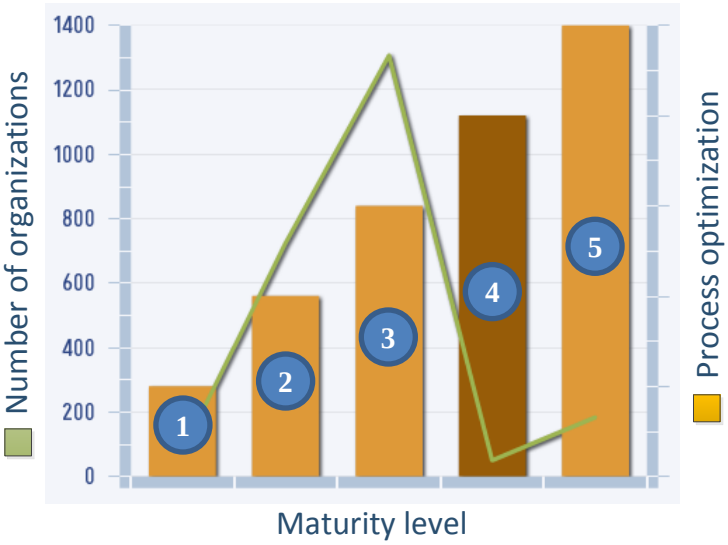
Figure 35: Assumed relationship between certification level (qualification target), scope (of IT-Grundschutz safeguards) and trustworthiness

3.1.1.2 Target Maturity

The target maturity level defines the target level of safeguard-process optimization and is aligned with the standard levels of the Capability Maturity Model.

The subjective estimation of safeguard maturities is aided by offering extensive information on IT-Grundschutz safeguard descriptions, additional control questions, as well as the reference of related threats to mitigate. The proposed model is designed to estimate risks based on underlying safeguard immaturities, resulting from a gap to the specified target level. Safeguards evaluated with the same or higher maturity levels than required are neglected during risk assessment, resulting in a risk assessment with zero risks when reaching all currently defined targets.

Again, to support a more granular specification, the target maturity can be defined for safeguards globally or specifically for module-, threat- and safeguard types (see Figure 5). The selection of the target maturity level is facilitated by alignment in the context of other organizations. This data is derived from the results of the CMMI Appraisals research reports [56], which outline the number of organizations aligned with specific CMM levels.



Maturity level	Description	Value	Number of compliant org.
Not identified	Need for processes not identified	0	-
Initial	Processes unpredictable, poorly controlled and reactive	1	80
Managed	Processes characterized for projects and is often reactive	2	726
Defined	Processes characterized for the organization and is proactive, tailored from org. standards	3	1306
Quantitatively Managed	Processes measured and controlled	4	51
Optimizing	Focus on process improvement	5	184

Figure 36: Assumed relationship between maturity level and process optimization, enriched using empirical data [56] on the maturity level distribution of organizations

3.1.1.3 Examined Protection Criteria and Evaluation Levels

The user can select the protection criteria to be examined from a pre-defined pool (confidentiality, integrity and availability), or he can extend and modify the available criteria. These relationships are accomplished by relating protection criteria to those threats that can potentially influence the respective criteria. The pre-defined relations have been defined by a team of information security experts in cooperation with SEC Consult.

For each protection criterion to be assessed within the risk model, organization-specific evaluation criteria have to be defined to help estimate protection criteria requirements and associated impacts. Users can define and value specific requirement levels, based on the estimated impact associated with their loss.

The scale on which a protection criterion requirement level is defined needs to be adapted to the level of detail of the asset assessment and the depth of the scenario analysis, because otherwise (e.g. in case of very comprehensive asset models or/and very deep scenario structures) the allocated exposure levels could dominate the calculation of the respective risk ($Risk = Impact \times Exposure$).

Without this corrective measure, the exposure level of e.g. 10 with a disastrous impact of 5 renders risk completely insignificant in relation to the risk of an asset with an exposure level of e.g. 80 and a minimal impact of 1. By adapting the scale of the impact levels corresponding to the exposure levels aggregated at the root of the scenario trees, this shift towards exposure can be evened out.

This adjustment provides a single point of control for the overall weighting of the impact and exposure factors, involved in the estimation of risks. In order to provide an even weighting of the factors involved in risk estimation by default, the maximum impact level is aligned with the maximum exposure aggregated at the root of the scenario trees.

The proposed method weighs the impact- and exposure-factor equally by default, using scales of [0, 10] to facilitate an easily comprehensible risk scale of [0, 100].

- Balanced (default): Impact (1) / Exposure (1)

  $Impact \in [0, 10], Exposure \in [0, 10] \rightarrow Risk \in [0, 100]$

- Impact dominant: e.g. Impact (1.6) / Exposure (0.625)

  $Impact \in [0, 16], Exposure \in [0, 6.25] \rightarrow Risk \in [0, 100]$

- Exposure dominant: e.g. Impact (0.5) / Exposure (2)

  $Impact \in [0, 5], Exposure \in [0, 20] \rightarrow Risk \in [0, 100]$

The impact and exposures are dynamically normalized to provide the bias desired by the risk manager. The example below shows three sets of protection criteria with multiple requirements levels, estimated on a user-defined scale of [0, 40], that is dynamically normalized to fit the balanced default weighting.

Because the proposed model uses distinct risk factor layers to aggregate current and maximum values (see Figure 29), each layer's respective maxima are used to provide an adapted normalization weight for the layer (e.g. the maximum protection criterion exposure of the root asset(s) of the risk model may be 100, while the maximum risk of a single safeguard may be only 20). This method has already proven useful in [67] when working with IT-Grundschutz.

The methodology for impact evaluation is aligned with the procedure of IT-Grundschutz [47], which suggests the identification of the following aspects:

- Violation of statutory law, regulations or contractual obligations
- Impairment of informational self-determination
- Impairment of physical integrity
- Impairment of task fulfillment
- Negative repudiation
- Financial impact

Protection criteria	Requirement level	User defined value	Normalized value (balanced)
Confidentiality	Public	0	0
	Internal	10	2.5
	Confidential	25	6.25
	Strictly Confidential	40	10
Integrity	Negligible	0	0
	Low	10	2.5
	Medium	25	6.25
	High	40	10
Availability	Negligible	0	0
	< 2 weeks	10	2.5
	< 1 week	20	5
	< 1 day	30	7.5
	< 1 hour	40	10

Figure 37: Selection of protection criteria and definition of organization-specific evaluation levels, normalized to the desired bias between impact and exposure.

3.1.1.4 Residual Exposure and Risk Levels

To provide more insight into the current state of risk treatment, the proposed model estimates all current risks and exposures as well as their respective maximum values, based on the maturity of safeguards and the respective qualification- and maturity-targets to provide a context-aware visualization of risks.

This information is derived from the continuous estimation of current and potential maximum risks and exposures, resulting from the underlying risk factor model. Because the estimation uses an energetic function to estimate current and maximum values, the increase of relative residual levels is not linear (see Figure 34), allowing a cautious view on the resulting attack vector (risk increases not only based on the maximum of its influencing factors, but also based on the amount of parallel sources).

The residual risk and exposure levels help to visualize the relative level of residual risk and exposure from untreated risks (depicting the residual attack vector) and can be user-defined.

As an example, a linear distribution of five levels is used to describe the residual exposure levels as shown in Figure 38. The residual risk levels, outlining the relative amount of risk associated with an asset in comparison with the maximum risk possible due to the context, are assumed as a non-linear distribution of four levels as shown in Figure 39.

Residual exposure level	Relative range in percentage
Low	0…20
Medium	21…40
High	41…60
Very high	61…80
Catastrophic	81…100

Figure 38: Definition of residual exposure levels to support a context-aware visualization of residual attack vectors, resulting from immature safeguards.

Residual risk level	Relative range in percentage
Low	0…30
Medium	31…50
High	51…70
Very high	71…100

Figure 39: Definition of residual risk levels to support a context-aware visualization of residual risks, resulting from asset exposure and impact.

3.1.1.5 Communication Establishment

Because IT-Grundschutz provides a generic set of ~60 IT-Grundschutz roles that are related to the IT-Grundschutz safeguards (responsible for planning/implementation), the establishment of risk communication can be facilitated by assigning those roles to the respective organizational personnel.

A system user can be registered for every user involved in the integrated assessment and management process. Depending on the involvement of the user, different authorization levels can be assigned:

a. Risk Managers can create, read, update and destroy all objects
b. Auditors can read all objects
c. IT-Grundschutz Managers can create, read, update and destroy all IT-Grundschutz objects (separate role to enable detailed risk assessments)
d. Agents can read objects and can create safeguard maturity evaluations and measure assessments (can be assigned to roles/individual users) in their realm of responsibility

Using this approach, as soon as the assets are identified, the agent users are automatically provided with the list of assets, threats and safeguards in their realm as well as all other relevant information available to support the evaluation.

3.1.1.6 Assessment Schedule

To support a continuous process, assessment schedules can be defined globally or specifically for module-, threat- and safeguard-types (scopes identical to types in Figure 5). As soon as a previous assessment is outdated, the system informs the respective users by email about the requirement for reassessment.

3.1.2 Risk Assessment

3.1.2.1 Risk Identification

The identification of risks is aligned with the structure analysis defined within IT-Grundschutz [47, p.37], which analyses the organizational structure using a top-down-approach. Starting with the identification of applications, related information and dependencies between assets that are required to perform business processes, the method examines related IT systems, networks and infrastructural components (rooms, buildings) based on network diagrams.

IT-Grundschutz uses this information to define a model as shown in Figure 7, which is used for documentation purposes and to help derive protection requirements.

The proposed approach extends this approach by allowing the definition of further components types (business processes, organizational entities, asset groups, etc.) that can be used to model more complex environments and enables the definition of dependency structures for scenarios that can be used for risk assessment.

Once the assets are identified, appropriate IT-Grundschutz modules have to be assigned to represent the risk factors associated with each asset. If no applicable IT-Grundschutz module can be identified, the representing module has to be created, following the process for risk analysis used by IT-Grundschutz [48]. This basically covers the selection/creation of specific threats and safeguards, the prioritization of those safeguards as well as the cross-referencing of safeguards and related threats.

Starting at the desired high level asset, the user can model any relations to assets that are required for its function. This allows an iterative risk assessment approach, starting with low analysis depth that can be detailed and extended during the subsequent iterations. Early iterations of the risk assessment can use a simple structure that does not assess detailed relationships, as shown in Figure 40.

Further iterations can be used to detail the dependencies, e.g. by modeling logical asset paths required between applications. The scenario asset structure should be modeled in any way that reflects the inheritance of exposures/failures of underlying assets.

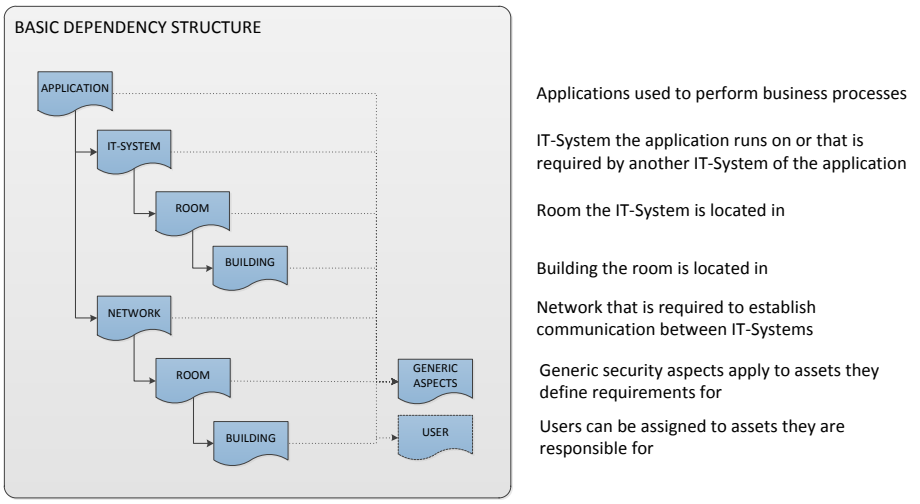


Figure 40: Basic dependency structure used for scenario analysis

An example structure showing more detailed dependencies (IT system 1 -> IT system 2) as well as assets groups that can be used to model and gain insight into specific asset groups (e.g. covering all IT systems of a specific department) is illustrated in Figure 41.

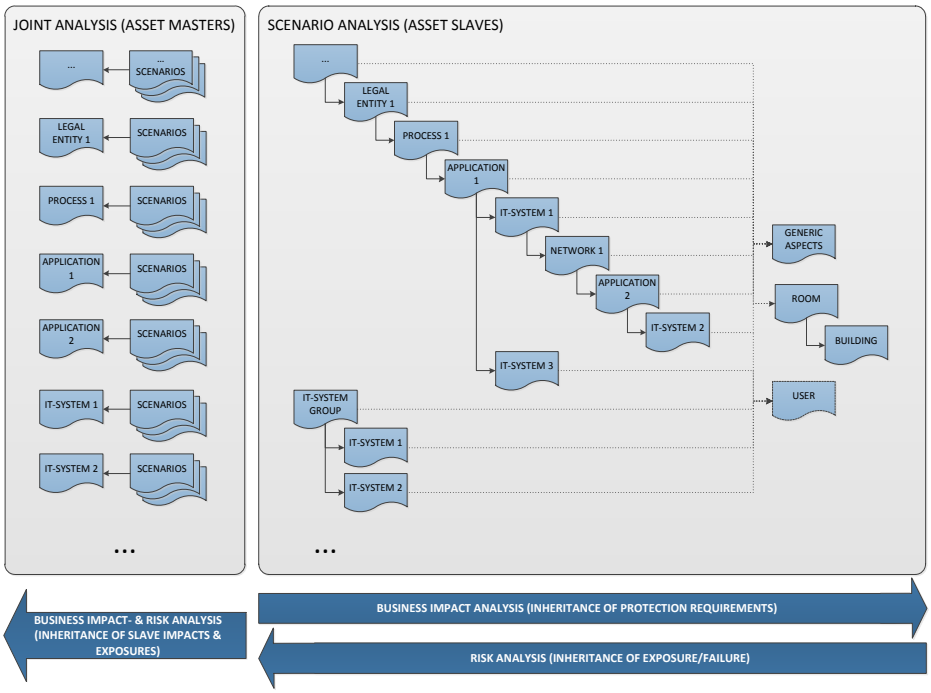


Figure 41: Assets and their representations within more complex scenarios

To achieve this analysis step, the proposed model provides a separate view on assets (masters) and their representations within asset scenarios (slaves). This enables a separate view on global asset risks and their risks within dependency scenarios. The dependency trees are used for BIA, in order to establish the requirement levels (impacts) for each asset within each scenario.

By establishing a scenario dependency, the parent asset is set to inherit the respective protection criteria exposures of its child asset (e.g. exposure of an application is based on its own exposures and the exposures of dependent assets). The type of aggregation function (a parent can have multiple children) can be defined explicitly for every parent protection criterion and the level of influence of any child can be weighted specifically for every child's protection criteria exposure. To illustrate a full dependency between protection criteria of the parent and its child, they can be marked as "knock-out" criteria for the respective scenario. This "knock-out" flag can be set to provide inheritance based on the relative weakest link instead of the weakest link. This is important to handle the following scenario in a risk-averse manner:

A highly complex parent asset (e.g. IT system) has a scenario dependency with a lower complexity child asset (e.g. room), that therefore has lower absolute exposure. If the parent asset's absolute exposure (and complexity) is significantly higher than those of the child, inherited exposure may be minimal. This could lead to false assumptions for risk inheritance, if the child's protection criterion directly affects the parent's protection criterion (e.g. availability). If this is the case, the parent's relative exposure should (at least) show the relative exposure of the child. This allows the inheritance of criteria exposures, as well as the more cautious view of criteria failures between dependent assets.

Scenario analysis enables the estimation of inherited risks between dependent assets, without the need to evaluate the respective risk factors individually (modules are shared between asset masters and their slaves). If, however, a distinguished estimation is desired, the respective asset can be duplicated along with its module(s), in order to enable separate estimations. When a user tries to estimate a risk factor within the assets, he can choose the appropriate evaluation scope (e.g. safeguard "Fire extinguisher" -> evaluations scope: Building 1, Building 2, etc.).

The proposed model uses functional relationships as aggregation functions within the risk assessment model, to estimate the aggregation of asset risk factors (see Figure 13, but without the measure layer), as well as the aggregation of risks between assets (see Figure 42).

The proposed model uses the energetic sum (see 3.1, Model Assumptions and Limitations) as a default estimation function, to provide a more realistic estimation of conditionally independent risks compared to maximum estimation. Other available aggregation functions include:

1. Maximum aggregation, suitable for estimation of overall exposure/risk based on mutually exclusive protection criterion exposure/risk, depending on the organizational requirements. Also, multiple identical components can be expressed using the maximum, if their amount has no or very little influence on the total attack surface (e.g. multiple identically configured IT systems within the same environment, handling the same data).

2. Sum aggregation, suitable for the integration of multiple modules into an asset, if the modules do not share any security relevant attributes (independent aspects/functionality). The sum aggregation is also suitable when estimating parent asset exposures based on child assets covering non-overlapping security relevant attributes (e.g. IT system (parent) → Network (child 1), Generic Aspects (child 2), Room (child 3)).

3. Minimum aggregation, suitable for the estimation of individual asset protection criteria risks, if the child assets provide some kind of failure safety regarding the protection criteria (e.g. minimum availability risk due to load balancing, clustering, remote backup, etc. of components).

The level of detail used to establish dependencies between physical assets, rooms and buildings as well as the assignment of generic aspects to those assets they define requirements for, is directly dependent on the desired analysis depth. The higher the level of detail and depth of the scenario trees, the higher the aggregated exposures at the root of the scenario trees (which is dynamically normalized to establish the impact-/exposure-bias desired by the risk manager). By also aggregating maximum values, it is possible to compare model complexity between risk models.

BIA starts at the root elements of the scenario trees by evaluating their estimated impacts and protection requirements. These requirement levels are then inherited to their children (maximum principle), unless the asset provides some kind of compensation (distribution effect). Because each scenario is assessed individually, the BIA only has to account for the functions required by the scenario (no need to assess the cumulative effect of other scenarios).

The proposed scenario analysis assumes that if a child asset is – based on environmental factors – requiring a lower protection criterion requirement level (impact), the respective risk that should be inherited is correspondingly lower (because of the lower impact).

When the BIA is finished for all scenario trees, the cumulative effect is assessed using joint analysis, which estimates the global asset impact based on the maximum impact of all its slave representations within the scenario trees.

3.1.2.2 Risk Estimation

For all assets showing protection requirements above normal, a detailed risk assessment according to IT-Grundschutz [48] has to be conducted to ensure that the predefined risk factors defined by the representing IT-Grundschutz module(s) are sufficient. Assets can be adjusted to the organizational context by adding and cross-referencing additional threats and prioritized safeguards, or – if the modules describe the organizational environment to an acceptable extent – by in- or decreasing the default weightings of the risk factors (see Figure 42) to adjust the estimated risks to appropriate levels.

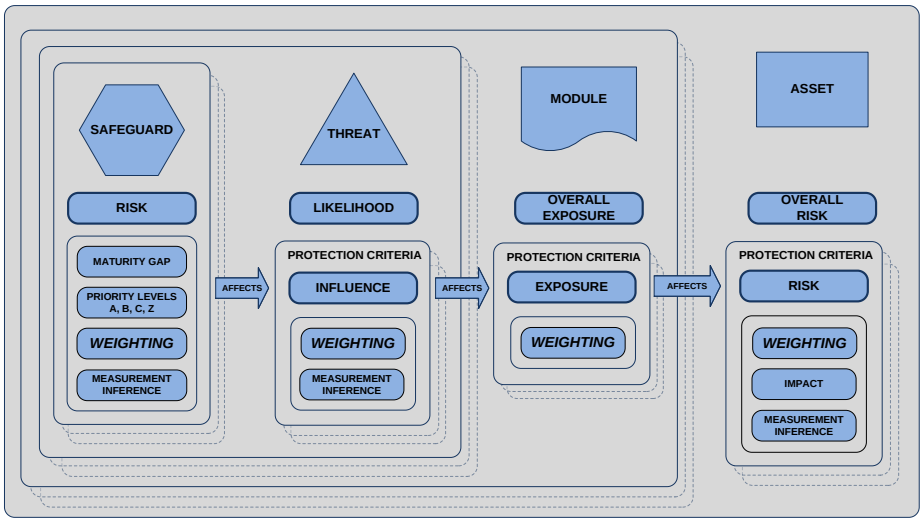


Figure 42: Asset structure based on modules and their weighable risk factors

1. Safeguards can be weighted to in-/decrease their importance, influencing the estimated baseline threat likelihood of cross-referenced threats
2. Threats can be weighted specifically for each protection criterion they potentially influence to in-/decrease the estimated the protection criteria exposures
3. At the module level, protection criteria exposures can be weighted to in-/decrease its impact on any specific protection on the higher level asset, and
4. At the asset level, each protection criterion risk can be weighted to in-/decrease the amount of risk inherited to their parent assets (if any).

Besides these variables, the proposed model is based on the estimation of safeguard maturities to estimate risks. When a safeguard is selected for evaluation, the user is

presented with all applicable assets, modules and threats related to that particular safeguard.

The current maturity level of low-level safeguards can be estimated individually for every related threat, but can also be estimated in general to allow a more rapid high-level estimation of the risk model.

To allow an even more rapid high-level assessment[7], the requirements of ISO/IEC 27001 [71] and controls of ISO/IEC 27002 [72] have been included as a cross-reference to IT-Grundschutz [57], allowing the evaluation of IT-Grundschutz safeguards in the context of the high-level controls.

The procedure to assess risks based on these estimations is outlined as follows, a detailed illustration of the assessment is provided in 4.

1. Safeguard risk is estimated based on safeguard maturity and the respective target level, the individual safeguard priority, weighting and influence provided by the integrated measure framework.
2. Threat likelihoods are estimated based on their cross-referenced safeguard risks. Depending on the influence weights (pre-defined by a team of security experts and extendable), the threat influences specific protection criteria.
3. Module protection criteria exposures are estimated based on all threats influencing the specific protection criterion. At the module level, an overall protection criterion exposure is estimated based on all module protection criteria exposures.
4. Asset protection criteria risks are estimated based on all protection criteria exposures and -impacts of assigned modules. Again, an overall risk is estimated for each asset based on all protection criteria risks of its modules.

The asset assessment provides the asset protection criteria risks that are inherited between dependent assets within the scenario trees. Each asset has a single “master”-representation within the risk model, as well as multiple “slave”-representations that are used to model scenario dependencies. The underlying module protection criteria exposures are unique, meaning they only have to be estimated once for each asset. Each slave asset has its own set of adaptable aggregation functions, protection criteria exposures, -impacts and -weights, specific to that scenario. This allows a very granular estimation of dependencies and related risks, while minimizing underlying estimation workload.

[7] Although the reference mapping’s primary purpose is to enable the assessment of ISO/IEC 27001 based on IT-Grundschutz, practice has shown that this assessment does provide useable, initial high-level insights into organizational risks, which can be detailed in further assessments.

The joint analysis step is used to estimate the aggregated master asset risk resulting from its slave asset risks within the scenario trees (for each protection criterion, as well as overall).

To integrate new estimations into the risk model, the complete risk model should be re-estimated. This may also be done only for assets that have changed, or assets that are dependent on those assets. The current implementation assumes risk factor evaluations to be valid until they are re-estimated, creating new aggregations with the respective time code for all objects within the risk model.

The re-estimation of the risk model can be initiated manually, or by defining re-estimation intervals for the risk model that trigger scheduled re-estimations.

3.1.2.3 Risk Evaluation

The decisions criteria that have been defined during context establishment (qualification-/maturity targets, residual exposure/risk levels) should be revisited and adjusted at this stage when more is known about the particular risks identified.

After the asset-, scenario- and joint-assessment is finished, the proposed model estimates the safeguard- and threat-sensitivity of each safeguard/threat based on their module structure and related scenario asset impacts. This supports the identification and adjustment of safeguard- and threat-risk factors with the highest impact on the overall situation.

Additionally, the scenario model provides insight into the dependency structure, including asset risks and relative exposure and risk levels, as well as details regarding specific module exposures, threat likelihoods and safeguard risks in order to decide upon activities for risk treatment.

3.1.3 Risk Treatment

There are four options available for the treatment of identified risks [1; p. 21]:

1. Risk avoidance, by making changes to the business area so that the actions engaging the risk are avoided
2. Risk reduction, by implementing mitigating safeguards
3. Risk transfer, by shifting the risk to another party (e.g. insurance)
4. Risk retention, by accepting the residual risk when the further treatment of risks is not economical

To support the risk treatment process, the decision for each safeguard (or particular assets involved) can be documented as part of a separate, self-definable set of actions (controls). Each module- and threat-specific safeguard representation within the risk model can be easily filtered, selected and referenced with these actions (see Figure 97). Actions are designed to consolidate and reference particular safeguard areas with a high-level object (e.g. policy, process) to reflect the organizational context.

This way, all required safeguards within the risk model can be mapped to organizational actions to document how these safeguards are handled by the organization (e.g. using policies, procedures, guidelines, etc.).

For every action, the user may estimate the initial and recurring costs and personnel required to support decision making. The implementation of additional safeguards can be supported by defining and documenting implementation projects, containing information about the objectives, scope, responsibilities, tasks, schedules and other relevant information.

Because of resource constraints, the research project focused on the establishment and integration of risk and indicator assessment, providing no advanced risk management functionality within the prototype implementation (no interfaces for document management, workflow-management, detailed cost-analysis, etc.).

3.1.4 Risk Acceptance

If risks ought to be accepted, the decision must be formally documented, including all associated threats, modules and assets and the residual risk involved. By accepting particular risks, the system assumes all referenced safeguards to be as mature as (currently) required, in order to mitigate their respective baseline threat likelihoods (and all subsequent risk factors) to zero. If maturity- or qualification targets change over time, the level of risk depends on the previously accepted level of risk.

3.1.5 Continuous Risk Communication, Monitoring and Review

The continuous risk communication-, as well as the monitoring and review process are supported by involving all roles relevant to the evaluation of security aspects and the provision of a centralized framework for modeling and assessing risks, respective actions and real-life, objective security measures. An assessment scheduling component can be used to track and remind users about their assessment activities and safeguard-related actions.

3.2 Metric Assessment & Management

The metric assessment and management process is aligned with the requirements of ISO/IEC 27004 to provide measurement results, relating to the effectiveness of controls and implementation processes, based on the derivation and analysis of low-level security measures.

The proposed model is designed to continuously re-evaluate influence vectors on specific risk factors within the risk model. Depending on measure indicators and their correlations, related risk factors that express the associated risks can be influenced by a fuzzy logic expert system, using formally defined rules and indicators that can be evaluated for correctness.

3.2.1 Measure Identification

The process to identify measurements is aligned with the procedure defined in ISO/IEC 27004. Measure identification is supported by the proposed model through the provision of:

1. reference resources for metrics (see Figure 10 and Figure 11), which provide guidelines and examples of useful security metrics
2. the IT-Grundschutz-Framework and related risk factors, which allow the derivation of appropriate security measurements on a pragmatic basis
3. reference resources for security measures (see Figure 12), which provide an externally evaluated source of measures
4. a set of pre-defined security metrics based on [43], [52] and [66] that have been integrated into the prototype (see Figure 101), categorized as

    a. Availability and reliability (13 metrics)
    b. Coverage and control (24 metrics)
    c. Organizational aspect metrics (6 metrics)
    d. Perimeter defense metrics (35 metrics)
    e. Vulnerability/Threat/Breach (8 metrics)

Based on these resources, the user can select pre-defined metrics or create and derive self-defined metrics. To outline this procedure, the following paragraphs cover the identification of two base measures and a derived measure, using a simplified notation based on [34; p. 26], enriched with specific fields required by the proposed model.

Based on the total number of reported breaches (since 2005) and the number of breaches during the last month, which are gathered automatically from DataLossDB[8], the relative increase in reported breaches is calculated. This derived measure can be used to provide an indicator for e.g. the IT-Grundschutz threat *T 2.106 Disturbance to business processes as a result of IT security incidents* in Figure 6 and is used as a basic example for an external measurement.

Because the indicator in Figure 45 is based on external data and relates to likelihood (opposed to impacts or vulnerabilities, see 3.3.2), the estimated influence should affect the threat's protection criteria only, increasing associated residual safeguard risks. This means, that if all threat-related safeguards are as mature as required, the influence has no effect (see 4.2.1.3). However, if there are residual safeguard risks associated with the influenced threat, the proposed model increases the threat's protection criteria exposures by increasing their influence weight (and those of the module and assets associated/dependent) to depict the potentially increased threat within the risk model.

Name	Number of (DataLossDB) reported breaches during the last month
Shortcut	number-reported-breaches
Type	Threat metric
Keywords	Public, Breach, Threat, Incident
Scope	Breach metric
Frequency	Monthly
Formula	- (base measure)
Usage	in all risk models (public measure)
Responsible	- (automatically provided through sensor)
Sensor	DataLossDB_Breaches
Source	http://datalossdb.org
Objective	This measure provides a current view on the number of reported breaches during the last month that has been collected by DataLossDB. Primary sources are various jurisdictions (http://datalossdb.org/primary_sources) in the United States of America.
Description	This metric provides a raw count of the number of security breaches that were identified by the Open Software Foundation and entered into the data loss database (DataLossDB). Counts can be aggregated based upon specified time periods as well as by several dimensions (segment (e.g. .bit, .edu, .med, etc.), breach type, data lost, source, third party involvement). This metric counts the number of breaches without any dimen-

[8] DataLossDB (http://datalossdb.org) is a research project aimed at documenting known and reported data loss incidents and data breaches world-wide.

	sional constraints within the last month. Limitations: This metric characterizes only the volume of security breaches. It does not take into account their severity or impact. Also, it relies upon the DataLossDB as maintained by OSF. Breaches that do not appear in the press or are not seen by OSF researchers do not appear in this database and are thus not counted.
Indicators	-

Figure 43: Base measure definition for "Number of reported breaches during the last month"

Name	Number of (DataLossDB) total reported breaches
Shortcut	number-reported-breaches-total
Type	Threat metric
Keywords	Public, Breach, Threat, Incident, Sources
Scope	Breach Metric
Frequency	Monthly
Formula	- (base measure)
Usage	in all risk models (public measure)
Responsible	- (automatically provided through sensor)
Sensor	DataLossDB_Breaches_Total
Source	http://datalossdb.org
Objective	This measure provides a current view on the total number of breach notifications sent to various jurisdictions (http://datalossdb.org/primary_sources) in the United States of America, starting from 2005.
Description	The primary sources archive is a collection of breach notification letters sent to various jurisdictions in the United States. These were gathered staff and volunteers through sponsorship funding and donations. Currently, a project is underway to accumulate more such notices via the Freedom of Information Act, and its various local and state legislative cousins. Counts can be aggregated based upon specified time periods as well as by several dimensions (segment (e.g. .bit, .edu, .med, etc.), breach type, data lost, source, third party involvement). This metric counts the number of total breaches without any dimensional constraints since 2005. Limitations: This metric characterizes only the volume of total security breaches. It does not take into account their severity or impact. Also, it relies upon the DataLossDB as maintained by OSF. Breaches that do not appear in the press or are not seen by OSF researchers do not appear in this database and are thus not counted.
Indicators	-

Figure 44: Base measure definition for "Number of total reported breaches"

Name	Relative (%) increase in (OpenLossDB) reported breaches during the last month
Shortcut	increase-reported-breaches-month
Type	Threat metric
Keywords	Public, Breach, Threat, Incident
Scope	Breach Metric
Frequency	Monthly
Formula	$\frac{\text{"Number of reported breaches during the last month"}}{\text{"Number of total reported breaches"}} \times 100$
Usage	in all risk models (public measure)
Responsible	- (automatically calculated derived measure)
Sensor	- (automatically calculated derived measure)
Source	http://datalossdb.org
Objective	This measure provides the last month's relative increase in reported breaches to the number of total breaches reported by DataLossDB.
Description	This metric counts the relative increase (in percentage) of reported incidents during the last month, as collected by DataLossDB. Limitations: This metric characterizes only the relative increase of security breaches. It does not take into account their severity or impact. Also, it relies upon the DataLossDB as maintained by OSF. Breaches that do not appear in the press or are not seen by OSF researchers do not appear in this database and are thus not incorporated.
Indicators	-

Figure 45: Derived measure definition for "Relative increase in (OpenLossDB) reported breaches during the last month"

3.2.2 Sensor Integration

The proposed model allows the integration of external sensor components to support the automatic gathering of measures. This is achieved by registering those components, in order to authorize the reporting of measures through that channel. Sensors are registered using the following information:

- Sensor name,
- Remote IP address(es) to allow reporting from
- Pre-shared-secret, in order to provide basic authentication

The implementation of remote sensor components is not part of this thesis, but can be done using various programming- or scripting-languages. The only requirement for the sensor-component is the possibility to perform a simple HTTP(S) request with the required information encapsulated using GET- or POST-parameters within the request.

Because of the potential high confidentiality- and integrity-requirements of risk assessment information, the web service components of the prototype have been made only available through the HTTPS protocol.

3.3 Expert Knowledge Management

The integrated expert knowledge management deals with the definition and the exchange of formalized expert knowledge describing insights and experiences regarding information security measurements and their related risk factors.

After evaluation of various knowledge management disciplines (see 2.3), fuzzy logic was identified to be suited best to support indicator definition as well as the exchange of formalized knowledge without exposing confidential information over business boundaries. This is because fuzzy logic allows a clean separation between graphical indicator terms, used to describe measurements and their organization-specific representation of undesired measure states, and expert rules, used to formalize generalized knowledge. Therefore, expert knowledge can be exchanged with external sources, while the representation of organization-specific evaluation of undesired measure states is handled separately.

3.3.1 Indicator Evaluation

According to ISO/IEC 27004, indicators are obtained by applying an analytical model to the derived measures. While the examples only provide thresholds as analytical models, the proposed approach allows the definition of the "riskiness" of the measurement range.

This is achieved by using fuzzy logic terms and membership functions (see 2.3.4). Because this approach allows a more fine-tuned evaluation than thresholds, a single indicator term can be used to describe the measure range, instead of multiple thresholds (cf. Figure 46, Figure 49).

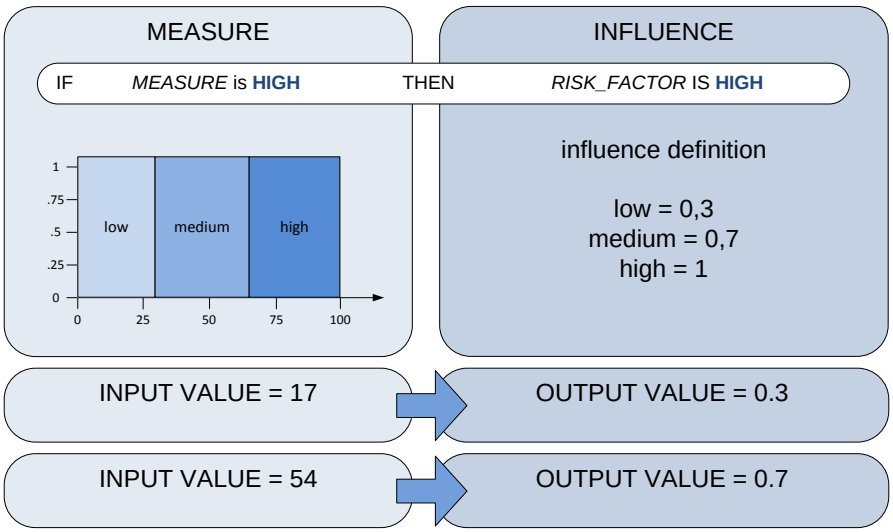


Figure 46: Usage of thresholds to describe a measure and its influence on a risk factor, leading to influence leaps when reaching thresholds

In order to decide upon the indicator definition for the derived measure in Figure 47, we should gain insight into the recent trends of the measure.

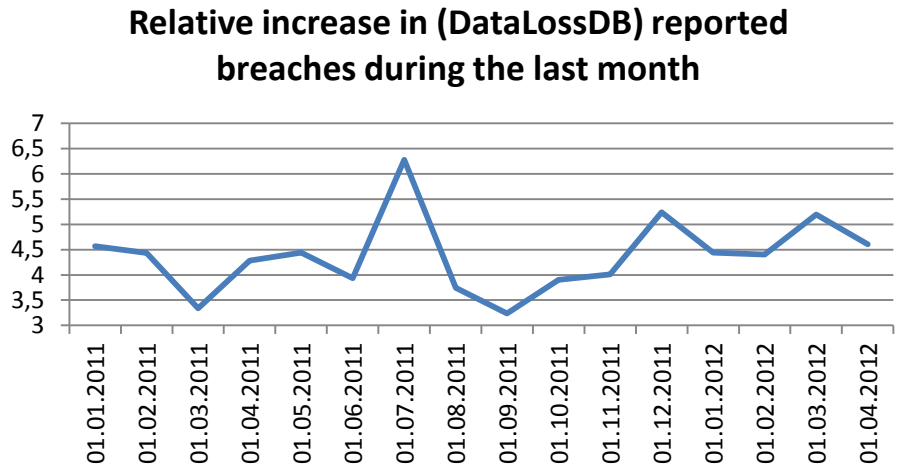


Figure 47: Derived measure trend (DataLossDB)

The average relative increase in reported breaches since 2011 has been 4.38 %, with a maximum of 6.28 %. Aligned with these values, the indicator for a *high* increase in reported breaches during the last month (16) is defined according to FCL specification format [39] using a membership function. The keyword *sigm*, followed by two numbers *g* and *c*, defines a sigmoid function with a gain of *g*, centered at *c*. Other suitable functions for this context include multi-point linear, triangle, trapezoidal and singleton.

```
FUZZIFY relative_increase_in_reported_breaches_during_the_last_month
   TERM high := sigm 5 5.5                                          (16)
END_FUZZIFY
```

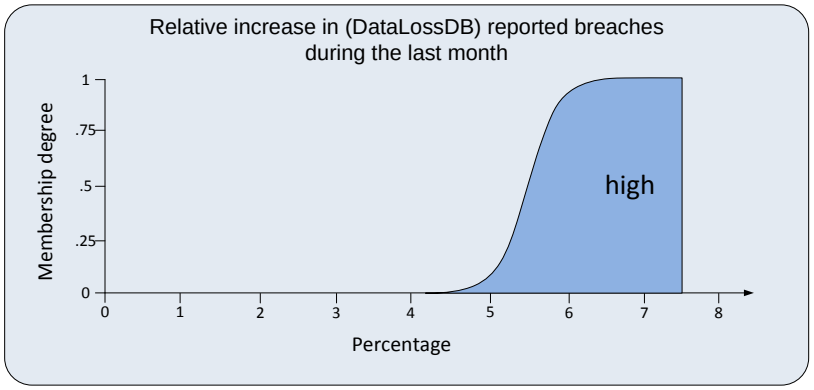


Figure 48: Example estimation for an indicator describing a "high" increase in (DataLossDB) reported breaches during the last month

3.3.2 Expert Knowledge Definition

The basic idea behind the usage of membership functions is to provide an easily manageable way of projecting measure indicators onto respective influence indicators, documenting expert knowledge of the estimated system behavior. The membership degree of a measure term is mapped to an indicator term, which corresponds to an influence value. This principle is shown in Figure 49.

