

## Inhaltsübersicht

<b>1 EINLEITUNG.....</b>	<b>1</b>
<b>2 GRUNDLAGEN UND AKTUELLER STAND DER INFORMATIONSSICHERHEIT UND DES BETRIEBLICHEN SICHERHEITSMANAGEMENTS .....</b>	<b>9</b>
<b>3 INFORMATIONSSICHERHEIT IN GESCHÄFTSPROZESSEN: EINE NEUAUSRICHTUNG DER SICHERHEITSBETRACHTUNG .....</b>	<b>85</b>
<b>4 SIMULATION DER INFORMATIONSSICHERHEIT .....</b>	<b>117</b>
<b>5 ENTWURF EINES SYSTEMS ZUR SIMULATION VON INFORMATIONSSICHERHEIT IN GESCHÄFTSPROZESSEN.....</b>	<b>149</b>
<b>6 PROTOTYPISCHE REALISIERUNG EINES SIMULATIONSWERKZEUGS....</b>	<b>263</b>
<b>7 EMPIRISCHE UNTERSUCHUNG DER EINSATZPOTENTIALE UND NUTZUNGS-RAHMENBEDINGUNGEN DES GESCHÄFTSPROZESS- ORIENTIERTEN SIMULATIONS-SYSTEMS .....</b>	<b>323</b>
<b>8 SCHLUSSFOLGERUNGEN FÜR WEITERE UNTERSUCHUNGEN.....</b>	<b>429</b>
<b>9 LITERATURVERZEICHNIS .....</b>	<b>437</b>
<b>10 ANHANG .....</b>	<b>475</b>

# Inhaltsverzeichnis

<b>GELEITWORT .....</b>	<b>V</b>
<b>VORWORT .....</b>	<b>VII</b>
<b>VERZEICHNISSE</b>	
<b>Inhaltsübersicht .....</b>	<b>IX</b>
<b>Inhaltsverzeichnis .....</b>	<b>XI</b>
<b>Abbildungsverzeichnis .....</b>	<b>XXI</b>
<b>Tabellenverzeichnis .....</b>	<b>XXV</b>
<b>Abkürzungsverzeichnis .....</b>	<b>XXVII</b>
<b>1 EINLEITUNG .....</b>	<b>1</b>
<b>1.1 Problemstellung und Zielsetzung der Arbeit .....</b>	<b>1</b>
<b>1.2 Aufbau der Arbeit und Vorgehensweise .....</b>	<b>4</b>
<b>2 GRUNDLAGEN UND AKTUELLER STAND DER INFORMATIONSSICHERHEIT UND DES BETRIEBLICHEN SICHERHEITSMANAGEMENTS .....</b>	<b>9</b>
<b>2.1 Informationssicherheit .....</b>	<b>10</b>
<b>2.1.1 Begriff und Abgrenzungen .....</b>	<b>10</b>
<b>2.1.1.1 Begriffsdefinitionen und Charakterisierung .....</b>	<b>10</b>
<b>2.1.1.2 Sicherheitsziele .....</b>	<b>13</b>
<b>2.1.1.3 Abgrenzung des Themengebiets „Informationssicherheit“ zu angrenzenden Forschungs- und Arbeitsgebieten .....</b>	<b>14</b>
<b>2.1.1.4 Strukturierung der Informationssicherheit .....</b>	<b>20</b>
<b>2.1.2 Kausalmodell der Sicherheit der Informationsverarbeitung .....</b>	<b>22</b>
<b>2.1.3 Rahmenbedingungen und aktuelle Entwicklungen der Informationssicherheit .....</b>	<b>29</b>
<b>2.1.4 Zusammenfassende Bewertung der heutigen Situation: Informationssicherheit als Eigenschaft von Informationstechnik-Systemen .....</b>	<b>34</b>

