

KES/KPMG-Sicherheitsstudie 2002

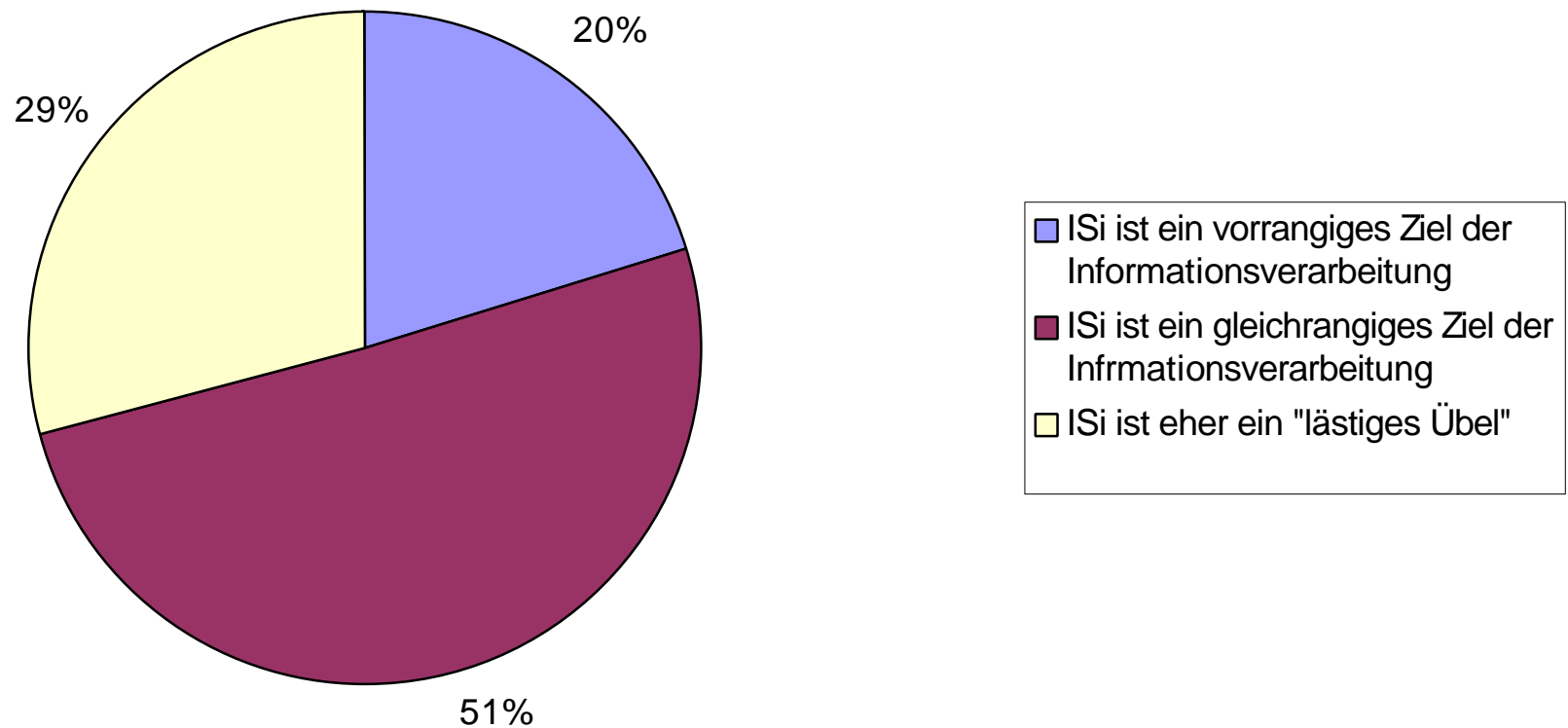
Kapitel 2: Management und Organisation der ISi

UIMC Dr. Vossbein GmbH & Co KG, Wuppertal

2.01

Welchen Stellenwert hat die ISi für Ihr Top-Management?		
	Nennungen	Prozent
ISi ist ein vorrangiges Ziel der Informationsverarbeitung	53	20%
ISi ist ein gleichrangiges Ziel der Infrmationsverarbeitung	131	50%
ISi ist eher ein "lästiges Übel"	76	29%
Summe	260	

Stellenwert ISi im Top-Management



2.02

Aufgabenverteilung/Verantwortlichkeit

Gibt es in Ihrem Unternehmen	Nennungen	%
zentraler Isi-Beauftragter	141	55%
dezentraler Isi-Beauftragter	37	14%
zentraler Datenschutzbeauftragter	171	67%
dezentraler Datenschutzbeauftragter	52	20%
Isi-Ausschuss (o.ä.)	57	22%
Leiter IV/DV/RZ	209	81%
IV/DV-Revision	96	37%
Leiter Organisation	127	49%
Leiter Sicherheit/Werkschutz	91	35%
Administratoren	212	82%
Benutzerservice	183	71%
DV-orientierter Jurist	40	16%