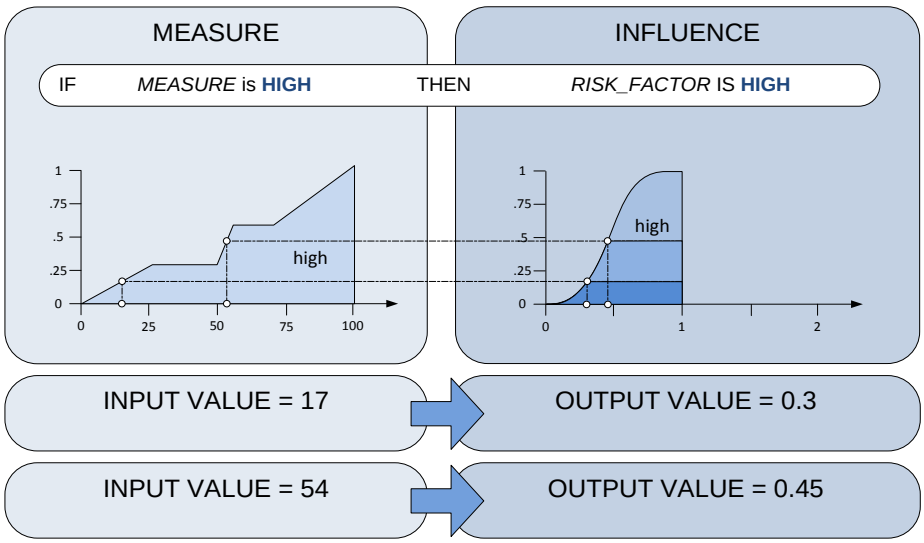


Figure 49: Usage of membership functions to describe relations between a measure (multi-point linear measure indicator *high* on the left side) and its influence on a risk factor (sigmoid influence indicator *high* on the right side)

The proposed model allows the definition of multiple influence terms that can be referenced within rules. These influence terms can be defined globally for the entire risk model, or specifically for each risk factor that should be influenced.

Based on the layout of the proposed risk assessment structure, three types of risk factors can be influenced:

1. Safeguard maturity: The manually estimated maturity can be influenced negatively. Risk factors should not be influenced in a positive way when indicators show lower risks, because the definition of the indicator reflects the subjective evaluation based on current safeguard maturity. Safeguard maturity influence adapts the related safeguard by means of subtraction from the estimated safeguard maturity in the interval [0, 5] (see 4.2.1.1).

2. Threat likelihood: The threat likelihoods of the model are correlated with the immaturity of related safeguards, reducing the estimated baseline threat likelihood to zero when meeting all defined requirements. By influencing threat weightings, all related safeguard risks are weighted accordingly. The in- or de-

crease of weightings on threat likelihoods that are fully reduced to baseline (all related safeguards are as mature as required and not negatively influenced) has no effect on further estimation. To provide the ability to influence threat-specific protection criteria individually, the threat likelihood influence adapts the related protection criteria influences by means of addition to their weighting in the interval [0, 2] (see 4.2.1.3).

3. Asset impact: The estimated asset protection criterion impact/requirement (and the related asset protection criteria risk) can be influenced positively or negatively (in- or decreasing the estimated impact/risk). The asset protection criterion exposure is correlated with the baseline threat likelihoods, reducing each protection criterion exposure to zero when all of the asset's threats that influence the particular protection criterion are mitigated to zero. To provide the ability to influence protection criteria-specific impacts, the asset impact influence adapts the related protection criteria weightings by means of addition in the interval [0, 2] (see 4.2.1.6).

The same principle can be used to relate multiple measures with their specific indicators to a generalized influence term that reflects the organizational belief in influence on the respective factors. Specific indicators can be defined to reflect specific behavior, both measure- and influence-indicators. During testing and evaluation, the usage of a set of two to three staggered influence indicators has been proven most useful, in order to provide a default- and one or two elevated influences for the description of correlation effects between indicators. The greater the negative influence of the correlating indicators is estimated, the greater – in terms of minimum and maximum – the influence indicator should be defined. This is outlined in Figure 50.

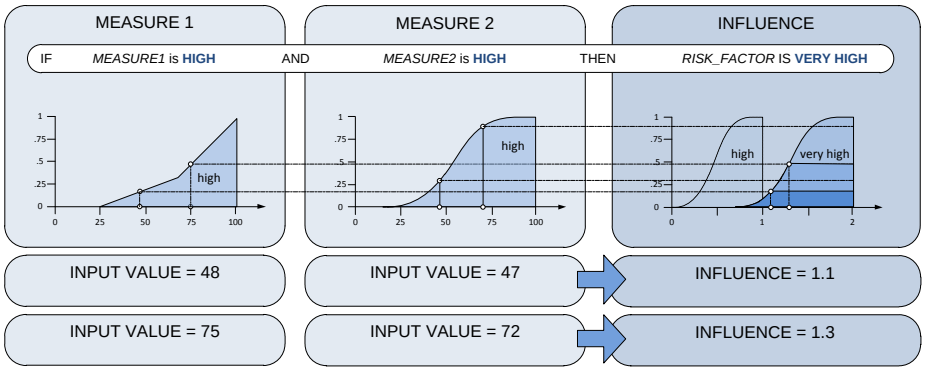


Figure 50: Usage of correlating measure indicators using AND (minimum operation) to estimate a *very high* influence on a risk factor

Each of the indicators outlined in Figure 50 can be used by themselves (without the AND correlation) to describe the high influence term, as shown in Figure 49. Because of the comprehensiveness of risk factors provided by IT-Grundschutz, these correlations may often be defined as a single rule influencing multiple risk factors based on the same correlation (same rule using same measure indicators), the influence output

can be regulated for every influenced risk factor by using a weighting. This is provided by the prototype through referencing of risk factors with adaptable weights within the context of a single rule (IF condition IS P_k THEN conclusion IS C_k WITH WEIGHT [0, 1]).

The following rules give examples of the definition of expert knowledge about indicators and their influence on risk factors (20) using the principle shown in Figure 49.

IF *Relative increase in reported breaches during the last month* IS *high*
THEN *T 2.106 Disturbance to business processes as a result of IT security incidents* IS *high* (20)

This can also be done specifically for each individual protection criterion of the threat, using the following syntax (weighting is optional):

IF *Relative increase in reported breaches during the last month* IS *high*
THEN *T 2.106 Disturbance to business processes as a result of IT security incidents*
PC *Confidentiality* IS *high* WITH WEIGHT 1,
PC *Integrity* IS *high* WITH WEIGHT 0.6,
PC *Availability* IS *high* WITH WEIGHT 0.8 (21)

Correlating indicators and their increased influence on risk factors can be achieved as shown in (22), using the principle shown in Figure 50.

IF *Months since last ISP revision* IS *high*
AND *Percentage of users trained regarding ISP* IS NOT *high* (22)
THEN *S 2.192 Drawing up an Information Security Policy* IS *very high*

In order to establish the correct connections to the relevant assets of the risk model, each generic rule has to be mapped to the appropriate scope (e.g. assets, modules and threats referencing the safeguard) within the risk model. This is achieved for each risk factor target (*S 2.312* and *S 3.5* in (23)) by selecting the appropriate scope as shown is Figure 51. Depending on the generic risk factor selected by the user, the prototype searches for all instances of that risk factor within the risk model and returns their representations including related threats, modules and assets in order for the user to select the appropriate scope and influence.

Due to some missing translations for the English IT-Grundschutz catalogues of the current version (2011), the screenshots of the prototype as well as some related examples show the German IT-Grundschutz texts.

IF *Percentage of personnel who received annual information security awareness training* IS NOT *high*
THEN *S 2.312 Design of an Information Security training and awareness program* IS *high*
AND *S 3.5 Training on Information Security safeguards* IS *high* WITH WEIGHT 0.8 (23)

Figure 51: German prototype interface for establishing indicator mappings between generic risk factors and their specific instances, related threats, modules and assets

The IT-Grundschutz safeguard *S 3.5 Training on Information Security safeguards* ("Schulung zu Sicherheitsmaßnahmen") used in the generic expert rule (23) is mapped to its specific representations within the scope of the risk model. The safeguard in question is only defined within the asset *Generic aspects* ("Übergreifende Aspekte") and its module *Personnel* ("Personal"). For each threat that is cross-referenced with this safeguard, individually weighted influence indicators can be defined in order to provide the most granular inference option. The generic measure indicator *high* is mapped with specific weights for the referenced threats *T 3.1 Loss of data confidentiality/integrity as a result of IT user error* ("Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer") and *T 3.3 Non-compliance with IT security measures* ("Nichtbeachtung von IT-Sicherheitsmaßnahmen").

Depending on the risk factor to be influenced, the proposed method allows the following relationships to be established:

1. Safeguard maturity: The user can choose the appropriate scope (the safeguards that are related to the indicator in question) out of all assets within the risk model that are cross-referenced with the safeguard in question. For each of these assets, the safeguard influence can be defined with specific weightings for each cross-referenced threat and related module (as shown in Figure 51).
2. Threat likelihood: The user can choose the appropriate scope out of all assets and modules within the risk model that are cross-referenced with the threat in question. For each of these threats, the threat likelihood influence can be defined with specific weightings for each cross-referenced protection criterion.
3. Asset impact: The user can choose the appropriate scope out of all assets and modules within the risk model that are related to the impact in question. For each of these assets and modules, the impact influence can be defined with specific weightings for each cross-referenced protection criterion.

3.3.3 Expert System Configuration Requirements

In order to establish the desired behavior of the expert system, the fuzzy logic operators for each phase of operation have to be defined. Based on the proposed model, these requirements are:

1. Indicators for measures (input) can be defined simply by term, as shown in Figure 48.

2. Indicators for risk factor influence (output) have to be defined with a generic or specific term for each influenced risk factor. The Left-Most-Maximum (LM) defuzzification method (see Figure 26) is used in order to provide the correctly aligned influence indicators as shown in Figure 49. A default value of zero should be used when no rule is activating the indicator, in order to reset the influence value. This information is defined within a "defuzzify" statement (24) according to FCL specification format [39].

```
DEFUZZIFY influence_on_risk_factor_representation
    TERM high := (0,0) (1,1);          // e.g. multi-point linear
    METHOD : LM;                       // Left-Most-Maximum
    DEFAULT := 0.0;                    // influence when not activated
END_DEFUZZIFY
```
(24)

3. Each rule that is defined within the proposed model and that has established specific scopes of risk factors within the risk model, creates a rule block using the syntax defined in (25). The activation uses the minimum (*Min*) operator in order to instruct the expert system to use the minimum operator for aggregation of *AND* conclusions (risk factor is only influenced as high as the minimum influence of correlating indicators), as well as the maximum operator for aggregation of *OR* conclusions. If a rule is activated by accomplishing all conditions, the degree of membership of the conclusion is determined based on the minimum of aggregated conditions. This intermediate stage is also used to adjust the conclusion using weighted rules, by multiplication of the conclusion (influence) with the weighting factor [0, 1]. Accumulation is done using the maximum operator separately for different rules, in order to circumvent the problem of accumulation shown in Figure 26. If multiple rules provide different influence estimations for a single risk factor, the overall estimation is based on the maximum of all estimations, in order to provide a worst-case estimation. This information is defined within a rule block statement according to FCL specification format [39], as shown in (25).

```
RULEBLOCK rule_name
    AND : Min;        // Aggregation: AND (Minimum), OR (Maximum)
    ACT : Min;        // Activation: Minimum
    ACCU : Max;       // Accumulation: Maximum

    RULE 1 : …
END_RULEBLOCK
```
(25)

Depending on the user preferences, the expert system can re-estimate influences in continuous intervals. This is provided by the proposed model by defining recalculation intervals for the risk model. A scheduling component triggers the continuous re-estimation of influences based on changed measurements, as well as the subsequent re-estimation of the risk model.

4 Example Assessment

The following illustrated assessment is based on the context defined below and uses the cross-references in Figure 6 as a basic example for the risk estimation procedure.

The risk factor influence shown in Figure 48 is used as a basic example for the influence estimation procedure to illustrate the integration of security measures and expert knowledge.

The example definitions and calculations listed throughout this section belong to one continuous example based on the evaluation model presented in 6.1.1 and are numbered in Roman numerals.

4.1 Context Establishment

To establish the risk environment for calculation, a few variables have to be defined as outlined in 3.1.1.

4.1.1 Qualification Targets

The safeguard qualification target $S_{qualification\ target}$ can be selected based on the available levels outlined in Figure 35. The example uses the highest qualification target for all areas, in order to involve all safeguards up to the additional priority level of the example in Figure 6. The qualification target scale is reversed, in order to express the increase in safeguard risk related to safeguards with higher priorities (e.g. an immature IT-Grundschutz safeguard with priority level A is assumed to pose higher risks than a priority level Z safeguard (e.g. A…4, B…3, C…2, Z…1)). If the qualification target would be set higher, safeguards with lower priority levels would be assumed to be negligible and would not be included in risk estimations (37).

$$S_{qualification\ target} = 1 \tag{I}$$

4.1.2 Target Maturities

The safeguard maturity target $S_{maturity\ target}$ can be specified for module-, threat- and safeguard-types based on the available levels outlined in Figure 36. The example uses "qualitatively managed" as a maturity target level for all safeguard types equally.

$$S_{maturity\ target} = 4 \tag{II}$$

4.1.3 Protection Criteria and Requirement Levels

The example uses the default protection criteria used within the context of information security risk assessments:

- confidentiality,
- integrity, and
- availability,

using the user-defined example impact levels outlined in 3.1.1.3. This means, that every threat, module and asset within the model, depending on the underlying threat-protection criteria influences, may share these protection criteria.

Because the proposed method allows the risk manager to define a bias between impact and exposure, the following normalization steps are necessary at the end of each recalculation of the risk model in order to identify the current maxima of impacts and exposures.

For this example, the user-defined bias between impact- and exposure-factors is weighted equally on a scale of [0, 10], with a resulting risk scale of [0, 100] (III).

$$\begin{aligned} A_{impact\ scale\ max} &= 10 \\ A_{exposure\ scale\ max} &= 10 \\ A_{risk\ scale\ max} &= 100 \end{aligned} \tag{III}$$

Because asset (*A*) exposures, module (*M*) exposures, threat (*T*) exposures and safeguard (*S*) risks are aggregated at distinct layers, their respective maxima are used to provide a normalized view for each layer.

To provide a uniform scale for all layers in this example, each layer is scaled corresponding to the previously defined maximum asset exposure scale $A_{exposure\ scale\ max}$ as shown in (IV).

$$\begin{aligned} M_{exposure\ scale\ max} &= 10 \\ T_{exposure\ scale\ max} &= 10 \\ S_{risk\ scale\ max} &= 10 \end{aligned} \tag{IV}$$

Distinct protection criteria on each layer are normalized using a single overarching normalization weight, in order to preserve their comparability.

4.1.3.1 Asset Impact Normalization

To achieve an easily comprehensible result and a balanced weighting between impact and exposure, the impact values are normalized to a maximum scale of $A_{impact\ scale\ max}$. The maximum impact $A_{impact\ max}$ that is possible within the risk model is identified using (26), based on *m* protection criteria and *n* related impact levels available by user definition. The resulting current impact normalization weight $A_{impact\ nweight}$ is given by (27).

In (26), $I = \{\, i \mid 1 \leq i \leq m \,\}$ and $J = \{j \mid 1 \leq j \leq n\}$, where *m* is the number of protection criteria in the risk model and *n* is the number of related impact levels.

$$A_{impact\ max} \coloneqq \max_{i \in I, j \in J} (A_{pc\ impact_{i_j}}) \tag{26}$$

$$A_{impact\ nweight} \coloneqq \begin{cases} \dfrac{A_{impact\ scale\ max}}{A_{impact\ max}}, A_{impact\ max} > 0 \\ 0 \qquad\qquad\qquad\quad , otherwise \end{cases} \tag{27}$$

The current user-defined impacts for this example are defined in Figure 37, giving the potential maximum impact in (V), which in turn gives the example's impact normalization weight $A_{impact\ nweight}$ as shown in (VI).

$$A_{impact\ max} = \max(0, 10, 25, 40, 0, 10, 25, 40, 0, 10, 20, 30, 40) = 40 \tag{V}$$

$$A_{impact\ nweight} = \frac{10}{40} = 0.25 \tag{VI}$$

4.1.3.2 Asset Exposure Normalization

Protection criteria exposures at the asset level are normalized to the maximum scale $A_{exposure\ scale\ max}$, based on the (current) accumulated maximum exposures of *m* protection criteria maxima $A_{pc\ exposure\ max}$ of all *n* assets within the risk model, using (28). This aggregated value expresses the total potential attack vector on any protection criterion of any asset within the example risk model. The variable $A_{exposure\ nweight}$ is given by (29) and is used as an exposure normalization weight for the asset layer.

In (28), $I = \{\, i \mid 1 \leq i \leq m \,\}$ and $J = \{j \mid 1 \leq j \leq n\}$, where *m* is the number of protection criteria in the risk model and *n* is the number of related asset exposure maxima.

$$A_{exposure\ max} \coloneqq \max_{i \in I, j \in J} (A_{pc\ exposure\ max_{i_j}}) \tag{28}$$

$$A_{exposure\ nweight} \coloneqq \begin{cases} \frac{A_{exposure\ scale\ max}}{A_{exposure\ max}}, A_{exposure\ max} > 0 \\ 0 \qquad\qquad\qquad\quad , otherwise \end{cases} \tag{29}$$

The example assumes a (current) accumulated maximum protection criterion exposure $A_{exposure\ max}$ of 141 for the root asset[9] (master) of the scenario tree (VII), providing the example asset normalization weight in (VIII). The distinct values in (VII) have been omitted for readability reasons due to the vast number of assets (incl. scenario representations) and protection criteria within the example (see 6.1.1).

The value presented in (VII) is estimated at the end of each recalculation of the risk model, following the complete assessment process up to 4.2.1.7, where the current maximum protection criteria exposures of assets are estimated using (28). Because normalization depends on the highest exposure within the risk model, data is stored unaltered within the server and normalized dynamically using the normalization weight of the appropriate re-estimation round when requested by the client.

$$A_{exposure\ max} = 141 \tag{VII}$$

$$A_{exposure\ nweight} = \frac{10}{141} = 0.07092199 \tag{VIII}$$

The exposure normalization steps described in the following are calculated analogous in regard to the respective layer.

[9] Because risk inheritance within the tree is depending on the modeled behavior between components, the root asset might not be the most exposed asset.

4.1.3.3 Module Exposure Normalization

Protection criteria exposures at the module level are normalized to the maximum scale $M_{exposure\ scale\ max}$, based on the (current) accumulated maximum exposures of *m* protection criteria $M_{pc\ exposure\ max}$ of all *n* modules within the risk model, using (30). This aggregated value expresses the total potential attack vector on any protection criterion of any module within the example risk model. The variable $M_{exposure\ nweight}$ is given by (31) and is used as an exposure normalization weight for the module layer.

In (30), $I = \{ i \mid 1 \leq i \leq m \}$ and $J = \{ j \mid 1 \leq j \leq n \}$, where *m* is the number of protection criteria in the risk model and *n* is the number of related module exposure maxima.

$$M_{exposure\ max} \coloneqq \max_{i \in I, j \in J} (M_{pc\ \ exposure\ max_{i_j}}) \tag{30}$$

$$M_{exposure\ nweight} \coloneqq \begin{cases} \dfrac{M_{exposure\ scale\ max}}{M_{exposure\ max}}, M_{exposure\ max} > 0 \\ 0 \qquad\qquad\qquad\quad , otherwise \end{cases} \tag{31}$$

The example assumes a (current) maximum module protection criterion exposure value of 38 for the module *SAP System* (IX), providing the example module normalization weight in (X). As with the previous layer, the distinct values in (IX) have been omitted for readability reasons due to the vast number of modules and protection criteria within the example (see 6.1.1).

The value presented in (IX) is estimated at the end of each recalculation of the risk model, following the assessment process up to 4.2.1.4, where the current maximum protection criteria exposures of modules are estimated using (30).

$$M_{exposure\ max} = 38 \tag{IX}$$

$$M_{exposure\ nweight} = \frac{10}{38} = 0.26315789 \tag{X}$$

4.1.3.4 Threat Likelihood / Exposure Normalization

Protection criteria exposures at the threat level are normalized to the maximum scale $T_{exposure\ scale\ max}$, based on the (current) accumulated maximum exposures of *m* protection criteria $T_{pc\ exposure\ max}$ of all *n* threat within the risk model, using (32). This aggregated value expresses the total potential attack vector on any influenced protection criterion of any threat within the example risk model. The variable $T_{exposure\ nweight}$ is given by (33) and is used as an exposure normalization weight for threat likelihood and threat protection criteria exposures[10].

In (32), $I = \{\, i \mid 1 \leq i \leq m \,\}$ and $J = \{j \mid 1 \leq j \leq n\}$, where *m* is the number of protection criteria in the risk model and *n* is the number of related threat exposure maxima.

$$T_{exposure\ max} := \max_{i \in I, j \in J} (T_{pc\ exposure\ max_{i_j}}) \tag{32}$$

$$T_{exposure\ nweight} := \begin{cases} \dfrac{T_{exposure\ scale\ max}}{T_{likelihood\ max}}, T_{likelihood\ max} > 0 \\ 0 \qquad\qquad\qquad\quad , otherwise \end{cases} \tag{33}$$

The example assumes a (current) maximum threat protection criterion exposure value of 30.3 for the threat *T 2.66 Lack of or inadequate IT Security management* within the module *Security Management* (XI), providing the example module normalization weight in (XII). As with the previous layers, the distinct values in (XI) have been omitted for readability reasons due to the vast number of threats and protection criteria within the example (see 6.1.1).

The value presented in (XI) is estimated at the end of each recalculation of the risk model (XXVII), following the assessment process up to 4.2.1.3, where the current maximum protection criteria exposures of threats are estimated.

$$T_{exposure\ max} = 30.3 \tag{XI}$$

$$T_{exposure\ nweight} = \frac{10}{30.3} = 0.33003300 \tag{XII}$$

[10] Threat likelihood is a generalized representation of a threat's exposure without taking influenced protection criteria into account. Because these underlying likelihoods are only used for calculation purposes and are never visualized, no separate threat likelihood normalization is required.

4.1.3.5 Safeguard Risk Normalization

The value $S_{risk\ max}$ depends on the maximum safeguard risk possible, due to their maturity, priority, weighting, as well as current qualification- and maturity targets (see 4.2.1.1). This value is based on the maximum safeguard risk $S_{risk\ max}$ of all *n* safeguards of the example risk model (34). The variable $S_{risk\ nweight}$is given in (35) and is used as a normalization weight for the safeguard layer.

In (34), $I = \{\, i \mid 1 \leq i \leq m \,\}$, where *m* is the number of safeguards within the risk model.

$$S_{risk\ max} \coloneqq \max_{i \in I}(S_{risk\ max_i}) \tag{34}$$

$$S_{risk\ nweight} \coloneqq \begin{cases} \dfrac{S_{risk\ scale\ max}}{S_{risk\ max}}, S_{risk\ max} > 0 \\ 0 \qquad\qquad\quad , otherwise \end{cases} \tag{35}$$

The example assumes a current maximum safeguard risk $S_{risk\ max}$ of 16 (XIII), providing the safeguard normalization weight in (XIV). As with the previous layers, the distinct values in (XIII) have been omitted for readability reasons due to the vast number of cross-referenced safeguards within the example (see 6.1.1).

The value presented in (XIII) is estimated at the end of each recalculation of the risk model (XIX), following the assessment process up to 4.2.1.1, where the current maximum risks of safeguards are estimated.

$$S_{risk\ max} = 16 \tag{XIII}$$

$$S_{risk\ nweight} = \frac{10}{16} = 0.625 \tag{XIV}$$

4.1.4 Residual Risk Levels

The example uses the alignment as shown in 3.1.1.4 to visualize a relative scale. This is incorporated into the following figures by coloring residual risks appropriately.

4.2 Risk Assessment

During risk assessment, risk factors are estimated and aggregated as well as evaluated using various sensitivity assessments.

4.2.1 Risk Estimation

The risk estimation process covers the estimation and aggregation of risk factors based on safeguards, threats and modules of the IT-Grundschutz model up to assets and their protection criteria as a first abstraction layer.

Dependencies among assets can be depicted using the scenario analysis abstraction layer, while the third abstraction layer automatically covers an asset joint analysis based on the modeled scenarios (see Figure 28).

4.2.1.1 Safeguard Risk

Safeguard risk is primary assessed through its subjectively estimated maturity. This estimated maturity can be lowered by the inferring safeguard indicators. The estimated degradation of the safeguard maturity value is done through the safeguard maturity influence field $S_{maturity\ influence}$ on the scale[11] of [0, 5], which defaults to zero if no influence indicator is activated. If a safeguard is estimated more mature than required ($S_{maturity} > S_{maturity\ target}$), any potential measure influence is used as the current maturity gap $S_{maturity\ gap}$, signaling that the subjective estimation is potentially wrong in context of the measure influence (36) (safeguards that are more mature as required should not show any increased measure influence indicators).

$$S_{maturity\ gap} := \begin{cases} S_{maturity\ target} - (S_{maturity} - S_{maturity\ influence}), \\ \qquad S_{maturity\ influence} \leq S_{maturity} \leq S_{maturity\ target} \\ S_{maturity\ influence} \qquad , S_{maturity} > S_{maturity\ target} \\ 0 \qquad , otherwise \end{cases} \quad (36)$$

The following example is based on the IT-Grundschutz module *M 1.0 Security Management* shown in Figure 52, focusing on the safeguard risk of *S 2.192 Drawing up an Information Security Policy* corresponding with its first referenced threat *T 2.66 Lack of or inadequate IT Security Management*. The safeguard's current subjective maturity estimation regarding the threat *T 2.66* is given in (XV), resulting in the safeguard maturity gap in (XVI). All safeguard maturity influences $S_{maturity\ influence}$ are assumed zero for this example.

[11] The maximum safeguard maturity influence is limited by the highest maturity level.

$$S_{maturity} = 3 \tag{XV}$$

$$S_{maturity\ gap} = 4 - (3 - 0) = 1 \tag{XVI}$$

The risk model variables are designed to be reduced to zero when being totally compliant with all target levels.

Safeguard risk S_{risk} is assessed based on safeguard priority $S_{priority}$, estimated safeguard maturity gap $S_{maturity\ gap}$ and a safeguard-specific weighting S_{weight} to enable user-specific safeguard prioritization without changing the underlying base definition (37). The model assumes safeguards with priorities lower (reversed scale) than the qualification target range ($S_{priority} \geq S_{qualification\ target}$) to be negligible.

$$S_{risk} := \begin{cases} S_{priority} \times S_{maturity\ gap} \times S_{weight}, S_{priority} \geq S_{qualification\ target} \\ 0 \qquad\qquad\qquad\qquad\qquad\quad , otherwise \end{cases} \tag{37}$$

To support a relative view, the proposed model keeps track of the maxima of all variables, estimated upon the respective worst case scenario.

$$S_{risk\ max} := \begin{cases} S_{priority} \times S_{maturity\ target} \times S_{weight}, S_{priority} \geq S_{qualification\ target} \\ 0 \qquad\qquad\qquad\qquad\qquad\quad , otherwise \end{cases} \tag{38}$$

$$S_{risk\ rel} := \begin{cases} \frac{S_{risk}}{S_{risk\ max}} \times 100, S_{risk\ max} > 0 \\ 0 \qquad\qquad\qquad , otherwise \end{cases} \tag{39}$$

Continuing the example, the safeguard priority of *S 2.192 Drawing up an Information Security Policy*, specific to the threat *T 2.66 Lack of or inadequate IT Security Management*, is given in (XVII), its risk in (XVIII) and maxima in (XIX), resulting in the relative safeguard risk shown in (XX). The safeguard-specific weight S_{weight} is assumed one (default) for all safeguards within this example.

$$S\ 2.192_{priority} = 4 \tag{XVII}$$

$$S\ 2.192\ (T\ 2.66)_{risk} = 4 \times 1 \times 1 = 4 \tag{XVIII}$$

$$S\ 2.192\ (T\ 2.66)_{risk\ max} = 4 \times 4 \times 1 = 16 \quad \text{(XIX)}$$

$$S\ 2.192\ (T\ 2.66)_{risk\ rel} = \frac{4}{16} \times 100 = 25\% \quad \text{(XX)}$$

Figure 52 shows an example estimation of safeguard risks based on the module cross-references of *M 1.0 Security Management*, outlined in Figure 7. These safeguard maturity estimations can be based on their threat scenarios to utilize the cross-reference-definitions, but can also be generally defined for the safeguard on a high level, depending on the desired assessment depth. Residual risks in Figure 52 are colored as defined in 4.1.4.

As soon as all safeguard risks of the risk model have been estimated, the current maximum safeguard risk can be identified for safeguard risk normalization as shown in (34) and (35).

The software prototype stores non-normalized values (safeguard maturity estimations are saved as evidence) and dynamically calculates and visualizes the normalized values using (40) and (41).

$$S_{nrisk} := S_{risk} \times S_{risk\ nweight} \quad (40)$$

$$S_{nrisk\ max} := S_{risk\ max} \times S_{risk\ nweight} \quad (41)$$

Based on the example's safeguard risk normalization weight shown in (XIV), the current normalized safeguard risk is given in (XXI) and its respective maxima in (XXII).

$$S\ 2.192\ (T\ 2.66)_{nrisk} = 4 \times 0.625 = 2.5 \quad \text{(XXI)}$$

$$S\ 2.192\ (T\ 2.66)_{nrisk\ max} = 16 \times 0.625 = 10 \quad \text{(XXII)}$$

The table in Figure 53 visualizes the estimations of Figure 52 in a normalized manner, again using colored residual risk levels as defined in 4.1.4.

Module 1.0 Security Management																	
Safeguards	Priority	T 2.66				T 2.105				T 2.106				T 2.107			
		M	R	RM	RR	M	R	RM	RR	M	R	RM	RR	M	R	RM	RR
S 2.192 Drawing up an Information Security Policy	4	3	4	16	25	2	8	16	50	3	4	16	25				
S 2.193 Defining the IT security objectives and strategy	4	4	0	16	0									2	8	16	50
S 2.195 Drawing up an IT security concept	4	4	0	16	0												
S 2.197 Drawing up an training concept for IT security	4	3	4	16	25												
S 2.199 Maintenance of IT security	4	4	0	16	0	2	8	16	50					3	4	16	25
S 2.200 Preparation of management reports an IT security	2	3	2	8	25												
S 2.201 Documentation of the IT security process	2	4	0	8	0												
S 2.335 Defining the IT security objectives and strategy	4	4	0	16	0					4	0	8	0	3	4	16	25
S 2.336 Acceptance of overall responsibility for IT security at the management level	4	3	4	16	25	3	4	16	25	4	0	16	0	4	0	16	0
S 2.337 Integration of IT security in organization-wide workflows and processes	4	4	0	16	0												
S 2.338 Creating target group oriented IT security policies	1	1	3	4	75												
S 2.339 Cost-effective use of resources for IT security	1					2	2	4	50					3	1	4	25
S 6.16 Taking out insurance	1					2	2	4	50	3	1	4	25				

M … Estimated safeguard maturity, R … Safeguard risk, RM … Maximum safeguard risk, RR … Relative safeguard risk

Threats
T 2.66 Lack of or inadequate IT Security Management
T 2.105 Violation of statutory regulations and contractual agreements
T 2.106 Disturbance to business processes as a result of IT security incidents
T 2.107 Uneconomic use of resources as a result of an inadequate IT Security Management

Figure 52: Example estimation of safeguard risks based on a non-normalized scale

.

Module 1.0 Security Management																							
Safeguards	Priority	T 2.66				T 2.105				T 2.106				T 2.107									
		M	NR	NR M	RR	M	NR	NR M	RR	M	NR	NR M	RR	M	NR	NR M	RR	M	NR	NR M	RR	M	NR	NR M	RR
S 2.192 Drawing up an Information Security Policy	4	3	2.5	10	25	2	5	10	50	3	2.5	10	25												
S 2.193 Defining the IT security objectives and strategy	4	4	0	10	0													2	5	10	50				
S 2.195 Drawing up an IT security concept	4	4	0	10	0																				
S 2.197 Drawing up an training concept for IT security	4	3	2.5	10	25																				
S 2.199 Maintenance of IT security	4	4	0	10	0	2	5	10	50									3	2.5	10	25				
S 2.200 Preparation of management reports an IT security	2	3	1.3	5	25																				
S 2.201 Documentation of the IT security process	2	4	0	5	0																				
S 2.335 Defining the IT security objectives and strategy	4	4	0	10	0					4	0	5	0	3	2.5	10	25								
S 2.336 Acceptance of overall responsibility for IT security at the management level	4	3	2.5	10	25	3	2.5	10	25	4	0	10	0	4	0	10	0								
S 2.337 Integration of IT security in organization-wide workflows and processes	4	4	0	10	0																				
S 2.338 Creating target group oriented IT security policies	1	1	1.9	2.5	75																				
S 2.339 Cost-effective use of resources for IT security	1					2	1.3	2.5	50									3	1.3	2.5	25				
S 6.16 Taking out insurance	1					2	1.3	2.5	50	3	0.6	2.5	25												

M … Estimated safeguard maturity, NR … Normalized safeguard risk, NRM … Normalized maximum safeguard risk, RR … Relative safeguard risk

Figure 53: Example visualization of safeguard risks using the current safeguard normalization weight

4.2.1.2 Threat Likelihood

Based on safeguard risks S_{risk} and their maxima $S_{risk\ max}$, threat likelihoods $T_{likelihood}$ (which are mitigated to a baseline level with IT-Grundschutz) and their maxima $T_{likelihood\ max}$ can be derived for each cross-referenced threat. To achieve a realistic view of the effects of immature controls (*n* referenced safeguard risks S_{risk}) on their threats, the proposed model uses the energetic sum as an aggregation function. As shown in in 3.1 (Model Assumptions and Limitations), this method can be used to give a cautious view on the estimated resulting attack vector of multiple parallel threats.

In (42), $I = \{\, i \mid 1 \leq i \leq n \wedge S_{risk_i} > 0\}$, where *n* is the number of safeguards that are cross-referenced with the threat.

$$T_{likelihood} := \begin{cases} 10 \times \log_{10}\left(\sum_{i \in I} 10^{\frac{S_{risk_i}}{10}}\right), I \neq \emptyset \\ 0 \qquad\qquad\qquad\qquad\quad , otherwise \end{cases} \tag{42}$$

Continuing with the example shown in Figure 52, the threat likelihood $T_{likelihood}$ of *T 2.66 Lack of or inadequate IT Security Management* is estimated based on its cross-referenced safeguard risks.

$$T2.66_{likelihood} = 10 \times \log_{10}\left(10^{\frac{4}{10}} + 10^{\frac{4}{10}} + 10^{\frac{2}{10}} + 10^{\frac{4}{10}} + 10^{\frac{3}{10}}\right) \cong 10.5 \tag{XXIII}$$

To support a relative view on threat likelihoods ($T_{likelihood\ rel}$ in (44)), the proposed model keeps track of their maxima $T_{likelihood\ max}$, estimated upon the respective worst case scenario.

In (43), $I = \{\, i \mid 1 \leq i \leq n \wedge S_{risk\ max_i} > 0\}$, where *n* is the number of safeguards that are cross-referenced with the threat.

$$T_{likelihood\ max} := \begin{cases} 10 \times \log_{10}\left(\sum_{i \in I} 10^{\frac{S_{risk\ max_i}}{10}}\right), I \neq \emptyset \\ 0 \qquad\qquad\qquad\qquad\quad , otherwise \end{cases} \tag{43}$$

$$T_{likelihood\ rel} := \begin{cases} \frac{T_{likelihood}}{T_{likelihood\ max}} \times 100, T_{likelihood\ max} > 0 \\ 0 \qquad\qquad\qquad\quad , otherwise \end{cases} \tag{44}$$

Applied to the continuous example, the maximum likelihood of the threat *T 2.66 Lack of or inadequate IT Security Management* is given in (XXIV), its relative value in (XXV). The results for the remaining threats of Figure 52 are shown in Figure 55.

$$T2.66_{likelihood\,max} = 10 \times \log_{10}\left(10^{\frac{16}{10}} + 10^{\frac{16}{10}} + 10^{\frac{16}{10}} + 10^{\frac{16}{10}} + 10^{\frac{16}{10}} + 10^{\frac{8}{10}} + 10^{\frac{8}{10}} + 10^{\frac{16}{10}} + 10^{\frac{16}{10}} + 10^{\frac{16}{10}} + 10^{\frac{4}{10}}\right) \cong 25.2 \quad \text{(XXIV)}$$

$$T2.66_{likelihood\,rel} = \frac{10.5}{25.2} \times 100 \cong 41\,\% \quad \text{(XXV)}$$

Because threat likelihoods are generalized representations of threat-specific protection criteria exposures without any user-specific weights, or differentiation between affected protection criteria, the results of this layer are not visualized and only stored for evidence.

Although not required for visualization, the normalizations for a threat's current and maximum likelihood are calculated based on the current threat exposure weight as shown in (45) and (46).

$$T_{nlikelihood} := T_{likelihood} \times T_{exposure\,nweight} \quad (45)$$

$$T_{nlikelihood\,max} := T_{likelihood\,max} \times T_{exposure\,nweight} \quad (46)$$

Because IT-Grundschutz is based on generalized threats that are mitigated to an acceptable level if all safeguards are as mature as required, there is essentially no need for the user to estimate the threat likelihoods himself. The user can, however, modify and adapt the threat protection criteria influences to in- or decrease the threat exposure for each protection criterion individually to match the environment.

This can also be achieved using inferring threat indicators. The estimated in- or decrease of the threat's protection criteria influence weights is done within the following section.

4.2.1.3 Protection Criteria Influences / Exposures

Because the IT-Grundschutz methodology was not intended to assess protection criteria risks, no pre-established relations between threats and the influenced protection criteria are available. These relations have been defined for the primary protection requirements assessed in information security – confidentiality, integrity and availability – by a team of information security experts at SEC Consult.

This example shows overarching threats that can potentially influence any of the basic information security protection criteria. These relations have been predefined at the threat level by a team of information security experts and can be extended and modified. The relations can be user-weighted for every threat instantiation contained in the risk model and default to one.

The results of the example are outlined in Figure 55. Depending on the protection criteria influences, every threat can be user-weighted specifically for any of the influ-

enced protection criteria, depending on the desired evaluation depth. This example uses specific weightings to express elevated protection criteria influences for threats, which leads to an increased estimation of threat likelihood when cross-referenced mitigating safeguards show gaps to the desired targets.

