Ali Sunyaev

Lehrstuhl für Wirtschaftsinformatik Prof. Dr. Krcmar
Technische Universität München

15.09.2009

Design and Application of a Security Analysis Method for Healthcare Telematics in Germany (HatSec)

Ali Sunyaev

Technische Universität München

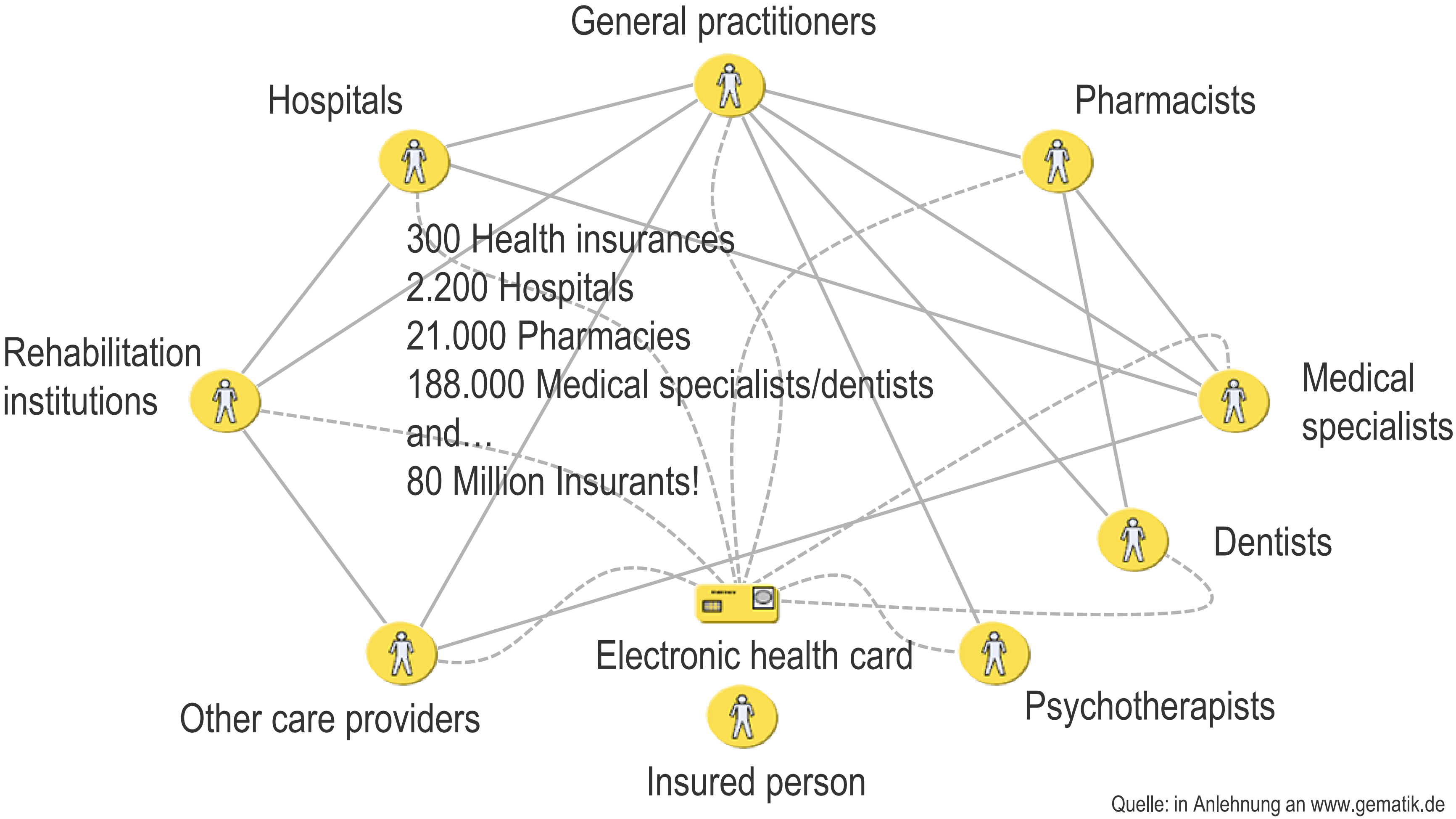
Fakultät für Informatik

Lehrstuhl für Wirtschaftsinformatik (I17)

Overview

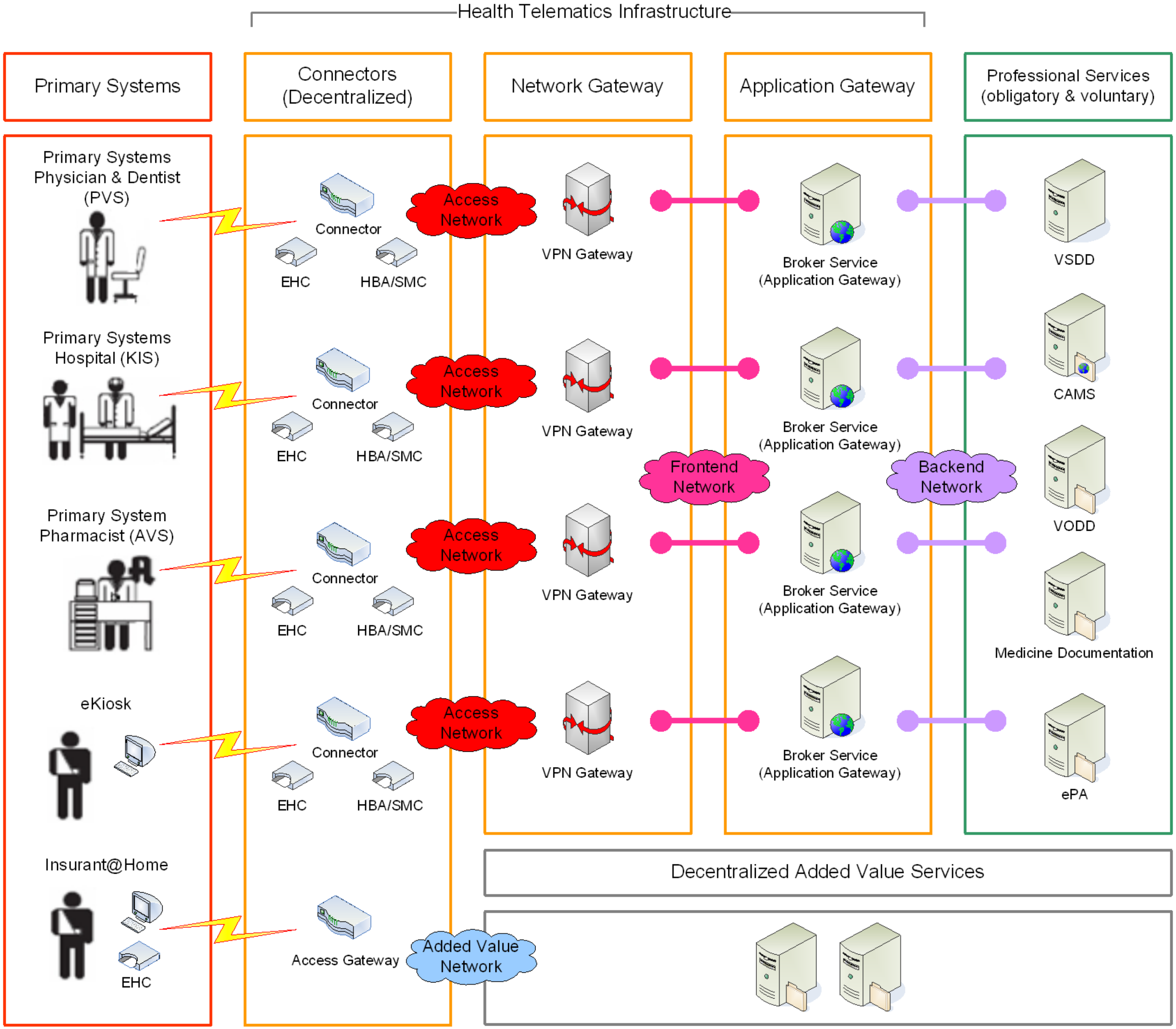
- Introduction
- Research Questions
- Results