Wer ist verantwortlich für: (Mehrfachnennungen möglich)								
	zentraler Isi-Beauftragter	dezentraler Isi-Beauftragter	zentraler Datenschutzbeauftragter	dezentraler Datenschutzbeauftragter	Isi-Ausschuss (o.ä.)	Leiter IV/DV/RZ	IV/DV-Revision	Leiter Organisation
Formulierung der ISI-Strategie (Ziele, Rahmenbed., Ressourcen)	109	12	25	4	36	93	18	23
Sensibilisierung / Schulung der Nutzer	78	19	34	16	15	67	7	15
Durchführung von Risikoanalysen/Sicherheitsanalysen	93	17	23	7	13	68	33	14
Erstellung von Konzepten, Richtlinien	98	18	35	4	31	111	21	40
Beschaffung und Betrieb von								
- Servern	7	0	5	0	3	142	3	18
- Clients/PCs	5	0	3	0	3	135	7	16
- mobilen Endgeräten	5	0	2	0	3	125	3	16
- technischer Infrastruktur (z. B. Klimaanlage, Gefahrenmeldeanl.)	12	5	3	0	6	108	0	37
Wirtschaftlichkeit der IT-Sicherheit	55	2	12	4	8	96	17	28
Notfall- und Eskalationsmaßnahmen	91	12	20	2	14	143	13	41

	Leiter Sicherheit/ Werkschutz	Administrator en	Benutzer- service	DV- orientierter Jurist	Top- Management	Einkauf/ Beschaffung	jeweilige Fachabteilung	andere
Formulierung der ISi-Strategie (Ziele, Rahmenbed., Ressourcen)	4	27	5	0	59	5	4	7
Sensibilisierung / Schulung der Nutzer	5	52	58	0	17	0	30	13
Durchführung von Risikoanalysen/Sicherheitsanalysen	9	43	3	0	11	2	17	8
Erstellung von Konzepten, Richtlinien	10	43	3	4	14	2	19	9
Beschaffung und Betrieb von								
- Servern	2	92	19	0	5	68	20	3
- Clients/PCs	2	81	27	0	5	72	25	3
- mobilen Endgeräten	2	75	27	0	5	67	35	1
- technischer Infrastruktur (z. B. Klimaanlage, Gefahrenmeldeanl.)	32	39	4	0	9	55	24	21
Wirtschaftlichkeit der IT-Sicherheit	2							
Notfall- und Eskalationsmaßnahmen	16	46	4	2	58	7	14	8

	zentraler Isi-Beauftragter	dezentraler Isi-Beauftragter	zentraler Datenschutz-beauftragter	dezentraler Datenschutz-beauftrater	Isi-Ausschuss (o.ä.)	Leiter IV/DV/RZ	IV/DV-Revision	Leiter Organisation
Formulierung der ISI-Strategie (Ziele, Rahmenbed., Ressourcen)	42%	5%	10%	2%	14%	36%	7%	9%
Sensibilisierung / Schulung der Nutzer	30%	7%	13%	6%	6%	26%	3%	6%
Durchführung von Risikoanalysen/Sicherheitsanalysen	36%	7%	9%	3%	5%	26%	13%	5%
Erstellung von Konzepten, Richtlinien	38%	7%	14%	2%	12%	43%	8%	16%
Beschaffung und Betrieb von								
- Servern	3%	0%	2%	0%	1%	55%	1%	7%
- Clients/PCs	2%	0%	1%	0%	1%	53%	3%	6%
- mobilen Endgeräten	2%	0%	1%	0%	1%	49%	1%	6%
- technischer Infrastruktur (z. B. Klimaanlage, Gefahrenmeldeanl.)	5%	2%	1%	0%	2%	42%	0%	14%
Wirtschaftlichkeit der IT-Sicherheit	21%	1%	5%	2%	3%	37%	7%	11%
Notfall- und Eskalationsmaßnahmen	35%	5%	8%	1%	5%	56%	5%	16%

