

ANHANG

Erhebung der Fachgruppe Security und der Clusis zur Organisation der Informationssicherheit

Teil 1: Aufgaben, Verantwortung, Kompetenzen und Organisation der Informationssicherheit					
1. Stellen	Sind die folgenden Stellen / Funktionen / Gremien in Ihrer Organisation im Bereich Informationssicherheit vorhanden? Wo sind diese angeordnet?				
		zentral	verteilt	projekt bezogen	externer Partner
a) Informationssicherheitsbeauftragter (ISiBe)	23	6	2	2	18
b) Informationssicherheitsausschuss oder vergleichbares Gremium (ISi-Forum)	17	4	4	1	4
c) Datenschutzbeauftragter (DSB)	15	4	1	1	7
d) Informatik-Revision (Info-Rev)	12	3	1	5	1
e) Zugeteilte Informations- / Datensammlungsverantwortliche, Data Owner, Inhaber von Datensammlungen, Verantwortlicher für Zugriff auf Daten (DVA)	11	17	8	1	3
f) Zugeteilte Verantwortliche für den Betrieb von Systemen, System Owner (SVA)	19	15	1	2	4
g) Verantwortliche für andere Schutzobjekte (DivVA), z.B. für Anwendungen, Systeme, Kommunikation, Infrastruktur	12	14	4	4	2
h) 1st-Level Support (Fachbereichs-Applikationsmanager), Super-User (1LS)	10	15	1	1	1
i) 2nd-Level Support (Hotline) (2LS)	20	4	2	2	2

j) 3rd-Level Support (Zentraler Benutzer- und Applikationssupport) (3LS)	16	6	4	7	1		
k) Root-Manager, System-Administratoren (SAdm)			23	7	2	2	5
l) Andere Verantwortliche (AndVA). Bezeichnung:			3	2	1	0	1

2. Verantwortlichkeiten	Wer ist in Ihrem Haus verantwortlich für... (Abkürzungen vgl. Frage 1)	ISiBe	ISi-Forum	DSB	Info-Rev	DVA	SVA	DivVA	1LS	2LS	3LS	SAdm	AndVA
	a) Formulierung Strategie der Informationssicherheit	15	15	2	0	2	2	0	0	0	0	1	1
	b) Sensibilisierung und Schulung im Bereich Informationssicherheit	19	6	2	1	1	3	0	0	1	0	1	1
	c) Durchführung Risikomanagement der Informationssicherheit	12	6	1	3	1	5	2	0	1	0	1	3
	d) Erstellung Konzepte, Richtlinien, Weisungen zur Informationssicherheit	19	9	1	0	5	7	3	0	1	0	2	1
	e) Beschaffung, Evaluation und Betrieb informationssicherheitsrelevanter Systeme	15	4	0	0	6	12	3	0	0	0	4	1
	f) Messung der Wirtschaftlichkeit der Informationssicherheit	9	7	0	2	1	3	0	0	0	0	0	1
	g) Prüfung der Einhaltung der geltenden Regelungen und Massnahmen	14	4	4	9	1	3	1	0	0	1	2	3
	h) Prüfung der Angemessenheit / Aktualität / Eignung der geltenden Regelungen und Massnahmen	10	7	3	6	2	4	0	0	0	0	2	3

3. ISi-Dokumente: Vorhandensein	Sind folgende Dokumente vorhanden und vom management verabschiedet?	besteht nicht	besteht, aber nicht verabschiedet	besteht und wurde verabschiedet
--	--	----------------------	--	--

a) Informatik-Strategie	7	2	20
b) Informationssicherheitsstrategie	5	12	13
c) Allgemeiner ISi-Massnahmenkatalog	10	4	15
d) Informationssicherheitskonzept und konkretisierter Umsetzungsplan (gesamt und/oder einzeln)	8	11	10
e) Weisung, Richtlinie zur Informationssicherheit	7	5	18

4. ISi-Dokumente: Abdeckung	Wie umfassend decken die Dokumente die Bedürfnisse der Informationssicherheit ab?	mehrheitlich bis vollständig	ansatzweise bis teilweise
a) Informatik-Strategie		12	12
b) Informationssicherheitsstrategie		15	10
c) Allgemeiner ISi-Massnahmenkatalog		10	13
d) Informationssicherheitskonzept und konkretisierter Umsetzungsplan (gesamt und/oder einzeln)		10	13
e) Weisung, Richtlinie zur Informationssicherheit		14	13

5. ISi-Dokumente: Einhaltung	In welchem Masse werden die Weisungen und Richtlinien in den Dokumenten eingehalten?	vollständig	mehrheitlich	teileise
a) Informatik-Strategie		5	16	3
b) Informationssicherheitsstrategie		3	16	7
c) Allgemeiner ISi-Massnahmenkatalog		1	13	10
d) Informationssicherheitskonzept und konkretisierter Umsetzungsplan (gesamt und/oder einzeln)		2	14	8
e) Weisung, Richtlinie zur Informationssicherheit		5	12	11