Electronic Health Card (eHC)



300 Health insurances
2.200 Hospitals
21.000 Pharmacies
188.000 Medical specialists/dentists
and…
80 Million Insurants!

Quelle: in Anlehnung an www.gematik.de


Health Telematics Infrastructure
Primary Systems
Connectors (Decentralized)
Network Gateway
Application Gateway
Professional Services (obligatory & voluntary)
Primary Systems Physician & Dentist (PVS)
Primary Systems Hospital (KIS)
Primary System Pharmacist (AVS)
eKiosk
Insurant@Home
EHC
Connector
EHC
HBA/SMC
Connector
EHC
HBA/SMC
Connector
EHC
HBA/SMC
Connector
EHC
HBA/SMC
Access Gateway
Access Network
Access Network
Access Network
Access Network
Added Value Network
VPN Gateway
VPN Gateway
VPN Gateway
VPN Gateway
Frontend Network
Broker Service (Application Gateway)
Broker Service (Application Gateway)
Broker Service (Application Gateway)
Broker Service (Application Gateway)
Backend Network
VSDD
CAMS
VODD
Medicine Documentation
ePA
Decentralized Added Value Services

Importance of Research

- „Bei der Mehrheit der gesetzlich Krankenversicherten (73%) bestehen zumindest geringe Bedenken, dass die Daten auf der eGK von unberechtigten Personen eingesehen und missbraucht werden könnten – ein gutes Drittel der Versicherten äußert sogar große Bedenken“ (Forsa, 2008)

- handling of these new electronic patient cards
- business process reorganisation
- technical dependability

Overview

Problem

„Research shows insufficiencies with the … current analysis methods lacking the techniques to analyse technical and social aspects of information security in a health environment.“ (Brooks, 2004)

The goal of this project is to provide a method for the analysis of security issues in health care

Whom

- domain: health care / health care telematics
- chief information security officers
- results: patients, physicians, pharmacists, hospitals, health insurance companies

Why

- in order to evaluate the current security status of health care telematics in Germany and give valuable hints for future developments in the health care sector

What are special Characteristics of Health Care with Respect to Security?

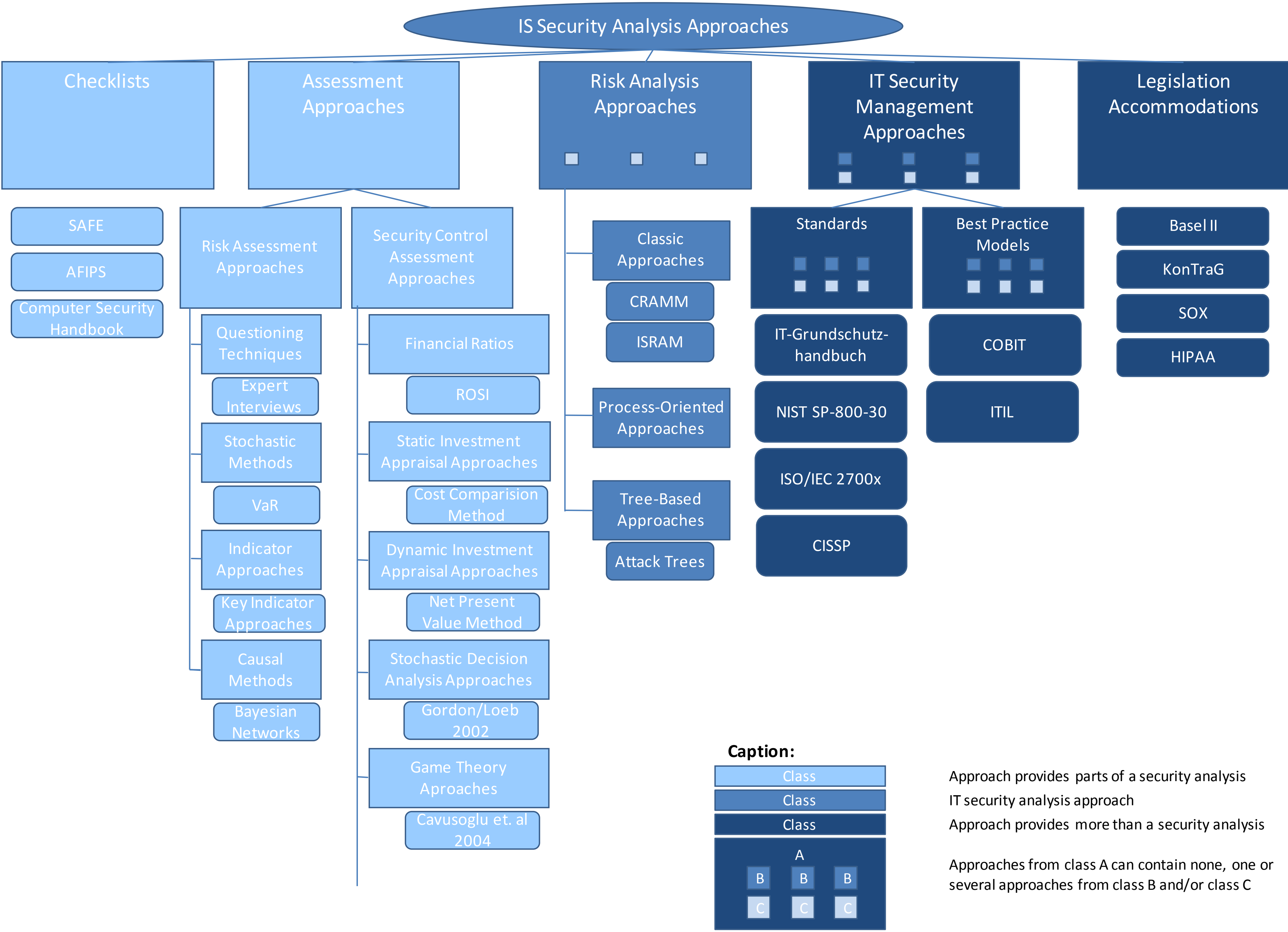
- Trade-off between availability (securing of an ideal treatment) and confidentiality (privacy)
- Strong regulations by law
- Local and heterogenous it-systems (not standardizied it-components)
- Contextual access rights
- Ad hoc and dynamic information exchange
- Physical property