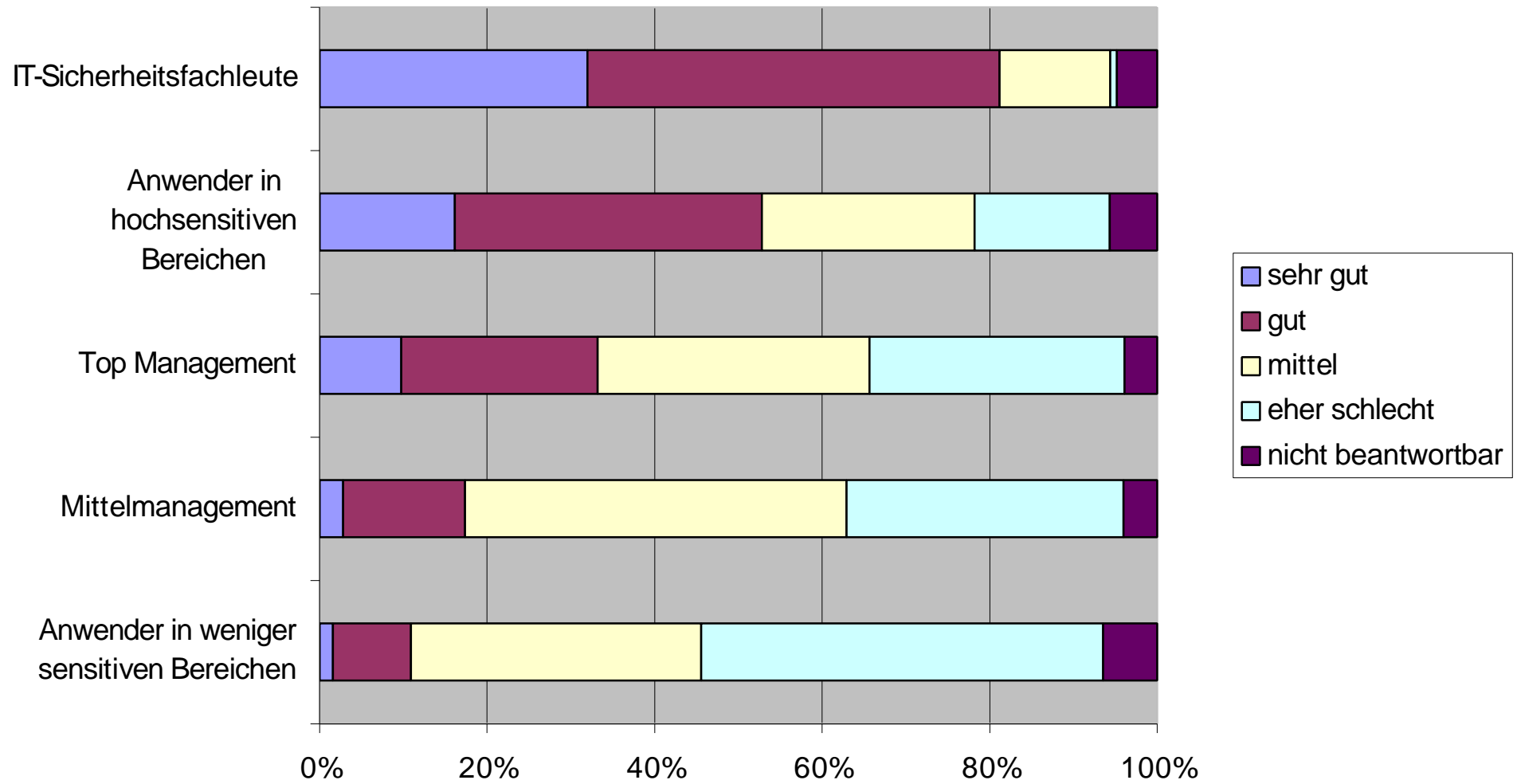
	Leiter Sicherheit/ Werkschutz	Administrator en	Benutzer- service	DV- orientierter Jurist	Top- Management	Einkauf/ Beschaffung	jeweilige Fachabteilung	andere
Formulierung der ISI- Strategie (Ziele, Rahmenbed., Ressourcen)	2%	11%	2%	0%	23%	2%	2%	3%
Sensibilisierung / Schulung der Nutzer	2%	20%	23%	0%	7%	0%	12%	5%
Durchführung von Risikoanalysen/Sicherh eitsanalysen	4%	17%	1%	0%	4%	1%	7%	3%
Erstellung von Konzepten, Richtlinien	4%	17%	1%	2%	5%	1%	7%	4%
Beschaffung und Betrieb von	0	0	0	0	0	0	0	0
- Servern	1%	36%	7%	0%	2%	26%	8%	1%
- Clients/PCs	1%	32%	11%	0%	2%	28%	10%	1%
- mobilen Endgeräten	1%	29%	11%	0%	2%	26%	14%	0%
- technischer Infrastruktur (z. B. Klimaanlage, Gefahrenmeldeanl.)	12%	15%	2%	0%	4%	21%	9%	8%
Wirtschaftlichkeit der IT-Sicherheit	1%	0%	0%	0%	0%	0%	0%	0%
Notfall- und Eskalationsmaßnahme n	6%	18%	2%	1%	23%	3%	5%	3%

2.03

Wie beurteilen Sie den Kenntnisstand zur ISi in Ihrem Unternehmen?							
	sehr gut (1)	gut (2)	mittel (3)	eher schlecht (4)	nicht beantwo rtbar	Summe	Kennzah l
IT-Sicherheitsfachleute	80	123	33	2	12	250	1,82
Anwender in hochsensitiven Bereichen	40	91	63	40	14	248	2,44
Top Management	25	60	83	78	10	256	2,87
Mittelmanagement	7	36	113	82	10	248	3,13
Anwender in weniger sensitiven Bereichen	4	23	86	119	16	248	3,38

Prozent	sehr gut	gut	mittel	eher schlecht	nicht beantwo rtbar
IT-Sicherheitsfachleute	32%	49%	13%	1%	5%
Anwender in hochsensitiven Bereichen	16%	36%	25%	16%	6%
Top Management	10%	24%	33%	31%	4%
Mittelmanagement	3%	14%	45%	33%	4%
Anwender in weniger sensitiven Bereichen	2%	9%	34%	48%	6%