<b>2.2 Management der Informationssicherheit.....</b>	<b>37</b>
2.2.1 Komponenten der betrieblichen Gestaltung der Informationssicherheit .....	37
2.2.1.1 Organisatorische Implementierung .....	38
2.2.1.2 Sicherheitsstrategie und Sicherheitskonzept.....	42
2.2.1.3 Sicherheitsbewußtsein.....	45
2.2.2 Konzepte für das Sicherheitsmanagement.....	46
2.2.2.1 Phasenmodelle des Sicherheitsmanagements .....	46
2.2.2.2 Integrationsansatz als Vorschlag für das Sicherheitsmanagement .....	50
2.2.3 Alternativen für das Risikomanagement.....	55
2.2.3.1 Typisierte Soll-Ist-Vergleiche von Sicherheitsmaßnahmen versus Individualanalysen.....	55
2.2.3.2 Ausprägungen des Risikomanagements in der Praxis .....	59
2.2.3.2.1 Generally Accepted Security Principles and Practices .....	60
2.2.3.2.2 Code of Practice for Information Security Management.....	61
2.2.3.2.3 Konzept „Grundschutz + X“ .....	62
2.2.4 Methoden und Verfahren zur individuellen Untersuchung der Informationssicherheit.....	67
2.2.4.1 Ansatz und Formen der Risikoanalyse .....	67
2.2.4.1.1 Komponenten von Risikoanalysen.....	68
2.2.4.1.2 Methoden mit schematischer Risikobewertung.....	70
2.2.4.1.3 Methoden mit heuristischen Risikobewertungen .....	72
2.2.4.1.4 Verwendung von Risikoanalysemethoden in der Praxis.....	75
2.2.4.2 Computerunterstützte Sicherheitsanalysen.....	76
2.2.5 Probleme der Anwendung existierender Methoden für das Risikomanagement.....	78
<b>3 INFORMATIONSSICHERHEIT IN GESCHÄFTSPROZESSEN: EINE NEUAUSRICHTUNG DER SICHERHEITSBETRACHTUNG .....</b>	<b>85</b>
3.1 Definitionen von Geschäftsprozessen .....	86
3.2 Arten und Eigenschaften von Geschäftsprozessen.....	89
3.3 Bedeutung der Geschäftsprozeß-Orientierung.....	93
3.4 Beziehungen zwischen Geschäftsprozessen und Informationssicherheit.....	96

3.4.1 Vorschlag: Erweiterung des Analyse- und Gestaltungsbereichs um Geschäftsprozesse .....	97
3.4.1.1 Nutzung von Geschäftsprozessen zur Ableitung und Konkretisierung von Sicherheitszielen .....	98
3.4.1.2 Geschäftsprozesse als Untersuchungsobjekte .....	103
3.4.1.3 Sachlogische und wirtschaftliche Beurteilung von Sicherheitsmaßnahmen .....	105
3.4.1.4 Geschäftsprozesse als Gestaltungsobjekte der Informationssicherheit....	106
3.4.2 Vorschlag: Verwendung von Geschäftsprozessen als interpersonales Kommunikationsmedium.....	108
3.4.3 Vorschlag: Geschäftsprozeß-orientierte Gestaltung des Sicherheits- managements .....	109
3.4.3.1 Strategisches Sicherheitsmanagement und Risikomanagement .....	110
3.4.3.2 Entwicklung und Betrieb von Sicherheitsmaßnahmen.....	111
3.4.3.3 Sicherheitsmanagement als Teil eines „Business Process Reengineering“-Projektes .....	112
<b>3.5 Zusammenfassung .....</b>	<b>115</b>
<b>4 SIMULATION DER INFORMATIONSSICHERHEIT .....</b>	<b>117</b>
<b>4.1 Ausprägungsformen der Simulation .....</b>	<b>117</b>
4.1.1 Definitionen von Simulation .....	117
4.1.2 Modellbildung .....	119
4.1.3 Durchführen von Experimenten am erstellten Modell.....	120
4.1.4 Charakterisierung von Simulationen .....	121
4.1.5 Simulationen betriebswirtschaftlicher Fragestellungen .....	123
<b>4.2 Analyse der vorhandenen Simulationsansätze in existierenden Methoden zur Untersuchung der Informationssicherheit .....</b>	<b>125</b>
4.2.1 CRAMM .....	125
4.2.1.1 Überblick .....	125
4.2.1.2 Beschreibung der Modellierungs- und Simulationskomponenten .....	126
4.2.2 IT-Sicherheitshandbuch .....	128
4.2.2.1 Überblick .....	128
4.2.2.2 Beschreibung der Modellierungs- und Simulationskomponenten .....	129