	Potential protection criteria influences		
Threats	Confidentiality	Integrity	Availability
T 2.66 Lack of or inadequate IT Security Management	X (1)	X (1)	X (1)
T 2.105 Violation of statutory regulations and contractual agreements	X (1)	X (1)	X (1)
T 2.106 Disturbance to business processes as a result of IT security incidents	X (1)	X (1)	X (1)
T 2.107 Uneconomic use of resources as a result of an inadequate IT Security Management	X (1)	X (1)	X (1)

Figure 54: Threats and the protection criteria they potentially influence

	Likelihood			Potential protection criteria exposures		
Threats	Value	Max.	%	Confidentiality	Integrity	Availability
T 2.66 Lack of or inadequate IT Security Management	10.5	25.2	41	1.2	1	1.2
T 2.105 Violation of statutory regulations and contractual agreements	12.6	21.0	60	1	1	1
T 2.106 Disturbance to business processes as a result of IT security incidents	5.8	19.5	30	1	1.1	1.2
T 2.107 Uneconomic use of resources as a result of an inadequate IT Security Management	11.0	22.1	50	1	1	1

Figure 55: User-defined weightings $T_{pc\ exposure\ weight}$ for every potentially influenced protection criterion

The protection criteria exposures $T_{pc\ exposure}$ of any threat are based on the underlying threat likelihood $T_{likelihood}$, the user-adaptable weight $T_{pc\ exposure\ weight}$ and the potential exposure influence $T_{pc\ exposure\ inference}$, supplied by the expert system (47).

$$T_{pc\ exposure} := T_{likelihood} \times \left(T_{pc\ exposure\ weight} + T_{pc\ exposure\ influence}\right) \quad (47)$$

The influence field $T_{pc\ exposure\ inference}$ is updated by the integrated expert system in the interval [0, 2][12], in order to in- or decrease $T_{pc\ exposure}$ if related security measurement indicators are activated. Exposure influence is only performed until the respective maximum exposure is reached (48).

$$T_{pc\ exposure} := T_{pc\ exposure\ max}, T_{pc\ exposure} > T_{pc\ exposure\ max} \quad (48)$$

Inference is only performed to increase the current level, so that the maximum threat exposures remain unchanged. However, each maximum exposure (49) is adaptable using $T_{pc\ exposure\ weight}$ in order to be able to reflect the organization-specific environment.
Again, to support a relative view on protection criteria exposures of threats, the proposed model keeps track of the maximum of all variables, estimated upon the respective worst case scenario.

$$T_{pc\ exposure\ max} := T_{likelihood\ max} \times T_{pc\ exposure\ weight} \quad (49)$$

$$T_{pc\ exposure\ rel} := \begin{cases} \frac{T_{pc\ exposure}}{T_{pc\ exposure\ max}} \times 100, T_{pc\ exposure\ max} > 0 \\ 0 \qquad\qquad\qquad\quad , otherwise \end{cases} \quad (50)$$

Continuing the example shown in Figure 55, the threat's confidentiality exposure is estimated in (XXVI), its maximum in (XXVII) and its relative value in (XXVIII). The example assumes all security measurement influences ($T_{pc\ exposure\ influence}$) to be zero. The results for the remaining threats and their protection criteria exposures are outlined in Figure 56.

[12] The interval [0, 2] has been chosen to allow threat indicators to maximally double any remaining threat protection criteria exposure. If required by the user, this scale can be adapted to allow higher influences.

$$T2.66_{confidentiality\ exposure} = 10.5 \times (1.2 + 0) \cong 12.6 \quad \text{(XXVI)}$$

$$T2.66_{confidentiality\ exposure\ max} = 25.2 \times 1.2 \cong 30.3 \quad \text{(XXVII)}$$

$$T2.66_{confidentiality\ exposure\ rel} = \frac{12.6}{30.3} \times 100 \cong 41\ \% \quad \text{(XXVIII)}$$

Threats	Likelihood			Potential protection criteria influence								
				Confidentiality			Integrity			Availability		
	Value	Max.	%	Value	Max.	%	Value	Max.	%	Value	Max.	%
T 2.66 Lack of or inadequate IT Security Management	10.5	25.2	41	12.6	30.3	41	10.5	25.2	41	12.6	30.3	41
T 2.105 Violation of statutory regulations and contractual agreements	12.6	21.0	60	12.6	21.0	60	12.6	21.0	60	12.6	21.0	60
T 2.106 Disturbance to business processes as a result of IT security incidents	5.8	19.5	30	5.8	19.5	30	6.3	21.4	30	6.9	23.4	30
T 2.107 Uneconomic use of resources as a result of an inadequate IT Security Management	11.0	22.1	50	11.0	22.1	50	11.0	22.1	50	11.0	22.1	50

Figure 56: Adaption of protection criteria influence weightings for threat likelihoods

The normalizations for a threat's current- and maximum protection criterion exposure are calculated based on the current threat exposure weight (33) as shown in (51) and (52).

$$T_{pc\ nexposure} := T_{pc\ exposure} \times T_{exposure\ nweight} \quad (51)$$

$$T_{pc\ nexposure\ max} := T_{pc\ exposure\ max} \times T_{exposure\ nweight} \quad (52)$$

Based on the example's threat exposure normalization weight shown in (XIV), the current normalized threat confidentiality exposure is given in (XXIX) and its respective maximum in (XXX). The results for the remaining threats of Figure 56 are shown in Figure 57.

$$T2.66_{confidentiality\ nexposure} = 10.5 \times 1.2 \cong 4.2 \quad \text{(XXIX)}$$

$$T2.66_{confidentiality\ nexposure\ max} = 25.2 \times 1.2 = 10 \quad \text{(XXX)}$$

Threats	Normalized likelihood			Normalized potential protection criteria influences								
				Confidentiality			Integrity			Availability		
	Value	Max.	%	Value	Max.	%	Value	Max.	%	Value	Max.	%
T 2.66 Lack of or inadequate IT Security Management	3.5	8.3	41	4.2	10.0	41	3.5	8.3	41	4.2	10.0	41
T 2.105 Violation of statutory regulations and contractual agreements	4.2	6.9	60	4.2	6.9	60	4.2	6.9	60	4.2	6.9	60
T 2.106 Disturbance to business processes as a result of IT security incidents	1.9	6.4	30	1.9	6.4	30	2.1	7.1	30	2.3	7.7	30
T 2.107 Uneconomic use of resources as a result of an inadequate IT Security Management	3.6	7.3	50	3.6	7.3	50	3.6	7.3	50	3.6	7.3	50

Figure 57: Visualization of normalized protection criteria influences for threat likelihoods using the current threat normalization weight.

4.2.1.4 Module Protection Criteria Exposures and Overall Exposure

The module protection criterion exposure $M_{pc\ exposure}$ estimates the total exposure that all *n* influencing threats pose on the specific protection criterion (53). Each module protection criterion can be user-weighted using $M_{pc\ weight}$ to adjust the estimation to the organizational context. At this layer, specific protection criteria can be adapted by the user more generically than with specific threat protection criteria weightings. It is assumed that the same aggregation procedure that has been applied to threat likelihoods can be applied when estimating protection criteria exposures, because they represent a derived generalization.

In (53), $I = \{\, i \mid 1 \leq i \leq n \wedge T_{pc\ exposure_i} > 0\}$, where n is the number of threats that the protection criterion is influenced by.

$$M_{pc\ exposure} := \begin{cases} 10 \times \log_{10}\left(\sum_{i \in I} 10^{\frac{T_{pc\ exposure_i}}{10}}\right) \times M_{pc\ weight}, I \neq \emptyset \\ 0 \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad , otherwise \end{cases} \tag{53}$$

As before, to support a relative view on protection criteria exposures of modules and their overall exposures, the proposed model keeps track of the maxima of all variables, estimated upon the respective worst case scenario, as shown in (54) and (55).

In (54), $I = \{\, i \mid 1 \leq i \leq n \wedge T_{pc\ exposure\ max_i} > 0\}$, where n is the number of threats that the protection criterion is influenced by.

$$M_{pc\ exposure\ max} := \begin{cases} 10 \times \log_{10}\left(\sum_{i \in I} 10^{\frac{T_{pc\ exposure\ max_i}}{10}}\right) \times M_{pc\ weight}, I \neq \emptyset \\ 0 \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad , otherwise \end{cases} \tag{54}$$

$$M_{pc\ exposure\ rel} := \begin{cases} \frac{M_{pc\ exposure}}{M_{pc\ exposure\ max}} \times 100, M_{pc\ exposure\ max} > 0 \\ 0 \qquad\qquad\qquad\qquad\qquad\qquad\qquad , otherwise \end{cases} \tag{55}$$

The module inherits all basic protection criteria (confidentiality, integrity, availability) from its threats. The respective exposures are calculated based on the energetic sum of their weighted threat protection criteria exposures.

The estimation of the overall exposure of the module can be done using maximum, sum, average or energetic sum of the individual protection criteria exposures, depending on their relation and interaction. The module overall exposure is only estimated as a local reference for the module and is not used for further derivation of asset exposure (only specific protection criteria exposures are used). To achieve a consistent cautious view on overall exposures, the proposed model uses the energetic sum by default to estimate the overall exposure $M_{overall\ exposure}$ based on all n protection criteria exposures $M_{pc\ exposure}$ of the module (56). Maximum and relative values are estimated based on (57) and (58).

In (56), $I = \{\, i \mid 1 \leq i \leq n \wedge M_{pc\ exposure_i} > 0\}$, where n is the number of protection criteria that the module is influenced by.

$$M_{overall\ exposure} := \begin{cases} 10 \times \log_{10}\left(\sum_{i \in I} 10^{\frac{M_{pc\ exposure_i}}{10}}\right), I \neq \emptyset \\ 0 \qquad\qquad\qquad\qquad\qquad\qquad\qquad , otherwise \end{cases} \tag{56}$$

In (57), $I = \{\, i \mid 1 \leq i \leq n \wedge M_{pc\ exposure\ max_i} > 0\}$, where n is the number of protection criteria that the module is influencing.

$$M_{overall\ exposure\ max} := \begin{cases} 10 \times \log_{10}\left(\sum_{i \in I} 10^{\frac{M_{pc\ exposure\ max_i}}{10}}\right), I \neq \emptyset \\ 0 \qquad\qquad\qquad\qquad\qquad\qquad\qquad , otherwise \end{cases} \tag{57}$$

$$M_{overall\ exposure\ rel} := \begin{cases} \frac{M_{overall\ exposure}}{M_{overall\ exposure\ max}} \times 100, M_{overall\ exposure\ max} > 0 \\ 0 \qquad\qquad\qquad\qquad , otherwise \end{cases} \quad (58)$$

Continuing the illustrated example, the current, maximum and relative confidentiality exposure of the module is estimated as shown in (XXXI), (XXXII) and (XXXIII).

$$M1.0_{confidentiality\ exposure} = 10 \times \log_{10}\left(10^{\frac{12.6}{10}} + 10^{\frac{12.6}{10}} + 10^{\frac{5.8}{10}} + 10^{\frac{11.0}{10}}\right) \cong 17.2 \quad \text{(XXXI)}$$

$$M1.0_{\ confidentiality\ exposure\ max} = 10 \times \log_{10}\left(10^{\frac{30.3}{10}} + 10^{\frac{21.0}{10}} + 10^{\frac{19.5}{10}} + 10^{\frac{22.1}{10}}\right) \cong 31.6 \quad \text{(XXXII)}$$

$$M1.0_{\ confidentiality\ exposure\ rel} = \frac{17.6}{35.6} \times 100 \cong 48\% \quad \text{(XXXIII)}$$

The estimated exposures are normalized for visualization with the current maximum module protection criterion exposure of the risk model as calculated in (30). The normalized module protection criterion exposure $M_{pc\ nexposure}$ is estimated based on (59), its potential maximum $M_{pc\ nexposure\ max}$ as shown in (60).

$$M_{pc\ nexposure} := M_{pc\ exposure} \times M_{exposure\ nweight} \quad (59)$$

$$M_{pc\ nexposure\ max} := M_{pc\ exposure\ max} \times M_{exposure\ nweight} \quad (60)$$

The normalized confidentiality exposure for the illustrated example of the module *M 1.0 Security Management* is estimated based on the current normalization weight (X) as shown in (XXXIV) and its maximum in (XXXV). Remaining protection criterion exposures are shown in Figure 58.

$$M1.0_{confidentiality\ nexposure} = 17.2 \times 0.26315789 \cong 4.5 \quad \text{(XXXIV)}$$

$$M1.0_{\ confidentiality\ nexposure\ max} = 31.6 \times 0.26315789 \cong 8.3 \quad \text{(XXXV)}$$

Module 1.0 Security Management	Weighting	Value	Max.	Normalized value	Normalized max.	%
Confidentiality exposure	1	17.2	31.6	4.5	8.3	54
Integrity exposure	1	16.7	28.8	4.4	7.6	58
Availability exposure	1	17.3	32.0	4.6	8.4	54
Overall exposure	-	21.8	35.8	5.7	9.4	61

Figure 58: User-definable protection criteria weightings for modules and their aggregated protection criteria exposures and their normalized variants using the current module exposure normalization weight.

The proposed model allows for the representation of multiple modules within a single asset, to allow the grouping of module aspects. To enable this, each asset defines a module aggregation function in the same manner that defines how to aggregate the module's protection criteria exposures.

4.2.1.5 Asset Base Protection Criteria Exposures and Overall Exposure

The first step at the asset layer is the aggregation of all of the asset's module exposures, providing a temporary asset base exposure. This base exposure is necessary, in order to estimate the exposures that are inherent to the asset's modules without taking exposures from dependent assets into account. The final asset exposure and related risk is estimated later within scenario analysis (for slave assets) and joint analysis (for master assets).

The asset base exposure for each protection criterion $AB_{pc\ exposure}$ is estimated based on all n module protection criterion exposures $M_{pc\ exposure}$ of the asset and a user-specific asset base protection criterion weight $AB_{pc\ weight}$ (61). Maximum and relative values are calculated in (62) and (63) according to the same principle as before.

It is also possible for an asset to have no modules assigned, either to act as a grouping element for dependent assets, or because an appropriate module has not been created yet. In that case, asset base protection criteria exposures do not exist.

In (61), $I = \{ i \mid 1 \leq i \leq n \wedge M_{pc\ exposure_i} > 0 \}$, where n is the number of modules that the protection criterion is influenced by.

$$AB_{pc\ exposure} := \begin{cases} 10 \times \log_{10}\left(\sum_{i \in I} 10^{\frac{M_{pc\ exposure_i}}{10}}\right) \times AB_{pc\ weight}, I \neq \emptyset \\ 0 \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad , otherwise \end{cases} \tag{61}$$

In (62), $I = \{ i \mid 1 \leq i \leq n \wedge M_{pc\ exposure_i} > 0 \}$, where n is the number of modules that the protection criterion is influenced by.

$$AB_{pc\ exposure\ max} := \begin{cases} 10 \times \log_{10}\left(\sum_{i \in I} 10^{\frac{M_{pc\ exposure\ max_i}}{10}}\right) \times AB_{pc\ weight}, I \neq \emptyset \\ 0 \quad , otherwise \end{cases} \tag{62}$$

$$AB_{pc\ exposure\ rel} := \begin{cases} \frac{AB_{pc\ exposure}}{AB_{pc\ exposure\ max}} \times 100, AB_{pc\ exposure\ max} > 0 \\ 0 \quad , otherwise \end{cases} \tag{63}$$

Similar to the module layer, the estimation of the overall exposure of the asset can be done using maximum, sum, average or energetic sum of the individual protection criteria risks, depending on the organizational requirements. To achieve a consistent cautious view on risks, the proposed model uses the energetic sum by default to estimate the asset overall exposure in (64), its potential maximum in (65) and its relative value in (66).

In (64), $I = \{ i \mid 1 \leq i \leq n \land AB_{pc\ exposure_i} > 0\}$, where *n* is the number of protection criteria the asset base is influenced by.

$$AB_{overall\ exposure} := \begin{cases} 10 \times \log_{10}\left(\sum_{i \in I} 10^{\frac{AB_{pc\ exposure_i}}{10}}\right), I \neq \emptyset \\ 0 \quad , otherwise \end{cases} \tag{64}$$

In (65), $I = \{ i \mid 1 \leq i \leq n \land AB_{pc\ exposure_i} > 0\}$, where *n* is the number of protection criteria the asset base is influenced by.

$$AB_{overall\ exposure\ max} := \begin{cases} 10 \times \log_{10}\left(\sum_{i \in I} 10^{\frac{AB_{pc\ exposure\ max_i}}{10}}\right), I \neq \emptyset \\ 0 \quad , otherwise \end{cases} \tag{65}$$

$$AB_{overall\ exposure\ rel} := \begin{cases} \frac{AB_{overall\ exposure}}{AB_{overall\ exposure\ max}} \times 100, AB_{overall\ exposure\ max} > 0 \\ 0 \quad , otherwise \end{cases} \tag{66}$$

Because during the subsequent steps, the focus lies on the inheritance of exposures (protection criteria impacts of slave assets represent the protection criteria requirement levels inherited through BIA in the opposite direction), the respective risk (risk = impact * exposure) is only calculated when presented to the user. This allows for a separate storage of exposure values and impact values, in order to access exposure levels for inheritance operations directly and without de-normalization.

Depending on the types of modules that are consolidated within the asset, the aggregation function should be one of the following:

1. Energetic sum: If most of the underlying safeguards and threats are shared, the estimation should be based on the energetic sum, which takes parallel sources into account.
2. Sum aggregation: The asset base exposure should be estimated based on the sum of the modules, if the modules predominantly represent different scopes of threats and safeguards.

The estimated exposures are normalized for visualization with the current maximum asset protection criterion exposure of the risk model as calculated in (28). The normalized asset protection criterion exposure $A_{pc\ nexposure}$ is estimated based on (67), its potential maximum $A_{pc\ nexposure\ max}$ as shown in (68).

$$AB_{pc\ nexposure} := AB_{pc\ exposure} \times A_{exposure\ nweight} \tag{67}$$

$$AB_{pc\ \ nexposure\ max} := AB_{pc\ \ exposure\ max} \times A_{exposure\ nweight} \tag{68}$$

As the basic principle of aggregation has been presented, the example is simplified by using no additional module within the asset *IS Management*. The estimated exposures are again normalized in (XXXVI) and (XXXVII) for visualization with the current maximum asset protection criterion exposure of the risk model, as identified in (VIII). Therefore, only the normalized values in Figure 59 differ from the ones in Figure 58.

$$IS\ Management\ (Base)_{\ confidentiality\ nexposure} = 17.2 \times 0.07092199 \cong 1.2 \tag{XXXVI}$$

$$IS\ Management\ (Base)_{\ confidentiality\ nexposure\ max} = 31.6 \times 0.07092199 \cong 2.2 \tag{XXXVII}$$

Asset (Base) IS Management	Weighting	Value	Max.	Normalized value	Normalized max.	%
Confidentiality exposure	1	17.2	31.6	1.2	2.2	54
Integrity exposure	1	16.7	28.8	1.2	2.0	58
Availability exposure	1	17.3	32.0	1.2	2.3	54
Overall exposure	-	21.8	35.8	1.5	2.5	61

Figure 59: User-definable protection criteria weightings for assets and their aggregated protection criteria exposures, normalized using the current asset exposure normalization weight

4.2.1.6 Scenario Analysis

Scenario analysis handles the aggregation of asset base exposures with the exposures that result from dependent assets. The estimation procedure starts with the leaf assets of the scenario trees (asset slaves without children). For all asset leafs, the asset base exposures can be directly used as asset exposures, because they won't inherit any dependency exposure.

$$A_{pc\ exposure} := AB_{pc\ exposure}, A_{number\ of\ children} = 0 \tag{69}$$

After each asset leaf has saved its new estimation values, it flags itself as calculated (for this round) and initiates the inheritance procedure of the parent asset. As soon as all of the parent's child assets have been flagged as calculated, the parent asset repeats this inheritance procedure until the root of the scenario tree has been reached.

During BIA, the protection criteria requirement levels (impacts) of dependent assets are established based on the organizational environment. Child assets inherit the protection criteria requirement levels of their parents (maximum principle), unless the child asset provides some kind of compensation (e.g. if a process with high availability requirements is dependent on multiple IT systems, the process may sustain the non-availability of some of these IT systems for a longer period of time, resulting in lowered estimated availability impacts for the IT systems within the scenario) [cp. 47; p. 47ff]. If the results of the BIA show that a specific protection criterion requirement of a child asset is negligible (0) within the scenario, the inheritance of this protection criterion exposure is inhibited for that child asset (e.g. a process needs multiple IT systems, but is not affected by the confidentiality exposure of one specific IT system).

As a result of testing and evaluation, the proposed model assumes that the aggregation of child exposures depends on the relation of their respective impacts with the estimated impact of the parent asset. To put special focus on the impact factor, the proposed method uses an aggregation function that automatically weights the protection criterion exposure of child assets $Child\ of\ A_{pc\ impact}$ relative to the respective estimated impact $A_{pc\ impact}$ of the parent asset. This leads to a lowered incorporation of child asset protection criteria exposures, if the scenario-dependent requirement level is lower than the estimated parent asset requirement level ($Child\ of\ A_{pc\ impact} < A_{pc\ impact}$). This is justified by the practical situation that an enterprise usually leads to prioritize strategies that deal with the highest estimated impacts.

$$CA_{pc\ impact\ relation} := \begin{cases} \frac{Child\ of\ A_{pc\ impact}}{A_{pc\ impact}}, A_{pc\ impact} > 0 \wedge Child\ of\ A_{pc\ impact} < A_{pc\ impact}{}^{13} \\ 0 \qquad\qquad\qquad\quad , otherwise \end{cases} \quad (70)$$

The aggregation function used for inheritance between parent asset base exposure $AB_{pc\ exposure}$ and the respective exposure $CA_{pc\ exposure}$ of n child assets depends on the component behavior that should be modeled. The result $A_{pc\ exposure}$ depicts the estimated current-, maximum- and relative mutual attack vector of the parent asset and its dependent assets in (71), (72) and (73).

The proposed model uses the energetic sum as a default aggregation function, in order to provide risk-averse insight into the increased exposure resulting from dependent assets. The children's exposures that are aggregated using the energetic sum are weighted using $CA_{pc\ impact\ relation}$ in order to lower the inherited exposure if the respective asset has lower protection criteria requirements for this scenario.

In (71), $I = \{ i \mid 1 \leq i \leq n \wedge CA_{pc\ exposure_i} > 0 \wedge CA_{pc\ impact\ relation_i} > 0 \}$, where n is the number of child assets that the protection criterion is influenced by.

[13] The protection criteria requirement levels of child assets are never higher than the protection criteria requirement of the parent asset, because the cumulating effect on requirements (as outlined in 3.1.2.1) does not need to be assessed for the scenario. The cumulative effect is established later during joint analysis by aggregating the protection criteria impacts of all asset-representations within the scenarios.

$$A_{pc\ exposure} := \begin{cases} 10 \times \log_{10}\left(10^{\frac{AB_{pc\ exposure}}{10}} + \sum_{i \in I} 10^{\frac{CA_{pc\ exposure_i} \times CA_{pc\ impact\ relation_i}}{10}}\right), \\ \qquad AB_{pc\ exposure} > 0 \\ 10 \times \log_{10}\left(\sum_{i \in I} 10^{\frac{CA_{pc\ exposure_i} \times CA_{pc\ impact\ relation_i}}{10}}\right), \\ \qquad I \neq \emptyset \ \wedge AB_{pc\ exposure} = 0 \\ 0 \qquad ,otherwise \end{cases} \tag{71}$$

In (72), $I = \{\, i \mid 1 \leq i \leq n \ \wedge\ CA_{pc\ exposure_i} > 0 \wedge CA_{pc\ impact\ relation_i} > 0\}$, where *n* is the number of child assets that the protection criterion is influenced by.

$$A_{pc\ exposure\ max} := \begin{cases} 10 \times \log_{10}\left(10^{\frac{AB_{pc\ exposure\ max}}{10}} + \sum_{i \in I} 10^{\frac{CA_{pc\ exposure\ max_i} \times CA_{pc\ impact\ relation_i}}{10}}\right), \\ \qquad AB_{pc\ exposure\ max} > 0 \\ 10 \times \log_{10}\left(\sum_{i \in I} 10^{\frac{CA_{pc\ exposure\ max_i} \times CA_{pc\ impact\ relation_i}}{10}}\right), \\ \qquad I \neq \emptyset \wedge AB_{pc\ exposure\ max} = 0 \\ 0 \qquad ,otherwise \end{cases} \tag{72}$$

$$A_{pc\ exposure\ rel} = \begin{cases} \frac{A_{pc\ exposure}}{A_{pc\ exposure\ max}} \times 100, A_{pc\ exposure\ max} > 0 \\ 0 \qquad ,otherwise \end{cases} \tag{73}$$

As this type of aggregation is suited to estimate the combined effect of overlapping risks, it should ideally be used to inherit risks between assets that share most of their threats. All asset exposures depicting non-overlapping aspects (e.g. applications as well as generic aspects, as shown in in Figure 61) should be added using the sum operation in order to provide a worst-case estimation of different attack vectors.

However, because the protection criteria exposures at the asset level are generalized depictions of threats that can potentially interfere with the protection criteria, they may be treated as overlapping aspects, in order to emphasize the risk-averse estimation of relative risks provided by the energetic sum. Also, the energetic sum may also be used to aggregate correlated aspects at an earlier stage, in order to minimize the required initial modeling workload. Due to the fact that maximum exposures are estimated too, changes to the aggregation function (at a later stage) are made transparent.

Other aggregations functions and their assumed applicability for the estimation of specific behavior between components have been outlined in 2.3.1.2 and 3.1.2.1.

The asset current- and maximum protection criterion exposure is normalized as shown in (74) and (75) using the maximum asset exposure identified in (28).

$$A_{pc\ nexposure} = A_{pc\ exposure} \times A_{exposure\ nweight} \tag{74}$$

$$A_{pc\ nexposure\ max} = A_{pc\ exposure\ max} \times A_{exposure\ nweight} \tag{75}$$

To provide an easy way of defining relative dependencies between parent and child asset protection criteria, each criterion can be marked as a "knock-out"-criterion ($Asset_{pc\ knockout} = true$). This increases the estimation of the parent protection criterion exposure to the *relative* level of the protection criterion exposure of the child asset, providing inheritance based on the *relative* weakest link instead of the *absolute* weakest link.

This allows the more cautious inheritance of relative criteria exposures between dependent assets, so that a parent's asset protection criterion risk is increased to the relative protection criterion risk of its child (76).

$$\begin{aligned} &A_{pc\ exposure} := A_{pc\ exposure\ max} \times\ Child\ of\ A_{pc\ exposure\ rel}, \\ &Child\ of\ A_{pc\ knockout} = true\ \wedge\ Child\ of\ A_{pc\ exposure\ rel} > A_{pc\ exposure\ rel} \end{aligned} \tag{76}$$

This type of inheritance can be used to depict dependencies between parent and child assets in a relative worst-case scenario. If a highly complex, but also highly mature parent asset (e.g. a manually defined process with low relative exposure) is fully dependent on a low complexity, immature asset (e.g. answering machine with a high relative exposure), this type of aggregation can be used to provide a worst-case estimation for the parent asset based on the relative achievement of maturity targets of the child assets.

In order to provide a point of inference for the expert system to influence impact factors, the respective user-defined impact value (non-normalized, e.g. 40.000 €) is increased by the impact indicator (77).

The impact influence field $A_{pc\ impact\ influence}$ therefore uses a scale that is aligned with the current user-defined impact scale maximum. This allows protection criteria impact indicators to transparently describe the user-defined amount of potentially increased impact.

Because related measure indicators are designed to describe elevated risks (in relation to the current situation), influence is only performed to increase the current, subjectively estimated impact for each protection criterion, in order to maintain the worst-case estimation (for the current situation) (77).

Impact influence is only performed up to the respective maximum impact defined for each protection criterion, in order to comply with normalization requirements for the impact scale (78).

$$A_{influenced\ pc\ impact} := A_{pc\ impact} + A_{pc\ impact\ influence} \tag{77}$$

$$A_{influenced\ pc\ impact} := A_{pc\ impact\ max}, \quad A_{influenced\ pc\ impact} > A_{pc\ impact\ scale\ max} \tag{78}$$

Protection criterion risk $A_{pc\ risk}$ of an asset is estimated for each protection criterion by multiplication of respective exposure $A_{pc\ exposure}$ and (influenced) impact $A_{influenced\ pc\ impact}$ as shown in (79).

$$A_{pc\ risk} := A_{pc\ exposure} \times A_{influenced\ pc\ impact} \tag{79}$$

The relative protection criteria risk is established based on the potential maximum exposure of the protection criterion and the currently estimated influenced impact as shown in (80) and (81). Because the influenced impact also increases the maximum risk, the relative residual risk remains unchanged and only the normalized risk increases. This is because the residual attack vector (exposure) is equal in both situations, so only the estimated current and maximum impact is increased by the influence.

A protection criterion impact of an asset already assigned with the highest estimated impact defined for a particular impact scale can therefore not be increased, because this could result in normalized risks greater than the maximum scale of 100. If impact indicators show increased risk on assets with maximum protection criteria requirements (e.g. critical), the respective asset owners should be immediately informed by system message/email, preferably in case the respective exposure is above a user-defined threshold (increased impact on an asset with low exposure is not as time-critical as if it had high exposure).

$$A_{pc\ risk\ max} := A_{pc\ exposure\ max} \times A_{influenced\ pc\ impact} \tag{80}$$

$$A_{pc\ risk\ rel} := \begin{cases} \frac{A_{pc\ risk}}{A_{pc\ risk\ max}} \times 100, A_{pc\ risk\ max} > 0 \\ 0 \qquad\qquad\qquad , otherwise \end{cases} \tag{81}$$

Influenced impact and risk of each protection criterion are also normalized as shown in (82), (83) and (84). The normalized relative protection criterion risk is established based on the maximum risk possible within the risk model as shown in (85).

$$A_{influenced\ pc\ nimpact} := A_{influenced\ pc\ impact} \times A_{impact\ nweight} \tag{82}$$

$$A_{pc\ nrisk} := A_{pc\ nexposure} \times A_{influenced\ pc\ nimpact} \tag{83}$$

$$A_{pc\ nrisk\ max} := A_{pc\ nexposure\ max} \times A_{influenced\ pc\ nimpact} \tag{84}$$

$$A_{pc\ nrisk\ rel} := \begin{cases} \dfrac{A_{pc\ nrisk}}{A_{exposure\ scale\ max} \times A_{impact\ scale\ max}} \times 100, & A_{exposure\ scale\ max} > 0 \wedge A_{impact\ scale\ max} > 0 \\ 0 & , otherwise \end{cases} \tag{85}$$

Estimation of the overall risk of the asset can be done using maximum, sum, average or energetic sum of the individual protection criteria exposures, depending on the organizational requirements and preferences. To achieve a consistent cautious view on residual attack vectors and associated risks, the proposed model uses the energetic sum by default to estimate the asset overall risk.

In order to not interfere with the estimated impacts, the overall impact $A_{overall\ impact}$ is established based on the maximum of m (influenced) protection criteria impacts $A_{influenced\ pc\ impact}$ of the asset (86), while the overall protection criterion exposure $A_{overall\ exposure}$ is aggregated based on the corresponding n protection criteria exposures $A_{pc\ expsoure}$ using the energetic sum (87). This is done in order to provide cautious overall estimation of residual attack vectors, without a potential overall decrease of protection criteria risks if an energetically estimated overall impact would create a new maximum impact (during impact normalization).

In (86), $I = \{ i \mid 1 \le i \le n \}$, where n is the number of (influenced) protection criteria of the asset.

$$A_{overall\ impact} := \max_{i \in I}\left(A_{influenced\ pc\ impact_i}\right) \tag{86}$$

In (87), $I = \{ i \mid 1 \le i \le n \wedge CA_{pc\ exposure_i} > 0 \wedge CA_{pc\ impact\ relation_i} > 0\}$, where n is the number of protection criteria the asset is influenced by.

$$A_{overall\ exposure} := \begin{cases} 10 \times \log_{10}\left(\sum_{i \in I} 10^{\frac{A_{pc\ exposure_i}}{10}}\right), & I \neq \emptyset \\ 0 & , otherwise \end{cases} \tag{87}$$

Again, in order to provide a relative view of residual attack vectors, the potential maximum and relative overall exposure are estimated based on the respective worst case scenario as shown in (88) and (89).

In (88), $I = \{ i \mid 1 \le i \le n \wedge CA_{pc\ exposure\ max_i} > 0 \wedge CA_{pc\ impact\ relation\ max_i} > 0\}$, where n is the number of protection criteria the asset is influenced by.

$$A_{overall\ exposure\ max} := \begin{cases} 10 \times \log_{10}\left(\sum_{i \in I} 10^{\frac{A_{pc\ exposure\ max_i}}{10}}\right), I \neq \emptyset \\ 0 \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad , otherwise \end{cases} \tag{88}$$

$$A_{overall\ exposure\ rel} := \begin{cases} \frac{A_{overall\ exposure}}{A_{overall\ exposure\ max}} \times 100, A_{overall\ exposure\ max} > 0 \\ 0 \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad , otherwise \end{cases} \tag{89}$$

The normalized overall exposure $A_{overall\ nexposure}$ is calculated using the asset's overall exposure $A_{overall\ exposure}$ and the current exposure normalization weight $A_{exposure\ nweight}$ (90). The respective normalized maximum exposure is based on the potential maximum overall impact $A_{overall\ impact}$ (91).

$$A_{overall\ nexposure} := A_{overall\ exposure} \times A_{exposure\ nweight} \tag{90}$$

$$A_{overall\ nexposure\ max} := A_{overall\ exposure\ max} \times A_{exposure\ nweight} \tag{91}$$

The normalized overall impact $A_{overall\ nimpact}$ for an asset is estimated based on the overall impact $A_{overall\ impact}$ and the current impact normalization weight $A_{impact\ nweight}$ as shown in (92).

$$A_{overall\ nimpact} = A_{overall\ impact} \times A_{impact\ nweight} \tag{92}$$

Finally, the normalized overall risk $A_{overall\ nrisk}$ of an asset can be estimated based on the normalized overall values of exposure $A_{overall\ nexposure}$ and pact $A_{overall\ nimpact}$ (93). The respective normalized maximum overall risk $A_{overall\ nrisk\ max}$ is based on the respective normalized maximum overall sure $A_{overall\ nexposure\ max}$ (94). Because the risk normalization is dependent on the user-defined scale, the relative normalized overall risk $A_{overall\ nrisk\ rel}$ is calculated based on the potential maximum risk scale, which is given by multiplication of the maximum impact scale $A_{impact\ scale\ max}$ and the maximum exposure scale $A_{exposure\ scale\ max}$ of the risk model (95).

$$A_{overall\ nrisk} := A_{overall\ nexposure} \times A_{overall\ nimpact} \tag{93}$$

$$A_{overall\ nrisk\ max} := A_{overall\ nexposure\ max} \times A_{overall\ nimpact} \tag{94}$$

$$A_{overall\ nrisk\ rel} := \begin{cases} \dfrac{A_{overall\ nrisk}}{A_{exposure\ scale\ max} \times A_{impact\ scale\ max}} \times 100, \\ \qquad A_{exposure\ scale\ max} > 0 \ \wedge A_{impact\ scale\ max} > 0 \\ 0 \qquad\qquad , \quad otherwise \end{cases} \tag{95}$$

The example shown in Figure 61 is based on the scenario tree subset shown in Figure 60.

The asset exposures of *IS Management* and two application assets *E-Mail* and *Active Directory* are inherited onto the asset base exposures of *Process Delivery* (see Figure 59), creating a final asset exposure and risk for the parent asset (see Figure 64).

Because the scenario trees are also used to inherit business impacts in the opposite direction (protection criteria requirement levels), the levels of dependency from specific components can be specified according to the organizational context (e.g. if a process (parent) is not affected by a loss of confidentiality of an IT system (child), the protection criteria can be marked "negligible (0)" for the scenario, resulting in a zero confidentiality risk for the child as well as the inhibited inheritance of the respective protection criterion exposure).

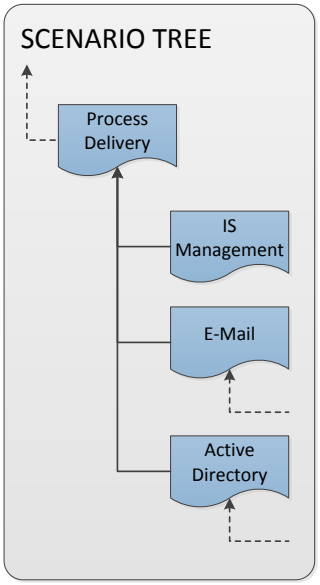


Figure 60: Example scenario tree subset

The example in Figure 61 assumes that the process *Delivery* can sustain the non-availability of the application *Active Directory* for up to one day, without significant problems to the overall process. This also means, that all components that *Active Directory* is dependent on, only need the lowered availability requirement level for this scenario. The example below assumes all impact inferences ($A_{pc\ impact\ influence}$) to be zero.

Asset (Parent) *Process Delivery*	Impact level (V/NV)	Asset base exposure					Asset base risk		
		V	M	NV	NM	%	NV	NM	%
Confidentiality	Confidential (25/6.25)	13.4	29.1	1.0	2.1	46	5.9	12.9	6
Integrity	Medium (25/6.25)	21.5	38.4	1.5	2.7	56	9.5	17.0	10
Availability	< 1 hour (40/10)	8.2	26.3	0.6	1.9	31	5.8	18.7	6
Overall	40/10	22.3	39.1	1.6	2.8	57	15.8	27.7	16

Asset (Child) *IS Management*	Impact level (V/NV)	Asset exposure					Asset risk		
		V	M	NV	NM	%	NV	NM	%
Confidentiality	Confidential (25/6.25)	17.2	31.6	1.2	2.2	54	7.6	14.0	8
Integrity	Medium (25/6.25)	16.7	28.8	1.2	2.0	58	7.4	12.8	7
Availability	< 1 hour (40/10)	17.3	32.0	1.2	2.3	54	12.3	22.7	12
Overall	40/10	21.8	35.8	1.5	2.5	61	15.5	25.4	15

Asset (Child) *E-Mail*	Impact level (V/NV)	Asset exposure					Asset risk		
		V	M	NV	NM	%	NV	NM	%
Confidentiality	Confidential (25/6.25)	34.2	45.7	2.4	3.2	75	15.2	20.3	15
Integrity	Medium (25/6.25)	12.7	48.2	0.9	3.4	26	5.6	21.4	6
Availability	< 1 hour (40/10)	14.2	45.4	1.0	3.2	31	10.1	32.2	10
Overall	40/10	34.3	51.4	2.4	3.6	67	24.3	36.5	24

Asset (Child) *Active Directory*	Impact level (V/NV)	Asset exposure					Asset risk		
		V	M	NV	NM	%	NV	NM	%
Confidentiality	Confidential (25/6.25)	24.6	38.4	1.7	2.7	64	10.9	17.0	11
Integrity	Medium (25/6.25)	31.2	42.5	2.2	3.0	73	13.8	18.8	14
Availability	< 1 day (30/7.5)	26.4	49.2	1.9	3.5	54	14.0	26.2	14
Overall	30/7.5	33.1	50.3	2.3	3.6	66	17.6	26.8	18

Figure 61: Scenario inheritance example of a process *Delivery*, which needs *IS Management* (Generic aspects), *E-Mail* and *Active Directory* (Applications). The inherited exposures of application-dependent components (IT systems, networks, rooms, buildings and users) have been omitted for readability reasons.