Research approach

- Literature review based upon the approach by Webster and Watson (2002)
- Examination of healthcare IS security issues currently receiving attention in the literature.
- Spanning the IS security, information management, information systems, healthcare informatics, risk- and security analysis and management literature
- Identification of relevant journals
- Examination of appropriate articles
- Full-text electronic search - > analyzed articles 1007
- Total number of 145 relevant articles
- In-depth review of 25 articles

Journals	Abstract	In-Depth Review	Of Interest
ACM Computing Surveys	1	1	1
ACM Transactions on Information and System Security	38	1	0
Bank Accounting & Finance	2	1	0
Communications of the ACM	54	8	1
Computers & Security	92	32	2
European Journal of Information Systems	4	1	1
HMD Praxis der Wirtschaftsinformatik	7	5	0
IEEE Security & Privacy	21	4	0
IM Information Management & Consulting	3	1	0
Information and Organization	2	1	0
Information Management & Computer Security	33	9	1
Information Systems Journal	13	2	2
Information Systems Management	12	1	0
Information Systems Security	41	9	0
Information Security Management	29	1	0
Internal Auditor	21	1	0
International Journal of Network Management	28	1	0
International Journal of Medical Informatics	9	2	0
Journal of Computer Security	7	1	0
Journal of Management Information Systems	4	1	0
Journal of Research and Practice in Information Technology	2	1	0
Strategic Finance	7	1	0
Andere	11	10	2
Total Journals	**441**	**95**	**10**
Articles of organizations and authorities	19	19	2
Dissertations/ Master's-/ Bachelor Theses/ Working Paper	39	39	5
Conferences/ Workshops	13	4	1
Total	**512**	**157**	**18**

According to: Webster, J.; Watson, R.T. (2002): Analyzing the past to prepare for the future: writing a Literature Review. In: MIS Quarterly, Vol. 26 (2002) Nr. 2, S. xiii-xxiii.



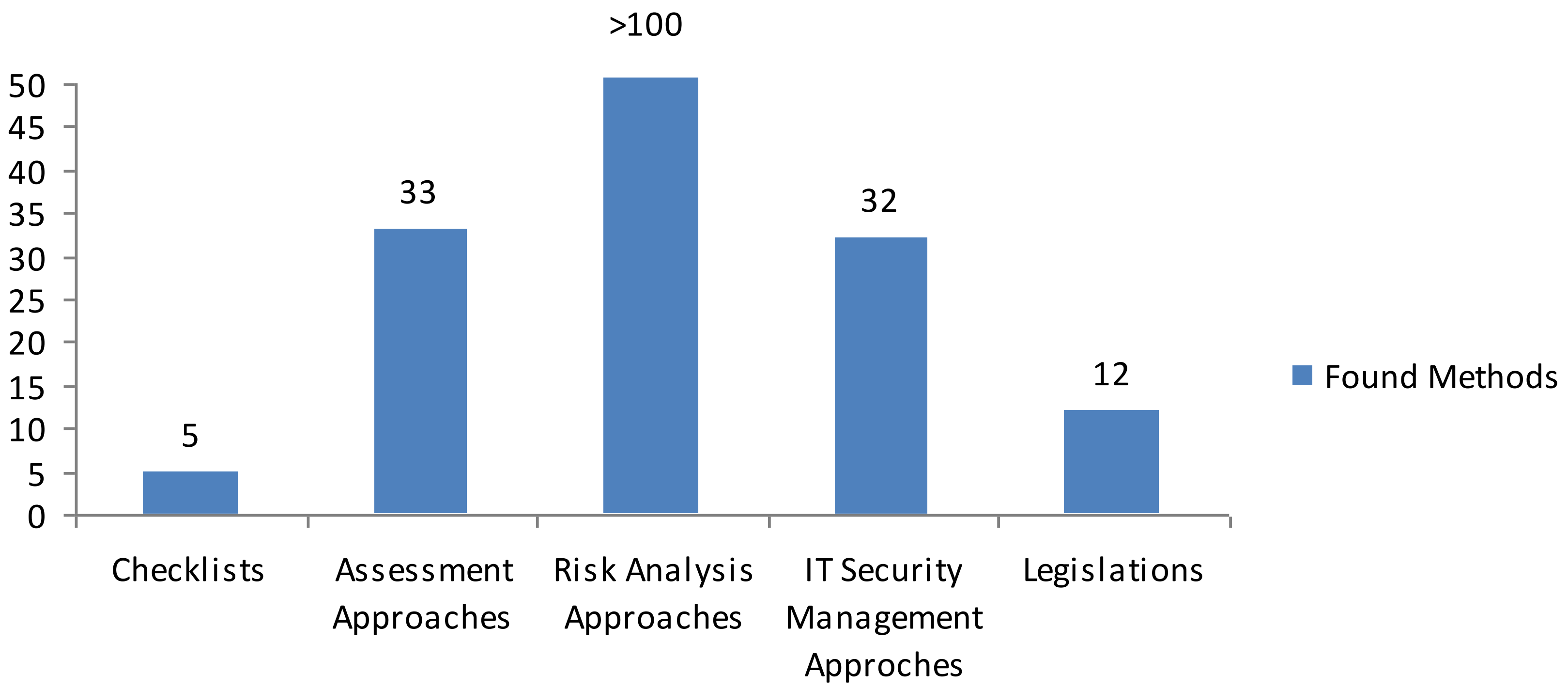
Approach provides parts of a security analysis

IT security analysis approach

Approach provides more than a security analysis

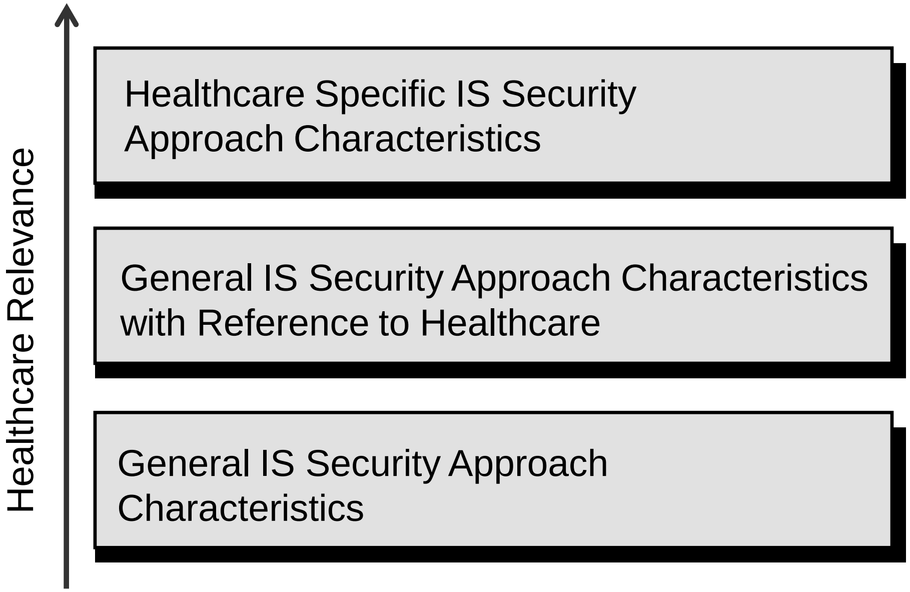
Approaches from class A can contain none, one or several approaches from class B and/or class C

Found Approaches



Characteristics of IS Security Approaches with Respect to Healthcare

Three different types:



Healthcare Specific IS Security Approach Characteristics

General IS Security Approach Characteristics with Reference to Healthcare

General IS Security Approach Characteristics

Important Aspects

- Focus on the healthcare sector;
- Provision of detailed information which identifies the IS security approach and could be used to create an approach identity card;
- Creation of information packages for healthcare organizations to help them select suitable methods for performing a security analysis;

General IS Security Approach Characteristics

- Basic Information

- Identification and Personalization of the profile of the researched IS security approach

- establish the relationship between the approaches and the different characteristics.