4.2.3 Wissensbasiertes, objektorientiertes Beratungssystem für die Risikoanalyse von Stelzer .....	131
4.2.3.1 Überblick .....	131
4.2.3.2 Beschreibung der Modellierungs- und Simulationskomponenten .....	132
4.2.4 Zusammenfassung.....	135
<b>4.3 Computerunterstützte Simulationen .....</b>	<b>137</b>
4.3.1 Charakterisierung von computerunterstützten Simulationen .....	137
4.3.2 Computerunterstützte Sicherheitssimulationen.....	137
<b>4.4 Defizite bisheriger Simulationsansätze.....</b>	<b>140</b>
4.4.1 Generelle Defizite existierender Simulationsmethoden.....	140
4.4.2 Defizite in der Modellierung .....	143
4.4.3 Defizite der Simulationen .....	145
4.4.4 Zusammenfassende Bewertung.....	147
<b>5 ENTWURF EINES SYSTEMS ZUR SIMULATION VON INFORMATIONSSICHERHEIT IN GESCHÄFTSPROZESSEN.....</b>	<b>149</b>
<b>5.1 Zielsetzungen und Ableitung von Anforderungen .....</b>	<b>149</b>
<b>5.2 Realisierungsansatz.....</b>	<b>154</b>
5.2.1 Bestandteile des geschäftsprozeß-orientierten Simulations-Systems .....	154
5.2.2 Grundlegende Merkmale.....	158
5.2.2.1 Semi-formale Modellierung von sicherheitsrelevanten Objekten und deren Beziehungen.....	158
5.2.2.2 Inkrementelle Simulation der Auswirkungen von Sicherheitsverletzungen .....	160
5.2.2.3 Erweiterung des Untersuchungs- und Gestaltungsbereichs um Geschäftsprozesse .....	162
5.2.2.4 Visualisierung von Untersuchungsmodellen und Simulationsergebnissen .....	164
<b>5.3 Beschreibungselemente für die Modellierung des Untersuchungsbereichs...</b>	<b>166</b>
5.3.1 Sicherheitsrelevante Objekte .....	167
5.3.1.1 Objektgruppen.....	167
5.3.1.2 Kontextattribute von sicherheitsrelevanten Objekten .....	171
5.3.1.3 Attribute zur Beschreibung der Sicherheitsinformationen.....	175

<b>5.3.2 Beziehungen .....</b>	<b>179</b>
5.3.2.1 Differenzierung von Beziehungen und sicherheitsrelevanten Abhängigkeiten.....	179
5.3.2.2 Attribute zur Beschreibung von Beziehungen .....	181
<b>5.4 Beschreibungselemente für die Durchführung von Simulationen .....</b>	<b>186</b>
5.4.1 Beziehungs- und Abhängigkeitsanalysen .....	186
5.4.2 Gefahren und Gefahr-Objekt-Kombinationen.....	187
5.4.2.1 Unterscheidung zwischen Gefahren und Gefahr-Objekt- Kombinationen.....	187
5.4.2.2 Gefahrenquellen von Gefahren .....	189
5.4.2.3 Beschreibungsattribute für Gefahren .....	190
5.4.2.4 Beschreibungsattribute für Gefahr-Objekt-Kombinationen .....	191
5.4.3 Simulationen der Konsequenzen von gefährdenden Ereignissen.....	193
5.4.3.1 Überblick .....	193
5.4.3.2 Simulationen zur Ist- und Soll-Risikosituation .....	194
5.4.3.3 Konsequenzen von gefährdenden Ereignissen .....	196
5.4.3.4 Einschub: Abschnitte und Teilergebnisse einer Simulation .....	198
5.4.3.5 Attribute zur Beschreibung einer Simulation.....	207
5.4.4 Sicherheitsmaßnahmen.....	212
5.4.4.1 Wirkungen von Sicherheitsmaßnahmen .....	212
5.4.4.2 Maßnahmenbündel .....	214
5.4.4.3 Attribute zur Beschreibung von Sicherheitsmaßnahmen .....	216
5.4.5 Zusammenhang der Beschreibungselemente .....	220
<b>5.5 Übergreifende Strukturkomponenten .....</b>	<b>222</b>
5.5.1 Strukturierung des Untersuchungsmodells .....	222
5.5.1.1 Beschreibungsebenen und Sichten .....	222
5.5.1.2 Modularisierung .....	226
5.5.1.3 Hierarchisierung .....	229
5.5.1.4 Inhaltliche Vormodellierungen .....	230
5.5.2 Visualisierung .....	233
5.5.2.1 Repräsentation des Untersuchungsmodells .....	235
5.5.2.2 Darstellung von Simulationsergebnissen im Untersuchungsmodell.....	237
5.5.3 Sammlung von Erfahrungswissen .....	238
5.5.4 Sicherstellung der sachlogischen Konsistenz.....	241
5.5.5 Aufbereitung der Ergebnisse .....	242