V…Value, M…Maximum value, NV…Normalized value,
NM…Normalized maximum value

$$Process\ Delivery_{availability\ exposure} = 10 \times \log_{10}\left(10^{\frac{8.2}{10}} + 10^{\frac{17.3\times\frac{40}{40}}{10}} + 10^{\frac{14.2\times\frac{40}{40}}{10}} + 10^{\frac{26.4\times\frac{30}{40}}{10}}\right) \cong 22.6 \quad \text{(XXXVIII)}$$

$$Process\ Delivery_{availability\ nexposure} = 22.6 \times \frac{10}{141} \cong 1.6 \quad \text{(XXXIX)}$$

$$Process\ Delivery_{availability\ exposure\ max} = 10 \times \log_{10}\left(10^{\frac{26.3}{10}} + 10^{\frac{32.0\times\frac{40}{40}}{10}} + 10^{\frac{45.4\times\frac{40}{40}}{10}} + 10^{\frac{49.2\times\frac{30}{40}}{10}}\right) \cong 45.6 \quad \text{(XL)}$$

$$Process\ Delivery_{availability\ exposure\ rel} = \frac{22.6}{45.6} \cong 50\ \% \quad \text{(XLI)}$$

$$Process\ Delivery_{influenced\ availability\ impact} = 40 + 0 \quad \text{(XLII)}$$

$$Process\ Delivery_{influenced\ availability\ nimpact} = 40 \times \frac{10}{40} = 10 \quad \text{(XLIII)}$$

$$Process\ Delivery_{availability\ nrisk} = 1.6 \times 10 \cong 16 \quad \text{(XLIV)}$$

$$Process\ Delivery_{availability\ nrisk\ max} = 3.2 \times 10 \cong 32.3 \quad \text{(XLV)}$$

$$Process\ Delivery_{availability\ nrisk\ rel} = \frac{1.6}{10 \times 10} \times 100 \cong 16\ \% \quad \text{(XLVI)}$$

Asset (Parent) *Process Delivery*	Impact level (V/NV)	Asset exposure					Asset risk		
		V	M	NV	NM	%	NV	NM	%
Confidentiality	Confidential (25/6.25)	34.8	46.7	2.5	3.3	75	15.4	20.7	15
Integrity	Medium (25/6.25)	31.8	49.6	2.3	3.5	64	14.1	22.0	14
Availability	< 1 hour (40/10)	22.6	45.6	1.6	3.2	50	16.0	32.3	16
Overall	40/10	36.7	52.4	2.6	3.7	70	26.0	37.2	26

Figure 62: Asset *Process Delivery* after scenario inheritance. The asset base exposure may be overwritten if the exposures from depending assets are estimated higher. However, the underlying exposures of the asset are still unchanged and provide insight into the exposures that arise from its modules.

4.2.1.7 Joint Analysis

In order to provide an estimation of the total protection criteria requirements for any asset, each (influenced) protection criterion requirement of the asset master $AM_{influenced\ pc\ impact}$ is estimated based on the maximum protection criteria requirements $AS_{influenced\ pc\ impact}$ of *n* asset slaves, used within different scenario trees.

In (96), $I = \{ i \mid 1 \leq i \leq n \}$, where *n* is the number of asset slaves.

$$AM_{influenced\ pc\ impact} = \max_{i \in I}\left(AS_{influenced\ pc\ impact_i}\right) \tag{96}$$

The proposed model assumes that the aggregation of exposures depends on the relation of their respective impacts with the estimated impact of the master asset (as outlined in 4.2.1.6). This leads to the lowered incorporation of slave asset protection criteria exposures, if the scenario-dependent requirement level is lower than the estimated asset master requirement level (97). It is irrelevant for the relation, if $AM_{influenced\ pc\ impact}$ is based on influenced or un-influenced impacts, because asset slave impacts are influenced equally (using the same asset representation), so their relation doesn't change. The variable $AM_{influenced\ pc\ impact}$ is used because it is required to estimate total protection criterion risk.

$$AS_{pc\ impact\ relation} := \begin{cases} \dfrac{AS_{influenced\ pc\ impact}}{AM_{influenced\ pc\ impact}}, AM_{influenced\ pc\ impact} > 0 \\ 0 \qquad\qquad\qquad\qquad , otherwise^{14} \end{cases} \tag{97}$$

The protection criterion exposure of each master asset is estimated based on the aggregated protection criteria exposures $AS_{pc\ exposure}$ of its *n* slaves, mitigated by their respective influenced protection criteria impact relations $AS_{pc\ impact\ relation}$, as shown in (101). Maximum and relative values are calculated as shown in (99) and (100).

In (98), $I = \{ i \mid 1 \leq i \leq n \wedge AS_{pc\ exposure_i} > 0 \wedge AS_{pc\ impact\ relation_i} > 0\}$, where *n* is the number of asset slaves. If the master asset has no asset slaves ($I = \emptyset$), the underlying asset base exposure $AB_{pc\ exposure}$ is used as calculated in (61).

[14] Only relevant if the influenced protection criteria impact of the asset master (and all slave representations) is negligible (0).

$$AM_{pc\ exposure} := \begin{cases} 10 \times \log_{10}\left(\sum_{i \in I} 10^{\frac{AS_{pc\ exposure_i} \times AS_{pc\ impact\ relation_i}}{10}}\right), I \neq \emptyset \\ AB_{pc\ exposure}, otherwise \end{cases} \quad (98)$$

In (100), $I = \{ i \mid 1 \leq i \leq n \wedge AS_{pc\ exposure\ max_i} > 0 \wedge AS_{pc\ impact\ relation_i} > 0 \}$, where n is the number of asset slaves. If the master asset has no asset slaves ($I = \emptyset$), the underlying asset base exposure maximum $AB_{pc\ exposure\ max}$ is used as calculated in (62).

$$AM_{pc\ exposure\ max} := \begin{cases} 10 \times \log_{10}\left(\sum_{i \in I} 10^{\frac{AS_{pc\ exposure\ max_i} \times AS_{pc\ impact\ relation_i}}{10}}\right), I \neq \emptyset \\ AB_{pc\ exposure\ max}, otherwise \end{cases} \quad (99)$$

$$AM_{pc\ exposure\ rel} := \begin{cases} \frac{AM_{pc\ exposure}}{AM_{pc\ exposure\ max}} \times 100, AM_{pc\ exposure\ max} > 0 \\ 0, otherwise \end{cases} \quad (100)$$

The asset master protection criterion risk $AM_{pc\ risk}$ is estimated based on the estimated total influenced protection criterion impact $AM_{influenced\ pc\ impact}$ and the estimated total protection criterion exposure $AM_{pc\ exposure}$ in (101).

$$AM_{pc\ risk} := \begin{cases} AM_{influenced\ pc\ impact} \times AM_{pc\ exposure}, I \neq \emptyset \\ 0, otherwise \end{cases} \quad (101)$$

Maximum and relative values of an asset master are calculated in (102) and (103) according to the same principle as before.

$$AM_{pc\ risk\ max} := \begin{cases} AM_{influenced\ pc\ impact} \times AM_{pc\ exposure\ max}, I \neq \emptyset \\ 0, otherwise \end{cases} \quad (102)$$

$$AM_{pc\ risk\ rel} := \begin{cases} \frac{AM_{pc\ risk}}{AM_{pc\ risk\ max}} \times 100, AM_{pc\ risk\ max} > 0 \\ 0, otherwise \end{cases} \quad (103)$$

Normalization functions for master assets are calculated similar to scenario assets as shown in (82) to (85).

An asset master can estimate its total protection criteria risks based on the aggregation of all its asset slave representations within the scenario trees. The default aggregation used for each protection criterion exposure is the energetic sum to establish a cautious risk view aligned with the rest of the risk model, but depends entirely on the organizational context and the desired estimation results. Other suitable aggregation methods include maximum, average, product and sum.

The energetic sum as a cautious default aggregation method also applies to the overall risk of the asset master.

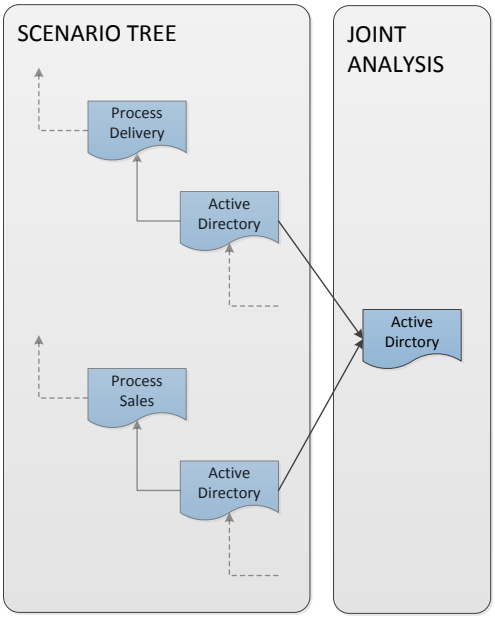


Figure 63: Example joint analysis of a scenario tree subset

The following example shows the joint aggregation (using the energetic sum) of the asset master „Active Directory", based on the asset slave used in the previous example and another representation within "Process Sales", which requires higher protection requirements than the asset slave within "Process Delivery". The exposures of the asset slave within "Process Delivery" are higher, indicating that the slave asset "Active Directory" of the "Process Sales" is dependent on additional, process-specific components (e.g. a sales-application that is authenticated via Active Directory Single-Sign-On).

Asset Active Directory (Master)	Impact level (V/NV)	Asset base exposure					Asset risk		
		V	M	NV	NM	%	NV	NM	%
Confidentiality	Confidential (25/6.25)	13.4	29.1	1.0	2.1	46	5.9	12.9	6
Integrity	Medium (25/6.25)	21.5	38.4	1.5	2.7	56	9.5	17.0	10
Availability	< 1 Hour (40/10)	8.2	26.3	0.6	1.9	31	5.8	18.7	6
Overall	40/10	22.3	39.1	1.6	2.8	57	15.8	27.7	16

Asset Active Directory @ Delivery	Impact level (V/NV)	Asset exposure					Asset risk		
		V	M	NV	NM	%	NV	NM	%
Confidentiality	Confidential (25/6.25)	24.6	38.4	1.7	2.7	64	10.9	17.0	11
Integrity	Medium (25/6.25)	31.2	42.5	2.2	3.0	73	13.8	18.8	14
Availability	< 1 day (30/7.5)	26.4	49.2	1.9	3.5	54	14.0	26.2	14
Overall	30/7.5	33.1	50.3	2.3	3.6	66	17.6	26.8	18

Asset *Active Directory @ Sales*	Impact level (V/NV)	Asset exposure					Asset risk		
		V	M	NV	NM	%	NV	NM	%
Confidentiality	Confidential (25/6.25)	34.2	45.7	2.4	3.2	75	15.2	20.3	15
Integrity	Medium (25/6.25)	12.7	48.2	0.9	3.4	26	5.6	21.4	6
Availability	< 1 hour (40/10)	14.2	45.4	1.0	3.2	31	10.1	32.2	10
Overall	40/10	34.3	51.4	2.4	3.6	67	24.3	36.5	24

Figure 64: Joint inheritance example of asset master *Active Directory* using two asset slave representations with varying protection criteria requirement levels (impacts) for availability.

V…Value, M…Maximum value, NV…Normalized value,
NM…Normalized maximum value

$$Process\ Delivery\ (master)_{availability\ exposure} = 10 \times \log_{10}\left(10^{\frac{8.2}{10}} + 10^{\frac{26.4\times\frac{30}{40}}{10}} + 10^{\frac{14.2\times\frac{40}{40}}{10}}\right) \cong 21.1 \quad \text{(XLVII)}$$

$$Process\ Delivery\ (master)_{normalized\ availability\ exposure} = 21.1 \times \frac{10}{141} \cong 1.5 \quad \text{(XLVIII)}$$

$$Process\ Delivery\ (master)_{availability\ exposure\ max} = 10 \times \log_{10}\left(10^{\frac{26.3}{10}} + 10^{\frac{49.2\times\frac{30}{40}}{10}} + 10^{\frac{45.4\times\frac{40}{40}}{10}}\right) = 46.0 \quad \text{(XLIX)}$$

$$Process\ Delivery\ (master)_{normalized\ availability\ exposure\ max} = 46.0 \times \frac{10}{141} \cong 3.3 \quad \text{(L)}$$

$$Process\ Delivery\ (master)_{availability\ exposure\ rel} = \frac{21.1}{46.0} \cong 46\ \% \quad \text{(LI)}$$

$$Process\ Delivery\ (master)_{normalized\ availability\ risks} = 1.5\ \times 10 \cong 15 \quad \text{(LII)}$$

$$Process\ Delivery\ (master)_{availability\ risk\ max} = 3.3 \times 10 \cong 32.6 \quad \text{(LIII)}$$

$$Process\ Delivery\ (master)_{availability\ risk\ rel} = \frac{15}{10 \times 10} \times 100 \cong 15\ \% \quad \text{(LIV)}$$

Asset *Active Directory* (Master)	Impact level (V/NV)	Asset exposure					Asset risk		
		V	M	NV	NM	%	NV	NM	%
Confidentiality	Confidential (25/6.25)	34.7	46.5	2.5	3.3	75	15.4	20.6	15
Integrity	Medium (25/6.25)	31.7	49.6	2.2	3.5	64	14.1	22.0	14
Availability	< 1 hour (40/10)	21.1	46.0	1.5	3.3	46	15.0	32.6	15
Overall	40/10	36.6	52.4	2.6	3.7	70	26.0	37.2	26

Figure 65: Asset *Active Directory* after joint inheritance. The asset base exposure itself may be overwritten, if the exposures from asset slaves are estimated higher. The underlying exposures of the asset master are still unchanged and provide insight into the asset exposures and risks that arise from its modules.

This procedure is continued, until all exposures have been aggregated. Because estimation of risks throughout the model requires normalization, the respective maximum asset and module exposures, threat likelihoods and safeguard risks are identified and saved along with all non-normalized values for this round. Upon visualization, the normalized values are calculated on-the-fly and presented to the user in form of a trend.

4.2.2 Risk Evaluation

In order to support decision making regarding safeguard prioritization and implementation, the proposed model estimates the safeguard sensitivity of each safeguard based on all associated safeguard risks and their related threat- and module exposures as well as asset risks to support the identification of the safeguards with the highest overall impact on the organization.

The safeguard analysis can be based on the results of the joint analysis (asset masters), providing generalized sensitivities, or on scenario analysis (asset slaves) to estimate detailed sensitivities based on all asset scenario instances.

Sensitivity analysis is done at a high level, providing a single generalized safeguard. The safeguard sensitivity analysis function for a single generalized IT-Grundschutz safeguard $GS_{sensitivity}$ incorporates:

- all of its related safeguard instances and their risks S_{risk},
- their cross-referenced threat protection criteria exposures $T_{pc\ exposure}$,
- further module protection criteria exposures $M_{pc\ exposure}$, and
- respective asset protection criteria risks $A_{pc\ risk}$ (masters/slaves)

to incorporate all information about the safeguard that is affecting the risk model.

Because the expert system might alter the safeguard maturities, threat protection criteria exposures or protection criteria impacts, their influenced variations are used within the calculation.

During testing, the usage of the energetic sum for establishing safeguard sensitivities turned out to provide quite homogenous results across the safeguard landscape, due to the amount of incorporated variables and the fact, that overall results strongly depended on peak risks with low to none incorporation of lower risks. Therefore, the estimation of safeguard sensitivities is using the sum operator.

All m safeguard instances S_{risk} are multiplied and summed up with their n threat protection criteria exposures (threat likelihood specific to each influenced protection criterion), related module protection criteria exposures $M_{pc\ exposure}$ and respective asset protection criteria risks (see (104) and (105)).

Basing the results on joint analysis (104) involves all *n* asset protection criteria risks $AM_{pc\ risk}$ of the master asset, which has the advantage of providing a generalized (but more uniformly distributed) evaluation of safeguard sensitivities that can be estimated without the need for an already established scenario tree.

In (104), $I = \{\, i \mid 1 \leq i \leq m \,\}$ and $J = \{j \mid 1 \leq j \leq n\}$, where *m* is the number of safeguard instances in the risk model and *n* is the number of related protection criteria.

$$GS_{joint\ sensitivity} := \sum_{i \in I} \sum_{j \in J} S_{risk_i} \times T_{pc\ exposure_j} \times M_{pc\ exposure_j} \times AM_{pc\ risk_j} \quad (104)$$

If sensitivity analysis is based on scenario analysis (105), every asset is involved with its *o* slave representations and their risk $AS_{pc\ risk}$, providing a highly granular estimation of safeguard sensitivities, covering all scenario dependencies.

In (108), $I = \{\, i \mid 1 \leq i \leq m \,\}$, $J = \{j \mid 1 \leq j \leq n\}$ and $K = \{k \mid 1 \leq k \leq o\}$, where *m* is the number of safeguard instances within the risk model, *n* is the number of related protection criteria and *o* is the number of related asset slave representations.

$$GS_{scenario\ sensitivity} := \sum_{i \in I} \sum_{j \in J} \sum_{k \in K} S_{risk_i} \times T_{pc\ exposure_j} \times M_{pc\ exposure_j} \times AS_{pc\ risk_{j_k}} \quad (105)$$

Similar to the previously outlined risk estimation procedure, risk evaluation additionally estimates the maximum and relative sensitivity based on joint analysis (see (106) and (107)) or scenario analysis (see (108) and (109)), using the potential worst-case scenario.

In (108), $I = \{\, i \mid 1 \leq i \leq m \,\}$ and $J = \{j \mid 1 \leq j \leq n\}$, where *m* is the number of safeguard instances within the risk model and *n* is the number of related protection criteria.

$$GS_{joint\ sensitivity\ max} := \sum_{i \in I} \sum_{j \in J} S_{risk\ max_i} \times T_{pc\ exposure\ max_j} \times M_{pc\ exposure\ max_j} \times AM_{pc\ risk\ max_j} \quad (106)$$

$$GS_{joint\ sensitivity\ rel} := \begin{cases} \frac{GS_{joint\ sensitivity}}{GS_{joint\ sensitivity\ max}} \times 100, GS_{joint\ sensitivity\ max} > 0 \\ 0 \qquad\qquad\qquad\qquad , otherwise \end{cases} \quad (107)$$

In (108), $I = \{ i \mid 1 \leq i \leq m \}$, $J = \{j \mid 1 \leq j \leq n \}$ and $K = \{k \mid 1 \leq k \leq o \}$, where *m* is the number of safeguard instances within the risk model, *n* is the number of related protection criteria and *o* is the number of related asset slave representations.

$$GS_{scenario\ sensitivity\ max} := \sum_{i \in I} \sum_{j \in J} \sum_{k \in K} S_{risk\ max_i} \times T_{pc\ exposure\ max_j} \times M_{pc\ exposure\ max_j} \times AS_{pc\ risk\ max_{j_k}} \quad (108)$$

$$GS_{scenario\ sensitivity\ rel} := \begin{cases} \frac{GS_{scenario\ sensitivity}}{GS_{scenario\ sensitivity\ max}} \times 100, GS_{scenario\ sensitivity\ max} > 0 \\ 0 \qquad\qquad\qquad\qquad , otherwise \end{cases} \quad (109)$$

To provide an easily interpretable result, all generalized safeguard sensitivities are normalized to a scale of [0, 100] with the maximum generalized safeguard sensitivity $GS_{rm\ sensitivity\ max}$, established on all *n* generalized maximum safeguard sensitivities within the risk model, shown in (110).

In (96), $I = \{ i \mid 1 \leq i \leq n \}$, where *n* is the number of safeguards within the risk model.

$$GS_{rm\ sensitivity\ max} = \max_{i \in I}(GS_{sensitivity\ max_i}) \quad (110)$$

Normalization functions for a joint analysis base are outlined in (111) and (112), for a scenario analysis base in (113) and (114).

$$GS_{joint\ nsensitivity} := \begin{cases} \frac{GS_{joint\ sensitivity}}{GS_{rm\ sensitivity\ max}} \times 100, GS_{rm\ sensitivity\ max} > 0 \\ 0 \qquad\qquad\qquad\qquad , otherwise \end{cases} \quad (111)$$

$$GS_{joint\ nsensitivity\ max} := \begin{cases} \frac{GS_{joint\ sensitivity\ max}}{GS_{rm\ sensitivity\ max}} \times 100, GS_{rm\ sensitivity\ max} > 0 \\ 0 \qquad\qquad\qquad\qquad , otherwise \end{cases} \quad (112)$$

$$GS_{scenario\ nsensitivity} := \begin{cases} \frac{GS_{joint\ sensitivity}}{GS_{rm\ sensitivity\ max}} \times 100, GS_{rm\ sensitivity\ max} > 0 \\ 0 \qquad\qquad\qquad\qquad , otherwise \end{cases} \quad (113)$$

$$GS_{scenario\ nsensitivity\ max} := \begin{cases} \frac{GS_{scenario\ sensitivity\ max}}{GS_{rm\ sensitivity\ max}} \times 100, GS_{rm\ sensitivity\ max} > 0 \\ 0 \qquad\qquad\qquad\qquad , otherwise \end{cases} \quad (114)$$

By showing which generalized IT-Grundschutz safeguard is most cross-referenced, with the highest threat protection criteria exposures, the highest module protection criteria exposures and the most influenced assets and highest asset protection criteria risks, the importance of the safeguard generalization can be related to others within the risk model.

Safeguard sensitivity can be calculated at any time to help identify the safeguards with the highest impact on the overall situation and to support decision making of risk management actions.

Sensitivities of assets, modules and threats can potentially be estimated following the same schema and removing the variables of the underlying layers, but have been omitted due to time restraints and the already high complexity of the prototype.

4.3 Influence Estimation using Expert Knowledge

The following influence estimation is based on the examples outlined in Figure 26. Based on two measure indicators, the framework provides independent (e.g. OR concatenation of measure indicators, defining separate rules) as well as conditional (AND-concatenation of measure indicators) influence estimations on a risk factor (safeguard maturity). Based on the indicators, measurements, rules and specific risk factor targets defined, the proposed model generates a FCL-compliant input file, calculates the estimated output using an open-source, FCP-compliant fuzzy logic library written in JAVA (JFuzzyLogic) and incorporates the results as risk factor influences into the risk model.

The following sections cover the calculation procedure required for fuzzy control, however, the functionality is covered by most fuzzy logic libraries.

4.3.1 Fuzzification

First of all, the indicators are used in combination with their current measurement to provide the membership degree of their respective indicators.

Measure indicator 1: *Months since last Information Security Policy (ISP) revision*

The membership function of the indicator term *high* for the measure in Figure 66 has been assumed as a multi-point linear function.

This is done according to FCL specification by separating every point combination with brackets $(e.g.(y_1, x_1)\ (y_2, x_2)\ \dots\ (y_n, x_n),)$ as shown in (LV).

```
FUZZIFY months_since_last_isp_revision
   TERM high := (0,6) (22,1) (24,1)                    (LV)
END_FUZZIFY
```

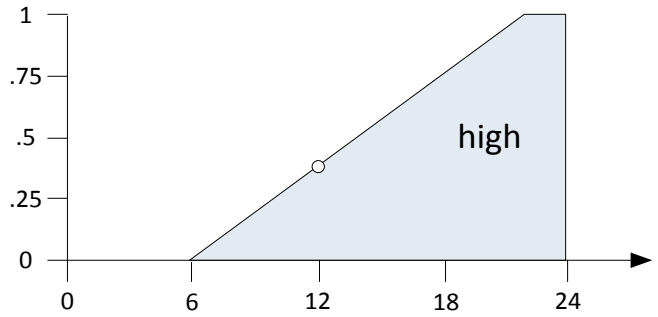


Figure 66: Fuzzification of measure *Months since last ISP revision* with the indicator term *high*

The membership value corresponding to an example measurement shown in Figure 66 is established in (LVI).

$$\mu_{months\ since\ last\ isp\ revision_{high}} = \frac{|6-12|}{|6-22|} = 0.375 \qquad \text{(LVI)}$$

The membership degree μ can be estimated for linear functions based on the left and right bound points of the membership definition. The example assumes a current measurement of 12 months for this measure, selecting the next lower and next higher points of the membership definition.

Measure indicator 2: *Percentage of users trained regarding the ISP*

The membership function of the indicator term *high* for the measure in Figure 67 has been assumed as a sigmoid function. This is done according to FCL specification using the syntax "sigm gain center" as shown in (LVII).

```
FUZZIFY percentage_of_users_trained_regarding_the_isp
   TERM high := sigm 0.1 50                                    (LVII)
END_FUZZIFY
```

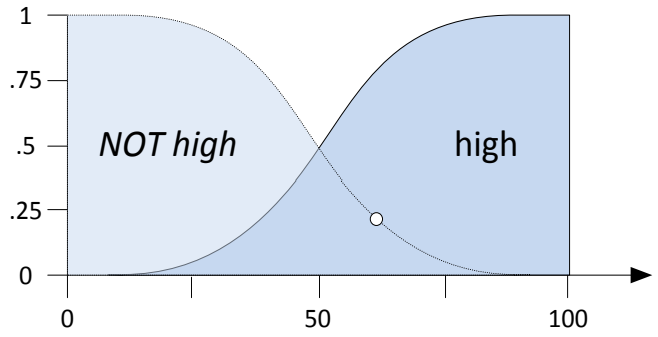


Figure 67: Fuzzification of measure *Percentage of users trained regarding the ISP* with the indicator term *high* and its inverse *NOT high*

The membership degree μ can be estimated for sigmoid functions using the formula outlined in (115). The respective *NOT high* is calculated by means of subtraction from the full membership degree as shown in (LX).

$$\mu_{sigmoid} := \frac{1}{\left(1 + \exp(-gain \times (x - center)\right)} \qquad (115)$$

The example in (LIX) assumes a current measurement of 62 percent for this measure.

$$Percentage\ of\ users\ trained\ regarding\ ISP = 62\ \% \tag{LVIII}$$

$$\mu_{percentage\ of\ users\ trained\ regarding\ isp_{high}} = \frac{1}{\left(1 + \exp(-0.1 \times (62 - 50)\right)} = 0.769 \tag{LIX}$$

$$\mu_{percentage\ of\ users\ trained\ regarding\ isp_{NOT\ high}} = 1 - \mu_{percentage\ of\ users\ trained\ regarding\ isp_{high}} = 0.231 \tag{LX}$$

Influence indicator 1 & 2: *low* and *high* safeguard influence

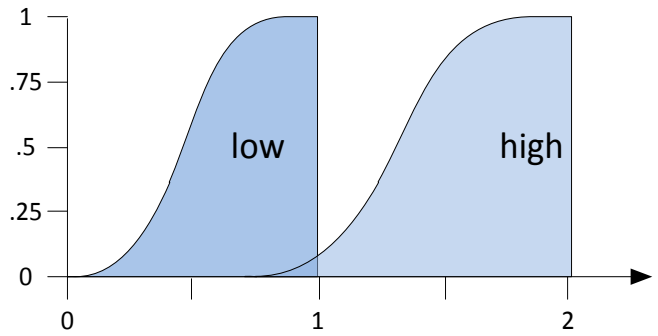


Figure 68: Influence indicators *low* and *high* used for safeguard influence

The influence indicators are designed to provide a result for the modification of respective risk factors (safeguard/threat/impact) and should be aligned with the influence scales outlined in 4.2.1. The terms used for example (LXI) are assumed as sigmoid functions, influencing the related safeguard maturity levels negatively by a factor of [0, 1] *low* and [0.7, 2] *high*. The influence indicators in (LXI) define the maximum decrease of the related safeguard maturity levels, raising the respective risks throughout the risk model accordingly.

```
FUZZIFY s_2_192_[safeguard id]_drawing_up_an_isp_influence
   TERM low := sigm 10 0.5
   TERM high := sigm 8 1.4
END_FUZZIFY
```
(LXI)

4.3.2 Aggregation and Activation

The first rule establishes a correlation effect (attack vector chain) between measures, creating *high* influence.

IF *Months since last ISP revision* IS *high* AND *Percentage of users trained regarding ISP* IS *NOT high*
THEN *S 2.192 Drawing up an Information Security Policy* IS *high*

IF (0.375 AND (1-0.769))
THEN *S 2.192 Drawing up an Information Security Policy* IS *high* (LXII)

IF MIN(0.375, 0.231)
THEN *S 2.192 Drawing up an Information Security Policy* IS 0.231 *high*

The second rule establishes a concatenation of measures that influence the respective factors independently. This can also be achieved by using multiple rules without any concatenation between conditions.

IF *Months since last ISP revision* IS *high* OR *Percentage of users trained regarding ISP* IS *NOT high*
THEN *S 2.192 Drawing up an Information Security Policy* IS *low*

IF (0.375 OR (1-0.769)) (LXIII)
THEN *S 2.192 Drawing up an Information Security* Policy IS *low*

IF MAX(0.375, 0.231)
THEN *S 2.192 Drawing up an Information Security Policy* IS 0.375 *low*

4.3.3 Accumulation

In order to provide a clean separation between influence ranges, the accumulation is done within separate rule blocks, as outlined in 3.3.3 and shown in Figure 26.

$\mu_{influence_{low}}$ = MIN(0.375) -> *low* influence on
S 2.192 Drawing up an Information Security Policy

(LXIV)

$\mu_{influence_{high}}$ = MIN(0.231) -> *high* influence on
S 2.192 Drawing up an Information Security Policy

4.3.4 Defuzzification

Because the accumulation is performed within different rule blocks, defuzzification is done for each rule individually. The defuzzification method used is the Left-Most-Maximum, according to the requirements defined in 2.3.4.3. The generic definition of the specific calculation function ((115) solved for x) for the sigmoid influence indicators is shown in (116). The example values shown in Figure 69 are calculated in (LXV) and (LXVI).

$$LM_{sigmoid\ specific} := \frac{center \times gain - \log\left(\frac{1}{\mu_{influence}} - 1\right)}{gain} \tag{116}$$

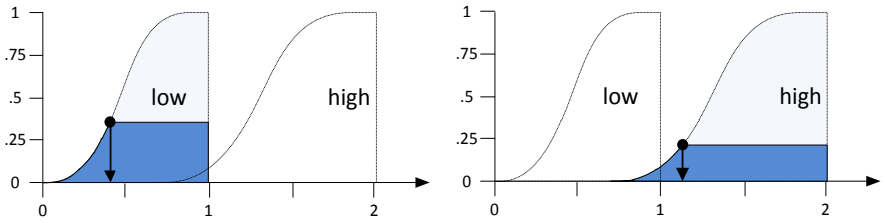


Figure 69: Activated influence indicators *low* with 0.375 and *high* with 0.231 used for defuzzification

$$LM_{influence_{low}} = \frac{0.5 \times 10 - \log\left(\frac{1}{0.375} - 1\right)}{10} = 0.449 \tag{LXV}$$

$$LM_{influence_{high}} = \frac{1.4 \times 8 - \log\left(\frac{1}{0.231} - 1\right)}{8} = 1.25 \tag{LXVI}$$

4.3.5 Risk Factor Influence

The expert system can provide multiple results based on all activated rules. The estimation of total influence $Influence_{total}$ on any factor is done by establishing the maximum (worst-case-scenario) of all n influence indicators $Influence_{indicator}$ as shown in (117). The safeguard-specific example is continued in (LXVII).

In (117), $I = \{\, i \mid 1 \leq i \leq n \,\}$, where n is the number of indicators.

$$Influence_{total} := \max_{i \in I}\left(Influence_{indicator_i}\right) \tag{117}$$

$$S\ 2.192\ Drawing\ up\ an\ Information\ Security\ Policy_{maturity\ influence} = \max(0.449, 1.25) = 1.25 \quad \text{(LXVII)}$$

Depending on the specific risk factor targets defined for the risk model (as outlined in Figure 51), all defined instances within the risk model are inferred accordingly.

The example result $S\ 2.192_{maturiy\ influence}$ shown in (LXVII) increases the estimated safeguard maturity gap $S_{maturity\ gap}$ as outlined in (36), resulting in adapted safeguard risks as shown in Figure 70.

Besides safeguard maturity influence outlined in 4.2.1.1, threat likelihoods and their specific influence on protection criteria can be manipulated as outlined in 4.2.1.3, as well as asset impacts on specific protection criteria, as outlined in 4.2.1.6.

Module 1.0 Security Management																			
Safeguards	Priori-	T 2.66				T 2.105				T 2.106				T 2.107					
		M	R	RM	RR	M	R	RM	RR	M	R	RM	RR	M	R	RM	RR		
S 2.192 Drawing up an Information Security Policy	4	3	4	16	25	2	8	16	50	3	4	16	25						

S 2.192 Drawing up an Information Security Policy	4	1.8	9	16	56	0.3	13	16	81	1.8	9	16	56						

Figure 70: Example influence (before/after) of safeguard maturities of *S 2.192 Drawing up an Information Security Policy*, covering all cross-referenced threats equally (WITH WEIGHT 1.0) on the example asset *IS Management*

M…Maturity, R…Safeguard risk, RM…Potential maximum safeguard risk, RR…Relative safeguard risk

The model can be continuously re-estimated in scheduled intervals or by manual initiation to create new risk assessment results based on changed measurements or risk factor evaluations.

5 Proposed Framework and Prototype

Due to time and resource constraints the prototype development focused on primary risk assessment aspects, with only basic integration of risk management functionality (e.g. actions can be related to their risk factors, including definition of responsibilities, dates and schedule, managing implementation projects, reporting, etc.). In order to incorporate the most recent version of the IT-Grundschutz catalogs and to ease evaluation and validation efforts within the German-speaking domain of the Austrian Federal Ministry of Defense, the prototype interfaces have been developed in German, using the 12th German version of the IT-Grundschutz catalogs, released in 2011[15].

Metric management interfaces allow the definition and derivation of measures using basic mathematical operators (addition, subtraction, multiplication, division, power, brackets). The expert system provides a rule generation interface, allowing the selection of specific risk factors[16].

The prototype has been named *RiskSense* and provides proof-of-concept interfaces for the management of the core-objects and respective supporting-object mappings in Figure 71.

[15] In June 2013, the 13th version of IT-Grundschutz was released by the German BSI and incorporated into the thesis. The prototype database, as well as all evaluation models are based on the 12th version and have not been updated, due to the fact that no structural modifications have been performed [70].

[16] Due to time constraints, the selection interface (front-end) for specific risk factor targets has only been implemented as a proof of concept for safeguard targets, allowing the highest granularity of control compared to threat and impact targets (higher level factors).

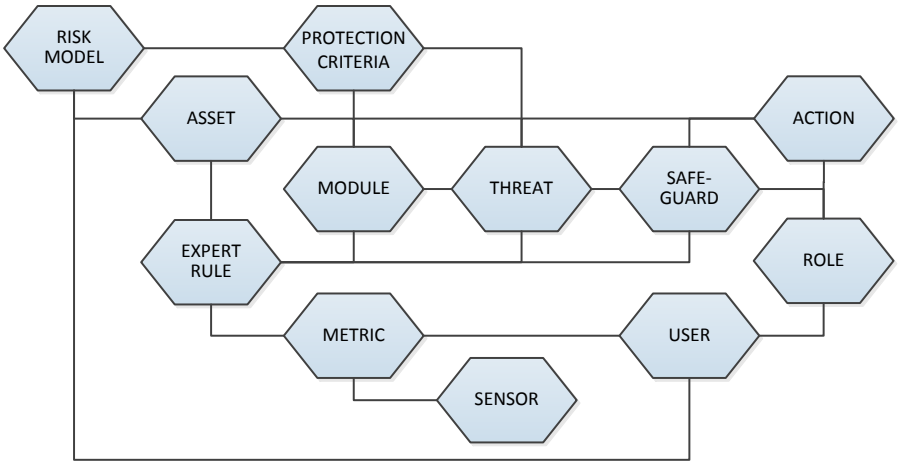


Figure 71: Primary objects and relations of RiskSense[17]

Due to the need for a continuously available component that handles measurement updates through automated sensors and the desired integration of all responsible personnel into the risk assessment process, the prototype has been developed as a web-service.

Because of its rapid prototyping abilities, clean model-view-controller design and high applicability for database-driven web-applications, Ruby on Rails (RoR) has been chosen as a server-side environment. Especially the database model handling via "Active-Record" enables the rapid definition of complex database models.

Because the prototype interface focuses on modeling and visualization of trends, the Adobe Flex Framework (Flex), which is used for highly complex charting and dashboard applications, has been chosen as a client-side environment for asynchronous communication. According to [59], the flash player, which is required to run Flex applications, is the most widespread RIA (Rich-Internet-Application) plugin with a ~99% penetration for Internet-connected PCs and ~82% penetration of mobile platforms.

While the rails back-end enables communication over HTTP(S) using multiple additional standard-ASCII-formats (e.g. XML, JSON, etc.), communication with the front-end is established using the binary-encoded transport protocol AMF3 (Adobe Action-Message-Format 3) which supports – amongst others – inner-object-references, enabling significant smaller objects for (de-)serialization and transmission.

The back-end uses a PostgreSQL database, enabling increased performance, integrity and scalability compared to e.g. MySQL, which is commonly used within RoR development.

[17] See Figure 73 for more details.

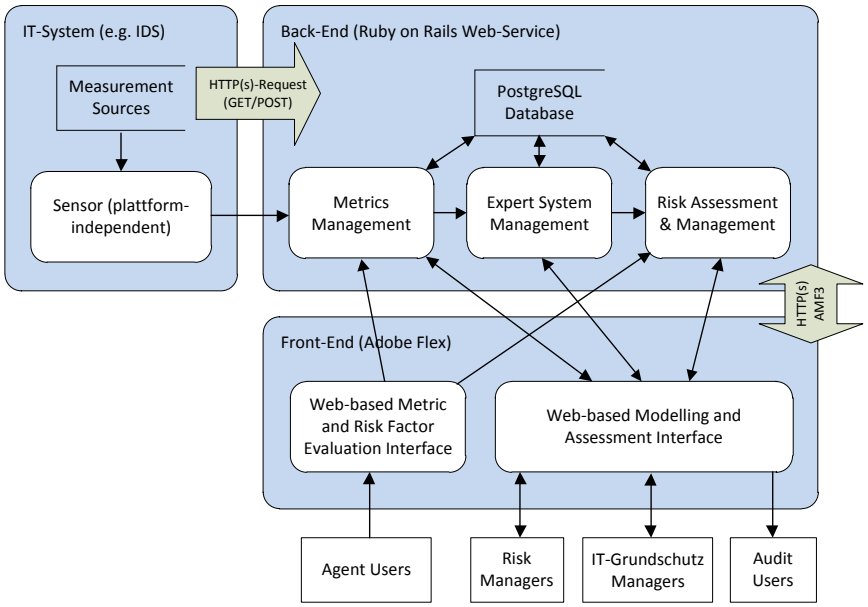


Figure 72: High-level overview of prototype architecture and components

The prototype enables the integration (authorization, measurement handling) of external sensors (e.g. scripts), that can be implemented on any external IT system that can communicate with the web-service over HTTP(S). Of course, these sensors do not need to be implemented on the IT system providing the measurement source, as long as a secure way of data acquisition and transfer can be established (e.g. implementing sensors on a separate IT system that gathers IDS measurements by logging into the IDS application over a secure channel, parsing the required information and delivering the data to the web-service).