Kenntnisstand zur ISi



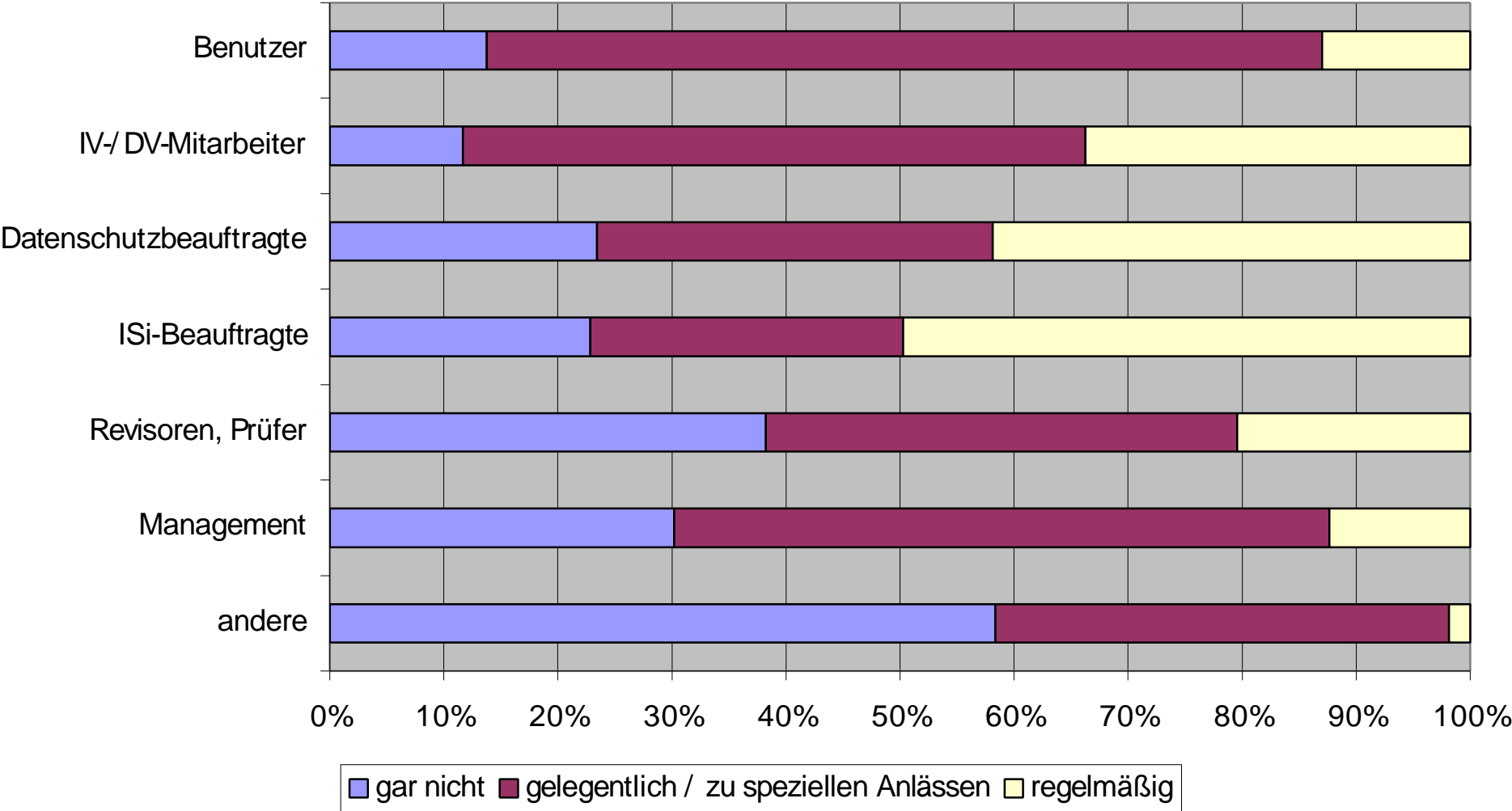
2.04

Wen informieren/schulen Sie über Fragen der ISi? (Mehrfachnennungen möglich)				
	gar nicht	gelegentlich / zu speziellen Anlässen	regelmäßig	Summe
Benutzer	35	186	33	254
IV-/DV-Mitarbeiter	28	131	81	240
Datenschutzbeauftragte	52	77	93	222
ISi-Beauftragte	45	54	98	197
Revisoren, Prüfer	73	79	39	191
Management	71	135	29	235
andere	63	43	2	108

Keine Angaben: 2

	gar nicht	gelegentlich / zu speziellen Anlässen	regelmäßig
Benutzer	14%	73%	13%
IV-/DV-Mitarbeiter	12%	55%	34%
Datenschutzbeauftragte	23%	35%	42%
ISi-Beauftragte	23%	27%	50%
Revisoren, Prüfer	38%	41%	20%
Management	30%	57%	12%
andere	58%	40%	2%