General IS Security Approaches Characteristics with Reference to Healthcare

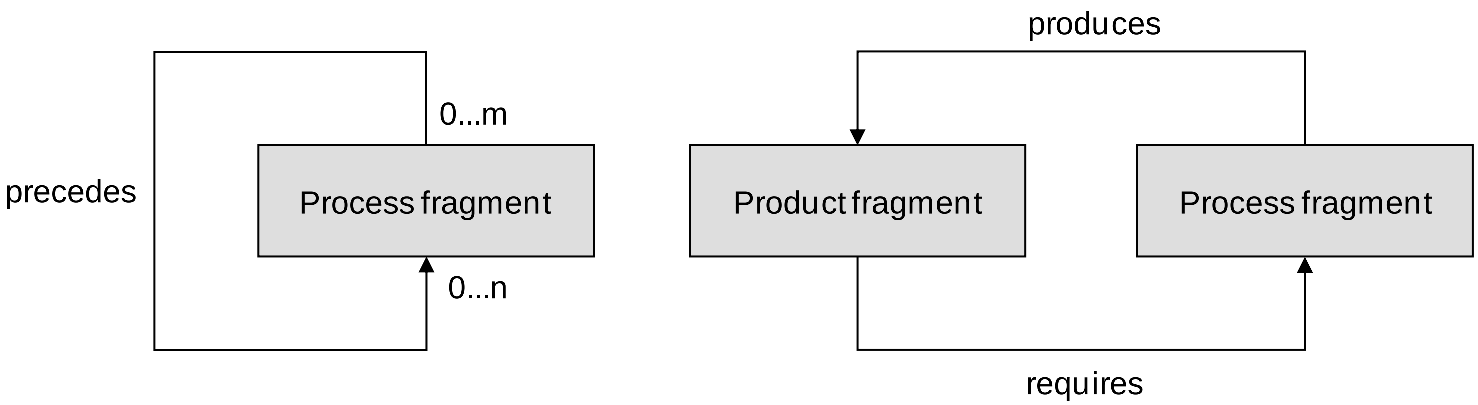
- Provide a better understanding of the specifics of healthcare.
- Similar to those of the first classification area but
- Could also be interpreted in a context that is applicable to the healthcare domain.

Healthcare Specific IS Security Approaches Characteristics

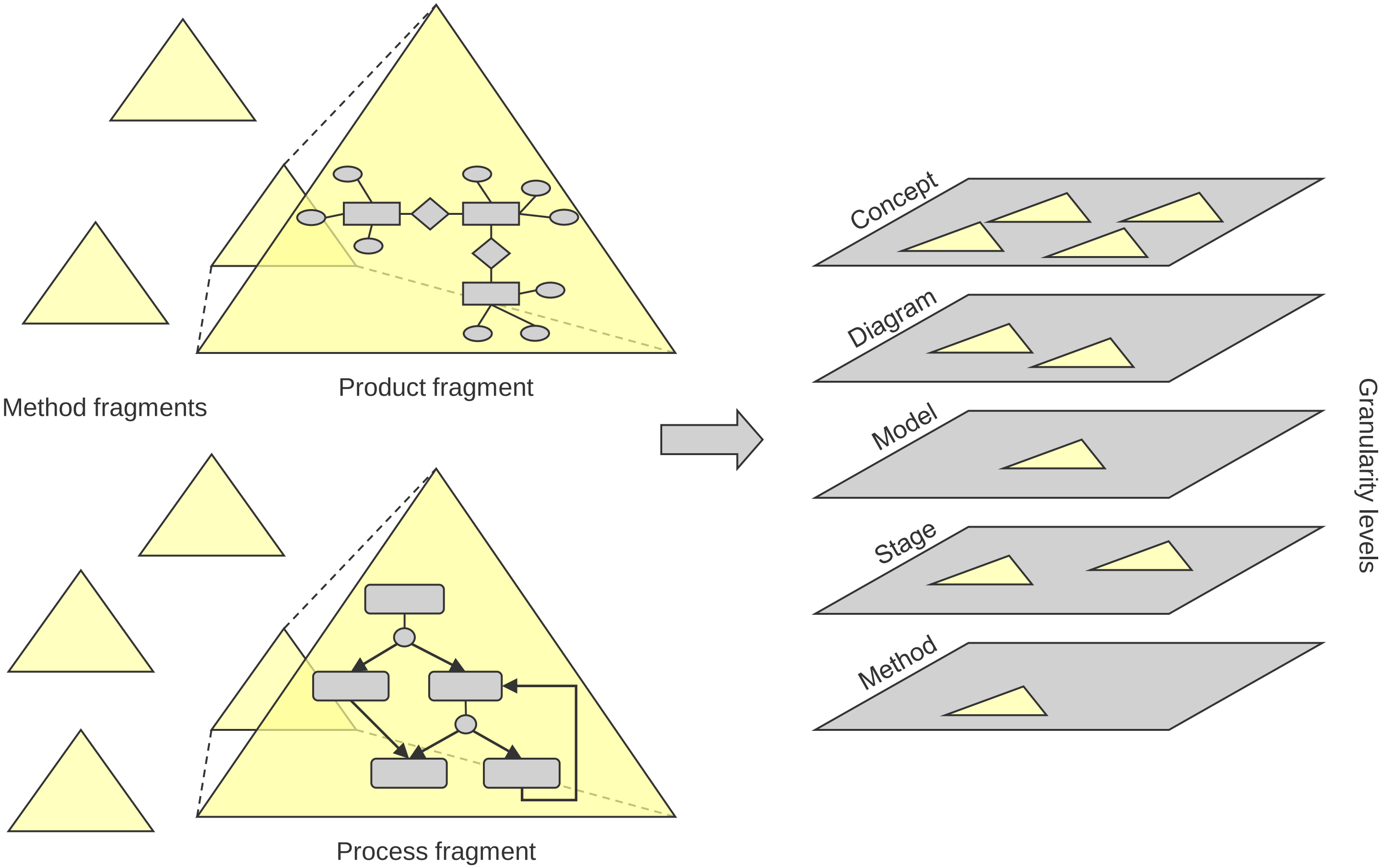
- Considers the special requirements such as the importance of protecting patient health information.
- Takes the uniqueness of the medical environment (ISO 2007, V) into consideration.
- Takes the specific laws concerning the security and privacy of health-related data into consideration