The back-end provides web-service components that handle the functions used for metrics-, expert system- and risk-assessment and –management. Depending on the user-credentials (role assignments and authorization), the front-end provides the users with the metric and risk factor estimation and evaluation interfaces showing only objects within their realm of responsibility (see 5.1.1).

In order to maximize compatibility with external sensors, a single controller action is accessible without authentication and without role-based authorization. This controller is used for the integration of automated sensors, but requires the communication to originate from the registered IP address and to include a shared secret registered for the sensor.

Figure 73 shows an overview of the implemented back-end domain model. Figure 74 shows an overview of the proposed integrated process and the following chapter provides detailed insights into the interfaces and process steps. The screenshots depicted in the following chapter show the risk model that has been used for testing and evaluation during prototype development and is described in detail in Annex A of [3].

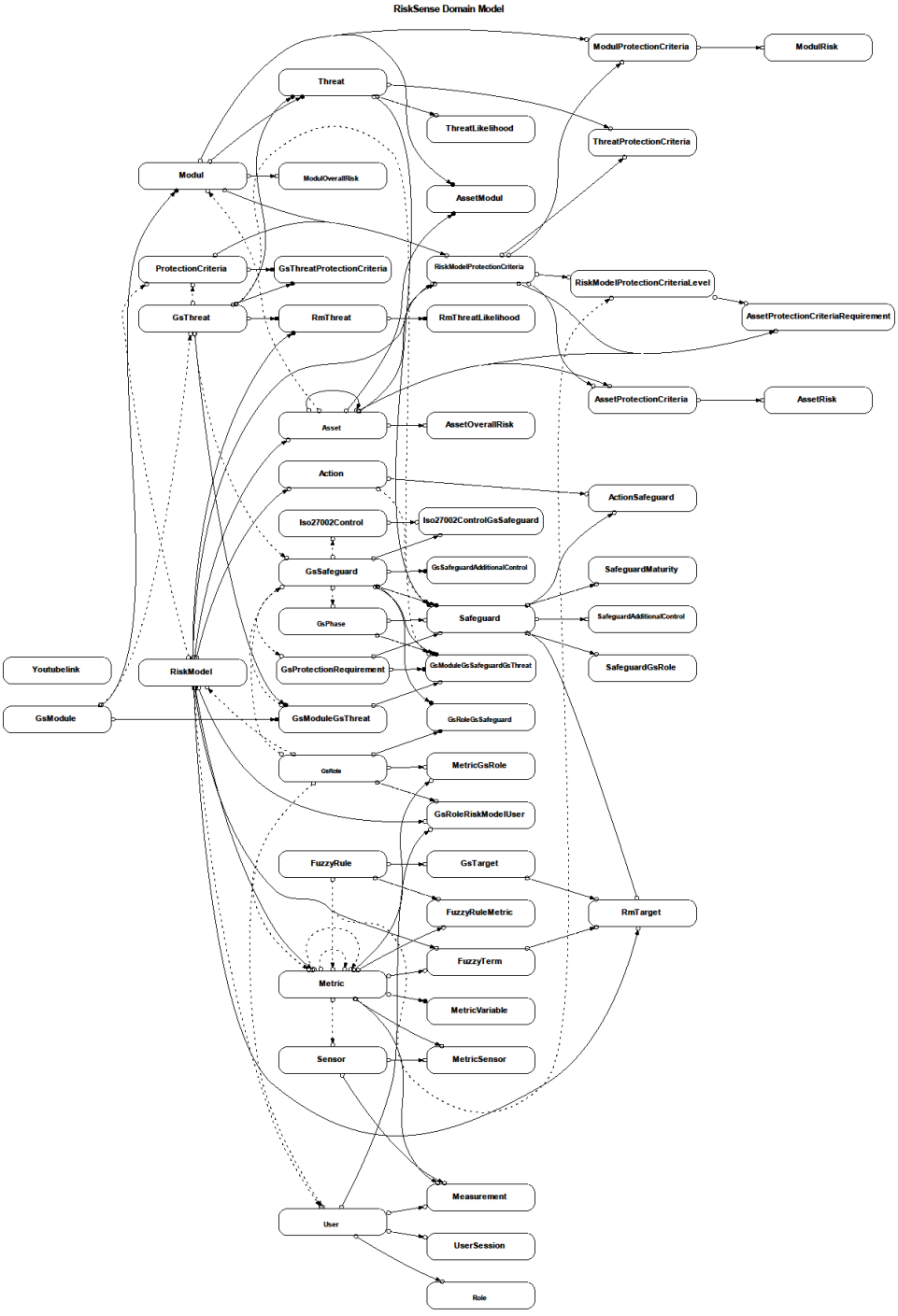


Figure 73: High-level domain-model of implemented prototype (some links have been omitted due to readability reasons).

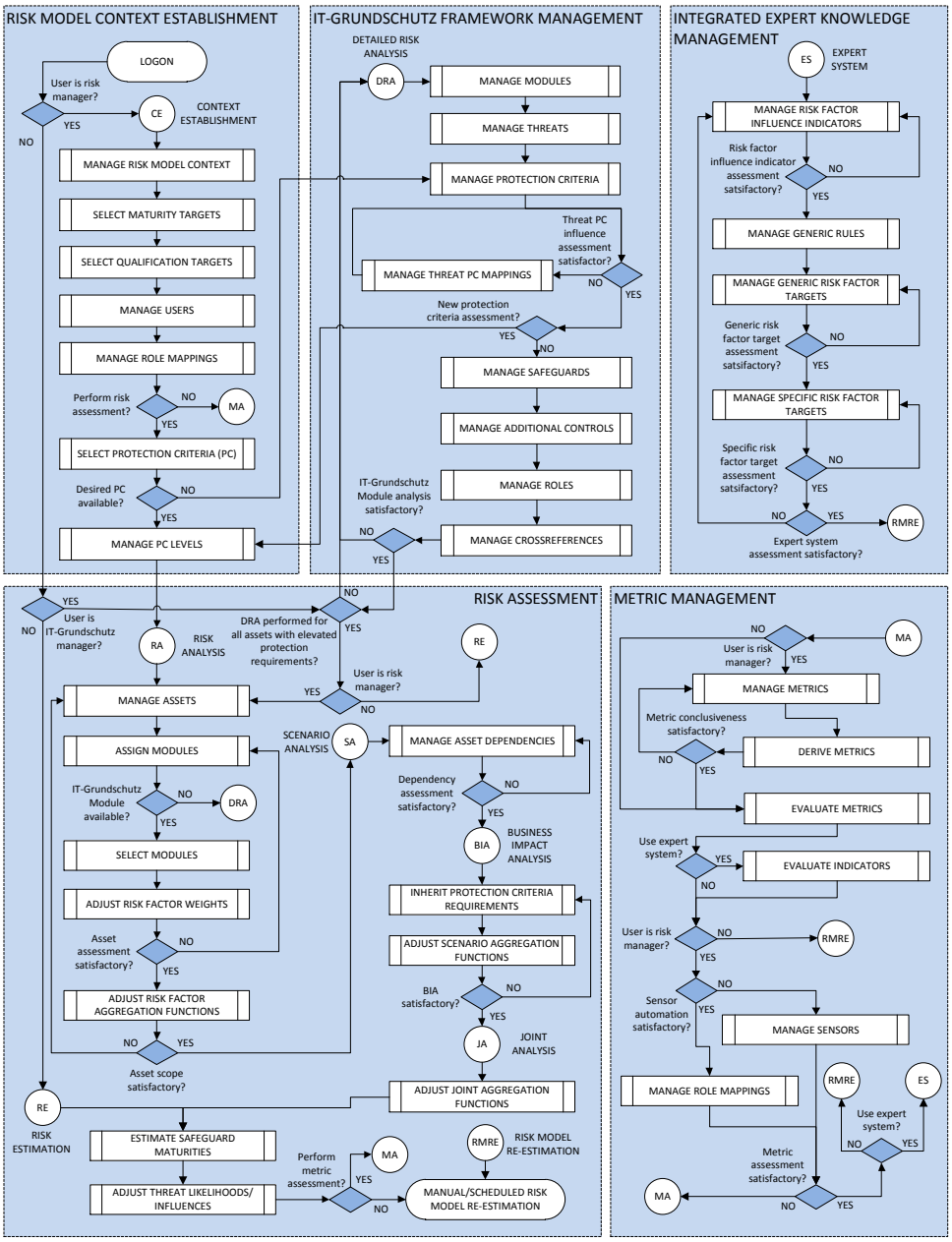


Figure 74: High-level overview of integrated prototype process steps

5.1 Interfaces and Process Steps

The prototype interfaces use a standardized layout as shown in Figure 75. The process navigation panel on the left provides an accordion component to guide the user through the proposed process outlined in Figure 74, presenting respective sub-process actions inline. Depending on the selected process step, the appropriate workspace panel and the respective sub-section of the overview panel are activated. The overview panel is used to show general information as well as selected and related objects. The workspace panels follow the standardized layout shown below and provide specific object views dependent on the processed objects. Nearly all workspace interfaces include sub-panels that provide fields and functions for creating, updating (single/ multiple) and deleting objects as well as display and filtering options for the respective workspace. The navigation and overview panels as well as all workspace sub-panels are retractable in order to adjust each components used space.

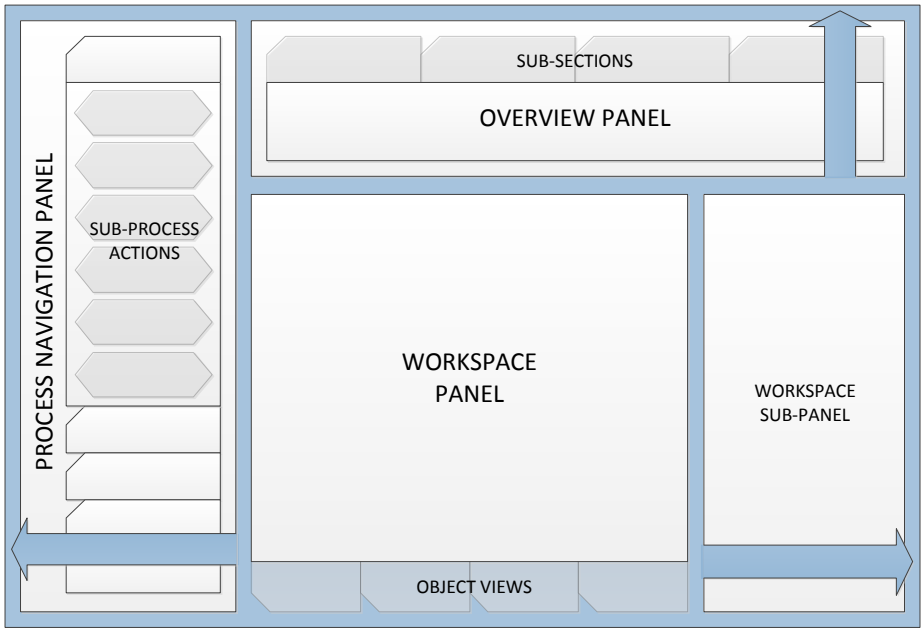
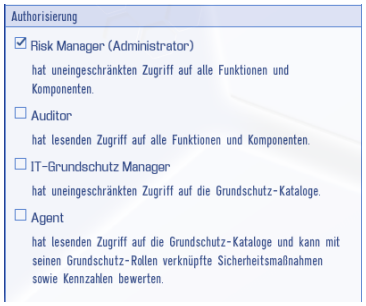


Figure 75: Standardized prototype interface layout

5.1.1 Logon and Authorization

The logon procedure establishes the scope of interfaces available to the authenticated user based on its authorization roles. The authorization is done at the client side (disabling certain interfaces) as well as on the server side (authorization rules for every accessible controller action). Implemented authorization roles are:



- Risk Managers (Administrators) can create, read, update and destroy all objects
- Auditors can read all objects
- IT-Grundschutz Managers can create, read, update and destroy all IT-Grundschutz objects
- Agents can read all objects and can create safeguard maturity evaluations and measure assessments (can be assigned to roles/individual users) in their realm of responsibility

Immediately after logon, the user is presented an overview and description of the process (see Figure 77). Until a risk model is selected, the user can access the user-, protection criteria-, IT-Grundschutz-, metric- and expert-system-interfaces in order to manage information independent of the risk model (management of overarching aspects).

To demonstrate the multi-media-capabilities of Flex and to provide an integrated training concept for users, an interface for the provision of awareness videos has been implemented (see Figure 78).

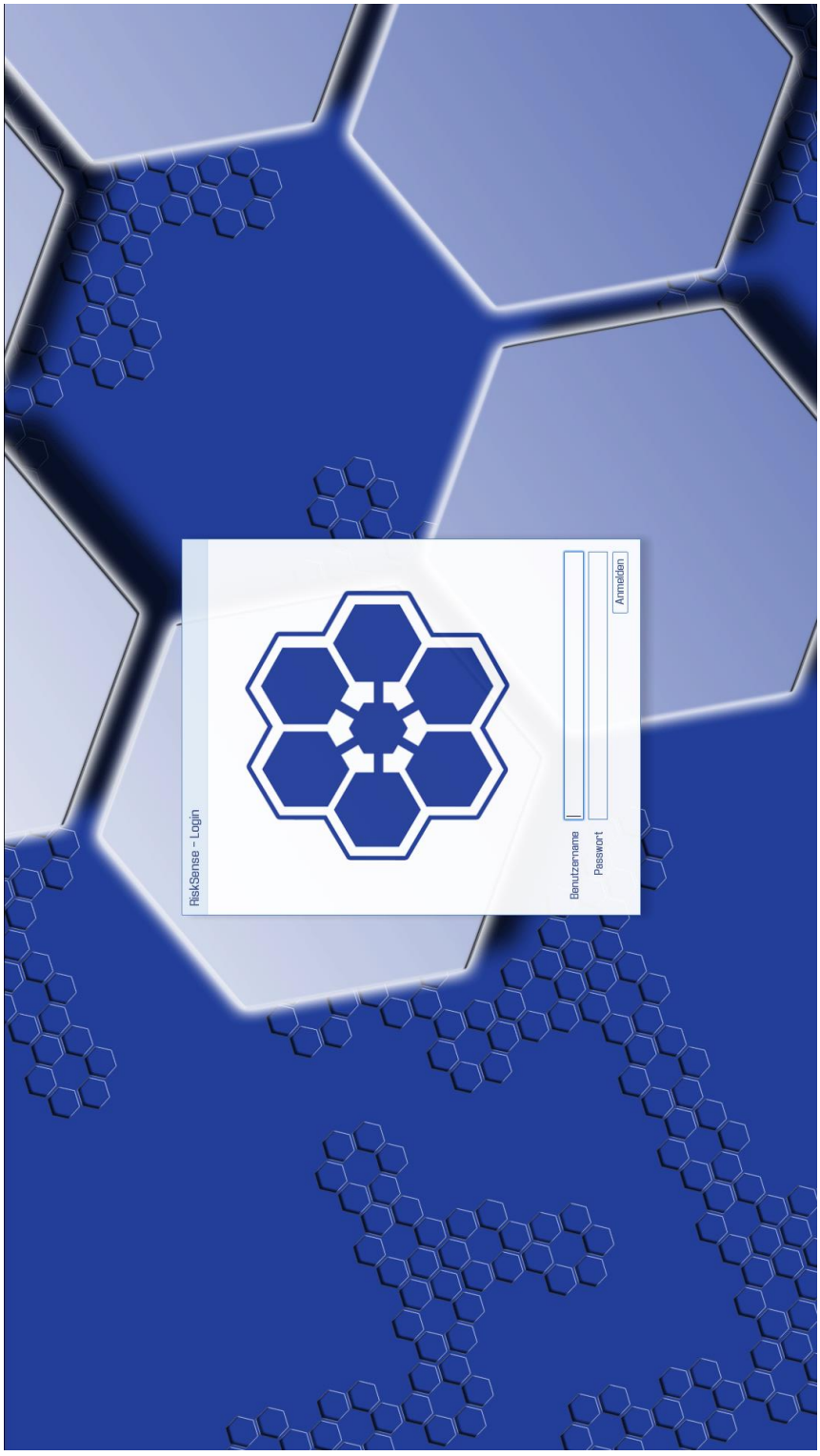


Figure 76: Prototype logon screen

Figure 77: Overview and description of the implemented process model

Figure 78: Management and provision of information security awareness videos

5.1.2 Risk Model Context Establishment

The risk managers can create, update, copy, delete and filter independent risk models. Every risk model enables the definition of the context, incorporating a strategic description, organizational details, scope definition, objective definition, qualification and maturity target definitions and global risk factor indicators for the risk model.

To aid visual perception of the primary security objectives, global qualification and maturity target levels are depicted as medal symbols.

In order to provide basic simulation capabilities within the prototype, risk models can be copied along with their related objects.

Users can be managed and IT-Grundschutz roles can be assigned to individual/multiple users after selection/creation of the desired risk model (see Figure 80). The mapping of IT-Grundschutz roles to users is performed at the IT-Grundschutz role interface (see Figure 89). Details of the current user, including its role assignments to the currently selected risk model are shown in the overview sub-panel "Session-Environment" (see Figure 80). After risk model selection, the overview sub-panel "Model-Environment" shows details on the core criteria, targets and objects of the risk model (see Figure 81).

Protection criteria can be managed and assigned to risk models to be included in the risk assessment (see Figure 81). If new protection criteria are defined, the definition of threat influences to those protection criteria can be done using the IT-Grundschutz threat interface (see Figure 85). If the usage of the risk assessment component is not required, the user can skip the following steps and jump right to the metric assessment.

For all protection criteria added to the risk model, evaluation levels and boundary definitions have to be established. These requirement levels can be defined individually for every protection criterion including user-defined impact values and descriptions of the primary aspects (see Figure 82).

Figure 79: Risk model management interface, showing risk model details

Figure 80: Managing users, authorizations and mappings to IT-Grundschutz roles, distinct for the selected risk model

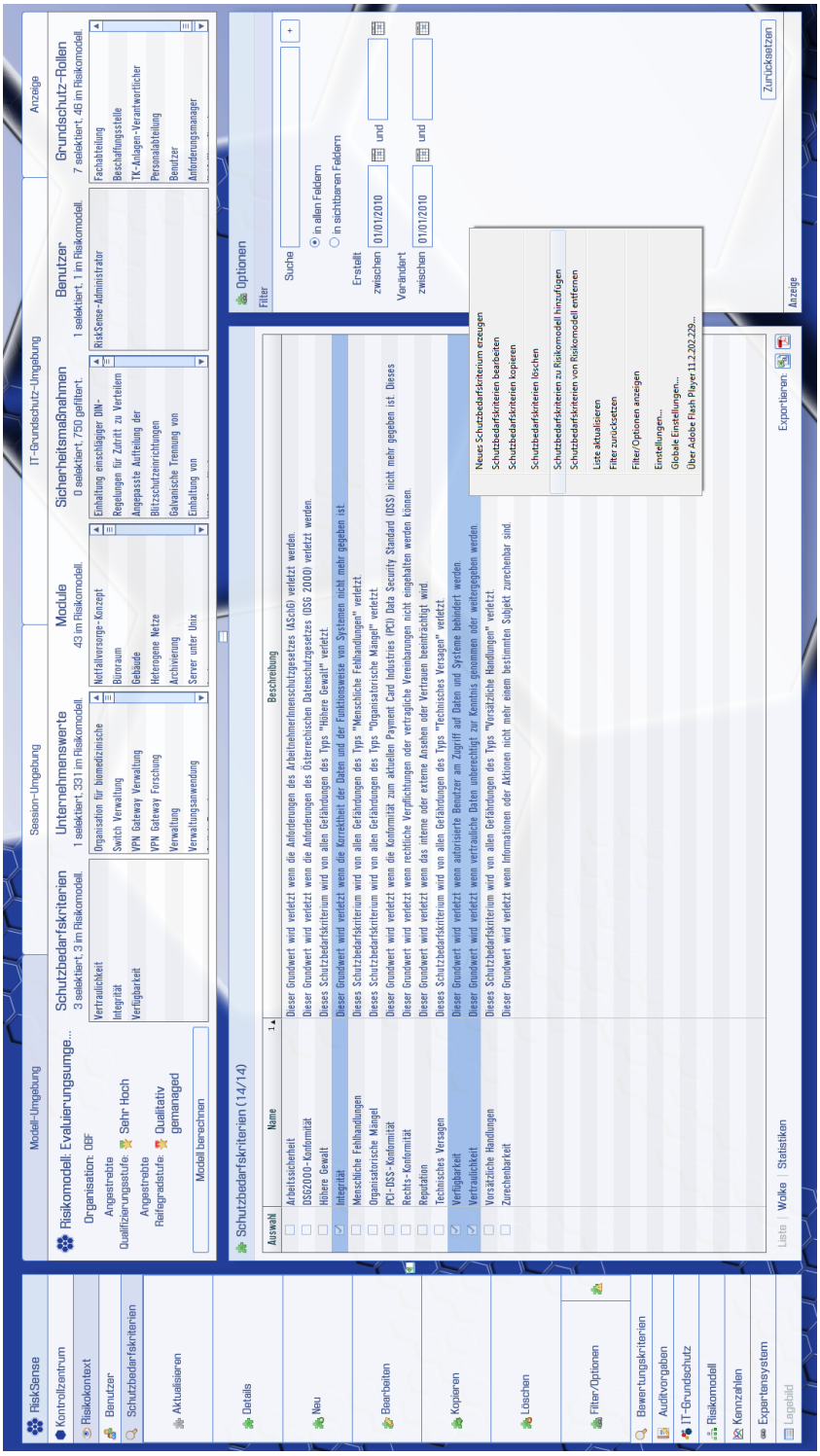


Figure 81: Protection criteria management and risk model assignment

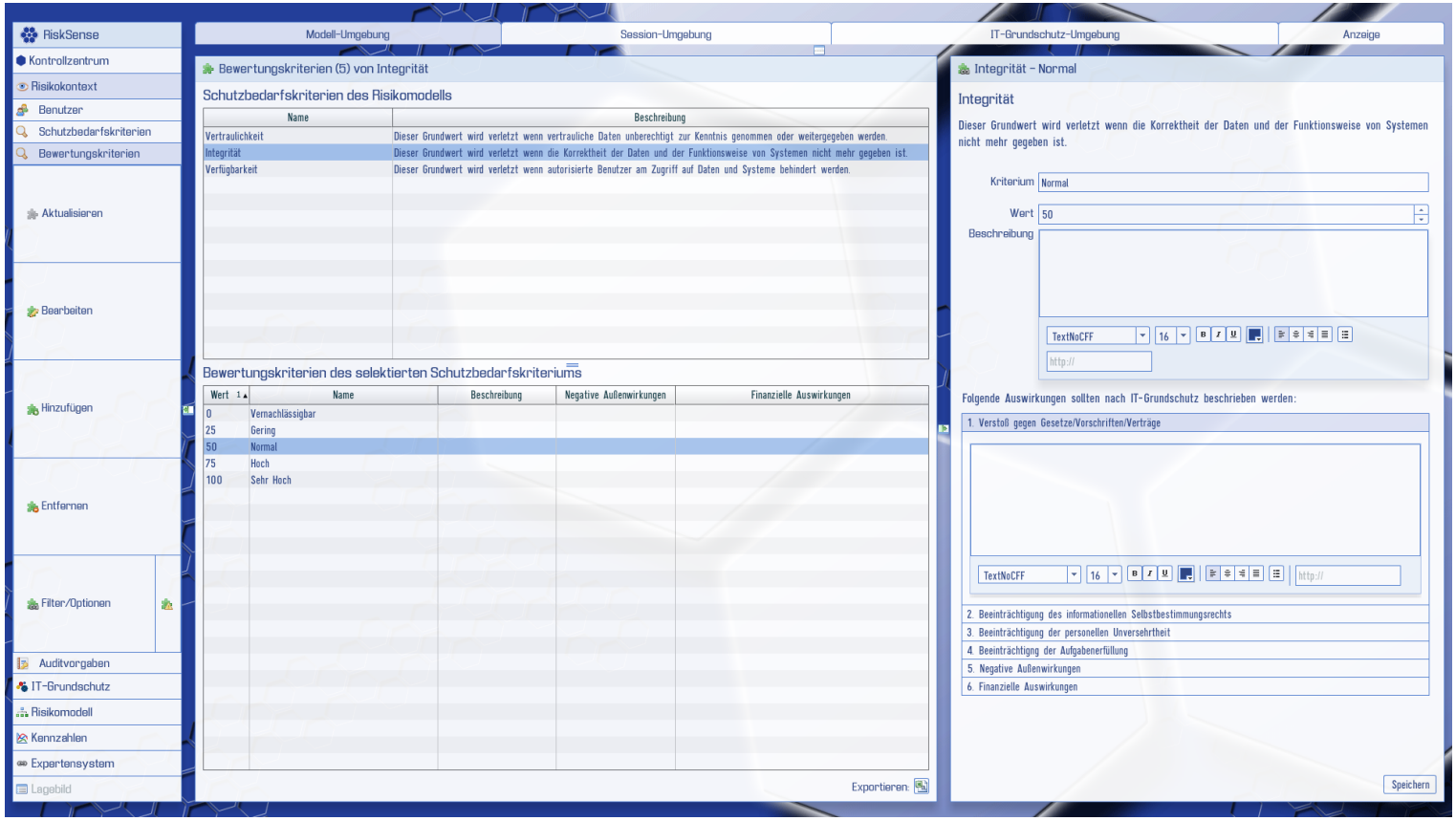


Figure 82: Protection criterion requirement level management

5.1.3 Risk Assessment

The process of risk assessment covers the identification of risks and the dependencies between assets, the estimation of risk factors and the evaluation of estimated risks.

5.1.3.1 Risk Identification

The IT-Grundschutz framework can be managed through separate interfaces for the management of modules, threats, safeguards and roles, used to demonstrate organizational assets. The interfaces include logic to view and manage cross-references between these objects, allowing the definition of new objects as well as the extension of existing objects to perform detailed analysis. To indicate the potential exposures associated with modules and their cross-references, generalized[18] exposures have been calculated similar to the procedure outlined in 4.2.1 (the more and higher prioritized safeguards are required to establish baseline protection, the higher the potential exposure, see Figure 83 and Figure 84 using a tree map view).

When switching to the IT-Grundschutz management interfaces, the overview subsection "IT-Grundschutz Environment" becomes active and provides information about selected/filtered objects as well as the currently selected mode of cross-reference view (e.g. showing all threats of the selected module(s)) (see Figure 83).

IT-Grundschutz threats, mappings to modules, as well as mappings to protection criteria can be managed to depict their potential influence. The interface offers several options for the display of different cross-references (assets, modules, safeguards and roles). As most interfaces, the threat interface allows the manipulation of multiple objects at once (fields as well as mappings) as shown in Figure 85.

The IT-Grundschutz safeguard interface (see Figure 86) provides safeguard and additional control management aspects, as well as the possibility to establish and extend detailed cross-references (see Figure 87). This allows the detailed analysis of security aspects for modules with elevated protection criteria requirements as required by [48].

Besides standard view and filtering options, the interface provides a mapping to ISO/IEC 27002 controls as shown in Figure 88. This enables the drill-down of specific IT-Grundschutz safeguard definitions and requirements based on generic ISO/IEC 27002 controls.

The IT-Grundschutz role interface is used to manage roles and their mappings to IT-Grundschutz safeguards. As most interfaces, the role interface offers the view option of a context- and mouse-sensitive cloud (tag cloud), as shown in Figure 89.

[18] Module exposures of the IT-Grundschutz framework are estimated without taking protection criteria influences into account, as the assessment of various protection criteria is subject to selection for every risk model.

Figure 83: IT-Grundschutz module management, outlining general exposure levels

Figure 84: TreeMap view of IT-Grundschutz modules and respective general exposures, grouped by type

Figure 85: IT-Grundschutz threat management, currently editing multiple threats

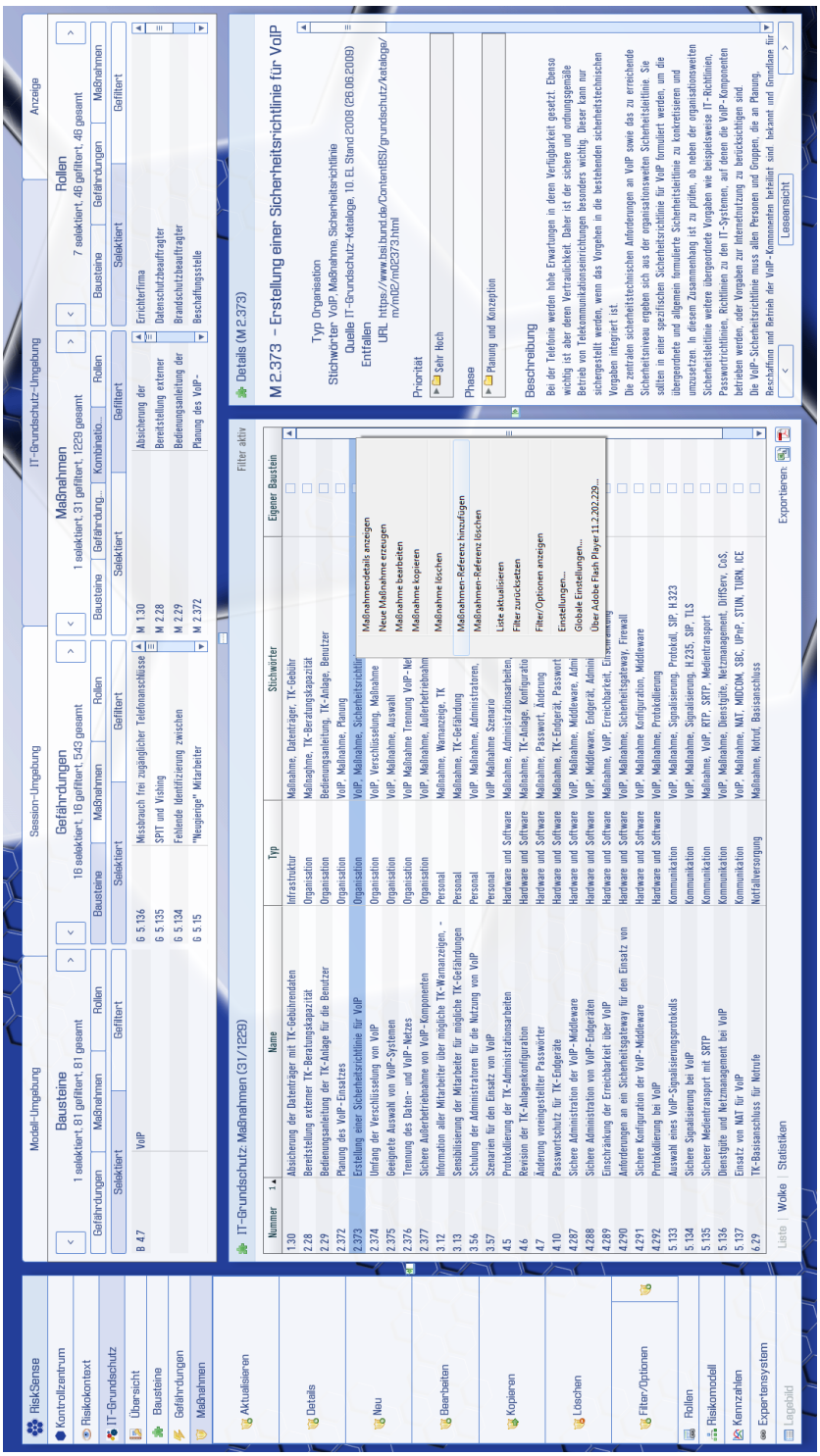


Figure 86: IT-Grundschutz safeguard management, currently showing safeguard details

Figure 87: Cross-reference management, currently prioritizing and assigning safeguard to threats (detailed risk analysis)

Figure 88: Incorporated ISO/IEC 27002 mapping with IT-Grundschutz safeguards

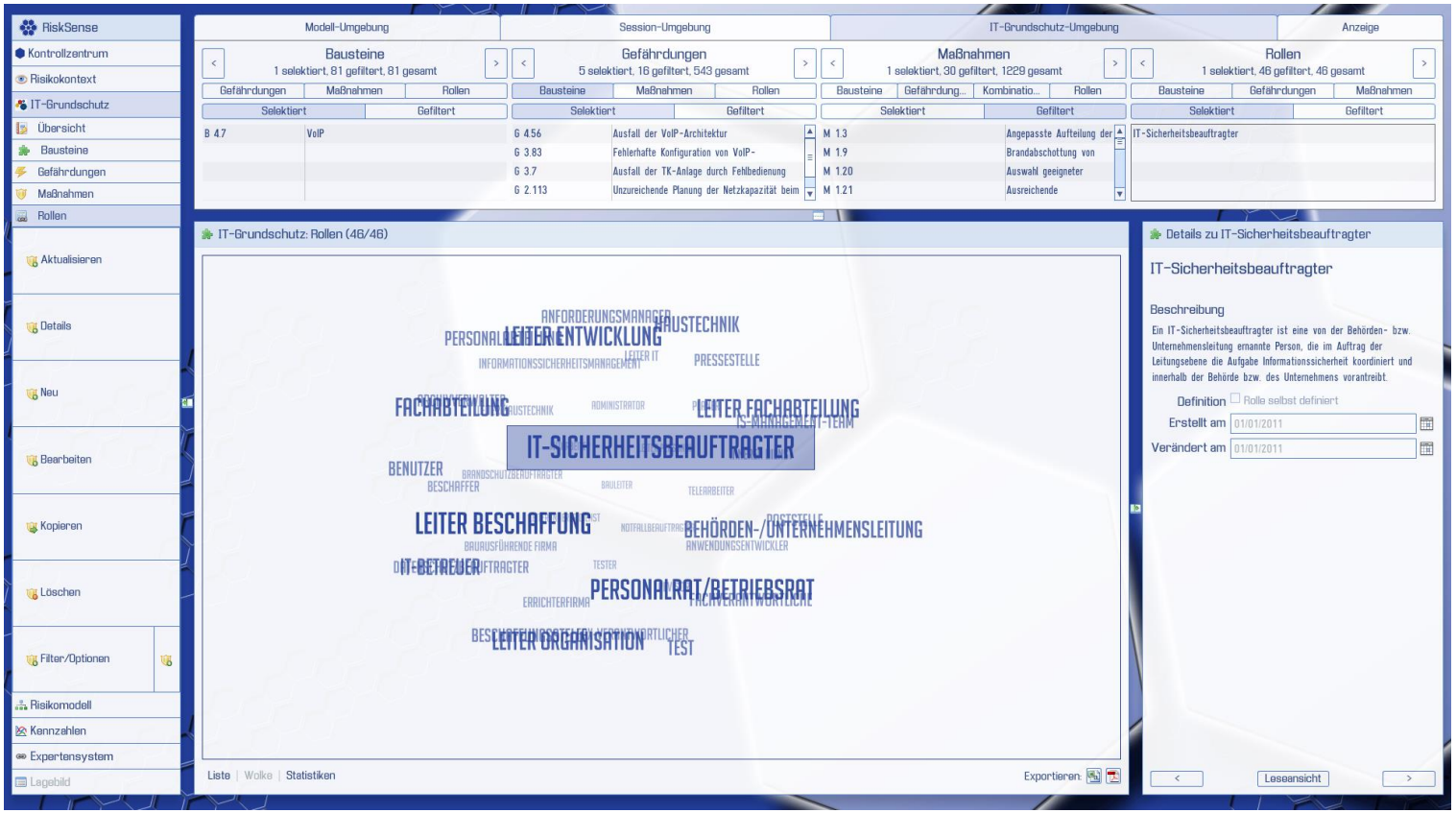


Figure 89: IT-Grundschutz role management, currently showing cloud view

5.1.3.2 Risk Estimation

The risk assessment component consists of separate interfaces for asset management (including scenario and joint analysis) and safeguard maturity estimation. The functionality for adjustment of risk factors is provided through the asset management interface (allowing the adjustment of protection criteria, modules, threats, safeguards and roles based on the asset catalog of the risk model), while the safeguard interface provides the ability to estimate threat-specific safeguard maturities based on the safeguard catalog of the risk model.

Figure 90 shows the asset management interface (master assets) with the subpanel showing asset details. Modules are assigned to master assets (and can be analyzed in detail) using the IT-Grundschutz interfaces and are simulated identically for all scenario assets, therefore allowing a comprehensive dependency analysis while minimizing the required estimation effort.

Figure 91 outlines the scenario asset tree(s) used to model dependencies between assets. The asset master list and the asset slave trees can be displayed side-by-side, allowing drag-and-drop assignment of dependencies. Also, established dependency sub-trees can be copied within the scenario analysis to avoid repetitive work.

The aggregation method used for each inheritance step and each protection criterion defaults to the energetic sum (see 3.1, *Model Assumptions and Limitations*), but can be adjusted to the context and organizational preferences (e.g. the cluster servers use the minimum availability exposure of their children due to their redundancy, while still using the energetic sum to estimate the accumulated confidentiality and integrity exposure, because both systems expose these protection criteria independently).

Starting at the root of the scenario tree(s), protection criteria requirements for scenario assets can be established, documented and inherited to their child assets. This is performed until all scenario assets have assigned requirement levels (filtering options available).

The information associated with each asset can be inspected and specific risk factors managed individually by drilling-down through its modules, threats, safeguards, roles and users (see Figure 93 and Figure 94). The interface also allows asset-, module- and threat-specific estimation of safeguard maturities related to individual assets.

5.1.3.3 Risk Evaluation

The second risk assessment interface provides the ability to estimate safeguard maturities based on ISO/IEC 27002 controls or IT-Grundschutz safeguards directly (depending on the desired assessment detail).

The back-end dynamically provides the user with assets, modules and threats cross-referenced with the selected safeguard(s) within the risk model. The framework gives the users the ability to estimate threat-specific safeguard maturities for all desired objects (depending on the desired assessment depth), aided by additional control questions defined for the safeguards in question.

Details on the selected IT-Grundschutz safeguard can be displayed within the subpanel to aid the estimation.

The interface also enables the sensitivity analysis of safeguards, showing their current impact on the overall model. Agents only see IT-Grundschutz safeguards within their realm of responsibility. The risk managers can simulate the view of specific roles using the filtering mechanism to establish distinct role estimation interfaces.