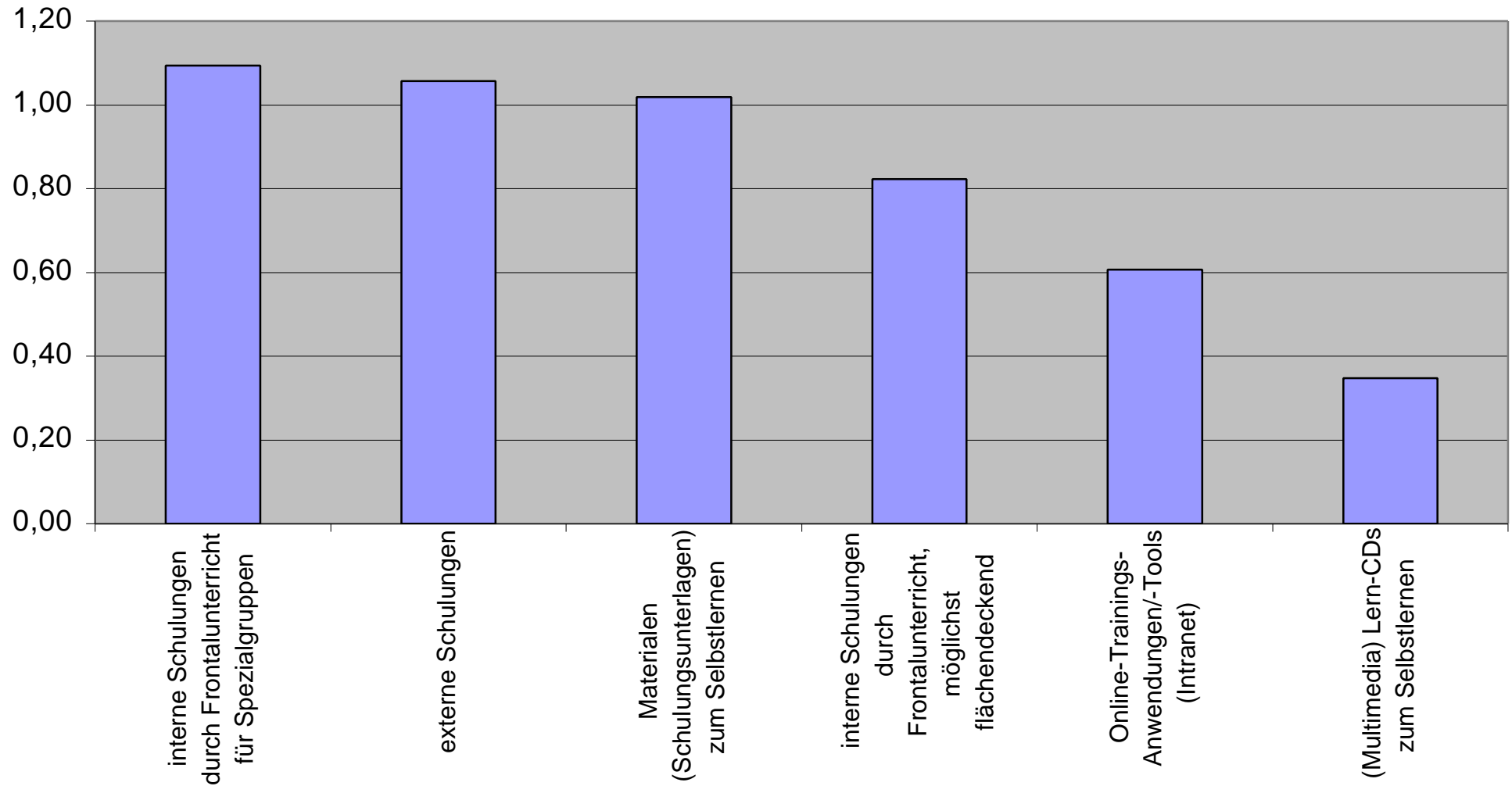
Schulungsaktivitäten



2.05

Welche Ausbildungsmethoden setzt Ihr Unternehmen auf dem Gebiet der ISi bevorzugt ein?							
	stark (3)	generell (2)	gelegentlich (1)	nicht (0)	nicht beantwortbar	Summe	Nutzungsgrad
interne Schulungen durch Frontalunterricht für Spezialgruppen	7	50	102	45	33	237	1,09
externe Schulungen	19	23	137	48	20	247	1,06
Materialien (Schulungsunterlagen) zum Selbstlernen	12	42	96	62	27	239	1,02
interne Schulungen durch Frontalunterricht, möglichst flächendeckend	15	23	81	90	29	238	0,82
Online-Trainings-Anwendungen/-Tools (Intranet)	6	24	56	115	39	240	0,61
(Multimedia) Lern-CDs zum Selbstlernen	4	4	51	145	34	238	0,35
	stark (3)	generell (2)	gelegentlich (1)	nicht (0)	nicht beantwortbar		
interne Schulungen durch Frontalunterricht für Spezialgruppen	3%	21%	43%	19%	14%		
externe Schulungen	8%	9%	55%	19%	8%		
Materialien (Schulungsunterlagen) zum Selbstlernen	5%	18%	40%	26%	11%		
interne Schulungen durch Frontalunterricht, möglichst flächendeckend	6%	10%	34%	38%	12%		
Online-Trainings-Anwendungen/-Tools (Intranet)	3%	10%	23%	48%	16%		
(Multimedia) Lern-CDs zum Selbstlernen	2%	2%	21%	61%	14%		

