

Inhaltsübersicht

1	Einleitung.....	14
TEIL I GRUNDLAGEN		27
2	Informationssicherheitsmanagement	28
3	Organisationskultur	36
4	Informationssicherheitskultur	43
TEIL II MANAGEMENTMODELL FÜR DIE INFORMATIONSSICHERHEITSKULTUR		61
5	Übersicht.....	62
6	Diagnose	67
7	Planung (Plan).....	85
8	Durchführung (Do)	121
9	Kontrolle (Check).....	122
10	Verbesserung (Act)	126
11	Unterstützung durch das Softwarewerkzeug ISIKTool.....	128
TEIL III ANWENDUNG DES MANAGEMENTMODELLS		141
12	Aktionsforschung in Aktion	142
13	Exkurs: Informationssicherheitskulturen in der Praxis	147
TEIL IV ABSCHLIESSENDE BETRACHTUNG.....		193
14	Schlussfolgerung.....	194
15	Ausblick.....	196
TEIL V ANHÄNGE UND VERZEICHNISSE		199

Inhaltsverzeichnis

Zusammenfassung	1
Inhaltsübersicht	3
Inhaltsverzeichnis	4
Abbildungsverzeichnis	7
Tabellenverzeichnis	10
Abkürzungsverzeichnis	11
Vorwort	12
1 Einleitung	14
1.1 Problemstellung und Zielsetzung	15
1.2 Stand der Forschung	16
1.3 Forschungsmethodik	20
1.3.1 Aktionsforschung	21
1.3.2 Vorgehen bei der Aktionsforschung	23
1.3.3 Vorgehen in dieser Arbeit	24
1.4 Aufbau der Arbeit	24
TEIL I GRUNDLAGEN	27
2 Informationssicherheitsmanagement	28
2.1 Aufgaben des Informationssicherheitsmanagements	28
2.1.1 Strategische Aufgaben	29
2.1.2 Taktische Aufgaben	30
2.1.3 Operative Aufgaben	32
2.2 Im Spannungsfeld von Mensch, Technik und Organisation	33
3 Organisationskultur	36
3.1 Definition	37
3.2 Wirkung der Organisationskultur	40
3.3 Einfluss der Organisationskultur auf die Informationssicherheit	41
4 Informationssicherheitskultur	43
4.1 Definition	43
4.2 Informationssicherheitskultur in Sicherheitsstandards	47
4.3 Studie: Management der Informationssicherheitskultur in Schweizer Organisationen	51
4.3.1 Untersuchungsrahmen	52
4.3.2 Resultate	53
TEIL II MANAGEMENTMODELL FÜR DIE INFORMATIONSSICHERHEITSKULTUR	61
5 Übersicht	62
5.1 Kritische Betrachtung	62
5.2 Anforderungen an ein Managementmodell	63
5.3 Managementzyklus	64
6 Diagnose	67

6.1	Ansatzpunkte und Methoden	67
6.2	Analyse-Framework	73
6.2.1	Dokumentenanalyse	74
6.2.2	Fragebogen	76
6.2.3	Interviews, Workshops und Gruppensitzungen	80
6.2.4	Beobachtungen	81
6.3	Bewertung und Interpretation der Diagnoseresultate	82
6.4	Zusammenfassung	84
7	Planung (Plan).....	85
7.1	Definition der SOLL-Informationssicherheitskultur	85
7.2	Gap-Analyse	88
7.3	Definition der Zielgruppen	89
7.4	Strategien zur Veränderung der Informationssicherheitskultur.....	90
7.4.1	Wege zur Veränderung	91
7.4.2	Phasen einer Informationssicherheitskultur	93
7.4.3	Prozess der Organisationsentwicklung	95
7.4.4	Zusammenfassung der Strategien	96
7.5	Massnahmenkatalog	96
7.5.1	Verantwortung	98
7.5.2	Internes Marketing und Kommunikation.....	101
7.5.3	Berücksichtigung interkultureller Aspekte	104
7.5.4	Dokumentensystem	106
7.5.5	Einbezug des Managements	108
7.5.6	Sensibilisierung aller Mitarbeitenden	110
7.5.7	Ausbildung und Schulung	111
7.5.8	Verpflichtung und Überwachung der Mitarbeitenden	115
7.5.9	Eingesetzte Instrumente in der Praxis.....	116
7.5.10	Zusammenfassung der Massnahmen	118
7.6	Projektplanung	119
7.7	Zusammenfassung	121
8	Durchführung (Do)	121
9	Kontrolle (Check).....	122
9.1	Motivation und Definition	122
9.2	Kontrollprozess.....	124
9.2.1	Überwachung	124
9.2.2	Überprüfung	125
9.3	Gesamtkontrollbild	126
10	Verbesserung (Act)	126
11	Unterstützung durch das Softwarewerkzeug ISIKTool.....	128
11.1	Entscheidungsunterstützende Systeme	128
11.2	Anforderungsdefinition	129
11.3	Architektur.....	130
11.4	Handhabung und Benutzeroberfläche	132
11.4.1	Umfragesubsystem (Diagnose).....	132
11.4.2	Reportingsubsysteme (Diagnose, Planung und Kontrolle).....	134
11.4.3	Administrationssysteme	137