Figure 90: Master assets, showing risks, currently showing asset details

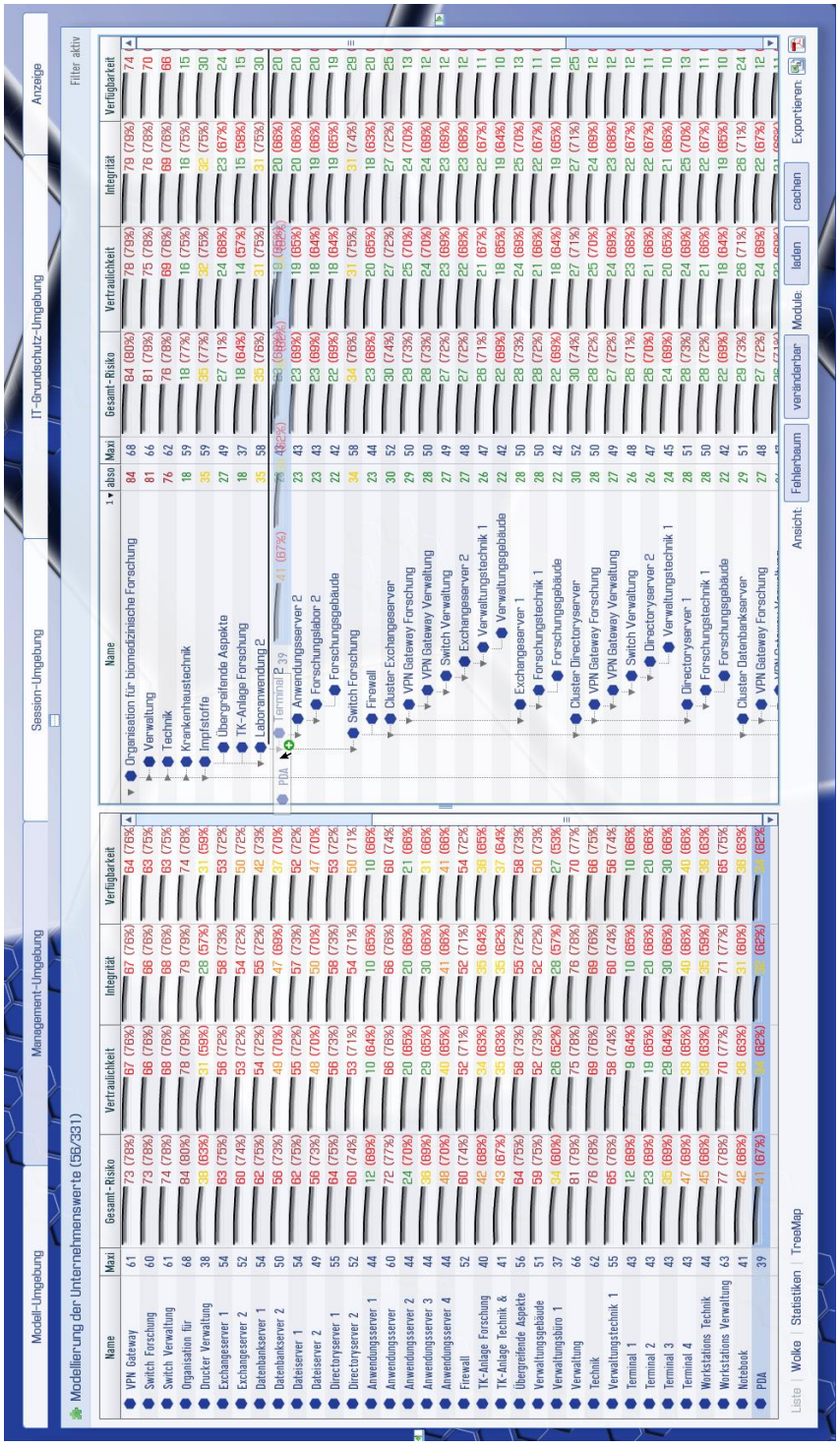


Figure 91: Drag-and-drop scenario dependency-assignment of assets, showing exposure trends of protection criteria and associated risks

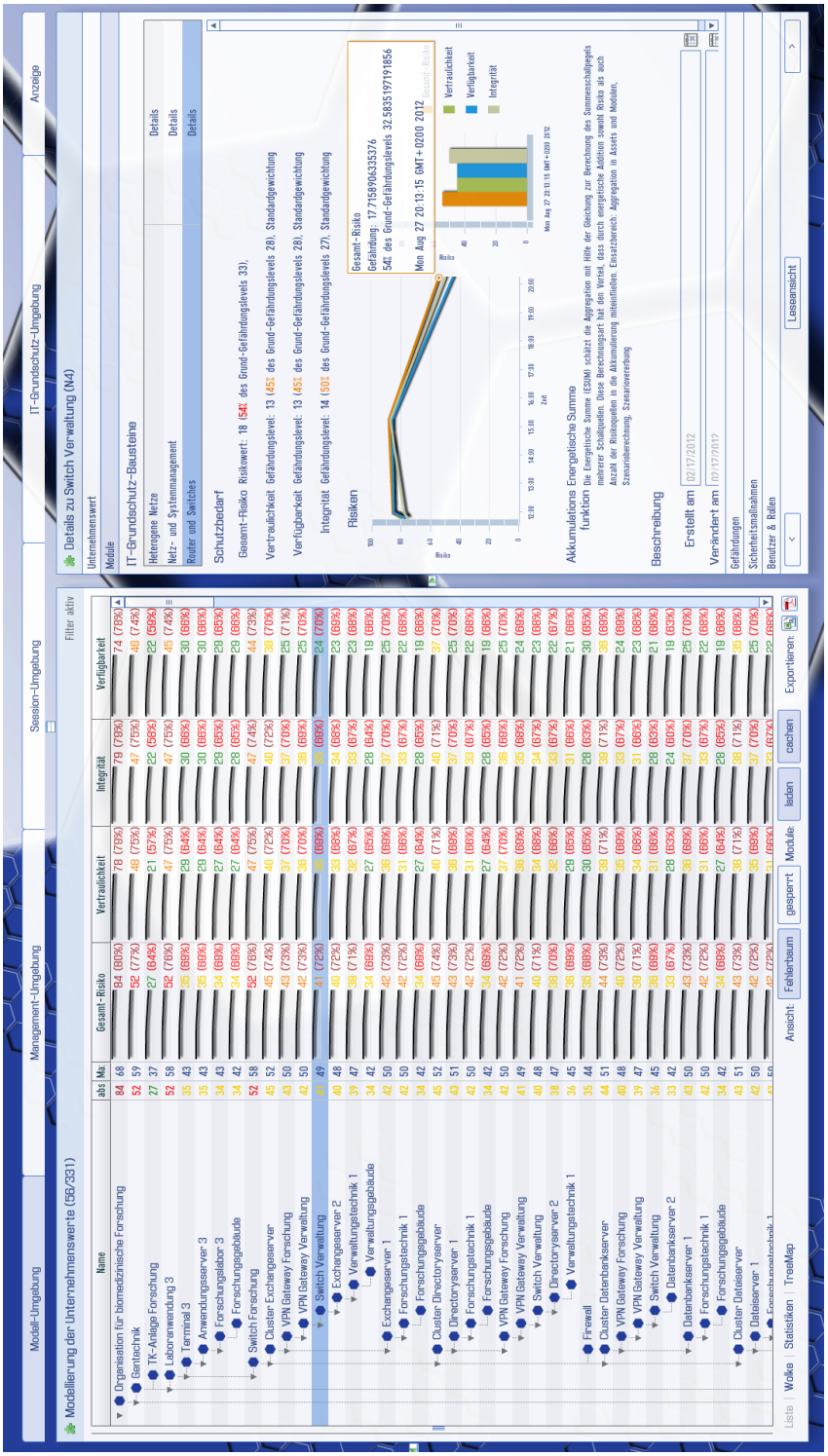


Figure 92: Scenario tree and asset details, currently showing information associated with one of its modules

Figure 93: Module-threat-safeguard-role-user information drill-down for every asset

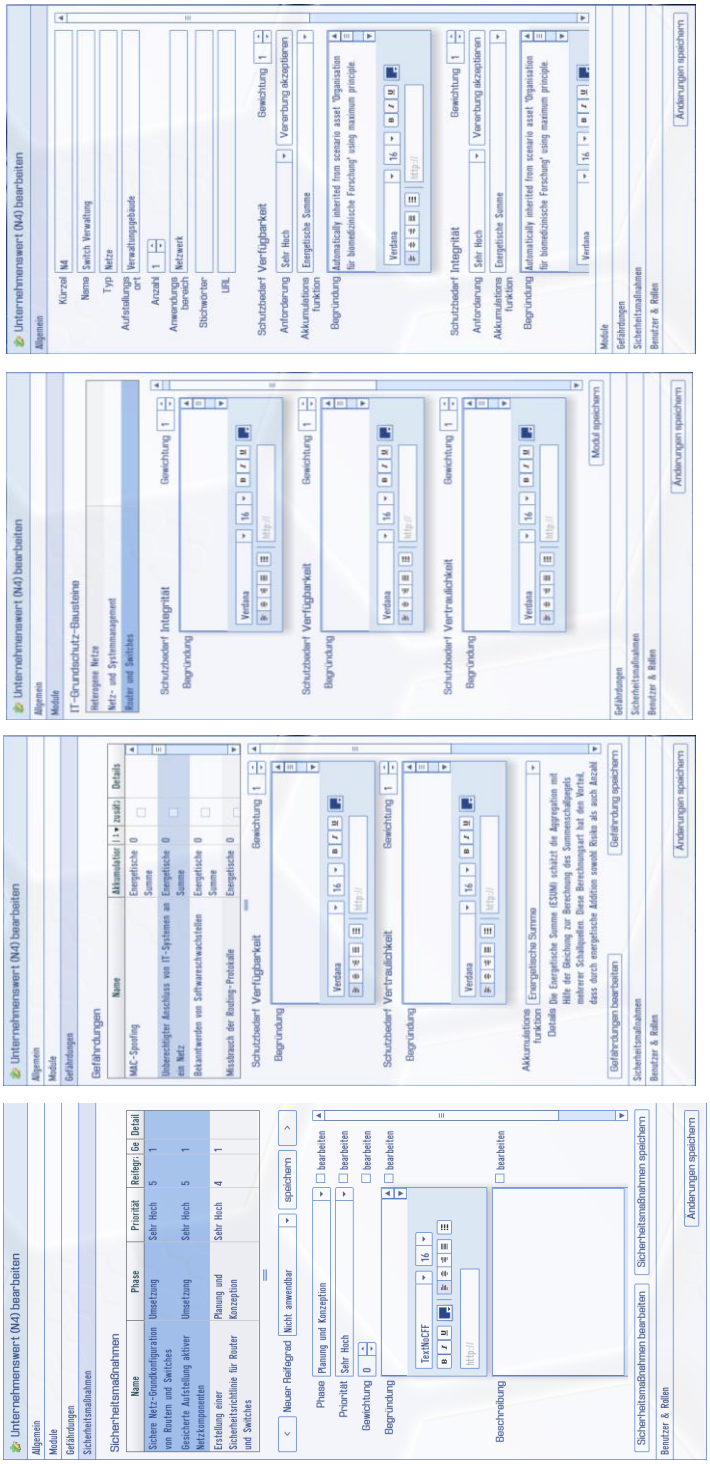


Figure 94: Module-threat-safeguard-role-user drill-down for adjustment of risk factors for every asset

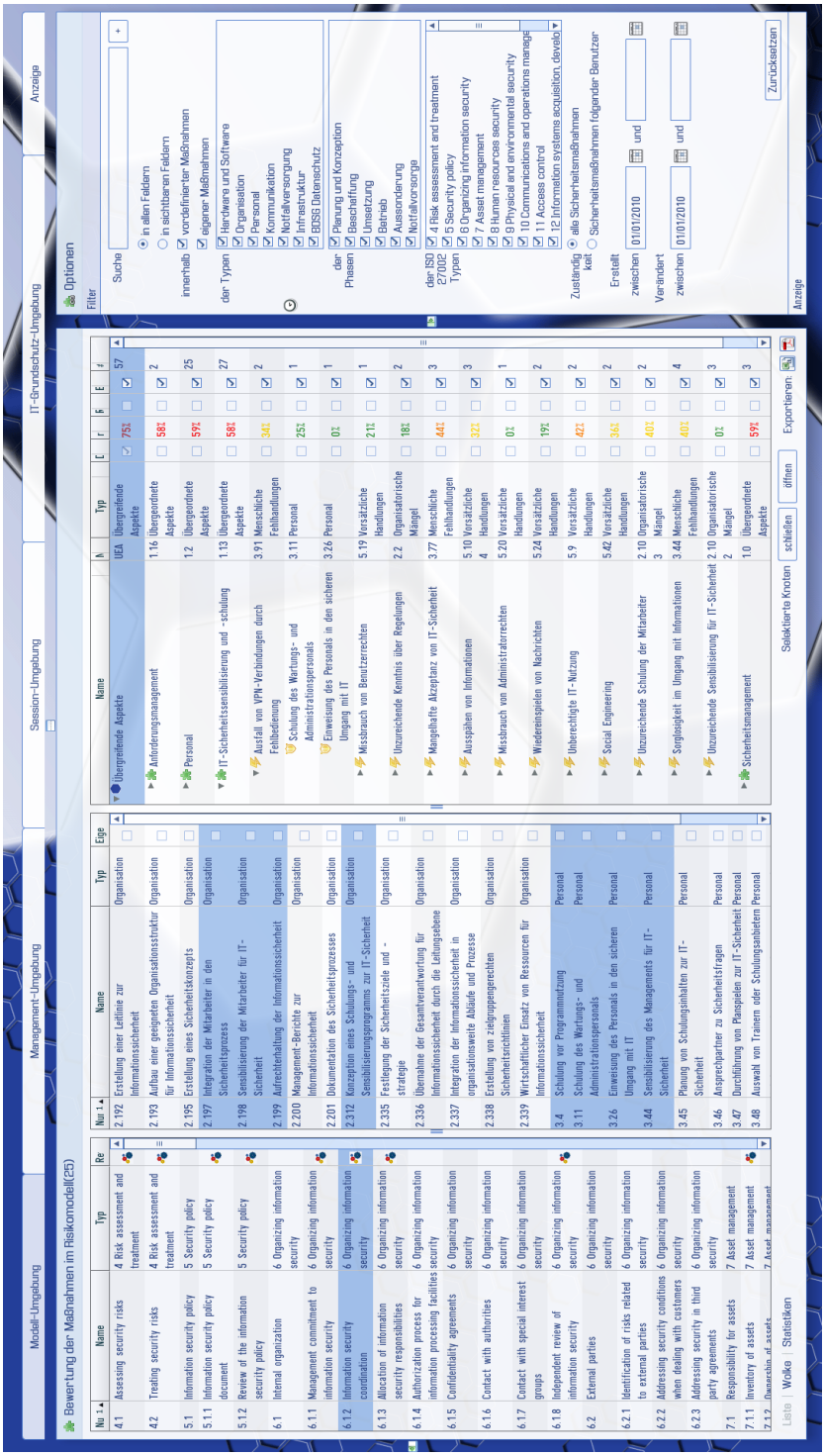


Figure 95: Safeguard management interface, currently using the ISO/IEC 27002 control mappings

Figure 96: Safeguard management interface showing sensitivity analysis and asset-, module- and threat-specific safeguard maturity evaluation, supported by additional control questions

5.1.4 Risk Treatment

Basic risk treatment options are supported within the prototype using actions (e.g. policies, procedures, guidelines, activities, etc.) that can be assigned to their respective risk factors within the risk model. This allows for multiple granularity levels when documenting treatment options, from very high-level assignments to highly granular asset-, module- and threat-specific documentation of safeguards involved in *risk reduction*.

To support all four options available for the treatment of identified risks, actions can also be defined to:

- represent projects or processes for *risk avoidance*,
- reference contracts, requirements and procedures for *risk transfer*, and
- document *risk retention*, by allowing a formal acceptance of clearly defined residual risks, as shown in 5.1.5.

Aside from general information about actions, states, schedule, due date, responsible users and initial/recurring costs can be documented. Agent users can only read and edit actions in their realm of responsibility and all users are dynamically provided with a calendar component outlining their actions (see Figure 97).

Figure 97: Subset of the risk management overview panel, allowing a user-specific view of safeguards, actions and their schedule, outlined using a calendar component

Using the safeguard interface, users can map asset-, module- and threat-specific safeguards to planned or existing actions, providing reference to organization-specific policies and procedures.

Advanced filtering and assignment options allow the easy establishment of very basic as well as highly detailed mappings between organizational risks and actions, providing the data basis for future Return-On(-Security)-Investment calculations.

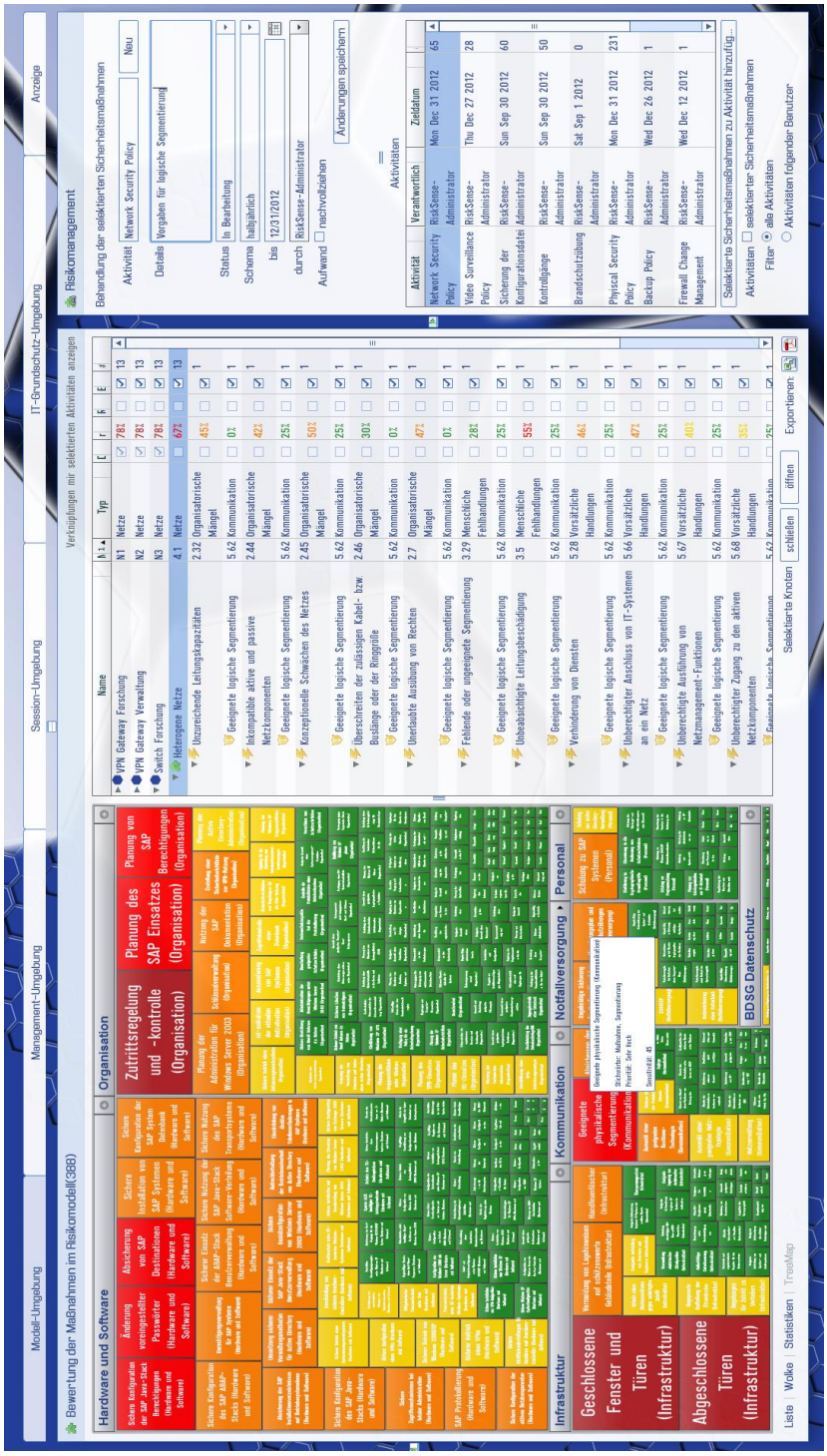


Figure 98: Safeguard management interface showing sensitivity analysis using TreeMap view and the action management sub-panel that allows asset-, module- and threat-specific safeguard-reference and filter operations

5.1.5 Risk Acceptance

All residual safeguard risks within the risk model can be formally accepted by the organization's top management.

Each acceptance of residual safeguard risks has to be justified and defined up to a specific date. Documentation of risk acceptance is supported using the safeguard evaluation interface, providing filtering and mapping functionality regarding asset-, module- and threat-specific safeguard maturity evaluations as well as organizational actions, as shown in Figure 99 .

Accepted safeguard risks are flagged to have a specific level of acceptable immaturity to account for dynamic changes to risk model target-maturities (and respective changes of residual risks) during the objects lifetime. Until each risk acceptance object becomes invalid, residual safeguard risks are neglected during model re-estimation up to their level of accepted safeguard immaturity.

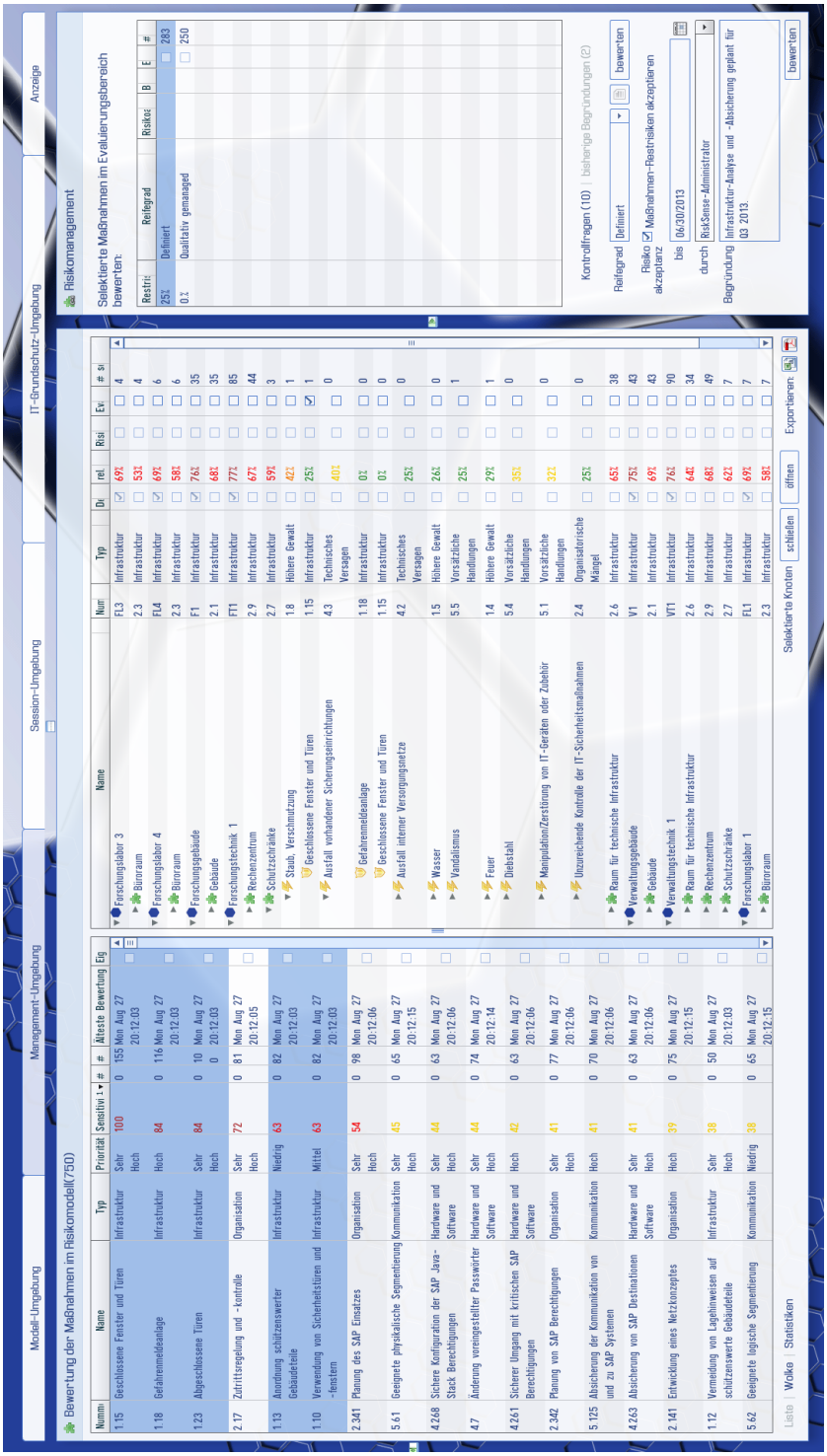


Figure 99: Safeguard management interface showing formal acceptance of residual risks, resulting from asset-, module- and threat-specific safeguard immaturities

5.1.6 Metric Assessment & Management

Within the metric management interface, risk managers can create, update, copy, delete and derive metrics, as well as register external sensors for automated data acquisition.

Base metrics can be evaluated by risk managers or agents with the appropriate role assignments. Derived metrics are calculated automatically.

The derivation of metrics is aided by providing a formula field with basic mathematical operators and a selection interface for base metrics. Agents only see metrics in their realm of responsibility.

If a metric should be used within the integrated expert knowledge management system, fuzzy terms can be defined to establish the required indicators.

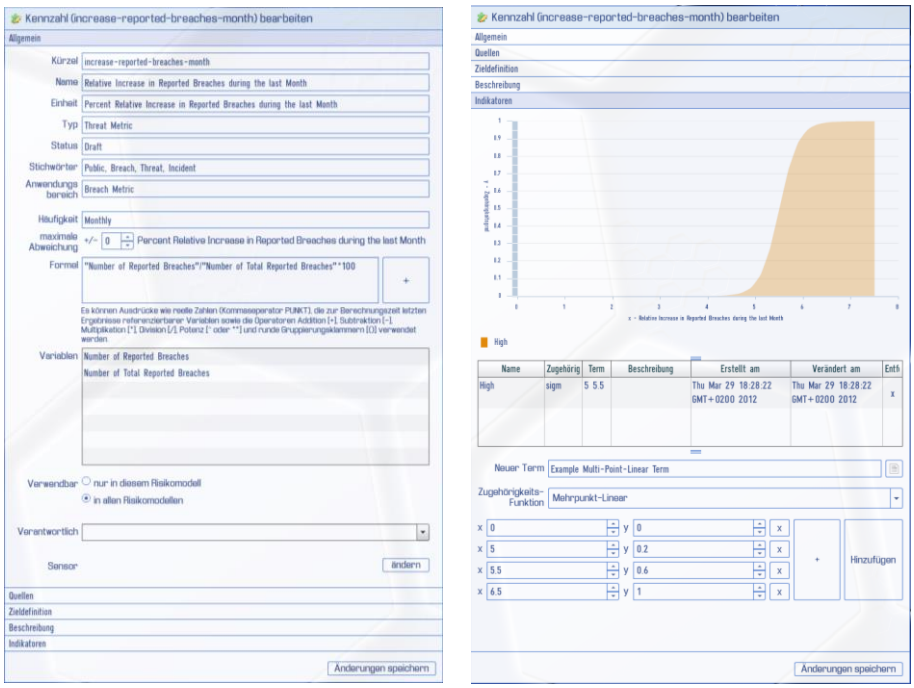


Figure 100: Metric and indicator management of a derived metric. Indicators have to be established for all metrics that shall be used within the integrated expert knowledge system.

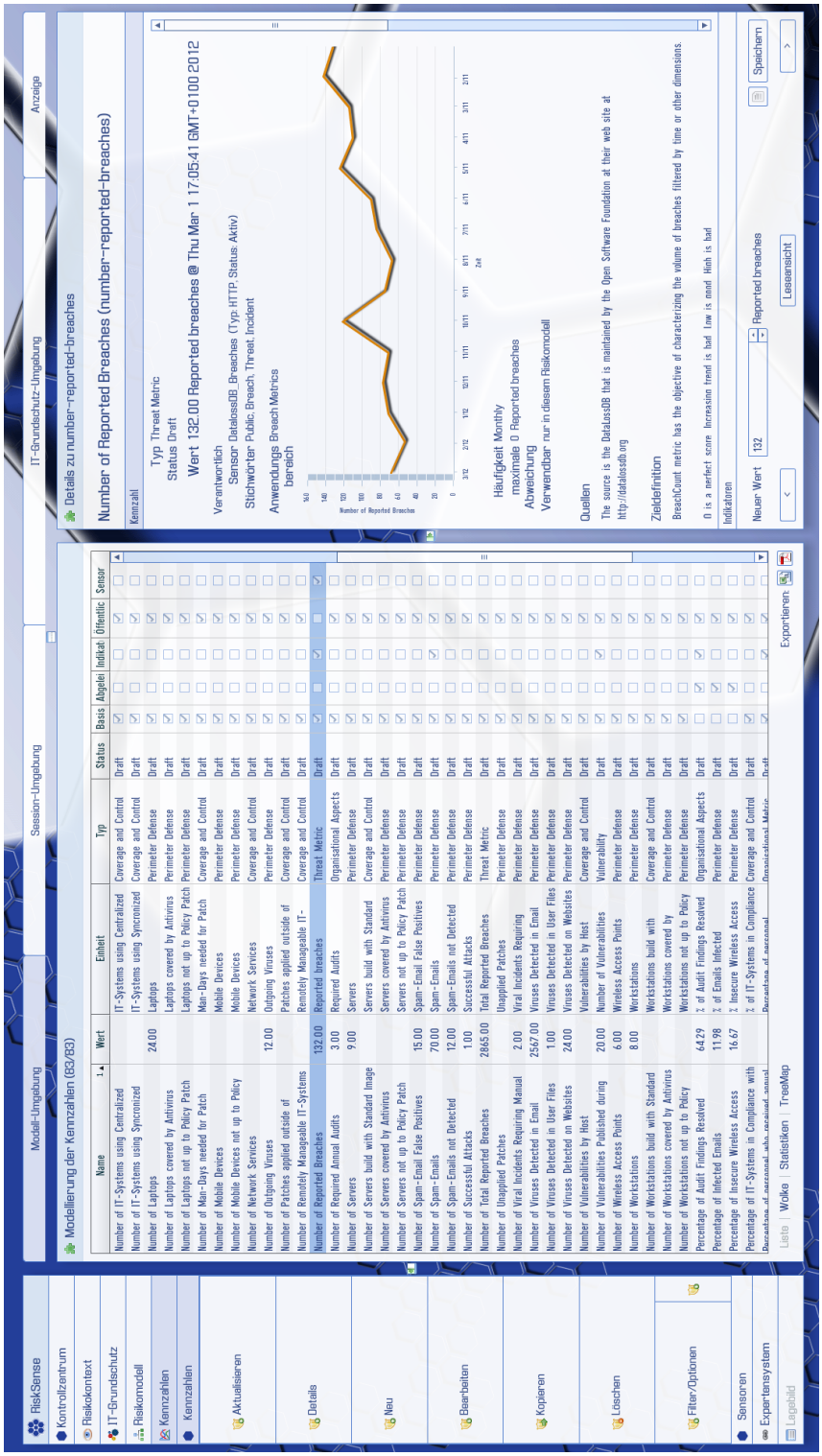


Figure 101: Metric management, currently showing metric details.

5.1.7 Expert Knowledge Management

The expert knowledge management system allows the definition of rules describing relationships between metrics, their indicators and risk factors.

To aid the exchange of expert knowledge between organizations, these rules are defined for generic risk factors as provided by IT-Grundschutz. Each generic risk factor target can be mapped to organization-specific instances to provide high granularity when establishing relations. Specific instances of general risk factor targets are identified within the risk model and presented to the risk manager for detailed assignment and weighting as shown in Figure 103 and Figure 104.

Because of time constraints, the development of selection interfaces for risk factors focused on IT-Grundschutz safeguards, allowing the highest granularity of control compared to threat and impact targets (higher level factors).

5.1.8 Sensor Integration

To aid integration and automation when dealing with security measurements, the prototype allows the management of sensors which are defined to accept measurements from registered, independent scripts or programs gathering respective measurements locally or on remote systems.

Using software authorization, sensors can be registered to provide respective measurements to the web-service, while communication can be protected by SSL and authenticated via pre-shared-secrets.

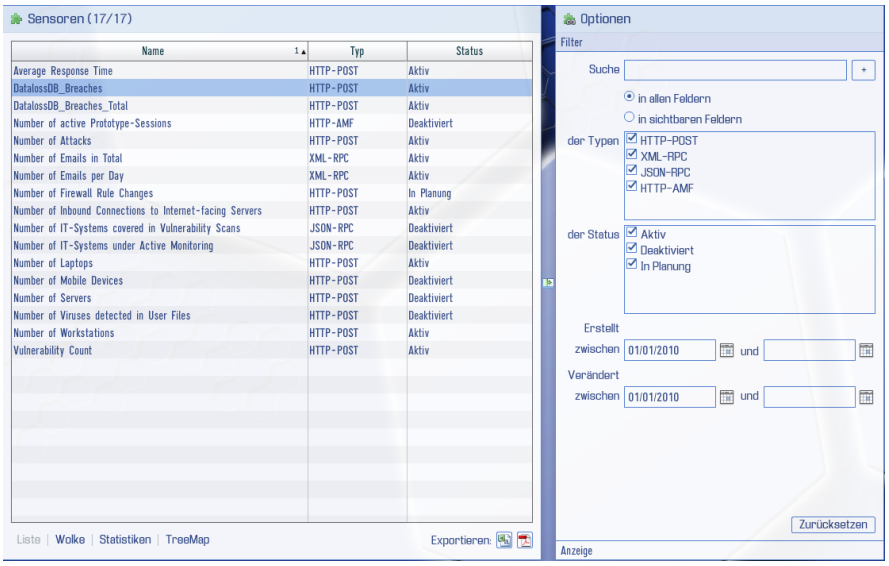


Figure 102: Management interface for external sensor integration

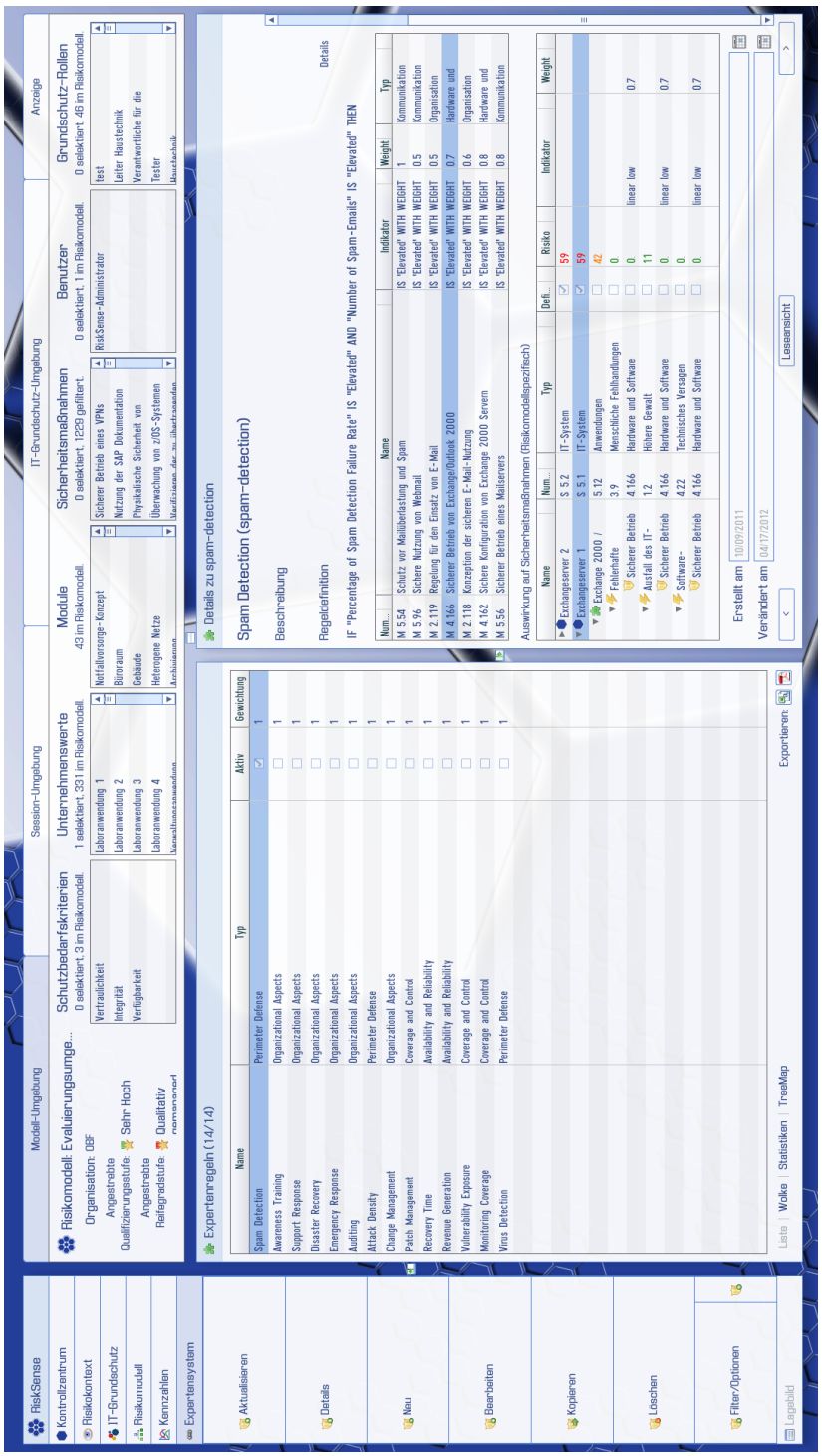


Figure 103: Expert knowledge management, currently showing expert rule details. Each general risk factor can be assigned and specifically weighted to influence specific risk factor instances within the risk model.

Figure 104: Management interface for risk factor targets within the risk model.

5.1.9 Continuous Risk Communication, Monitoring and Review

The proposed model and prototype interfaces enable collaboration aspects to support continuous risk communication as well as various schedules for activities, risk factor estimations and security measurements to support continuous monitoring and review.

The dashboard view is included in most interfaces as an additional view (e.g. IT-Grundschutz module interface, see Figure 105 and Figure 106) that is dynamically updated with the object selection and allows the consolidation and analysis of various security relevant aspects.

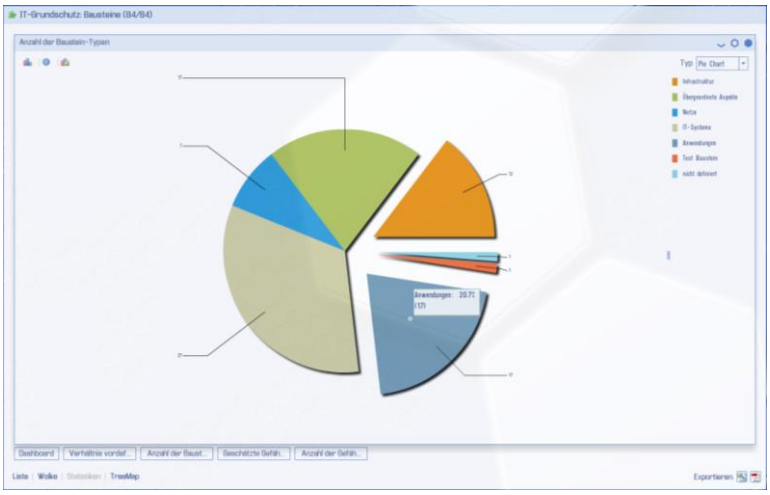


Figure 105: Example IT-Grundschutz module dashboard, showing the relation and number of available module types

Figure 106: Example IT-Grundschutz module dashboard, showing the estimated number of threats and likelihoods of filtered and selected modules

6 Evaluation & Validation

The prototype has been used to apply the proposed model, including the evaluation of the applicability of functional relationships for risk assessment (see 2.3.1 and 3.1) and fuzzy logic for measurement inference based on expert knowledge (see 2.3.4 and 3.3).