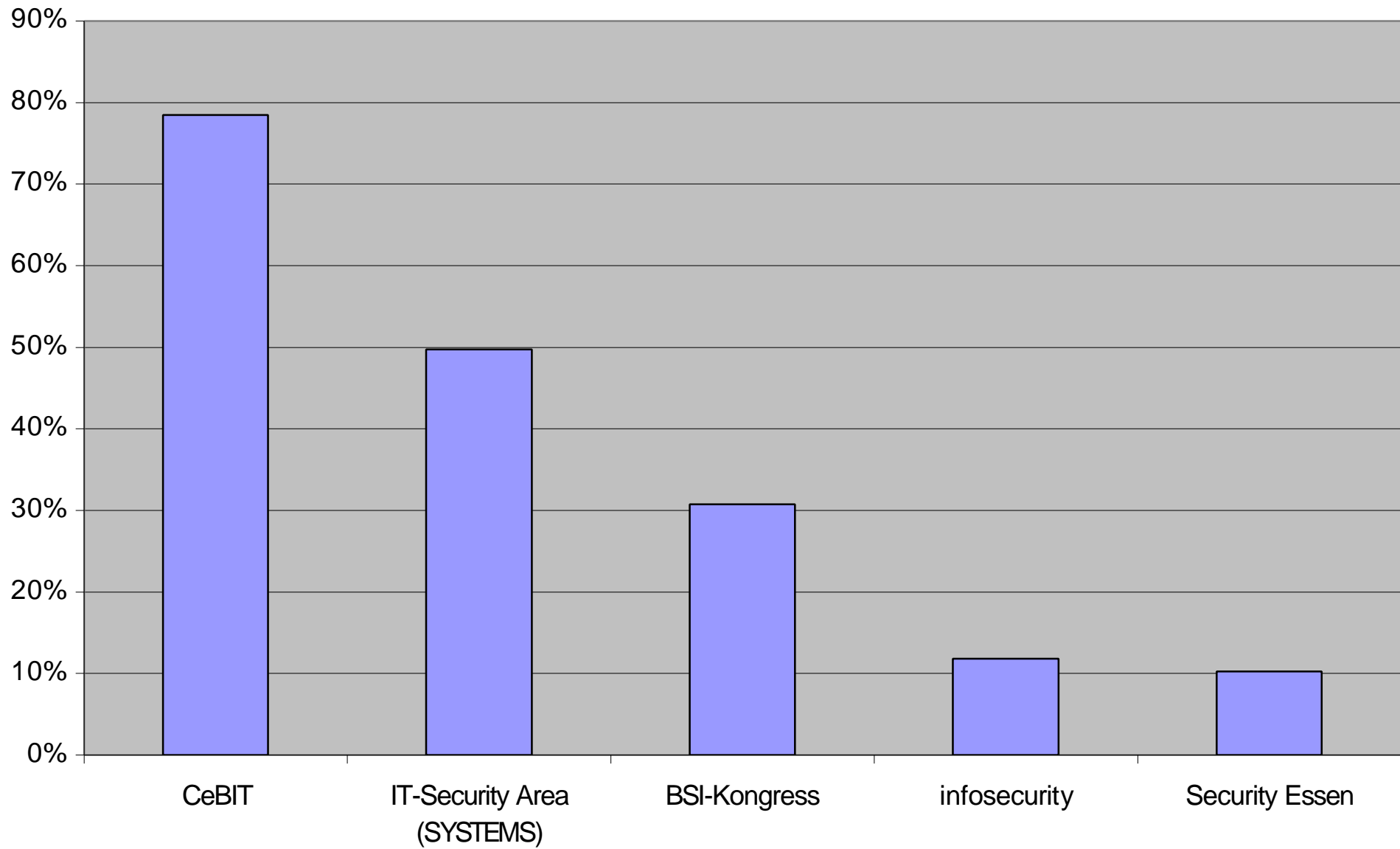
Nutzungsgrad Ausbildungsmethoden - ISi



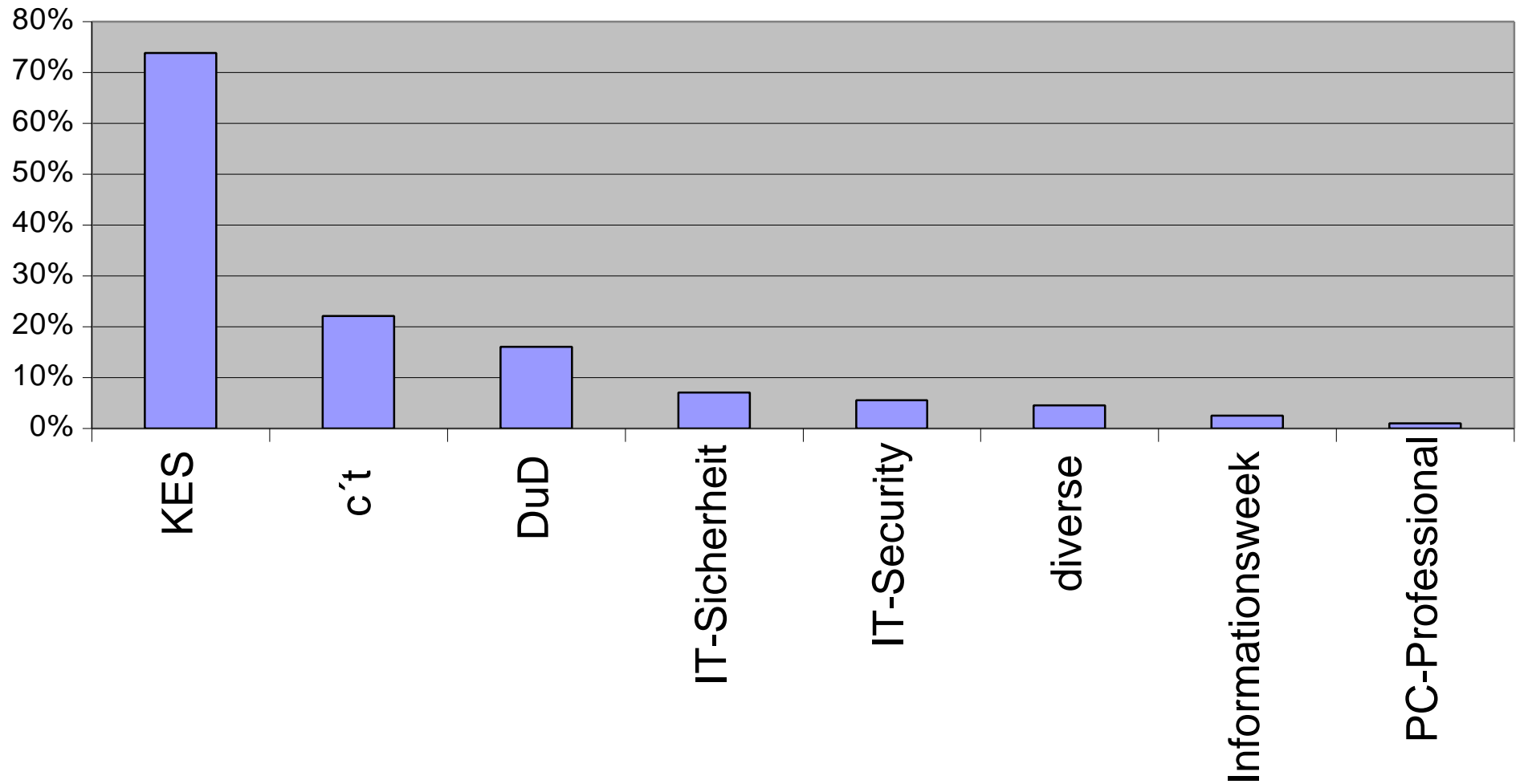
2.06

Wo informieren Sie sich über ISi? (Mehrfachnennungen möglich)		
Basis der Prozentuierung:		195
	Nennungen	Prozentua l
CeBIT	153	78%
IT-Security Area (SYSTEMS)	97	50%
BSI-Kongress	60	31%
infosecurity	23	12%
Security Essen	20	10%