TEIL III ANWENDUNG DES MANAGEMENTMODELLS	141
12 Aktionsforschung in Aktion	142
12.1 Überprüfung des Analyse-Frameworks	142
12.2 Überprüfung des Managementmodells und des ISIKTools	145
13 Exkurs: Informationssicherheitskulturen in der Praxis	147
13.1 Anwendungsfall 1: Telekom	147
13.1.1 Untersuchungsrahmen	147
13.1.2 Diagnose	150
13.1.3 Planung	166
13.2 Anwendungsfall 2: Finanz	169
13.2.1 Untersuchungsrahmen	169
13.2.2 Diagnose	171
13.2.3 Planung	188
TEIL IV ABSCHLIESSENDE BETRACHTUNG.....	193
14 Schlussfolgerung	194
15 Ausblick	196
TEIL V ANHÄNGE UND VERZEICHNISSE	199
Anhang A Arbeitsgruppe Informationssicherheitskultur	200
Anhang B Studie zum Management der Informationssicherheitskultur in Schweizer Organisationen.....	202
Anhang C Design und Implementierung des ISIKTools	209
Anhang D Anwendungsfall Telekom: statistisches Material	216
Anhang E Anwendungsfall Finanz: statistisches Material	218
Literaturverzeichnis.....	220
Stichwortverzeichnis.....	236

Abbildungsverzeichnis

Abbildung 1:	Dimensionen des Informationssicherheitsmanagements (nach Trompeter und Eloff 2001).....	14
Abbildung 2:	Aktionsforschungszyklus (nach Baskerville 1999).....	23
Abbildung 3:	Aufbau der Arbeit.....	26
Abbildung 4:	Überblick über Teil I.....	27
Abbildung 5:	Ziele des Sicherheitsmanagements.....	29
Abbildung 6:	Sicherheitsdispositiv (Schlienger und Teufel 2000).....	30
Abbildung 7:	Kernprozess des ISO GMITS (nach ISO/IEC 2004).....	32
Abbildung 8:	Verhältnis zwischen Mensch, Technik und Organisation.....	35
Abbildung 9:	das 7-S-Modell (nach Pascale und Athos 1981; Peters und Waterman 1982).....	38
Abbildung 10:	Zürcher Ansatz: Trilogie Strategie, Struktur, Kultur (nach Rühli 1996:45).....	39
Abbildung 11:	Die drei Ebenen der Organisationskultur (nach Schein 1985).....	40
Abbildung 12:	Lernen aus Fehlern (Schlienger, Baur et al. 2004:15).....	42
Abbildung 13:	Merkmale einer Sicherheitskultur (nach IAEA 1991).....	45
Abbildung 14:	Hindernisse der Informationssicherheitskultur (1=sehr kleines Hindernis, 5 = sehr grosses Hindernis).....	54
Abbildung 15:	sicherheitskulturfördernde Massnahmen heute und in zwei Jahren ...	56
Abbildung 16:	Lohnen sich Investitionen in eine geeignete Informationssicherheitskultur?.....	56
Abbildung 17:	Investitionen in Informationssicherheitskultur pro Jahr und Kopf.....	57
Abbildung 18:	Interesse an einem anonymen Vergleich der Informationssicherheitskultur (Benchmarking).....	58
Abbildung 19:	Übersicht über Teil II.....	61
Abbildung 20:	PDCA Modell des ISMS (nach Humphreys 2003:2).....	65
Abbildung 21:	das zyklische Modell zum Management der Informationssicherheitskultur.....	66
Abbildung 22:	Aspekte des Fragebogens.....	77
Abbildung 23:	Informationssicherheitskultur-Radar.....	80
Abbildung 24:	Kriterien zur Bewertung der Informationssicherheitskultur (nach Sackmann 2002:145; Sackmann 2004).....	82
Abbildung 25:	Definition der SOLL-Informationssicherheitskultur.....	87
Abbildung 26:	Gap-Analyse der IST- und SOLL-Informationssicherheitskultur.....	89
Abbildung 27:	Wege zur Veränderung der Informationssicherheitskultur.....	92
Abbildung 28:	Modell zur Änderung der Informationssicherheitskultur (nach Bate 1997:261; Sackmann 2002:47).....	94
Abbildung 29:	Prozess der Organisationsentwicklung von Lewin (nach Vecchio 2000:370).....	96