	Brooks-Evaluation	HIPAA	ODESSA	CRAMM	IT-Grundschutz-handbuch	ISO/IEC 17799	NIST SP 800-30
Fokus/Zielsetzung	Gesundheitswesen; techn. und orga. Sicherheitsaspekte	Gesundheitswesen; techn. und orga. Sicherheitsaspekte	Gesundheitswesen; techn. und orga. Sicherheitsaspekte	Allgemein, technische Sicherheitsaspekte	Allgemein, techn. und orga. Sicherheitsaspekte	Allgemein, organisatorische Sicherheitsaspekte	Allgemein, techn, orga. und ökonom. Sicherheitsasp.
Vorgehensweise	- Analyse und Modellierung der IT-Landschaft - Analyse d. Sicherheits-Maßnahmen - Soll-Ist-Vergleich - Implementierung geeigneter Sicherheitsmaßn.	Vollständiger Risikoanalyse- und Risikomanagement-prozess	- Implementierung v. Basis-Sicherheitsmaßn. - Identifikation geeigneter Sicherheitsmaßnahmen - Ableitung und Bewertung passender Sicherh.maßn.	- Identifikation und Bewertung von Assets - Identifikation und Bewertung von Bedrohungsszenarien - Ableitung geeigneter Sicherheitsmaßnahmen	- Modellierung der IT-Landschaft - Soll-Ist-Vergleich - Ableitung der Sicherheitsmaßnahmen	- Durchführung Risikoanalyse - Definition Soll-Zustand - Auswahl und Umsetzung der Sicherheitsmaßn.	Vollständiger Risikoanalyse- und Risikomanagement-prozess
Vollständigkeit	Nein	Ja	Ja	Nein	Nein	Ja	Ja
Aufwand/Umsetzungskosten	Mittel – Hoch	Hoch	Mittel	Mittel	Mittel	Mittel – Hoch	Hoch
Methodik der Informations-gewinnung	Befragungs-techniken	Befragungs-techniken	Befragungs-techniken	Befragungs-techniken	Analyse der IT-Landschaft	Hinweis auf ISO/IEC 13335	Befragungs-techniken
Aktualität Updates	2004 Nicht bekannt	1996 Nein	1997 Nicht bekannt	2005 Ja	2007 Ja	2005 Ja	2002 Nein
Regionale Bestimmungen	Australien, Hinweis auf nationale Vorgaben	USA, Richtlinien des „Code of Federal Regulations (CFR)“	Keine Informationen Verfügbar	UK, Einhaltung des HIPAA & GLBA	Deutschland, Hinweis auf gesetzl. Bestimmungen	Weltweit, Einhaltung gesetzl. Bestimmungen	USA
Internationalität	Keine Informationen verfügbar	Keine Informationen verfügbar	Keine Informationen verfügbar	Ja	Ja	Ja	Keine Informationen verfügbar
Zertifizierungs-möglichkeit	Ja HB 174-2003	Keine Informationen verfügbar	Keine Informationen verfügbar	Ja BS 7799	Ja ISO 27001	Ja ISO/IEC 17799	Keine Informationen verfügbar
Toolunterstützung	Keine Informationen verfügbar	Nein	Ja	Ja	Ja	Nein	Keine Informationen verfügbar

Relationship between Method Fragments



Granularity levels



HatSec Method

- Seven steps:

(1) scope identication

(2) asset identication

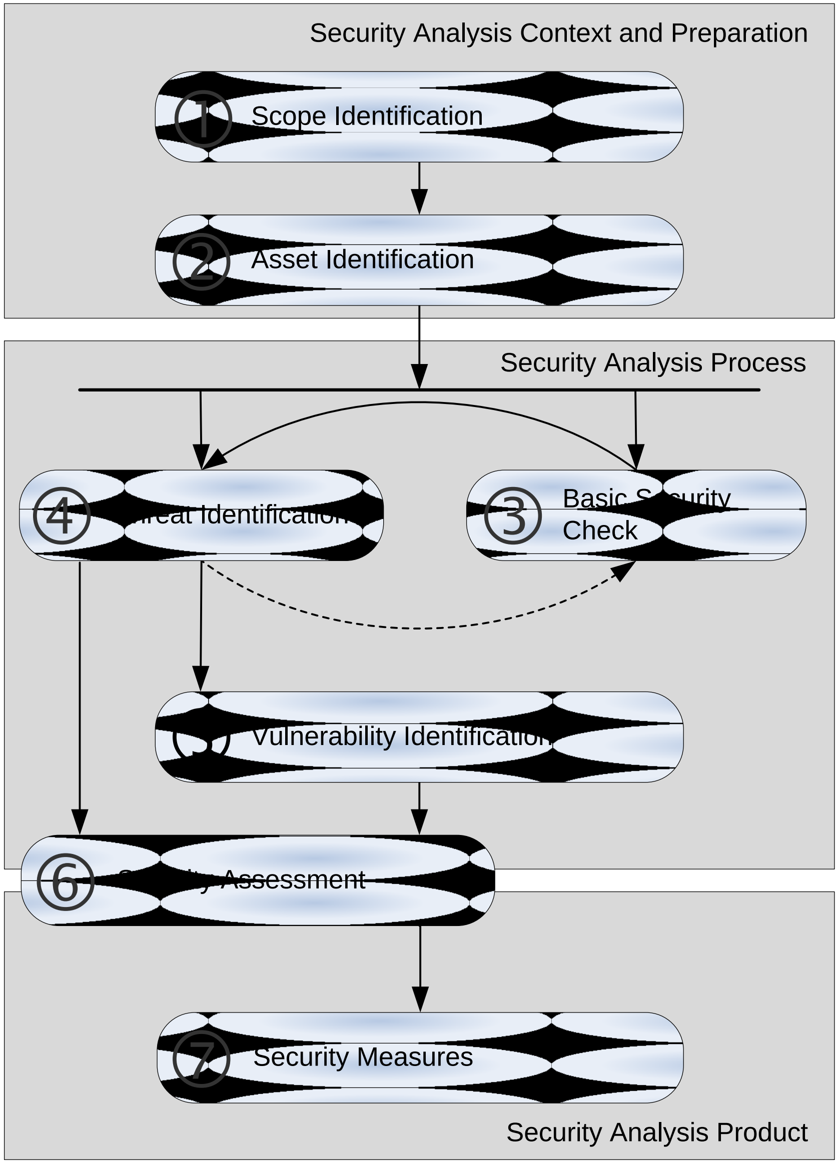
(3) basic security check

(4) threat identication

(5) vulnerability identication

(6) security assessment

(7) security measures



Security Analysis Context and Preparation

① Scope Identification

② Asset Identification

Security Analysis Process

④ Threat Identification

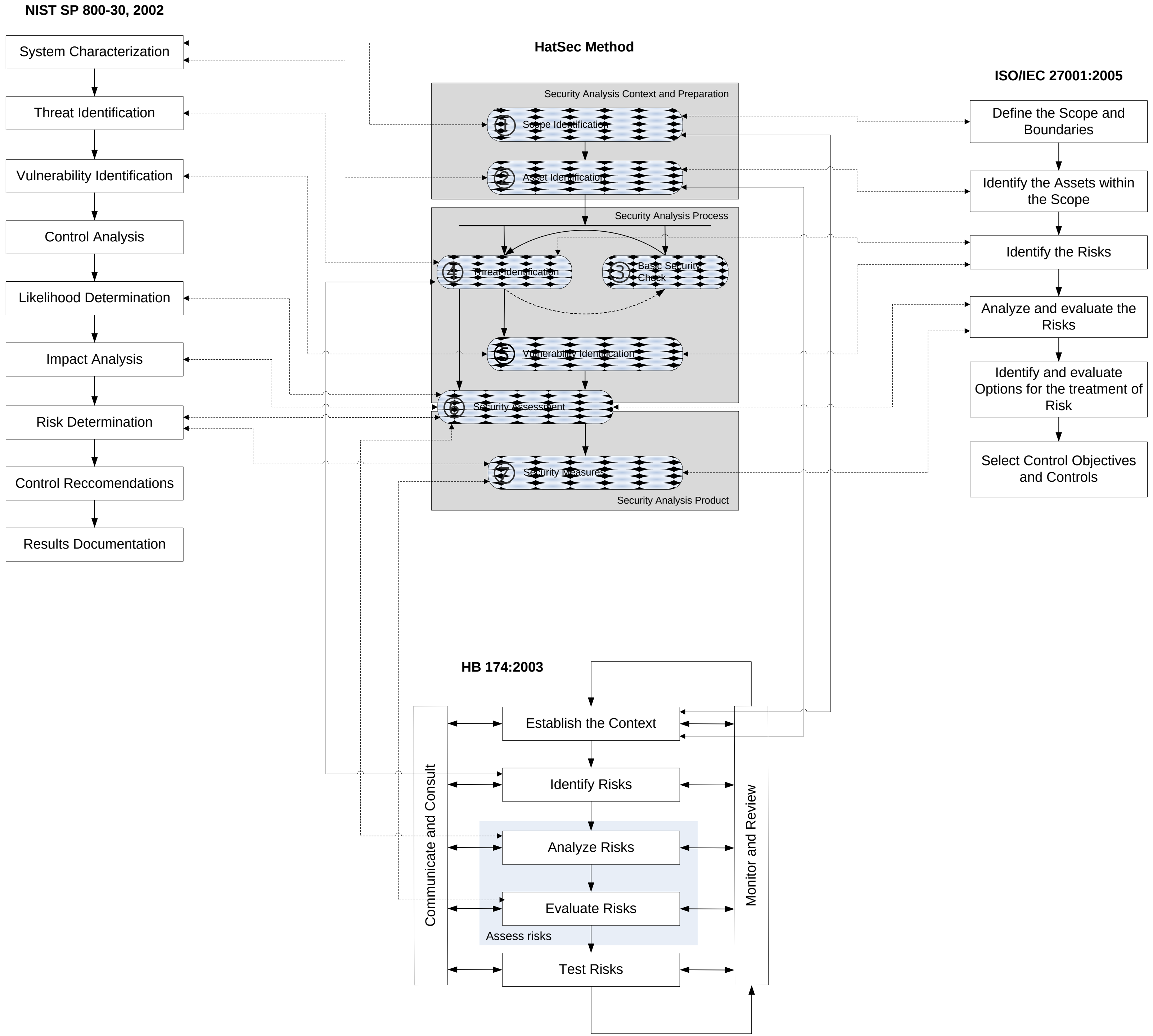
③ Basic Security Check

⑤ Vulnerability Identification

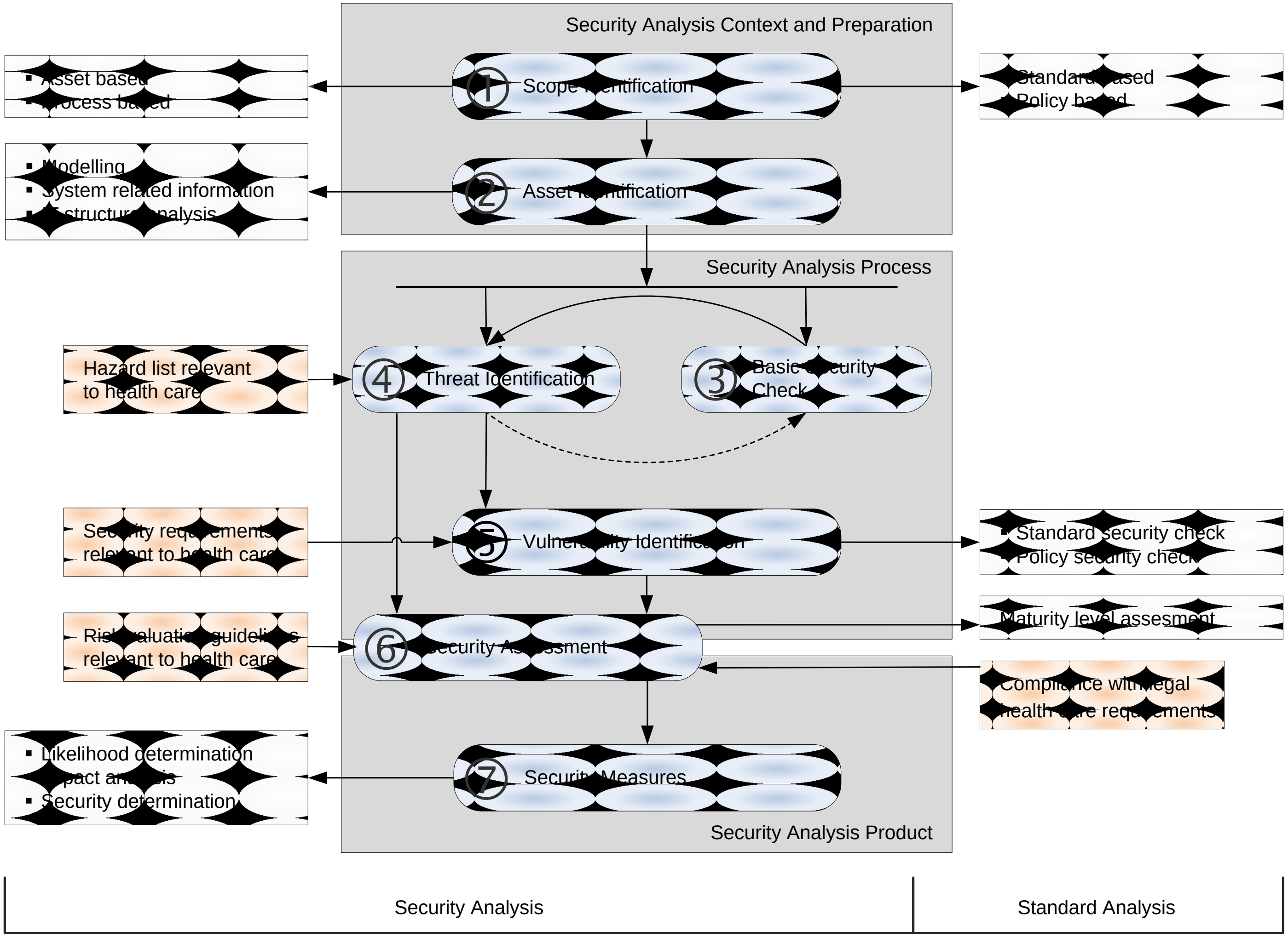
⑥ Security Assessment

⑦ Security Measures

Security Analysis Product


NIST SP 800-30, 2002
System Characterization
Threat Identification
Vulnerability Identification
Control Analysis
Likelihood Determination
Impact Analysis
Risk Determination
Control Reccomendations
Results Documentation
HatSec Method
Security Analysis Context and Preparation
1 Scope Identification
2 Asset Identification
Security Analysis Process
4 Threat Identification
3 Basic Security Check
5 Vulnerability Identification
6 Security Assessment
7 Security Measures
Security Analysis Product
ISO/IEC 27001:2005
Define the Scope and Boundaries
Identify the Assets within the Scope
Identify the Risks
Analyze and evaluate the Risks
Identify and evaluate Options for the treatment of Risk
Select Control Objectives and Controls
HB 174:2003
Communicate and Consult
Establish the Context
Identify Risks
Analyze Risks
Evaluate Risks
Assess risks
Test Risks
Monitor and Review