The practicability and reasonability of the approach has been tested and validated in the course of several simulations, a comprehensive risk model based on the evaluation model defined in Annex A of [3], as well as through the extensive evaluation by a unit of the Federal Ministry of Defense (see Annex A).

Further evaluation of the prototype has been done within the context of SEC Consult to achieve an ISO/IEC 27001 certification.

The validation of metrics is aligned with the requirements defined in ISO/IEC 27004 [51, p.20] to ensure usefulness and cost-effectiveness of selected measures.

As no extensive empirical studies on measure to risk relations are readily available in the context of information security, the evaluation and validation of relevant relations of measures, indicators and expert rules is part of on-going research. A potential method for the validation of indicators could be based on an economic survey incorporating indicator estimations of several standard measurements within the context of an overall corporate governance maturity level according to [44], allowing a statistical mapping of measurement maturity to corporate maturity using linear regression. Using this information, measurement indicators could be extrapolated based on the desired maturity of the organization.

Because the proposed model constitutes a highly complex model based on a multitude of cross-references variables and possible options for the estimation of various behaviors, further research and development will include continuous testing and evaluation efforts.

The following list outlines the primary “lessons learned” during the course of the research project:

- Due to the comprehensive IT-Grundschutz framework, the information load is very high, including database intensive queries, so further development should focus on optimization of database structure and queries
- Due to the high information load, serialization and rendering of client side information as well as the management of asynchronous updates to handle the continuously changing risk model has to be highly optimized
- Because Adobe handed the development of the Flex SDK to the Open-Source-Community (Apache Flex) in early 2012, the usage of HTML5 (which is assumed to ultimately become the successor of Flex and similar browser plugins) for asynchronous communication should be facilitated for further development, including lazy-loading and push technologies.
- Near term extensions to the model should prioritize comprehensive collaboration, document management and risk management components (e.g. mapping of IT-Grundschutz safeguards to user-defined high level controls, implementation projects, etc.) to increase the prototypes usability within complex real-world assessments.

- To allow the usage of the prototype without special training, work-flows as well as an online help should be integrated.
- Further development should allow the user- customizable integration of further aggregation functions and the potential to use different aggregation functions in parallel to support comparison of results.
- To provide comprehensive consolidation, reporting and dash-boarding capabilities, meta-languages should be integrated and used to describe the required data.
- Because multiple different users potentially estimate certain risk factors within the model, their estimations should be consolidated using advanced techniques like Delphi analysis to provide overall estimations for an assessment cycle.

6.1 Evaluation & Validation Models

Several evaluation and validation scenarios have been studied during method design and software testing to aid a modeling-structure and framework that can be used to depict basic, as well as highly complex dependencies between system components.

The proposed model is compliant with all BSI-Standards, ISO/IEC 27001 (certificate based on IT-Grundschutz) [71], ISO/IEC 27005 (risk management) [1] as well as ISO/IEC 27004 (security measurement) [34] and includes safeguard mappings with ISO/IEC 27002 [57].

After completion of prototype development and testing, a fictitious model used for evaluation of risk management tools based on previous research (see 6.1.1) as well as a comprehensive real-life model based on an internal assessment model of the Department of Defense (see 6.1.2) have been defined and evaluated to analyze:

- the usability of the approach,
- the transparency and conclusiveness of estimation results, and
- the amount of complexity that could be depicted using the proposed model and prototype.

6.1.1 Biomedical Research Organization (fictitious model)

The risk model used to evaluate risk management tools in previous research [3], [55] has been re-modeled within the prototype, outlining a fictitious organization with two physically separated buildings for biomedical research and administration.

The research building contains four laboratories *FL1…FL4* with increasing protection criteria requirements as well as a technical room *FT1*, hosting network infrastructure and a failsafe data center.

The backup data center is located separately in the technical room *VT1* of the administrative building, connected using VPN over a dedicated line (*N1*, *N2*).

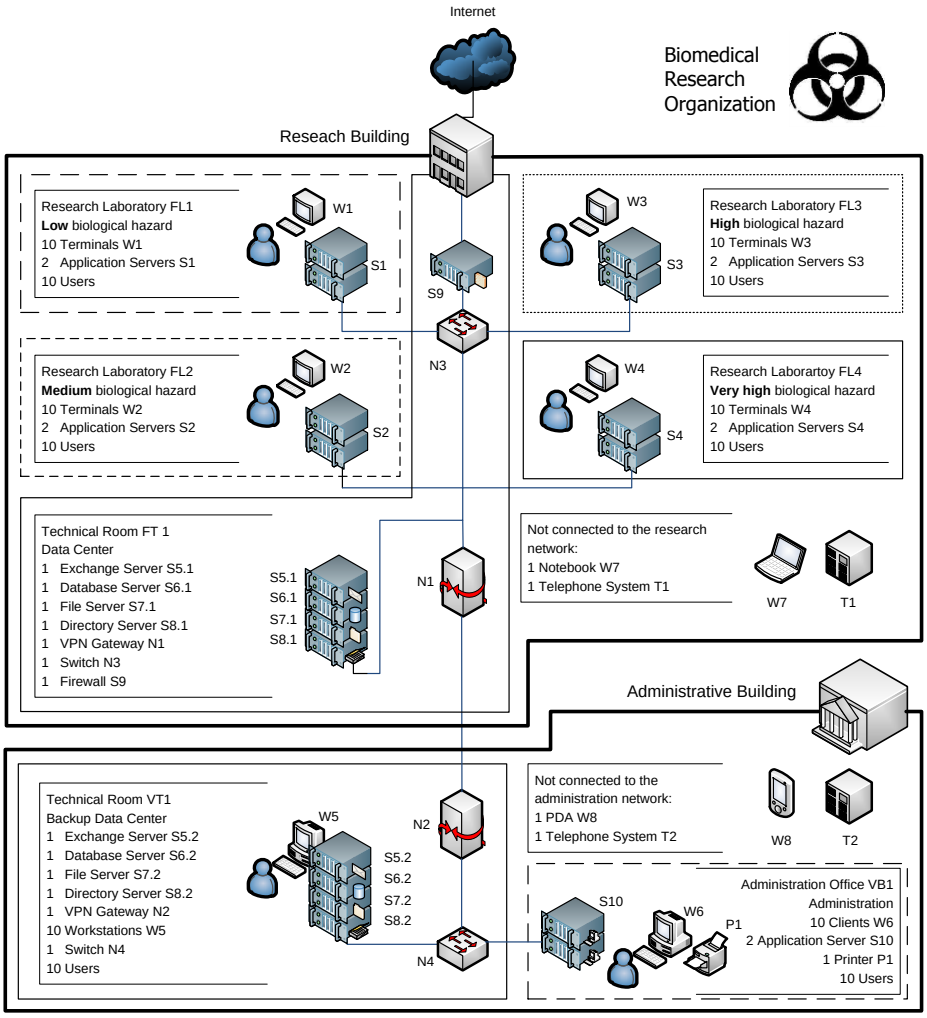


Figure 107: High-level overview of the ficitious evaluation model [cp. 3, p. A-3]

The increase in protection criteria requirements (impacts) in *FL1…FL4* as well as S1…S4 is clearly reflected by the increasing risks of their respective assets as shown in Figure 90.

Housing both data centers with maximum protection criteria requirements, *FT1* and *VT2* reasonably show increased risks as well as the core communication systems *N1*, *N2*, *N3*, *N4* and *S9*, which are not implemented redundantly.

The clustering of the application servers S5.*… S8.* is modeled using cluster assets, which – during impact analysis – where configured to inherit the minimum exposure of availability of their redundant systems as shown in the scenario trees in Figure 91 and Figure 92.

Dependencies and communication paths between applications as well as infrastructural dependencies could be modeled easily and efficiently, allowing the depic-

tion of highly detailed scenario-specific models as required for e.g. assessment of critical infrastructures.

6.1.2 Department of Defense (real-world model)

The Austrian Department of Defense was provided with the prototype system as well as detailed information about the underlying model for detailed evaluation.

> *"For testing purposes, artifacts of real-live military installations of the Department of Defense have been modeled and estimated with real- as well as fictitious-estimations using the RiskSense prototype."*
> [cp. Annex A, p. A-3]

Due to confidentiality requirements of safeguards and risk factor estimations, the full evaluation model has not been disclosed by the Department of Defense.

A short summarization of evaluation results is given as follows, the detailed German evaluation report can be found in Annex A.

> *"The applied estimation method appears to be a usable approach for the evaluation of an organization's level of security."*
> [cp. Annex A, p. A-4]

> *"The ability to integrate security sensors provides interfaces to real-time-systems, allowing the generation of accurate and up-to-date situational reports."*
> [cp. Annex A, p. A-4]

> *"The internal modeling structure of RiskSense has proven most useful, as adaptions and extensions quickly allow the analysis of attack vectors."*
> [cp. Annex A, p. A-5]

> *"The excellent impressions of the prototype have been confirmed with this test and have shown that RiskSense has the potential to satisfy the need for information security assessments of commercial companies as well as the Department of Defense."* [cp. Annex A, p. A-5]

6.2 Market Assessment

An assessment of the market potential has been done by SEC Consult (see Annex B) based on its vast experience in implementing risk management for information security. It clearly showed that RiskSense is especially valuable for large companies, government and defense organizations with high risk sensitivity as well as a small set of small companies with strong focus on security. Assessment details can be found in Annex B.

"The segment of large corporate-, government- and defense-organizations is assumed to build a sound revenue potential for the solution."
[cp. Annex B, p. B-3]

"SEC Consult sees the clear potential to use this comprehensive approach manifested in RiskSense to leverage its expertise and to create growth in one of the future markets within information security."
[cp. Annex B, p. B-3]

Based on the evaluation requirements proposed in [3] as well as the evaluation of risk assessment and management tools over the past years, the criteria catalog has been updated and extended in order to estimate degrees of accomplishment using the following high-level criteria:

- Risk Assessment
- Risk Management
- Collaboration and Continuity
- Business Integration
- Situation Report, Simulation and Decision Support

Figure 108 shows a high-level comparison of evaluated tools using the evaluation criteria outlined in Figure 109. The scale shown in Figure 108 is a result of the potential maximum score, due to the underlying requirement questionnaire and the weighted summation of tool-specific requirement fulfillment.

Figure 109 lists the evaluation criteria as well as their weighted cross-references with the topics outlined above. Tool-specific evaluation scores have been omitted for readability reasons.

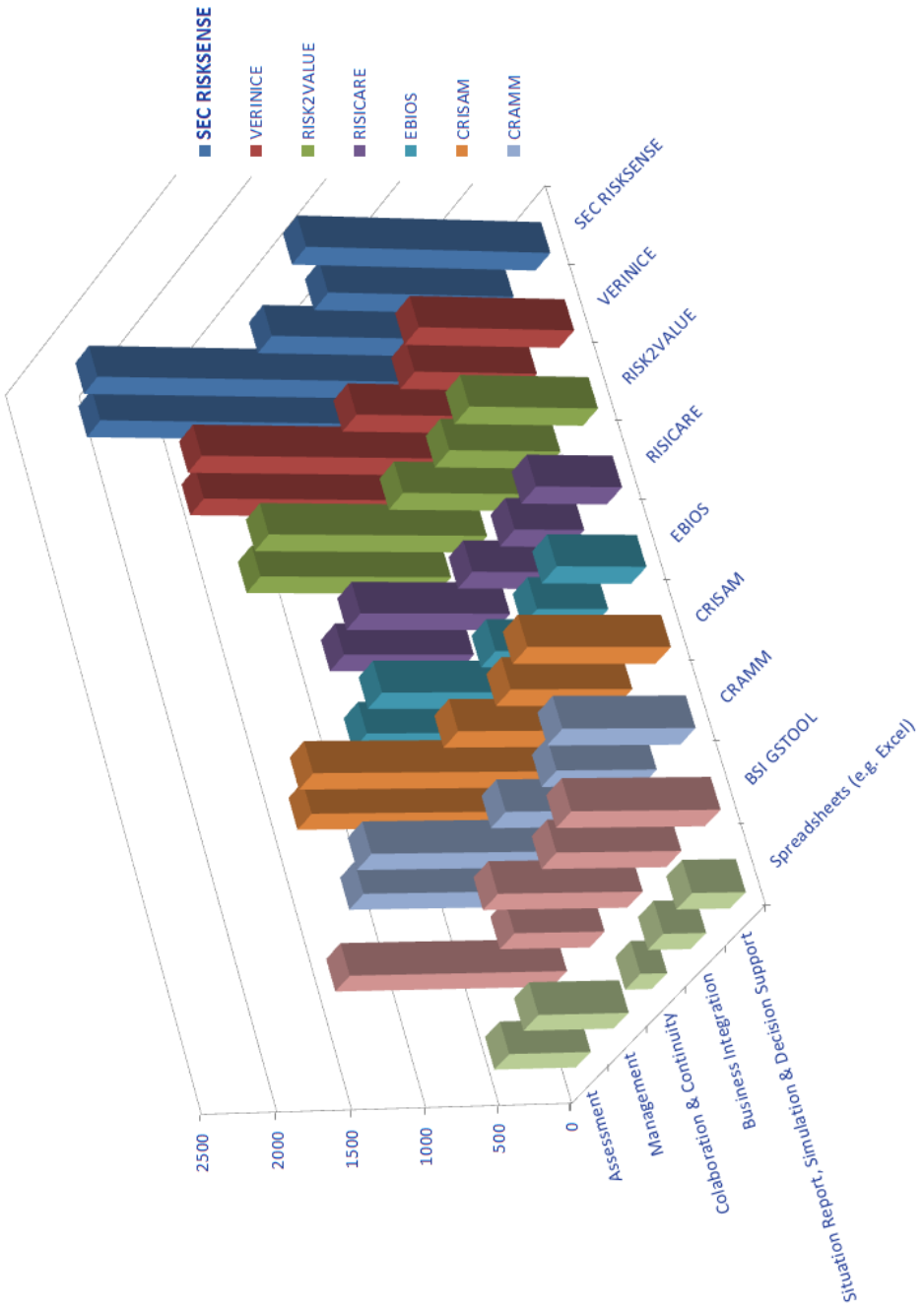


Figure 108: High-level comparison of evaluated risk-assessment and -management tools based on [3]

Assessment	Management	Collaboration & Continuity	Business Integration	Situation Report, Simulation & Decision Support	Nr.	Criteria	Criteria Weighting
1	2				1	How often are updates concerning controls/measures released	5
2	1	1			2	How often are updates concerning assets/modules released	4
2	1	1			3	How often are updates concerning threats/vulnerabilities released	4
	1		2	1	4	How often are updates concerning the supporting tool released	4
2				1	5	How high are the human resources dedicated to continuous development regarding the risk factor catalogs	8
1	2	2	2	2	6	How high are the human resources dedicated to continuous development regarding the tool	5
2		1		1	7	How high is the level of detail of the Risk-Assessment catalog	7
	2	1		1	8	How high is the level of detail of the Risk-Management catalog	9
2	1			1	9	How high is the adaptability of the risk factor parameters	7
2	1			1	10	How high is the adaptability of the risk aggregation algorithms	7
1	1			2	11	Are temporary simulations regarding the risk factors possible	10
2	2	1	1		12	Does the model/tool focus on technical security aspects	7
2	2	1	1		13	Does the model/tool focus on organizational security aspects	8

Assessment	Management	Collaboration & Continuity	Business Integration	Situation Report, Simulation & Decision Support	Nr.	Criteria	Criteria Weighting
	2				14	How high is the price of the method/tool	4
	2		2		15	How high are integration and continuous supporting/consulting costs	8
	2	2			16	How high are the resources needed concerning user training	4
	2	2	1		17	How much resources are needed to provide risk management continuity	7
1	1	1	1	1	18	How high is the public recognition of the method/tool	3
	2	2	1		19	Does the method/tool support initial risk management activities (e.g. ISMS related documentation, role-based responsibilities, etc.)	7
2	2	1	2	1	20	How high is the level of detail concerning the method documentation	7
1	2	1	1	2	21	How high is the level of detail concerning the tool documentation	8
2	2	1			22	How high is the level of detail of online-documentation concerning the risk factors	6
2	2	2	1	1	23	Can the tool be used intuitively	6

Assessment	Management	Collaboration & Continuity	Business Integration	Situation Report, Simulation & Decision Support	Nr.	Criteria	Criteria Weighting
2	2		1	2	24	How clearly is information presented within the tool	8
1	1	1	1	2	25	How high is the level of detail concerning data drill-down (e.g. reasoning) within the tool	9
2	2		2		26	Can the asset/module catalog be extended	5
2	2		2		27	Can the asset/module parameters be adapted to organizational needs	5
2	2		2		28	Can the risk factor catalog be extended	5
2		1	2	1	29	Can organizational support systems (e.g. SAP, Active Directory, etc.) be easily integrated into the assessment model	7
1	2	1	1	1	30	How high is the adaptability of risk reporting (e.g. XML)	8
1	2	1	1	1	31	How many (customizable) reports are predefined	8
2	2	2		1	32	Can risk assessment and management continuity be managed, visualized and reported	9
2	2	2	1	1	33	Is the method/tool documented and supported in multiple languages	8
2	2	2	1	1	34	Does the tool support internationalization (i8n)	8
2	2	2	1	2	35	Can access to strictly confidential information be restricted and cryptographically protected (e.g. four-eye-principle, token authentication, etc.)	6

Assessment	Management	Collaboration & Continuity	Business Integration	Situation Report, Simulation & Decision Support	Nr.	Criteria	Criteria Weighting
1	2	2	2	1	36	Is the tool analyzed/tested for security vulnerabilities	8
	2	1		1	37	How high is the level of detail concerning risk management activities (e.g. safeguard/control descriptions, etc.)	8
2	1			1	38	Are effectiveness measures (e.g. maturity levels, control questions) available to support risk evaluation	7
2	1			1	39	How high is the level of detail concerning risk assessment factors (e.g. threat/vulnerability descriptions, etc.)	6
2	1			1	40	How high is the level of adaptability of the risk factor model	6
2	2		1	2	41	How high is the level of detail and adaptability concerning the realizable model complexity (e.g. dependencies, expert rules, alarm trigger, etc.)	8
2	1	1		2	42	How high is the level of detail and reliability concerning pre-evaluated risk factor parameters	10
1	2	1	1	2	43	How high is the adaptability and level of detail of scope and target definitions for context establishment (e.g. various target levels, by asset/threat/control types)	9

Assessment	Management	Collaboration & Continuity	Business Integration	Situation Report, Simulation & Decision Support	Nr.	Criteria	Criteria Weighting
1	1	1	2	2	44	Does the model/tool support automated assessment and management of security measures (e.g. sensor/script integration to gather security measures from e.g. IDS, DC, AV-Gateway, etc.)	8
2	1	1	2	2	45	Can knowledge about security measures and their relations (e.g. attack vectors, correlating measures) be integrated into the assessment model	7
1	1	2	1	2	46	Does the method/tool support real/short-time situational reporting	6
1	1	2	2	1	47	Does the tool offer off-line support (e.g. remote audits w/o network connection, risk model separation, linkage and segregation by group/country/entity data boundaries, separation according to confidentiality requirements, etc.)	3
1	1	2		1	48	Does the tool offer risk management collaboration (e.g. multi-user capabilities, user-role risk factor assignments, scheduling of events, reassignment of actions, etc.)	9
1	2	2	2	1	49	Are business continuity aspects (e.g. modeling of dependencies, availability risk details, continuity management, etc.) considered within the method/tool	6

Assessment	Management	Collaboration & Continuity	Business Integration	Situation Report, Simulation & Decision Support	Nr.	Criteria	Criteria Weighting
2	2	1		2	50	Visualization and information drill-down capabilities	8
1	2	1	2	2	51	Return-On-(Security-)Investment (ROSI/ROI) capabilities, Sensitivity Analysis and Simulation	10
2	2	1	2	1	52	Are mappings to widespread standards (e.g. ISO 27001/2, IT-Grundschutz, NIST control catalogs, etc.) available	7

Figure 109: Cross-referenced tool-requirement-questionnaire, based on [3]

7 Outlook & Future Work

The prototype has already been deployed as an internal risk assessment tool at SEC Consult and has been used to achieve an ISO/IEC 27001 certification.

Additionally, a subsequent research project is conducted at the Austrian Institute of Technology, funded by the Austrian Research Promotion Agency (FFG) under the KIRAS national security program [3687486], with the Austrian Institute of Technology (AIT), the Federal Ministry of Internal Affairs (BMI), the Federal Ministry of Defense (BMLVS), several industry partners and the doctoral student.

The comprehensiveness of the German IT-Grundschutz catalogs, the incrementally improving risk-, measure- and knowledge-assessment and management process as well as the collaborative role-based approach which the system is based on, means that performance requirements for running the system can get considerably high in comparison with common risk assessment systems.

By merging security relevant information regarding organizational risks, dependencies, key-goal and -performance indicators, measures and expert knowledge, the presented approach offers novel insights into organizational risks.

7.1 Major Contributions and Limitations of this Research

The major scientific contributions of the research described in this thesis are:

- the definition of a highly adaptable information security risk-assessment and -management model based on the IT-Grundschutz framework
- the evaluation and identification of a practical knowledge management approach to relate empirical measures to subjectively estimated risk factors
- the definition of an integrated process covering continuous risk-, measure- and knowledge-management
- the design and development of a prototype to demonstrate and evaluate the practicability and usefulness of the proposed model and process

The foundations laid through the results achieved in this work now enable us to develop analysis models that offer near-real-time risk-based situational reporting capabilities, incorporating empirical measures into analytical risk models using exchangeable expert knowledge.

There are however some limitations of this research. The correctness of results can only be guaranteed if the following assumptions hold true:

- the environment in which the method is deployed has to have clearly defined secu-

rity requirements[19], so that stakeholders have a uniform understanding of real-world residual risks underlying the generalized security requirements of a baseline security approach, as provided by IT-Grundschutz
- the assets within the risk model are modeled to incorporate all modules to depict their relevant exposures
- the dependencies between assets and the aggregation functions used to depict the real-world behavior of risk-inheritance between dependent assets must reflect the characteristics of the modeled environment
- the results of detailed risk assessments in IT-Grundschutz [48] must be consistent with the level of detail and safeguard prioritization of existing modules, in order to allow a uniform distribution of security requirements across the risk model
- security metric indicators have to be evaluated consistently with the maturity targets defined for the risk model, in order to support correct application of expert knowledge
- the correctness of automatically gathered security metrics can only be guaranteed if sensors and related schema evolution is performed in a timely and accurate manner
- the definition of generalized expert knowledge must reflect the real-world correlation between metrics and their abstracted risk factors, which in turn has to be correctly mapped to its specific asset instances within the risk model

While most of them are of little practical importance, these limitations are clearly relevant, but can be overcome by several controls as shown in the section on future work.

From a more practical perspective, the opportunities generated by the proposed model and supporting prototype are:

- High level of assessment detail based on a comprehensive set of module-, threat- and safeguard-descriptions and additional control questions
- Low initial implementation- and continuous maintenance-costs because of pre-estimated and cross-referenced risk factors with role mappings
- Assessment of highly complex dependencies between assets
- Sensor- and user-supplied metric-management and associated business intelligence benefits
- Collaboration- and knowledge-management benefits
- Decision support based on near-real-time insights into the risk-based organizational situation

[19] through national or international standards, contractual agreements or requirement specifications

7.2 Future Work

Because the prototype development focused on the risk assessment and proof-of-concept integration of measurements and expert knowledge, further development should include a reimplementation of the prototype to satisfy end-user requirements (e.g. simplified user interfaces with work-flow support, detailed risk management options, adjustable reporting components, performance enhancements, etc.) and adapt new technologies (e.g. HTML5, clustering, indexing and in-memory database integration, etc.).

The consolidation of highly sensitive information concomitantly leads to increased security requirements of the architecture, secure software development lifecycle and organizational safeguards needed to provide adequate security for the management system. Therefore, future implementations are planned to be designed, developed and potentially certified according to the requirements defined in the Austrian ÖNORM A7700 standard [51] which focuses on the security of web-applications.

Detailed risk analysis is supported by a comprehensive method and set of risk factors, but extensions to the IT-Grundschutz modeling domain always need to be checked for estimated threat levels when compared to other modules. While common for a risk management expert, this task might not be suitable for an average user. Future development will consequently support a collaborative role based risk analysis approach, including workflow-models to enable collective analysis and estimation efforts using Delphi Analysis [4], the Analytical Hierarchy Process (AHP) [10] and more advanced dynamic visualization and comparison capabilities.

As the proposed method does not provide residual threat likelihood- or vulnerability estimations, the level of real-world residual risk is not estimated. Instead, as defined by IT-Grundschutz, residual risks are reduced to a generally acceptable baseline. This has the drawback of not showing risks that would remain after baseline protection has been accomplished. This could be achieved by estimating the residual threat likelihood for every threat globally, for every module's threat-reference once, or as a most detailed estimation, based on each module-threat-safeguard-reference. Because the landscape of real-world residual risks can be an important factor for decision making from a top-management and stakeholder point of view[20], future research will evaluate methods to allow a view on residual risks, even when security targets are fully established.

To facilitate synergies with standards and existing information from related management systems, future development will improve importing and exporting capabilities and provide interfaces to common management systems (e.g. Active Directory).

As a result of risk inheritance, the view on inherent risks of assets (based on their modules) near the root of the scenario tree may be limited, if the inherited risks of dependent assets overshadows them. This can currently be compensated by keeping

[20] The view on real-world residual risks is especially important in industry sectors and environments where security requirements are not clearly defined or standardized.

track of respective module risks (asset risk drill-down). Future developments will also include separate views on inherent and inherited risks at the asset layer.

In addition to the presented inheritance of protection criteria risks, individual threats or threat types and groups can be used to model and assess influences in future developments to allow an even more detailed and retraceable risk inheritance between assets as well as improved options regarding attack vector analysis.

A framework-internal sensor interface should provide risk assessment and management related data as measures automatically and the identification and evaluation of further aggregation functions, especially non-linear functions that allow a more cautious estimation of risks should be facilitated.

Subjective estimation of risk factors (impact level, threat likelihood, safeguard maturity) could be aided by answering additional control questions, rated using AHP.

Sensors could also be used to receive or trigger events between information systems (SIEM-functionality) and automatically incorporate work-flow related information into the risk model (e.g. certain measures could trigger change management workflows, responsible personnel could be automatically notified of configuration changes to critical IT systems, etc.).

Another improvement for future development includes the incorporation of expense factors and respective sensors, to include measurements related to initial and recurrent risk mitigation and management costs. Based on an extended domain model and an evaluation and integration of Return-On-Security-Investment models[21], the risk management system would enable even more detailed decision making based on financial aspects.

Improved clustering and data synchronization support should be integrated to enable centralization of multiple stand-alone systems with independent risk models (e.g. used by subsidiaries). Unidirectional-security-gateway functionality (data diodes), cryptography as well as detailed authorization methods should be deployed to ensure multiple layers of defense, protecting confidentiality of data across all risk models.

Asset-, module- and threat-sensitivity assessment interfaces should be implemented following the schema outlined in 4.2.2 to support highly detailed comparison between those risk factors across the risk model.

Based on the comprehensive modelling base established using IT-Grundschutz as a library of risk factors, additional analysis methods or steps can be integrated requiring less additional effort. Promising methods for future evaluation include, but are not limited to, Bayesian Networks [83], Marcov chains [84], Petri nets [85], Social Network Analysis [86] and System Dynamics models [87].

[21] e.g. using the Hummer model [61], which is based on IDS measurements, the Hoover model [61], which is based on software development metrics, the CMU (Carnegie Mellon University) model [61], based on regression analysis of CERT's statistical attack data and the Sonnenreich model [62], based on risk exposure and relative mitigated risk, fitting the proposed model perfectly.

References

[1] International Organization of Standardization, ISO/IEC 27005, “ISO/IEC 27005 - Information technology -- Security techniques -- Information security risk management”, second edition, 2011.

[2] Bundesamt für Sicherheit in der Informationstechnik, “Cross-reference-tables of IT-Grundschutz”. 2011, 13. EL. Available: https://www.bsi.bund.de/cae/servlet/contentblob/474914/publicationFile/55551/kreuzreferenz_tabellen.zip

[3] S. Schiebeck, “IT-Risikomanagement – Anforderungen, Vorschriften und Toolevaluierung”, Master-Thesis, FHOÖ Campus Hagenberg, 2007. Available: http://www.schiebeck.at/download/Risikomanagement_Anforderungen_Vorschriften_Evaluierung.pdf

[4] Österreichisches Normungsinstitut, ONR 49002-2, “Risikomanagement für Organisationen und Systeme, Teil 2: Leitfaden für die Methoden der Risikobeurteilung, Leitfaden für die Anwendung von ISO/DIS 31000 in der Praxis”, 2008.

[5] Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz (German version), “IT-Grundschutz”, 2013, 13. EL. Available: https://www.bsi.bund.de/cln_183/sid_7411A168F87C40D0B96AE229BFCE9EFC/DE/Themen/ITGrundschutz/StartseiteITGrundschutz/startseiteitgrundschutz_node.html

[6] ISACA, COBIT, “Mapping to ISO/IEC 17799:2000 with COBIT”, 2006. Available: http://www.isaca.org/Knowledge-Center/Research/Documents/COBIT-Mapping-ISO17799-2000-2nd-Ed.pdf

[7] itSMF Arbeitskreis ITIL/Cobit-Mapping, “Praxishandbuch ITIL/Cobit-Mapping”. Available: http://www.itsmf.de/ak_itil-cobit-mapping.html

[8] ISACA, COBIT Mapping: “Mapping SEI’s CMM for Software With COBIT 4.0”, Available: http://www.isaca.org/Knowledge-Center/Research/Documents/SEI-CMM-Mapping-With-COBIT-27Sept2006.pdf

[9] C. Wang, W. Wulf, “Towards a Framework for Security Measurement”, Department of Computer Science, University of Virginia, 1997. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.100.9803&rep=rep1&type=pdf

[10] T. Saaty, “Multicriteria decision making - the analytic hierarchy process. Planning, priority setting, resource allocation”, RWS Publishing, Pittsburgh, 1990.

[11] M. Simonsson, R. Lagerström, P. Johnson, “A Bayesian Network for IT Governance Performance Prediction”, 10th Int. Conf. on Electronic Commerce (ICEC) Innsbruck, Austria, 2008. Available: http://portal.acm.org/citation.cfm?id=1409542

[12] J. Cohen, P. Cohen, “Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences”. Lawrence Erlbaum Associates, 1983.

[13] C. Walsh, “Statistics for the Social Sciences with Computer Applications”. Harper & Row Publishers, 1990.

[14] R. Rojas, “Neural Networks - A Systematic Introduction”, Springer, Berlin, New-York, 1996. Available: http://page.mi.fu-berlin.de/rojas/neural/index.html.html

[15] D. Whitley, “A Genetic Algorithm Tutorial”, Computer Science Department, Colorado State University. Available: http://samizdat.mines.edu/ga_tutorial/ga_tutorial.ps

[16] S. Haykin, “Neural Networks: A Comprehensive Foundation”, Person Education.

[17] Y. Peng, J. Reggia, “A Probabilistic Causal Model for Diagnostic Problem Solving – Part I: Integration Symbolic Causal Inference with Numeric Probabilistic Inference”, Ieee Transactions on Systems, Man, and Cybernetics, Vol. 17, No. 2, 1987. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4309056

[18] M. Henrion, “Some practical issues in constructing belief networks”, Uncertainty in Artificial Intelligence 3, L. Kanal, T. Levitt, and J. Lemmer, Eds. New York, Elsevier Science Publishing Company, Inc., p. 161–173, 1989.

[19] D. Heckerman, J. Breese, “Causal Independence for Probability Assessment and Inference Using Bayesian Networks”, Ieee Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans, Vol. 26, No. 6, p. 826-831, 1996.

[20] F. Dıez, J. Mira, E. Iturralde, S. Zubillaga, “DIAVAL, a Bayesian expert system for echocardiography”, Artificial Intelligence in Medicine, vol. 10, pp. 59–73, 1997.

[21] M. Pradhan, G. Provan, B. Middleton, M. Henrion, “Knowledge engineering for large belief networks”, Proceedings of the Tenth Annual Conference on Uncertainty in Artificial Intelligence (UAI–94). San Francisco, CA: Morgan Kaufmann Publishers, 1994, pp. 484–490.

[22] M. Shwe, B. Middleton, D. Heckerman, M. Henrion, E. Horvitz, H. Lehmann, G. Cooper, “Probabilistic diagnosis using a reformulation of the INTERNIST–1/QMR knowledge base: I. The probabilistic model and inference algorithms”, Methods of Information in Medicine, vol. 30, no. 4, pp. 241–255, 1991.

[23] J. Kim, J. Pearl, “A computational model for causal and diagnostic reasoning in inference engines”. In Proceedings Eighth International Joint Conference on Artificial Intelligence. Karlsruhe, West Germany. Pages 190-193. International Joint Conference on Artificial Intelligence, 1983.

[24] M. Friagault, W. Lingyu, S. Anoop, J. Sushil, “Measuring network security using dynamic Bayesian networks”, Conference on Computer and Communications Security, Proceedings of the 4th ACM workshop on Quality of protection. 2008. Available: http://portal.acm.org/citation.cfm?id=1456368

[25] R. Alguliev, S. Derakhshandeh, “Application of Information and Communication Technologies”, AICT 2009. 2009. Available: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5372521

[26] S. Mo, P. Beling, K. Crowther, “Quantitative assessment of cyber security risk using bayesian network-based model”, Systems and Information Engineering Design Symposium, 2009. SIEDS, 2009. Available: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5166177

[27] A. Dempster, N. Laird, D. Rubin, “Maximum Likelihood from Incomplete Data via the EM Algorithm”. Journal of the Royal Statistical Society. 1977. Series B (Methodological) 39 (1): 1–38. JSTOR 2984875. MR0501537

[28] D. Koller, N. Friedman, “Probabilistic Graphical Models: Principles and Techniques”, MIT Press, 2009.

[29] S. Lauritzen, D. Spiegelhalter, „Local computations with probabilities on graphical structures and their application to expert systems”. Journal of the Royal Statistical Society, Series B, *50(2):157*--224, 1988.

[30] A. Darwiche, “Recursive Conditioning”. Artificial Intelligence. Vol 126, No 12, pages 541, 2001.

[31] D. Gamerman, H. Lopes, “Markov Chain Monte Carlo: Stochastic Simulation for Bayesian Inference”, Second Edition, University Federal Do Rio de Janeiro, Brazil, 2006.

[32] R. Dechter, I. Rish, “Mini-buckets: A general scheme for bounded inference”, Journal of the ACM (JACM), Volume 50, Issue 2, 2003. Pages: 107 – 153. Available: http://portal.acm.org/citation.cfm?id=636866

[33] D. Driankov, H. Hellendoorn, M. Reinfrank, “An introduction to fuzzy control”, Springer 1996. Available: http://books.google.com/books?id=T1P1XeyNvl4C&printsec=frontcover&hl=de&source=gbs_ge_summary_r&cad=0

[34] International Organization of Standardization, ISO/IEC 27004, “ISO/IEC 27004 - Information technology -- Security techniques -- Information security management -- Measurement”. 2009.

[35] L. Zadeh, “Fuzzy Sets, Information and Control”, 1965.

[36] L. Zadeh, “Outline of a New Approach to the Analysis of Complex Systems and Decision Processes”, 1973.

[37] L. Zadeh, “Fuzzy algorithms Info. & Ctl.”, Vol. 12, 1968, pp. 94-102.

[38] L. Zadeh, “Making computers think like people”, IEEE. Spectrum, 8/1984, pp. 26-32.

[39] International Electrotechnical Commission (IEC) - Technical Committee No. 65: Industrial Process Measurement And Control Sub-Committee 65 B: DEVICES, IEC 1131 - Programmable Controllers, “Part 7 - Fuzzy Control Programming”, Committee Draft CD 1.0 (Rel. 19 Jan 97). Available: http://jfuzzylogic.sourceforge.net/doc/iec_1131_7_cd1.pdf (22.10.08)

[40] M. Neil, M. Tailor, D. Marquez, “Inference in Hybrid Bayesian Networks using dynamic discretization”, Department of Computer Science, Queen Mary, University of London. Available: http://www.agenarisk.com/resources/technology_articles/DD.pdf

[41] M. Stallinger, “IT-Governance im Kontext Risikomanagement”, PhD thesis, Johannes Kepler Universität Linz, ISBN 978-3836487399, 2007.

[42] Software Engineering Institute, “Capability Maturity Model Integration”, Carnegie Mellon University, 2010. Available: http://www.sei.cmu.edu/cmmi/tools/index.cfm

[43] IEC, IEC 61025, “Fault-Tree-Analysis (FTA)”, 2006.

[44] P. Weill, J. Ross, “IT Governance: How Top Performers Manage IT Decision Rights for Superior Results”, Harvard Business School Press, Boston, 2004.

[45] ENISA, “Reference Source for threats, vulnerabilities, impacts and controls in IT-Risk-Assessment”, ENISA, 2007. Available: http://www.enisa.europa.eu/act/rm/files/deliverables/reference-source-for-threats-vulnerabilities-impacts-and-controls-in-it-risk-assessment-and-risk-management/at_download/fullReport

[46] Bundesamt für Sicherheit in der Informationstechnik, BSI Standard 100-1, „Information Security Management Systems“, 2008, Version 1.5. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf;jsessionid=6E45CBB2381608260C0796862C32F1D4.2_cid251?__blob=publicationFile

[47] Bundesamt für Sicherheit in der Informationstechnik, BSI Standard 100-2, „IT-Grundschutz Methodology“, 2008, Version 2.0. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.pdf;jsessionid=6E45CBB2381608260C0796862C32F1D4.2_cid251?__blob=publicationFile

[48] Bundesamt für Sicherheit in der Informationstechnik, BSI Standard 100-3, „Risk Analysis used by IT-Grundschutz“, 2008, Version 2.5. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-3_e_pdf.pdf;jsessionid=6E45CBB2381608260C0796862C32F1D4.2_cid251?__blob=publicationFile

[49] Bundesamt für Sicherheit in der Informationstechnik, BSI Standard 100-4, „Business Continuity Management“, 2008, Version 1.0. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.pdf?__blob=publicationFile

[50] M. Stoddard, D. Bodeau, R. Carlson, C. Glantz, Y. Haimes, C. Lian, J. Santos, J. Shaw, “Process Control Systems Security Metrics”, Department of Homeland Security, 2005. Available: http://www.thei3p.org/docs/publications/ResearchReport1.pdf

[51] Austrian Standards Institute, ÖNORM A 7700, “Information technology – Technical requirements concerning the security web-applications”, ON-Committee ON-K 001 Information technology, 2008.

[52] MetricsCenter, Metric Catalog Project, PlexLogic LLC, 2012, Available: http://www.metricscenter.org

[53] Deutsches Institut für Normung, DIN 25424-1, “Fehlerbaumanalyse, Teil 1: Methode und Bildzeichen”, fourth edition, 1990.

[54] S. Fenz, A. Tjoa, M. Hudec, “Ontology based generation of Bayesian networks”, Institute of Software Technology and Interactive Systems, Vienna University of Technology, 2009.

[55] R. Dworschak, A. Leitner, J. Pöttinger, „Evaluierung von Risikoanalysetools“, FHOÖ Campus Hagenberg, 2008.