<b>5.6 Vorgehensmodell .....</b>	<b>244</b>
5.6.1 Vorgehensschritte.....	244
5.6.1.1 Aktuellen Untersuchungsbereich modellieren.....	246
5.6.1.2 Gefahren zuordnen .....	248
5.6.1.3 Ist-Risikosituation untersuchen.....	250
5.6.1.4 Soll-Risikosituation untersuchen.....	251
5.6.1.5 Maßnahmen evaluieren.....	254
5.6.2 Input-Action-Output-Tabelle.....	255
5.6.3 Organisationsspezifische Anpassungen .....	258
<b>5.7 Gegenüberstellung von Anforderungen und Komponenten des Simulations- Systems .....</b>	<b>260</b>
<b>6 PROTOTYPISCHE REALISIERUNG EINES SIMULATIONSWERKZEUGS....</b>	<b>263</b>
<b>6.1 Zielsetzung und Leitlinien für die Prototypentwicklung.....</b>	<b>263</b>
<b>6.2 Basisfunktionalitäten für Modellierung und Simulation.....</b>	<b>267</b>
6.2.1 Überblick.....	267
6.2.2 Modellieren.....	268
6.2.2.1 Sicherheitsrelevante Objekte generieren und bearbeiten.....	268
6.2.2.2 Beziehungen modellieren und bearbeiten.....	272
6.2.2.3 Darstellung von Objekten und Beziehungen in Ebenenfenstern.....	274
6.2.3 Gefahren zuordnen.....	276
6.2.3.1 Beziehungs- und Abhängigkeitsanalysen.....	276
6.2.3.2 Gefahr-Objekt-Kombinationen bestimmen.....	278
6.2.4 Ist-Risikosituation simulieren .....	280
6.2.4.1 Bestimmung und Evaluierung der direkten Konsequenzen .....	280
6.2.4.2 Bestimmung und Evaluierung der indirekten Konsequenzen.....	283
6.2.4.3 Simulationen handhaben.....	286
6.2.5 Soll-Risikosituation simulieren.....	288
6.2.5.1 Soll-Analysen handhaben .....	288
6.2.5.2 Modellierung potentieller Sicherheitsmaßnahmen.....	290
6.2.6 Maßnahmenbündel evaluieren .....	292
6.2.6.1 Entscheidungsvorschlag erarbeiten .....	293
6.2.6.2 Maßnahmen priorisieren .....	296