Basis der Prozentuierung:		199
	Zeitungen / Magazine	
	Nennungen	Prozentua l
KES	147	74%
c´t	44	22%
DuD	32	16%
IT-Sicherheit	14	7%
IT-Security	11	6%
diverse	9	5%
Informationsweek	5	3%
PC-Professional	2	1%

Informationen über ISi bei Veranstaltungen



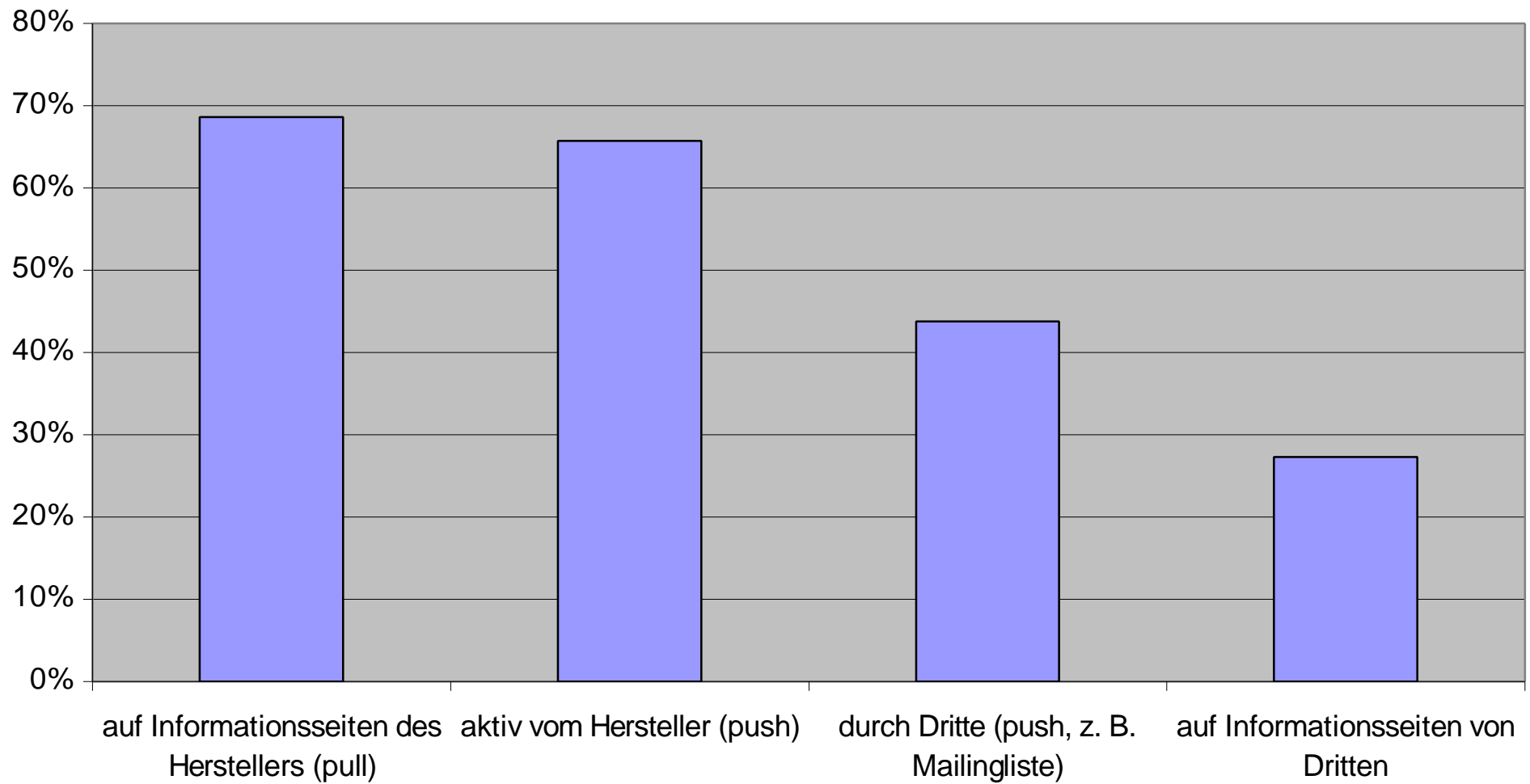
Informationen über ISi durch Zeitungen / Magazine