ISi-Massnahmen	6. Verwenden Sie folgende Vorgehensweisen, Massnahmen, Standards und Hilfsmittel?	systematisch	auf Anfrage	
			auf Anfrage	mit externer Beteiligung
	a) Inventarisierung	20	4	1
	b) Übergeordnete Risikoanalyse	8	9	7
	c) Detaillierte Risikoanalyse	4	14	7
	d) Schwachstellenanalyse	8	9	6
	e) Netzwerk- und Systemkonfigurationstests (ohne Penetration Tests)	13	10	6
	f) Penetration Tests	9	6	9
	g) Software-Qualitätstests und -prüfungen (ohne Zertifizierung)	9	11	2
	h) Software-Zertifizierungen	4	6	2
	i) Simulationen	5	9	2
	j) Übungen	5	12	1
	k) Sensibilisierung bzgl. Social Engineering	8	10	3
	l) Passwort-Checks	15	10	2
	m) Hilfsmittel zur Verwaltung der sicherheitsrelevanten Objekte	10	12	1
	n) Andere. Welche?	1	0	0

7. ISi-Standards	Verwenden Sie folgende Verfahren und Standards?	systematisch	auf Anfrage	
			auf Anfrage	mit externer Beteiligung
	a) BSI IT-Sicherheitshandbuch	6	6	3
	b) BSI IT-Grundschutzhandbuch	7	8	5
	c) Code of Practice (BS 7799)	5	9	6
	d) ISO General Management of IT Security	0	6	4
	e) COBIT	3	9	5
	f) Andere. welche?	4	0	0

8. Outsourcing	Betreiben Sie Outsourcing folgender Funktionen?	vollständig	mehrheitlich	teilweise	ansatzweise	keine
	a) Informatik-Planung, Entwurf, Konzeption allgemein	0	0	0	7	23
	b) Informationssicherheitsplanung, -entwurf, -konzeption	0	1	2	4	25
	c) Informatik-System-Entwicklung und -Erstellung	1	0	1	4	24
	d) Informatik-Betrieb Applikationen, Rechenzentrum (RZ), Information Center (IC) allgemein	1	0	2	1	30
	e) Betrieb informationssicherheitsrelevanter Applikationen und Systeme	0	0	1	1	32
	f) Informatik-Betrieb LAN	1	0	0	2	28
	g) Informatik-Betrieb WAN	1	0	1	1	27
	h) Informatik-Betrieb Client-Support und -Management	0	0	1	1	28
	i) Archivierung	0	0	1	0	29
	j) WWW-Server-Betrieb	4	1	1	0	24
	k) WWW-Server Design + Programmierung	1	0	1	1	25

9. Outsourcing	Kontrollieren Sie Ihren Outsourcer hinsichtlich	systematisch	auf Anfrage	mit externer Beteiligung	keine Kontrolle
	a) Vorhandensein von Regelungen zur Informationssicherheit	10	8	5	5
	b) Einhaltung von Regelungen zur Informationssicherheit	7	9	4	6
	c) Durchführung von Tätigkeiten zum Management der Informationssicherheit	5	6	4	8
	d) Qualifikation und Interessenkonflikte des eingesetzten Personals	7	4	4	10

10. Stellenwert der Informationssicherheit	Welchen Stellenwert hat Ihrer Meinung nach die Informationssicherheit...	sehr hoch	hoch	gering	kein

a) ... für Ihr Top-Management?	11	13	7	0
b) ... in Ihrer Branche?	16	10	5	0
Welchen Stellenwert hat Ihrer Meinung nach folgende Themen für Ihre Unternehmung?	sehr hoch	hoch	gering	kein
c) Hacking, Intrusion, Intrusion Detection	12	14	5	0
d) Unterwanderung, trojanische Pferde, Backdoors in Ihren Systemen	12	14	5	0
e) Information Warfare, Spionage	7	9	12	3
Wie entwickelt sich Ihrer Meinung nach die Informationssicherheit ...	wird viel wichtiger	wird wichtiger	bleibt gleich	wird weniger oder viel weniger wichtig
f) ... gesamthaft weltweit	19	11	1	0
g) ... für Ihr Top-Management	12	12	6	1
h) ... für Ihre Unternehmung	14	14	3	0
i) ... für Ihre Branche	9	17	6	0
Wie entwickelt sich Ihrer Meinung nach die Übertragung von Aufgaben der Informationssicherheit an Externe ...	wird viel wichtiger	wird wichtiger	bleibt gleich	wird weniger oder viel weniger wichtig
j) ... gesamthaft	8	16	9	2
k) ... für Ihre Unternehmung	3	3	22	3
l) ... für Ihre Branche	6	11	14	3

11. Budget für Informationssicherheit	Wieviel Prozent Ihres Informatik-Budgets verwendet Ihre Unternehmung für ...	weiss nicht	mehr als 20%	10-20%	5-10%	2-5%	weniger als 2%
		a) ... Informatik-Sicherheit	6	0	0	8	9
b) ... Informationssicherheit	6	0	0	4	9	6	

Teil 2: Information zur Unternehmung		
Branche	Ihre Unternehmung gehört zu folgender Branche:	3 - Beratung / professional Services 1 - Gesundheitswesen inkl. Krankenkassen 6 - Industrie 7 - Banking 3 - andere Finanz inkl. Versicherungen 6 - Energie, Verkehr 1 - Ausbildung, Forschung 5 - Informatik, Informationstechnik, Hardware+Software, Telekom 3 - öffentliche Verwaltung 0 - Media 1 - Handel
	Ihre Unternehmung hat Betriebe	15 - nur in der Schweiz 18 - in der Schweiz und im Ausland
Land des Hauptsitzes	Der Hauptsitz Ihrer Unternehmung befindet sich	24 - in der Schweiz 8 - im Ausland
Personal	Wieviele Mitarbeiter beschäftigt Ihre Unternehmung in der Schweiz?	13- unter 200 8- zwischen 200 und 2000 8 - über 2000