HatSec Method



Security Analysis Context and Preparation

- Asset based
- Process based

① Scope Identification

- Standard based
- Policy based

- Modelling
- System related information
- IT structure analysis

② Asset Identification

Security Analysis Process

Hazard list relevant to health care

④ Threat Identification

③ Basic Security Check

Security requirements relevant to health care

⑤ Vulnerability Identification

- Standard security check
- Policy security check

Maturity level assesment

Risk evaluation guidelines relevant to health care

⑥ Security Assessment

Compliance with legal health care requirements

- Likelihood determination
- Impact analysis
- Security determination

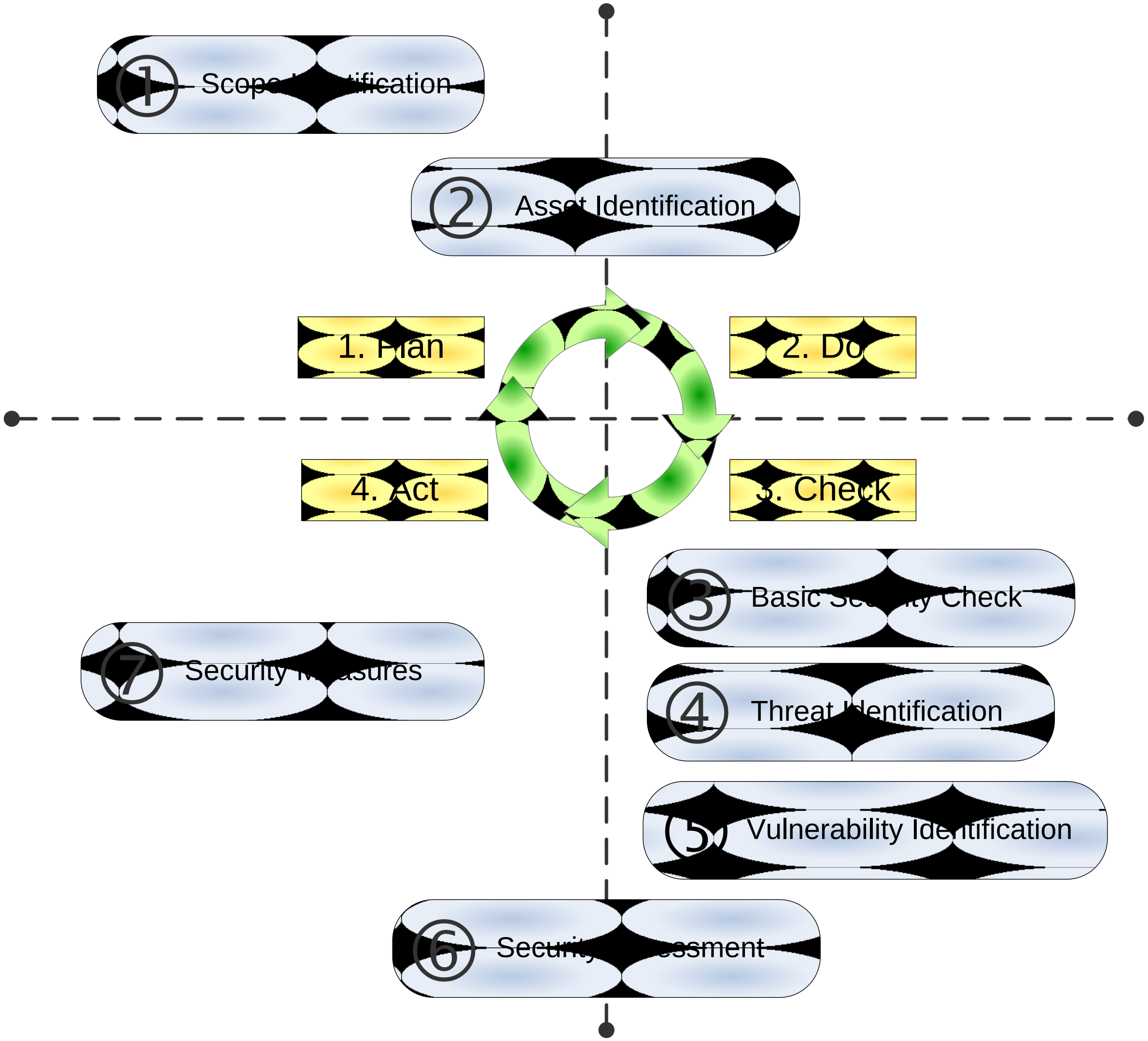
⑦ Security Measures

Security Analysis Product

Security Analysis

Standard Analysis

PDCA Mapping



① Scope Identification

② Asset Identification

1. Plan

2. Do

4. Act

3. Check

③ Basic Security Check

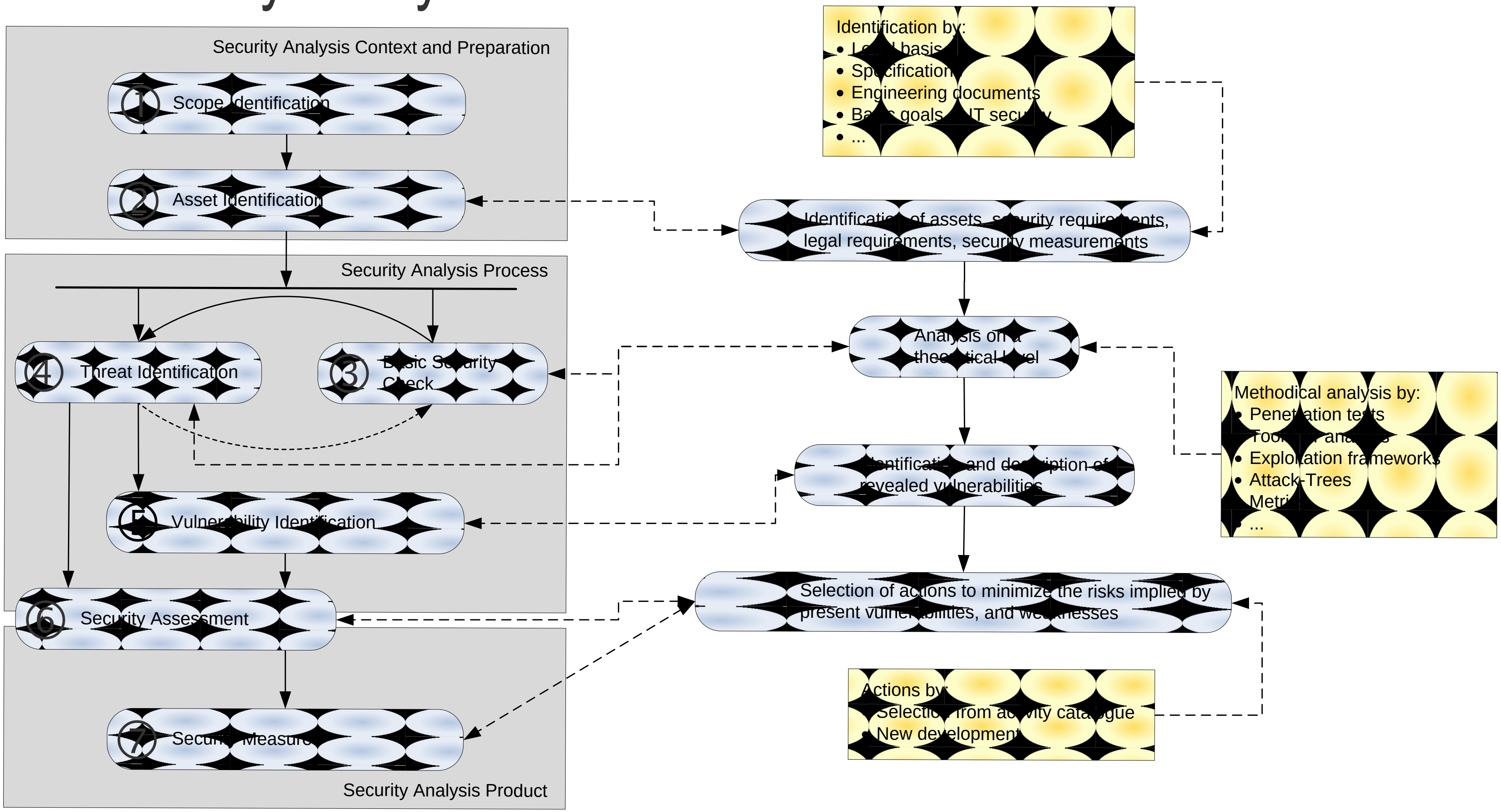
⑦ Security Measures

④ Threat Identification

⑤ Vulnerability Identification

⑥ Security Assessment

Security Analysis



Security Analysis Context and Preparation

1 Scope Identification

2 Asset Identification

Security Analysis Process

4 Threat Identification

3 Basic Security Check

5 Vulnerability Identification

6 Security Assessment

7 Security Measure

Security Analysis Product

Identification by:
- Legal basis
- Specification
- Engineering documents
- Basic goals of IT security
- ...

Identification of assets, security requirements, legal requirements, security measurements

Analysis on a theoretical level

Methodical analysis by:
- Penetration tests
- Tools for analysis
- Exploitation frameworks
- Attack-Trees
- Metrics
- ...

Identification and description of revealed vulnerabilities

Selection of actions to minimize the risks implied by present vulnerabilities, and weaknesses

Actions by:
- Selection from activity catalogue
- New development

A safe freeway with insecure on-ramps?

- The connection between the primary systems and the connector should be encrypted
- Security specifications for primary systems should be defined
- Backup processes for essential health care telematics processes and services should be defined
- Long-term confidentiality of encrypted medical data
- Handling of electronic health cards and of health professional cards especially in hospitals

Design and Application of a Security Analysis Method for Healthcare Telematics in Germany (HatSec)

Ali Sunyaev

Technische Universität München

Fakultät für Informatik