Abbildung 30:	Massnahmenkatalog: das Haus der Informationssicherheitskultur	97
Abbildung 31:	Einbettung der Informationssicherheitsfunktionen in die Organisationsstruktur (nach ISO/IEC 2004)	99
Abbildung 32:	Kommunikationsprozess (nach Burkart 1983:48).....	103
Abbildung 33:	Funktionen der internen Kommunikation.....	104
Abbildung 34:	Dokumentensystem	107
Abbildung 35:	Lernmodell für die Informationssicherheit (nach Wilson, de Zafra et al. 1998:13)	113
Abbildung 36:	in der Praxis eingesetzte Instrumente zur Veränderung der Informationssicherheitskultur.....	117
Abbildung 37:	Kontrollbegriff.....	123
Abbildung 38:	Kontrollschema (nach Rühli 1993:194)	124
Abbildung 39:	Architektur des ISIKTools als kombiniertes Use Case und Komponentendiagramm	131
Abbildung 40:	Ausschnitt aus dem Fragebogen	133
Abbildung 41:	Einstiegsseite des Reportingsubsystems.....	133
Abbildung 42:	Übersichtsergebnis und Navigation.....	135
Abbildung 43:	Gebietsaggregation: der Informationssicherheitskultur-Radar.....	135
Abbildung 44:	Ergebnis einer Einzelfrage mit Problembeschreibung und Massnahmenvorschlägen.....	136
Abbildung 45:	SurveyAdmin: Definition von Untersuchungen	137
Abbildung 46:	SurveyAdmin: Fragen zu einer Untersuchung	138
Abbildung 47:	SurveyAdmin: Definition einer Frage	138
Abbildung 48:	MeasuresAdmin: Verwaltung der Kulturveränderungsmassnahmen	139
Abbildung 49:	Übersicht über Teil III	141
Abbildung 50:	trichotome Fragestellung	152
Abbildung 51:	Übersicht über die Antworten.....	155
Abbildung 52:	Informationssicherheitskultur-Radar	156
Abbildung 53:	Detaillauswertung	157
Abbildung 54:	Clusteranalyse.....	159
Abbildung 55:	Auditzeitreihe des Volumens der privaten Benutzerdaten	164
Abbildung 56:	Auditzeitreihe schwache Passwörter	165
Abbildung 57:	Massnahmenvorschläge.....	167
Abbildung 58:	Übersicht über die Antworten.....	176
Abbildung 59:	Informationssicherheitskultur-Radar	176
Abbildung 60:	Detaillauswertung Ebene Organisation	177
Abbildung 61:	Detaillauswertung Ebene Gruppe	178
Abbildung 62:	Detaillauswertung Ebene Individuum	180
Abbildung 63:	Clusteranalyse.....	183
Abbildung 64:	Massnahmenvorschläge.....	190
Abbildung 65:	Überblick über Teil IV	193
Abbildung 66:	Subsystem Survey.....	210

Abbildung 67:	Subsystem Reports.....	211
Abbildung 68:	Subsysteme SurveyAdmin und MeasuresAdmin	213
Abbildung 69:	Datenbankmodell.....	215

Tabellenverzeichnis

Tabelle 1:	Prinzipien einer Informationssicherheitskultur (nach OECD 2002:10ff)	46
Tabelle 2:	Einordnung der behandelten Informationssicherheits-Dokumente	48
Tabelle 3:	Informationssicherheitskultur in Informationssicherheitsstandards anhand der OECD-Richtlinie.....	49
Tabelle 4:	Informationssicherheitskultur in Informationssicherheitsstandards anhand des INSAG Sicherheitskultur-Konzeptes.....	50
Tabelle 5:	Verantwortung für die Informationssicherheitskultur	55
Tabelle 6:	Häufigkeit der Analyse der Informationssicherheitskultur und dazu eingesetzte Verfahren	58
Tabelle 7:	Datenerhebungsmethoden (nach Sackmann 2002:122, 135).....	72
Tabelle 8:	Methoden und Ansatzpunkte für die Analyse der Informationssicherheitskultur	73
Tabelle 9:	Aspekte der Dokumentenanalyse (adaptiert nach Schein 1999:29) ...	75
Tabelle 10:	Fragebogen zur Erhebung der Informationssicherheitskultur	79
Tabelle 11:	Massnahmen zur Sensibilisierung (Quellen s. Text)	112
Tabelle 12:	Einsatz und Entwicklungstendenz der Instrumente in der Praxis.....	118
Tabelle 13:	Beispiel für ein Gesamtkontrollbild der Massnahmen zur Veränderung der Informationssicherheitskultur	126
Tabelle 14:	eingesetzte Analysemethoden.....	147
Tabelle 15:	Analyse der Informationssicherheitspolitik	151
Tabelle 16:	Fragebogen	153
Tabelle 17:	Auswertung der Zusatzfrage Schwierigkeitsgrad.....	154
Tabelle 18:	Auswertung der Zusatzfragen Abteilung und Position.....	154
Tabelle 19:	Faktoranalyse.....	161
Tabelle 20:	SWOT-Analyse betreffend Informationssicherheitskultur.....	163
Tabelle 21:	SWOT-Analyse betreffend Fragebogen	163
Tabelle 22:	eingesetzte Analysemethoden.....	170
Tabelle 23:	Analyse der Informationssicherheitspolitik.....	172
Tabelle 24:	Fragebogen	174
Tabelle 25:	Auswertung der Zusatzfragen Land, Abteilung und Position	175
Tabelle 26:	Faktoranalyse (in Klammern nicht weiter berücksichtigte Zweitzuweisungen).....	184
Tabelle 27:	SWOT-Analyse betreffend Informationssicherheitskultur.....	186
Tabelle 28:	Massnahmen und deren konkrete Umsetzung beim Partner.....	191