[56] Software Engineering Institute, “Published Appraisal Results”, Carnegie Mellon, Available: http://sas.sei.cmu.edu/pars/pars.aspx

[57] Bundesamt für Sicherheit in der Informationstechnik, „Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz“, 2011, Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Vergleich_ISO27001_GS.pdf?__blob=publicationFile

[58] M. Whitman, H. Mattord, “Management of Information Security”, Course Technology, ISBN 978-1435488847, 2010.

[59] Millward Brown Survey, “Adobe Flash Player PC Penetration Statistics”, July 2011, Available: http://www.adobe.com/products/flashplatformruntimes/statistics.html

[60] F. Roberts, “Measurement Theory, with Applications to Decision-Making, Utility, and the Social Sciences”, Addison-Wesley, 1979.

[61] C. Magnusson, J. Molvidsson, S. Zetterqvist, “Value creation and Return On Security Investment (ROSI)”, IFIP International Federation for Information Processing, 2007. Available: http://www.springerlink.com/content/l673387x312x7t52/

[62] W. Sonnenreich, J. Albanese, B. Stout, “Return On Security Investment (ROSI): A practical quantitative model”, Journal of Research and Practice in Information Technology, 2005. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.83.5483

[63] D. Bies, C. Hansen, “Engineering Noise Control, Theory and Practice”, 4th edition, Span Press, ISBN 978-0415487078, 2009.

[64] Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz (English version), „The IT-Grundschutz-Catalogues“, 2005. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/it-grundschutz-kataloge_2005_pdf_en_zip.zip?__blob=publicationFile

[65] D. Bies, C. Hansen, “Engineering Noise Control, Theory and Practice”, Fourth Edition, Spon Press, 2009. Available: http://books.google.at/books?hl=de&lr=&id=v98PaeB8nQkC&oi=fnd&pg=PP1&dq=Bies,+David+A.,+and+Hansen,+Colin.+(2003).+Engineering+Noise+Control.&ots=4m5h7g-_16&sig=zBbRihOYPYK3Tr9I9suCELWHr9Y

[66] A. Jaquith, „Security Metrics: Replacing Fear, Uncertainty, and Doubt“, Addison-Wesley Professional, ISBN 978-0321349989, 2007.

[67] I. Mayr, “Entwicklung eines halbautomatisierten, bedarfsträgerorientierten Auditberichts und Meldewesen im ÖBH“, Baccalaureate thesis, Secure Information Systems, FHOÖ Campus Hagenberg, 2010.

[68] Bundeskanzleramt Österreich, „Österreichisches Informationssicherheitshandbuch“, Version 3.1.5, 2013. Available: https://www.sicherheitshandbuch.gv.at/downloads/sicherheitshandbuch.pdf

[69] SystemExperts Corporation, B. Johnson, „Looking at the SANS 20 Critical Security Controls – Mapping the SANS 20 to NIST 800-53 to ISO 27002”, 2011. Available: http://systemexperts.com/media/pdf/SystemExperts-SANS20-1.pdf

[70] Bundesamt für Sicherheit in der Informationstechnik, „Neues in der 13. Ergänzungslieferung der IT-Grundschutz-Kataloge“, German version, 2013, Available: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Allgemeines/Neues/neues_node.html

[71] International Organization of Standardization, ISO/IEC 27001, “ISO/IEC 27001 - Information technology -- Security techniques -- Information security management systems -- Requirements”, 2013.

[72] International Organization of Standardization, ISO/IEC 27002, “ISO/IEC 27002 - Information technology -- Security techniques -- Code of practice for information security controls”, 2013.

[73] ISACA, COBIT Framework, “Control Objectives for Information and Related Technology (COBIT) 5”, version 5, 2012.

[74] National Institute of Standards and Technology, U.S. Department of Commerce, NIST Special Publication 800-30, Information Security, “Guide for Conducting Risk Assessments”, Revision 1, 2012.

[75] National Institute of Standards and Technology, U.S. Department of Commerce, NIST Special Publication 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations”, Revision 4, 2013.

[76] International Organization of Standardization, ISO/IEC 15408-1, Common Criteria for Information Technology Security Evaluation, “Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model”, version 3.1, revision 4, 2009.

[77] Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI), “Expression des besoins et identification des objectifs de sécurité”, EBIOS, 2010. Available: http://www.ssi.gouv.fr/IMG/pdf/EBIOS-1-GuideMethodologique-2010-01-25.pdf

[78] Ministerio de Administraciones Publicas, MAGERIT V3, “Methodology of risk analysis and management of information systems”, 2012. Available: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_m%C3%A9todo_es_NIPO_630-12-171-8.pdf

[79] Software Engineering Institute, Carnegie Mellon University, OCTAVE, “Operationally Critical Threat, Asset, and Vulnerability Evaluation”, version 2, 2008. Available: http://www.cert.org/octave/

[80] Carnegie Mellon University, “The Systems Security Engineering – Capability Maturity Model (SSE-CMM)”, version 2, 1999. Available: http://csrc.nist.gov/groups/SMA/fasp/documents/incident_response/SSAIRBSP/SSECMMv2Final.pdf

[81] Club de la Sécurité de l'Information Français (CLUSIF), MEHARI, “Method for Harmonized Analysis of Risk”, 2010, Available: https://www.clusif.asso.fr/fr/production/ouvrages/pdf/DB-Mehari_2010_Exc_2-2-en.zip

[82] Office of Government Commerce (OGC), ITIL 2011, “Information Technology Infrastructure Library”, 2011.

[83] T. Bayes, “An Essay towards solving a Problem in the Doctrine of Chances”, Philosophical Transactions of the Royal Society, pp. 370–418, 1763.

[84] A. Markov, “Extension of the limit theorems of probability theory to a sum of variables connected in a chain”, reprinted in Appendix B of: R. Howard. Dynamic Probabilistic Systems, volume 1: Markov Chains, John Wiley and Sons, 1971.

[85] C. Petri, „Kommunikation mit Automaten“, PhD Thesis, University of Bonn, 1962.

[86] R. Hanneman, M. Riddle, “Concepts and Measures for Basic Network Analysis – The Sage Handbook of Social Network Analysis”, Sage, ISBN 978-1-84787-395-8, 2011.

[87] J. Forrester, “Counterintuitive behavior of social systems”, Technology Review, pp. 52–68, 1971.

List of Figures

List of Equations

List of Examples

Stefan Schiebeck, MSc

DISSERTATION

Annex A

Evaluation Report

Federal Ministry of Defense Austria
Intelligence Agency (Abwehramt)
Department C

of

RiskSense

An Approach to Continuous Information Security
Risk Assessment focused on Security Measurements

Stefan Schiebeck, MSc
Faculty of Computer Science, MIS Research Group
University of Vienna
Stefan.Schiebeck@univie.ac.at

A B W E H R A M T
A b t C

Erprobung des Prototypen RISKSENSE im FB IT-Sih (BMLVS)
Ergebnis

B E R I C H T

1 Aktivität

Der Prototyp RISKSENSE wurde durch den Referatsleiter IT-Grundlagen Hptm Mag(FH) Ingo Siegfried MAYR, BSc getestet.

2 Rahmenbedingungen

Testumgebung

Zur Durchführung der Erprobung wurde durch Hr. Stefan SCHIEBECK eine VM bereitgestellt, die auf BMLVS eigenen Systemen installiert und betrieben wird.

Als Grundlage der Testung dienen BMLVS interne Prüfkataloge, deren Struktur grundsätzlich an das IT-Grundschutzmodell des BSI angelehnt, deren Inhalte allerdings aus nationalen und multilateralen Vorschriften und Richtlinien abgeleitet wurden.
Diese Prüfkataloge werden im BMLVS zur Durchführung von Sicherheitsaudit verwendet.

Es werden diese Prüfkataloge zur Durchführung von Sicherheitsaudits an spezifischen Geräten verwendet, weshalb der Arbeitsschritt der Generalisierung gemäß IT-Grundschutz des BSI nicht angewendet wird. Dadurch bedingt, ist der erstellte Informationsverbund deutlich umfangreicher und komplexer als ein vergleichbarer Informationsverbund gemäß IT-Grundschutz des BSI. Nachfolgende Abbildung soll das verdeutlichen:

Annex A - Figure 1: Evaluation Report, Page 1 of 5 (scanned)

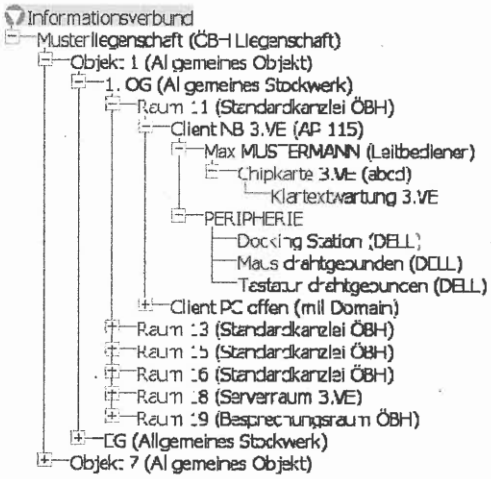


Abbildung: Auszug einer im FB IT-Sih verwendeten Modellstruktur. Deutlich ist zu erkennen, dass Objekte (z.B. Standardkanzlei ÖBH) nicht generalisiert, sondern individuell modelliert und bewertet werden.

Testdaten

Für die eigentliche Erprobung wurden Auszüge aus realen Liegenschaften des BMLVS im Prototyp RISKSENSE modelliert und mit realen und z.T. auch fiktiven Bewertungen versehen.

Aufgrund des Schutzbedarfs der Realdaten (Systeme, Anforderungen, udgl) wurden ausschließlich Systeme und Anforderungen mit geringem Klassifikationsgrad modelliert.

Die nachfolgenden Objekte und Systeme wurden im Wesentlichen modelliert:

- Systeme des internen Netzwerk BMLVS 3.VE.
- Systeme für den Anschluss an das „dienstliche Internet".
- Durch Mitarbeiter eingebrachte, nicht dienstliche Systeme.
- Absicherungssysteme wie etwa Feuerlöscher, Bewegungsmelder u.a.
- Räume und Gebäude.

Nicht-Ziele der Erprobung

Nicht bewertet werden folgende Parameter:

- Performance der Applikation: Begründung: Der Prototyp zeigt vor allem die Stärken und Schwächen der verwendeten Methode auf. Durch eine Optimierung des Programmcode und der Verwendung ausreichend leistungsfähiger Hardware ist eine deutliche Performanceverbesserung nach h.o. Beurteilung erwartbar.
- Verwendete Entwicklungsumgebung: Begründung: Fehlende Fachexpertise.

Annex A - Figure 2: Evaluation Report, Page 2 of 5 (scanned)

3 Ergebnis der Erprobung

Methode

Die in RISKSENSE verwendete Berechnungsmethode erscheint nach der h.o. durchgeführten Erprobung als geeignetes Werkzeug zur Evaluierung des Sicherheitsniveaus eines Unternehmens auf Basis der festgestellten Kennzahlen (manuell und/oder automatisiert).

Die Fuzzy-Unterstützte Auswertung von RISKSENSE liefert grundsätzliche gute und nachvollziehbare Ergebnisse. Es ist dabei zu beachten, dass die Ergebnisse stark von den gewählten Basisdaten (Gewichtungen und Faktoren der einzelnen Anforderungen/Prüfmaßnahmen) abhängen.
Da die in RISKSENSE integrierten Basisdaten für den IT-Grundschutzkatalog nicht angewendet werden können (infolge der BMLVS eigenen Prüfkataloge), wären weiterführende Hilfsmittel zum Einstellen der Basisdaten hilfreich. Es hat sich bei der Eingabe der eigenen Prüfkataloge gezeigt, dass das gegenseitige Abstimmen der Anforderungen bzw. Prüfmaßnahmen ein aufwändiger und zeitintensiver Prozess ist, der bei einer schlechten Auswahl an Basisdaten zum Über- bzw. Unterreagieren von Anforderungen/Prüfmaßnahmen führen kann. Es wäre daher sinnvoll, die Integration eines internen oder externen Moduls zu überprüfen, mit dessen Hilfe die Basisdaten effizienter konfiguriert werden können[1].
Diese Kritikpunkt soll/darf nicht als Einschränkung der Applikation RISKSENSE verstanden werden, sondern begründet sich allgemein im Wesen der Beurteilung von Auswirkungen und Risiken von Anforderungen bzw. Prüfmaßnahmen.

Die Möglichkeit dass Kennzahlen durch Sensoren generiert oder manuell eingegeben werden können, bietet eine leistungsfähige Schnittstellen zu Echtzeit-[2] und Nicht-Echtzeitdaten[3] mit deren Hilfe genaue und aktuelle Lagebilder generiert werden können. Es kann mithilfe von RISKSENSE somit nicht nur der „Gesundheitszustand" der IKT-Infrastruktur, sondern auch die korrekte Umsetzung von erforderlichen Absicherungsmaßnahmen (vor allem Organisation und Objektsicherheit) erfasst und in der Analyse berücksichtigt werden.

Als besonders leistungsfähig hat sich die RISKSENSE-interne Datenstruktur erwiesen, da mit Unterstützung durch Hr. SCHIEBECK auch Auswertungen umgesetzt werden konnten,

[1] Es könnte zweckmäßig sein, dass in einem „Projekt" über- bzw. unterreagierende Kennzahlen durch den Anwender markiert, und mit einer erwartbarer Kennzahl versehen werden. Von der Applikation sollte dann ein Vorschlag für die Basisdaten von einzelnen und/oder mehreren Anforderungen berechnet werden, mit deren Hilfe die vorgegebenen bzw. korrekten Kennzahlen erreicht werden können.
[2] Automatisierte Statusmeldungen von Netzwerkkomponenten, die an Management-Systeme übermittelt werden.
[3] Überprüfungsergebnisse von menschlichen Auditoren, die beispielsweise die Umsetzung von physikalischen Absicherungsmaßnahmen oder von Geheimschutzbestimmungen vor Ort überprüfen.

Annex A - Figure 3: Evaluation Report, Page 3 of 5 (scanned)

die in dieser Art und Weise nicht vorgesehen sind, ohne das eine Änderung des Programmcodes erforderlich war.
Als Beispiel soll etwa die Auswertung auf Basis von Angriffsvektoren[4] dienen bei der eine Gruppe von zusammenwirkenden Anforderungen bzw. Prüfmaßnahmen zusammengefasst werden.
Am Beispiel des IT-Grundschutzkatalog des BSI könnten etwa die Maßnahmen „Geschlossene Fenster und Türen", „Zutrittsregelung", „Einbruchschutz", „Verwendung von Sicherheitstüren und –fenstern" und „Abgeschlossene Türen" eine Gruppe sein, die eine Erfolgswahrscheinlichkeit von physikalischen Angriffen erfasst. Für relevante Systeme[5] können dann Verwundbarkeiten gegen verschiedene Angriffsformen berechnet werden.
Es wird h.o. erwartet, dass mit einer solchen Auswertung sehr gute Informationen über das Sicherheitsniveau des Informationsverbundes und seiner Teile getroffen werden können, mit deren Hilfe auch kurzfristig wirksame Gegenmaßnahmen (Sofortmaßnahmen) gesetzt werden können, die zumindest bis zum Beheben der eigentlichen Schwachstelle, das Risiko reduzieren können.

System	Angriff	Erfolg
Server abcd	Unbefugter Zugriff durch Außentäter infolge Einbruch	Mittel
	Unbefugter Zugriff durch Innentäter	Gering
Client bcde	Unbefugter Zugriff durch Innentäter	Hoch

Tabelle: Beispiel für eine mögliche Darstellung nach Angriffsvektoren.

Die Auswertung nach Angriffsvektoren ist im vorliegenden Prototypen technisch durchführbar und liefert auch nachvollziehbare Ergebnisse, die anhand von Schwellwerten weiterverarbeitet werden können. Da RISKSENSE diese Auswertemethode nicht direkt unterstützt, ist der Arbeitsaufwand zur Durchführung derzeit sehr hoch und besitzt kein brauchbares Kosten/Nutzen-Verhältnis.
Mit einer verbesserten Unterstützung kann diese Auswertung das ohnehin hohe Potential von RISKSENSE weiter steigern.

Anmerkungen zur GUI
Das GUI von RISKSENSE ist im Wesentlichen übersichtlich und logisch aufgebaut. Eine chronologische Arbeitsweise in der Applikation ist möglich und es werden viele Informationen nicht nur in Textform, sondern auch graphisch dargestellt.
Verbesserungen an der GUI sind für ein endgültiges Produkt sicher erforderlich,

[4] Ein Angriffsvektor kann etwa ein „physikalischer Angriff gegen die Vertraulichkeit von klassifizierten elektronischen Informationen durch Außentäter" sein.
[5] Die Anforderungen bzw. Prüfmaßnahmen werden dabei aus den Elternobjekten, wie z.B. Raum, Stockwerk, Gebäude und Liegenschaft, übernommen.

Annex A - Figure 4: Evaluation Report, Page 4 of 5 (scanned)

allerdings ist diese Notwendigkeit Hr. SCHIEBECK bekannt und wird daher nicht weiter ausgeführt.

Davon abgesehen soll der Prototyp RISKSENSE vor allem die Leistungsfähigkeit der zugrunde liegenden Analyse- und Auswertemethode zeigen, weshalb die GUI in diesem Stadium eine untergeordnete Rolle besitzt.

4 Zusammenfassung

Der Fortschritt des Prototypen RISKSENSE wurde seit den Anfängen durch die Abt C begleitet und beobachtet. Der sehr gute Eindruck von RISKSENSE hat sich mit dieser Erprobung bestätigt und hat aufgezeigt, dass RISKSENSE das Potential hat, einen wesentlichen Bedarf im Bereich der Beurteilung des Informationssicherheitszustands von Unternehmen zu decken.
Zu dieser Bedarfsdeckung wären

- Schnittstellen für den Datenimport aus anderen Auditwerkzeugen,
- verbesserte Schnittstellen zu Sensoren und Managementsystemen,
- ein verbessertes GUI,
- eine verbesserte Wartbarkeit der Basisdaten und
- verbesserte Ausgabemöglichkeiten der Ergebnisse

hilfreich.

Im BMLVS wäre nach h.o. Beurteilung der Bedarf für ein solches Werkzeug gegeben.

Der Berichtsleger

Hptm Mag(FH) MAYR Ingo, BSc

Annex A - Figure 5: Evaluation Report, Page 5 of 5 (scanned)

Stefan Schiebeck, MSc

DISSERTATION

Annex B

Market Assessment

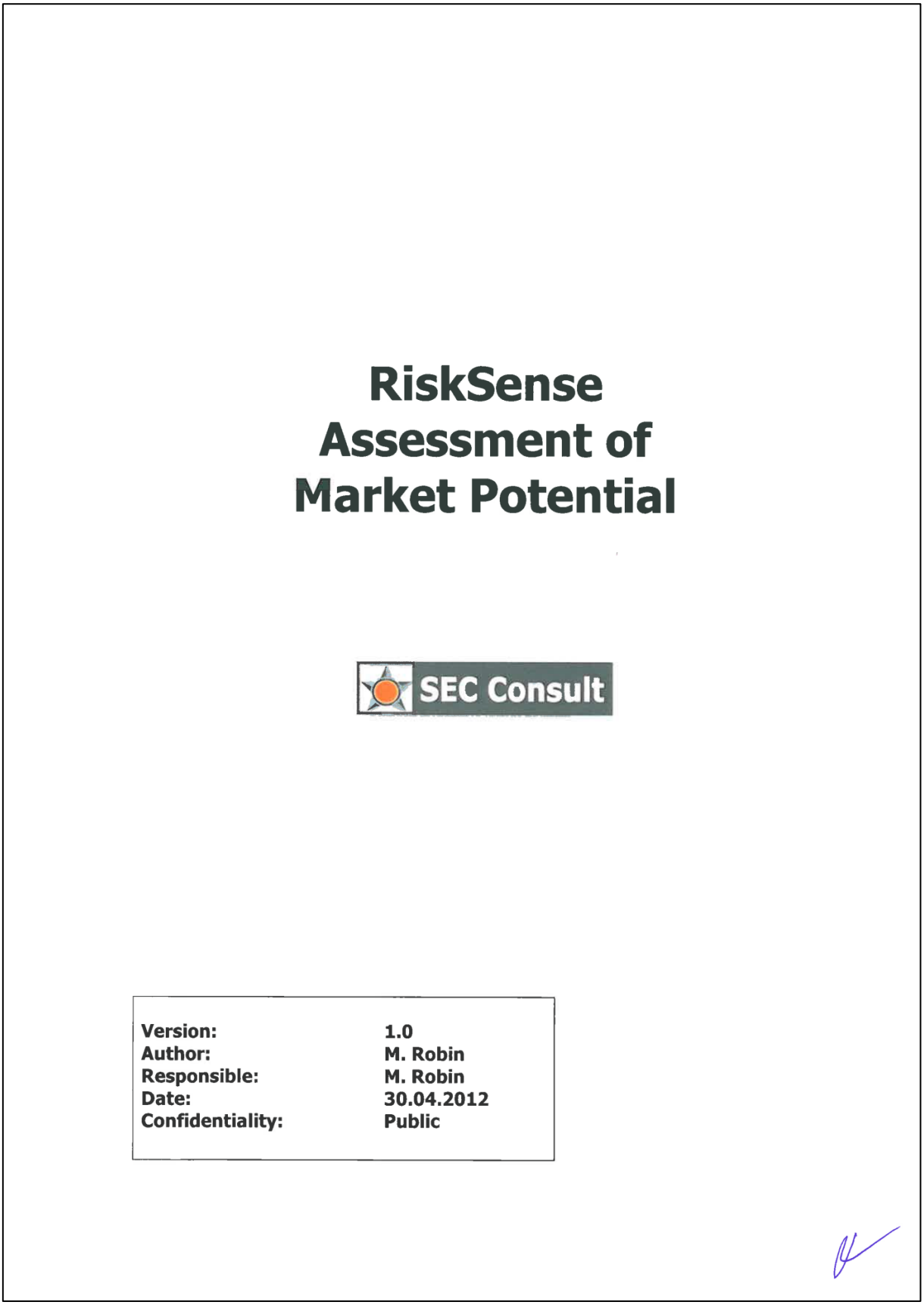
SEC Consult Unternehmensberatung GmbH
Advisor for your Information Security
M. Robin, General Manager

of

RiskSense

An Approach to Continuous Information Security
Risk Assessment focused on Security Measurements

Stefan Schiebeck, MSc
Faculty of Computer Science, MIS Research Group
University of Vienna
Stefan.Schiebeck@univie.ac.at



Annex B - Figure 1: Assessment of Market Potential, Page 1 of 2 (scanned)

1 Current Situation

An increased number of attacks and pressure for compliance (PCI-DSS, ISO 27001, SOX, BASEL II, etc.) force companies to increase their investments in information security. Also, the quality and reliability of companies will be measured by the effort they invest in their risk management efforts in this respect. Multiple national and international vendors provide software tools for information security risk management, but the vast experience of SEC Consult by implementing risk management for information security in the past years shows that all of the evaluated solutions suffer from obvious limitations and do not follow a truly comprehensive approach.

SEC Consult therefore supported the research and development of Mr. Stefan Schiebeck for RiskSense.

2 Assessment of Market Potential

To assess the market potential of RiskSense, the target customers have to be identified. Due to its specific comprehensive approach, RiskSense is especially valuable for

- large corporate customers
- government and defense organization with high risk sensitivity
- selected small companies with strong focus on information security

The segment of large corporate and government and defense organizations with high risk sensitivity build a sound revenue potential for the solution. In terms of geographic segmentation we see the market in

- Central and Eastern Europe
- but also some of the fast growing countries in Asia (e.g. Singapore)

as potential target markets. In the German market alone, the DAX-listed companies can be a significant revenue stream for RiskSense as especially these large organizations demand a state-of-the-art comprehensive approach.

The market for information security risk management solutions is growing significantly, and the demand will further increase as companies shift their focus on resilience of their businesses. However, as it is not a mature market yet, there are no reliable market data available to determine and monitor market share on an European level.

3 Resume

SEC Consult sees the clear potential to use this comprehensive and robust approach manifested in RiskSense to leverage its expertise and to create growth in one the future markets within information security. SEC Consult by itself will use RiskSense as to achieve an ISO 27001 certification based on IT-Grundschutz.

With best regards

DI Markus Robin
General Manager

SEC Consult
Unternehmensberatung GmbH
A-1190 Wien, Mooslackengasse 17
T: +43 1 8903043-0, F: -15

Annex B - Figure 2: Assessment of Market Potential, Page 2 of 2 (scanned)

Stefan Schiebeck, MSc

DISSERTATION

Annex C

Research Partners

of

RiskSense

An Approach to Continuous Information Security
Risk Assessment focused on Security Measurements

Stefan Schiebeck, MSc
Faculty of Computer Science, MIS Research Group
University of Vienna
Stefan.Schiebeck@univie.ac.at

The doctoral student, Stefan Schiebeck, was partly contracted as CISO and senior security consultant for SEC Consult Unternehmensberatung GmbH during the establishment of this thesis. While his work focused on organizational security topics like GRC (Governance, Risk & Compliance), including implementation and audit of Information Security Management Systems, he also led and performed many technical security audits using the Black Box and White Box approach, as well as multiple security architecture and concept reviews.

During his work he became Certified Ethical Hacker, accredited ISO/IEC 27001 Lead- and Internal Auditor as well as ONR 49003 Certified Risk Manager. His research interests include many aspects of organizational and technical information security, with strong focus on Risk-Assessment and -Management. Stefan Schiebeck has held national and international talks as well as university lectures regarding Information Security and Risk Management. His master thesis "Risk Management – Requirements, Regulations and Evaluation" was done at the University of Applied Sciences Hagenberg, in Cooperation with the Federal Ministry of Defense Austria.

Due to the success of his doctoral thesis and supporting prototype, he continues his research in a subsequent, nationally funded research project at the Austrian Institute of Technology (FFG [3687486]).

Gerald Quirchmayr holds doctors degrees in computer science and law from Johannes Kepler University in Linz (Austria) and currently is Professor at the Department of Distributed and Multimedia Systems at the University of Vienna.

In 2001/2002 he held a Chair in Computer and Information Systems at the University of South Australia. He first joined the University of Vienna in 1993 from the Institute of Computer Science at Johannes Kepler University in Linz (Austria) where he had previously been teaching.

In 1989/1990 he taught at the University of Hamburg (Germany). His wide international experience ranges from the participation in international teaching and research projects, very often UN- and EU-based, several research stays at universities and research centers in the US, Asia and EU Member States to extensive teaching in EU staff exchange programs in the United Kingdom, Sweden, Finland, Germany, Spain, and Greece, as well as teaching stays in the Czech Republic and Poland. International teaching and specialist missions include UN-coordinated activities in Egypt, Russia and the Republic of Korea.

He has served as a member of program committees of many international conferences, chaired several of them, has contributed as reviewer to scientific journals and has also served on editorial boards. He is a member of the Austrian and German computer societies and a member of IFIP working groups. For his contributions to the international IT community he has received the IFIP Silver Core Award in 1995.

His major research focus is on information systems in business and government with a special interest in security, applications, formal representations of decision making and legal issues. His publication record comprises approximately 150 peer reviewed papers plus several edited books and conference proceedings as well as nationally and internationally published project reports.

In July 2002 he was appointed as Adjunct Professor at the School of Computer and Information Science of the University of South Australia. From January 2005 until December 2010 he headed the Department of Distributed and Multimedia Systems, Faculty of Computer Science, at the University of Vienna and served as Vice

Dean of the Faculty of Computer Science from October 2008 until October 2010. Since January 2011 he serves as deputy head of the MIS group.

The Federal Ministry of Defense with its extensive IT-infrastructure has to function as an emergency organization, when others lose the ability to help. This is why the Federal Ministry of Defense has to prepare – amongst others – technical and organizational structures and controls to support safety and security in the field of information security.

The Federal Ministry of Defense has supported the project as a mentor by delivering input about practical examples, test cases and evaluation and validation efforts. The responsible persons of the Federal Ministry of Defense delivered input regarding directions for further research and have provided a written reference documenting the relevance of the research outcomes for governmental bodies.

Due to the slowly spreading of measurement activities worldwide and the lack of logics for information security risk indication (risk sensing), the Federal Ministry of Defense has special interest in further research outcomes of the proposed doctoral thesis.

SEC Consult, the former employer of the doctoral student, has years of extensive experience in the area of information security consulting, and members of the company have worked for a wide range of companies and organizations in various industries over the last years. However, most of the clients do come from the financial services industry and government authorities. Key personnel within SEC Consult have extensive experience and expertise in the area of information security and are well respected in the information security industry.

SEC Consult has a broad knowledge when it comes to risk management in the area of information security consulting and its team is highly specialized in conducting individual and manual application security audits using different methodologies to advice clients on the specific threats and risks.

Stefan Schiebeck, MSc

DISSERTATION

Annex D

Curriculum Vitae

Stefan Schiebeck, MSc
Faculty of Computer Science, MIS Research Group
University of Vienna
Stefan.Schiebeck@univie.ac.at

Curriculum Vitae

Stefan Markus Schiebeck, MSc

Education

Sep. 1992 – July 1996	High School Mürzzuschlag.
Sep. 1996 – June 2001	Federal Secondary College of Engineering for Electrical Engineering & Electronics Kapfenberg, college thesis and graduation with excellent results.
Oct. 2002 – July 2005	University of Applied Sciences, FHOÖ Campus Hagenberg, bachelor degree in "Computer- and Media-Security".
Oct. 2005 – July 2007	University of Applied Sciences, FHOÖ Campus Hagenberg, master degree in "Secure Information Systems", major "Law and Experts", master thesis and graduation with excellent results.
Oct. 2007 – now	University of Vienna, PhD study of Social and Economic Sciences, major "Business Informatics", "An Approach to Continuous Information Security Risk Assessment focused on Security Measurements", Information Security Risk Management.

Certifications

April 2006	Certified Ethical Hacker, EC-Council Ethical Hacking and Countermeasures.
January 2008	Certified ISO/IEC 27001 Lead Auditor, BSI registered Lead Auditor.
October 2009	Certified ISO/IEC 27001 Internal Auditor, BSI registered Internal Auditor.
December 2009	Certified ONR 49003 Risk Manager, ONCert Certified Person.

Working experience

Apr. 2007 – Mar. 2013	SEC Consult Unternehmensberatung GmbH., Chief Information Security Officer, Information Security Management, Risk Management, Security Metrics, Governance, Risk & Compliance, Penetration Testing.
Since Oct. 2013	Austrian Institute of Technology GmbH. Safety & Security Department, Scientist, Project "Meta-Risk" – Advancements in Risk Management based on doctoral thesis results, National Sponsorship (FFG).

Lebenslauf

Stefan Markus Schiebeck, MSc

Ausbildung

Sep. 1992 – Juli 1996	Bundesrealgymnasium Mürzzuschlag.
Sep. 1996 – Juni 2001	HTL für Elektrotechnik & Elektronik in Kapfenberg, HTL Diplomarbeit und Abschluss mit ausgezeichnetem Erfolg.
Okt. 2002 – Juli 2005	FHOÖ Campus Hagenberg, Bakkelaureats-Studiengang "Computer- und Mediensicherheit".
Okt. 2005 – Juli 2007	FHOÖ Campus Hagenberg, Master-Studiengang "Sichere Informationssysteme", Schwerpunkt „Law and Experts", Masterthese und Abschluss mit ausgezeichnetem Erfolg.
Okt. 2007 – heute	Universität Wien, Doktorats-Studium der Sozial- und Wirtschaftswissenschaften, „Ein Ansatz für kontinuierliches Informationssicherheits-Risiko-Assessment fokussiert auf Sicherheitskennzahlen", Informationssicherheits-Risikomanagement.

Zertifizierungen

April 2006	Certified Ethical Hacker, EC-Council Ethical Hacking and Countermeasures.
Jänner 2008	Certified ISO/IEC 27001 Lead Auditor, BSI registered Lead Auditor.
Oktober 2009	Certified ISO/IEC 27001 Internal Auditor, BSI registered Internal Auditor.
Dezember 2009	Certified ONR 49003 Risk Manager, ONCert Certified Person.

Praktische Tätigkeiten

Apr. 2007 – März 2013	SEC Consult Unternehmensberatung GmbH., Leiter Informationssicherheit, Informationssicherheits- & GRC-Berater, Penetration Tester.
Seit Okt. 2013	Austrian Institute of Technology GmbH., Safety & Security Department, Wissenschaftlicher Mitarbeiter, Projekt "Meta-Risk" – Weiterentwicklung der Dissertationsergebnisse, Nationale Förderung (FFG).

Stefan Schiebeck, MSc

DISSERTATION

Annex E

Abstract

of

RiskSense

An Approach to Continuous Information Security
Risk Assessment focused on Security Measurements

Stefan Schiebeck, MSc
Faculty of Computer Science, MIS Research Group
University of Vienna
Stefan.Schiebeck@univie.ac.at

An Approach to Continuous Information Security Risk Assessment focused on Security Measurements

Stefan Schiebeck

Abstract

This thesis proposes a concept for the knowledge based integration of security measurements into a comprehensive risk assessment model that allows us to continuously adjust subjective estimations based on empirical measurement data.

The evaluation of the concept and the prototype by a unit of the Federal Ministry of Defense has shown that basing the model on the German IT-Grundschutz framework was the right choice. The novel ability to model and relate security measures with respective risk factors has turned out to be a powerful instrument, enabling the assessment of attack vectors and their correlations and associated insights into organizational risks. As the threat and safeguard library is comprehensive and well maintained, keeping a detailed system current can be achieved with considerably less effort. Another benefit of this decision is that it is much easier to integrate with security requirements based on the Austrian Information Security Manual, which heavily references the German IT-Grundschutz framework.

Following a role based approach is also becoming the standard in security modeling and measurement and is consequently supported by the approach, as is the ability to define multiple qualification and maturity targets for different scopes or assets.

The visualization of relative exposure and the continuous overview of organizational risks and trends add to the usability of the approach. Being sensor-based, situation-related data can be updated either continuously or in defined intervals and the integration of the IT-Grundschutz cross-reference framework makes it possible to also estimate perceived threats. Graphical indicators and an adapted knowledge management approach help to reduce the effort usually associated with the definition of measure to risk relations and provide a practical and manageable way for the integration of empirical measurement data into an initially subjectively estimated risk assessment model. Risks within the model are calculated both separately for every dependency-scenario as well as in total, allowing a scenario specific risk trend view in addition to the overall risks associated with organizational assets.

The prototype now allows us to establish a highly customizable risk model using a role based analysis and estimation approach, utilizing knowledge and responsibilities throughout the organization, while providing a maximum amount of pre-modeled and pre-estimated modular assets to minimize initial and recurring risk assessment and management efforts. By extending the IT-Grundschutz framework with risk modeling and estimation options, the proposed model enables synergies with all continuously updated standards, guidelines and related information provided by the German Federal Office for Security in Information Technology (German BSI). Additionally, the basic analysis concepts of detailed analysis, consisting of a threat analysis paired with the assignment of prioritized safeguards to mitigate risks, can support the modeling of a multitude of governance-, risk- and compliance-assessment and -management efforts (GRC umbrella).

Due to the demonstrated usefulness and the high practical potential of the proposed model, further research has been funded by the Austrian Research Promotion Agency (FFG) as a national security program [3687486].

Ein Ansatz für kontinuierliches Informationssicherheits-Risiko-Assessment fokussiert auf Sicherheitskennzahlen

Stefan Schiebeck

Kurzfassung

Diese Dissertation schlägt ein Konzept für die wissensbasierte Integration von Sicherheitskennzahlen in ein umfangreiches Risikomodell vor, welches die kontinuierliche Anpassung von subjektiven Schätzungen durch empirisch gemessene Daten ermöglicht.

Die Evaluierung des Konzeptes und Prototyps durch eine Abteilung des Abwehramtes zeigte, dass die Entscheidung zur Verwendung des umfangreichen IT-Grundschutz Frameworks die richtige war. Die neuartige Möglichkeit, Sicherheitskennzahlen zu modellieren und mit Risikofaktoren zu verknüpfen zeigte sich als besonders wertvoll, da Angriffsvektoren dargestellt und deren Korrelationen beurteilt werden können, welche Einblicke in die damit zusammenhängenden Risiken ermöglichen. Durch den hohen Detailgrad und die einfache Wartbarkeit der Gefährdungs- und Sicherheitsmaßnahmen-Kataloge können auch komplexe Modelle mit relativ geringem Aufwand auf dem neuesten Stand gehalten werden. Ein weiterer Vorteil besteht in der einfachen Integration mit Anforderungen des Österreichischen Informationssicherheitshandbuches, welches IT-Grundschutz stark referenziert.

Die Verwendung eines rollenbasierten Ansatzes sowie die Möglichkeit, mehrere Ziel-Qualifizierungslevels und -Reifegrade für unterschiedliche Bereiche oder Unternehmenswerte zu managen, wird durch die Vorgehensweise konsequent unterstützt.

Die Visualisierung der relativen Gefährdungspotentiale sowie die Bereitstellung von Sichten auf die kontinuierlichen Risiko- und Kennzahl-Trends erhöht die Verwertbarkeit der Ergebnisse. Durch die Einbindung von Sensoren kann auf situationsbezogene Daten kontinuierlich oder in einstellbaren Intervallen reagiert werden, wobei die Integration der IT-Grundschutz Kreuzreferenzen eine Schätzung der Gefährdungspotentiale unterstützt. Grafische Indikatoren und ein anpassbarer Wissensmanagement-Ansatz reduzieren den Aufwand, der üblicherweise benötigt werden würde, um die Relation zwischen Sicherheitskennzahlen und Risiken darzustellen, und stellt so eine handhabbare Methode zur Verfügung, um empirische Daten in ein subjektives Risikomodell zu integrieren. Risiken des Modells werden unter Berücksichtigung aller Abhängigkeiten der modellierten Szenarien einzeln sowie gesamtheitlich berechnet, sodass Szenario-spezifische Risikotrends gesondert dargestellt werden können.

Der Prototyp erlaubt die rollenbasierte Erstellung und Bewertung eines stark anpassbaren Risikomodells, um Wissen und Verantwortlichkeiten der gesamten Organisation einzubinden, während ein Maximum an vormodellierten und –priorisierten modularen Unternehmenswerten zur Verfügung gestellt wird, um minimale initiale und kontinuierliche Aufwände bei hohem Detailgrad des Risikomodells zu ermöglichen. Durch Erweiterung des IT-Grundschutz Frameworks um Risikomodellierungs- und -bewertungsoptionen ermöglicht die vorgestellte Methodik Synergien mit allen verfügbaren Standards, Richtlinien und zusätzlichen Informationen, welche durch das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Verfügung gestellt werden. Zusätzlich ermöglicht das Konzept der detaillierten Risikoanalyse die Modellierung einer Vielzahl von Governance-, Risk- und Compliance-Anforderungen (GRC-Schirm).

Aufgrund der Verwertbarkeit und des Potentiales des vorgestellten Modells wurde ein weiterführendes Forschungsprojekt durch die Österreichische Forschungsförderungsgesellschaft (FFG) im Zuge eines nationalen Sicherheitsforschungsprogramms [3687486] gefördert.