Lehrstuhl für Wirtschaftsinformatik (I17)

References

- **Brooks, W.; Warren, M. (2004)**: Health information security evaluation: continued development of an object-oriented method. Paper presented at the 2nd Australian Information Security Management Conference, Perth, Western Australia, S. 135-150.
- **Webster, J.; Watson, R.T. (2002):** Analyzing the past to prepare for the future: writing a Literature Review. In: MIS Quarterly, Vol. 26 (2002) Nr. 2, S. xiii-xxiii.
- **Harmsen, F.; Brinkkemper, S.; Oei, H. (1994):** Situational Method Engineering for Information System Project Approaches. In: Methods and Associated Tools for the Information Systems Life Cycle. Hrsg.: Verrijn-Stuart, A.A.; Olle, T.W. Elsevier Science B.V., Amsterdam 1994, S. 169-194.
- **Ralyté, J.; Rolland, C. (2001):** An Approach for Method Reengineering. In: Conceptual Modeling. Proceedings of the 20th International Conference on Conceptual Modeling, Yokohama, Japan, November 27-30, 2001. Hrsg.: Kunii, H.S.; Jajodia, S.; Solvberg, A. Springer-Verlag, Berlin, Heidelberg 2001, S. 471-484.
- **Olle, T.W.; Hagelstein, J.; MacDonald, I.; Rolland, C.; Van Assche, F.; Verrijn-Stuart, A.A. (1988):** Information Systems Methodologies: A Framework for Understanding. Addison- Wesley, Wokingham 1988.
- **Jayaratna, N. (1994):** Understanding and Evaluating Methodologies: NIMSAD, a Systematic Framework. McGraw-Hill Book Company, London 1994.
- **Hidding, G.J. (1997):** Reeinventing Methodology: Who Reads It And Why? In: Communications of the ACM, Vol. 40 (1997) Nr. 1, S. 102-109.
- **Iivari, J.; Maansaari, J. (1998):** The usage of systems development methods: are we stuck to old practices? In: Information and Software Technology, Vol. 40 (1998) Nr. 9, S. 501-510.
- **Russo, N.L.; Stolterman, E. (2000):** Exploring the assumptions underlying information systems methodologies – Their impact on past, present and future ISM research. In: Information Technology & People, Vol. 13 (2000) Nr. 4, S. 313-327.
- **Henderson-Sellers, B.; Gonzalez-Perez, C.; Serour, M.K. (2005):** Method Engineering and COTS Evaluation. In: http://citeseer.ist.psu.edu/283885.html, zugegriffen am: 23.10.2007.
- **Brinkkemper, S. (1996):** Method engineering: engineering of information systems development methods and tools. In: Information and Software Technology, Vol .38 (1996) Nr. 4, S. 275-280.
- **Cronholm, S.; Ågerfalk, P.J. (1999):** On the Concept of Method in Information Systems Development. In: http://citeseer.ist.psu.edu/283885.html, zugegriffen am: 28.08.2007.