<b>6.3 Querschnittsfunktionalitäten .....</b>	<b>298</b>
6.3.1 Basiselemente pflegen .....	298
6.3.2 Berichte und Auswertungen .....	299
6.3.3 Import- und Exportfunktionen .....	304
6.3.4 Simulationswissen .....	307
6.3.5 Ebenenfenster .....	309
6.3.6 Konsistenzprüfungen und Fehlerbehandlung .....	312
6.3.7 Datenmanagement .....	313
6.3.7.1 Verwaltung der Projektdatenbank .....	313
6.3.7.2 Datenmodell .....	314
<b>6.4 IV-systemtechnische Charakterisierung .....</b>	<b>317</b>
6.4.1 Auswahl der Entwicklungsumgebung Visual Basic Professional .....	317
6.4.2 Programmkomponenten des Software-Prototypen SIMSI .....	319
6.4.3 Einbindung des Software-Prototypen in die Betriebssystemumgebung .....	320
<b>7 EMPIRISCHE UNTERSUCHUNG DER EINSATZPOTENTIALE UND NUTZUNGS-RAHMENBEDINGUNGEN DES GESCHÄFTSPROZESS-ORIENTIERTEN SIMULATIONS-SYSTEMS .....</b>	<b>323</b>
<b>7.1 Konzeption der empirischen Untersuchung .....</b>	<b>323</b>
7.1.1 Ziele der empirischen Untersuchung .....	324
7.1.2 Struktur und Vorgehensweise .....	325
7.1.3 Zielgruppen .....	328
<b>7.2 Entwicklung von Thesen .....</b>	<b>329</b>
<b>7.3 Konzeption des Interviewleitfadens .....</b>	<b>332</b>
<b>7.4 Praktische Durchführung und Erfahrungen mit der empirischen Untersuchung .....</b>	<b>333</b>
7.4.1 Vorbereitung und Durchführung des Experten-Workshops .....	333
7.4.2 Vorbereitung und Durchführung der Intensivinterviews .....	335
7.4.3 Erfahrungen mit der empirischen Untersuchungsmethodik .....	338
7.4.3.1 Erfahrungen mit dem Experten-Workshop .....	338
7.4.3.2 Erfahrungen mit den Interviews .....	339

<b>7.5 Ergebnisse des Experten-Workshops .....</b>	<b>342</b>
<b>7.6 Ergebnisse der Intensivinterviews .....</b>	<b>347</b>
7.6.1 Sichere Informationsverarbeitung als Service für Dritte .....	348
7.6.2 Management von Informationssicherheit in finanzwirtschaftlichen Kooperationen .....	349
7.6.3 Sichere Geschäftsprozesse in der Telekommunikation.....	352
7.6.4 Durchsetzung eines konzernweiten Grundschutzes .....	353
7.6.5 IT-Sicherheit in besonderem Umfeld.....	355
7.6.6 Informationssicherheit aus der Sicht der EDV-Revision.....	358
7.6.7 Gewährleistung der Vertraulichkeit von Gesundheitsdaten.....	361
7.6.8 Kundenorientierte Informationssicherheit eines IT-Dienstleisters .....	364
7.6.9 Gestaltung sicherer Bankanwendungen .....	367
7.6.10 Dezentralisiertes IT-Sicherheitsmanagement in einer Versicherung .....	370
<b>7.7 Gesamtauswertung und Interpretation der Ergebnisse der empirischen Untersuchung.....</b>	<b>374</b>
7.7.1 Geschäftsprozesse und Informationssicherheit .....	376
7.7.2 Methodische Sicherheitsanalysen .....	387
7.7.3 Computerunterstützte Simulationen .....	403
7.7.3.1 Basisfunktionalitäten für Modellierung und Simulation .....	404
7.7.3.2 Querschnittsfunktionalitäten und Benutzeroberfläche.....	405
7.7.3.3 Fragen zu spezifischen Gestaltungsoptionen für den Software-Prototypen.....	406
7.7.4 Vorschläge für Modifikationen und Weiterentwicklungen .....	408
7.7.4.1 Konkrete Vorschläge zum Software-Prototypen.....	409
7.7.4.2 Strukturelle Vorschläge zum geschäftsprozeß-orientierten Simulations-System.....	418
7.7.4.3 Vorschläge zur Integration mit anderen Methoden und Werkzeugen ..	420
7.7.4.4 Vorschläge zur organisatorischen Einbindung .....	421
7.7.5 Multidimensionale Bewertung der Vorschläge für Weiterentwicklungen .....	422
<b>8 SCHLUSSFOLGERUNGEN FÜR WEITERE UNTERSUCHUNGEN.....</b>	<b>429</b>
<b>8.1 Weiterentwicklungspfade .....</b>	<b>430</b>
<b>8.2 Weitergehende Forschungsfragen .....</b>	<b>433</b>

<b>9 LITERATURVERZEICHNIS .....</b>	<b>437</b>
<b>10 ANHANG .....</b>	<b>475</b>
<b>10.1 Ausgangssituation des Anwendungsszenarios.....</b>	<b>475</b>
<b>10.2 Interviewleitfaden .....</b>	<b>478</b>
<b>10.3 Teilnehmer am Experten-Workshop .....</b>	<b>488</b>
<b>10.4 Interviewpartner .....</b>	<b>489</b>