2.07

Wo erhalten Sie Informationen über aktuelle Patches gegen Sicherheitslücken? (Mehrfachnennungen möglich)		
Basis der Prozentuierung:	242	
	Nennungen	Prozentanteil
auf Informationsseiten des Herstellers (pull)	166	69%
aktiv vom Hersteller (push)	159	66%
durch Dritte (push, z. B. Mailingliste)	106	44%
auf Informationsseiten von Dritten	66	27%

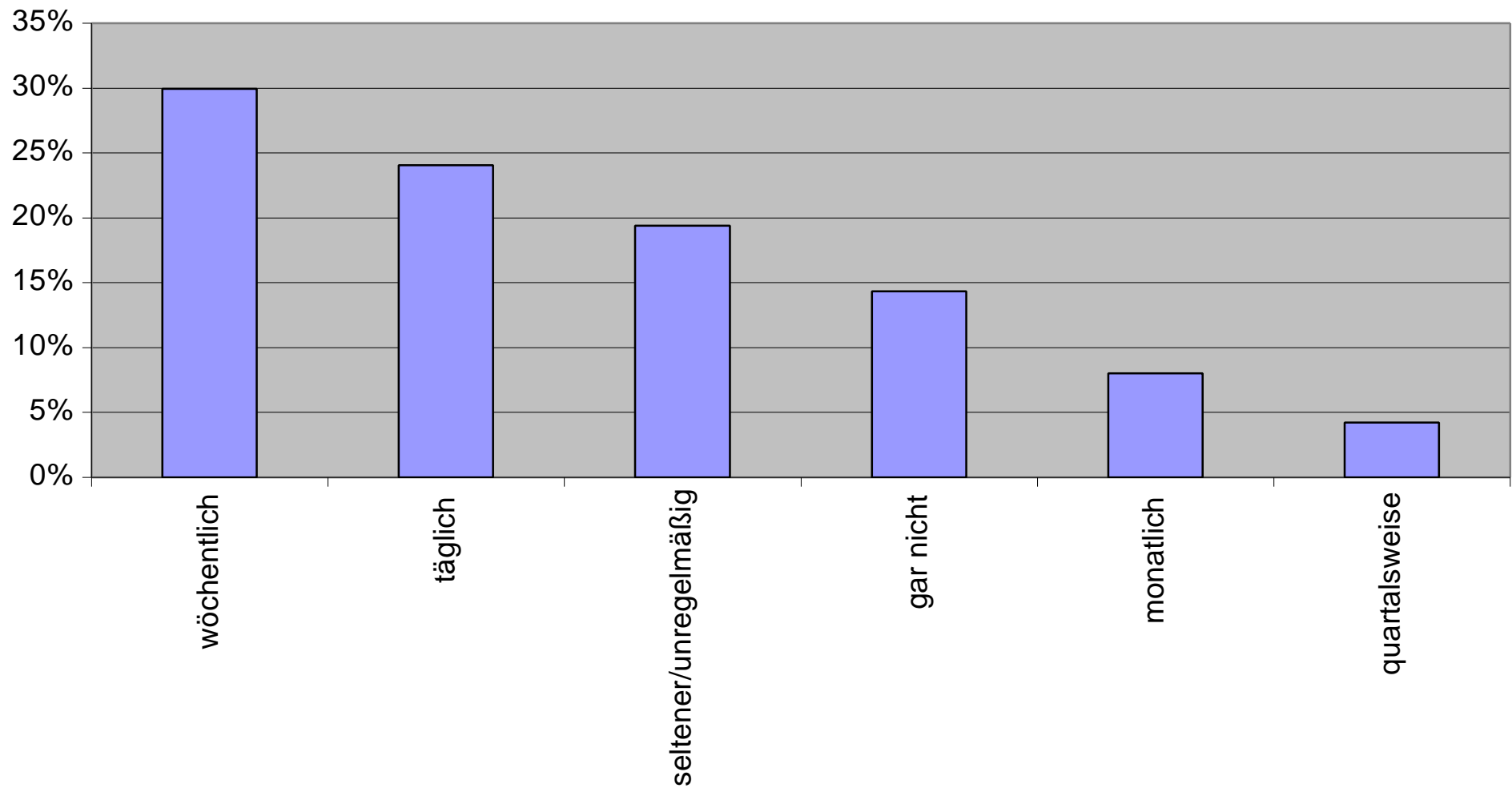
Informationen über aktuelle Patches bei Sicherheitslücken



2.07a

In welcher Frequenz prüfen Sie passive Kanäle?		
Basis der Prozentuierung: 237		
	Nennunge n	Prozentua l
wöchentlich	71	30%
täglich	57	24%
seltener/unregelmäßig	46	19%
gar nicht	34	14%
monatlich	19	8%
quartalsweise	10	4%

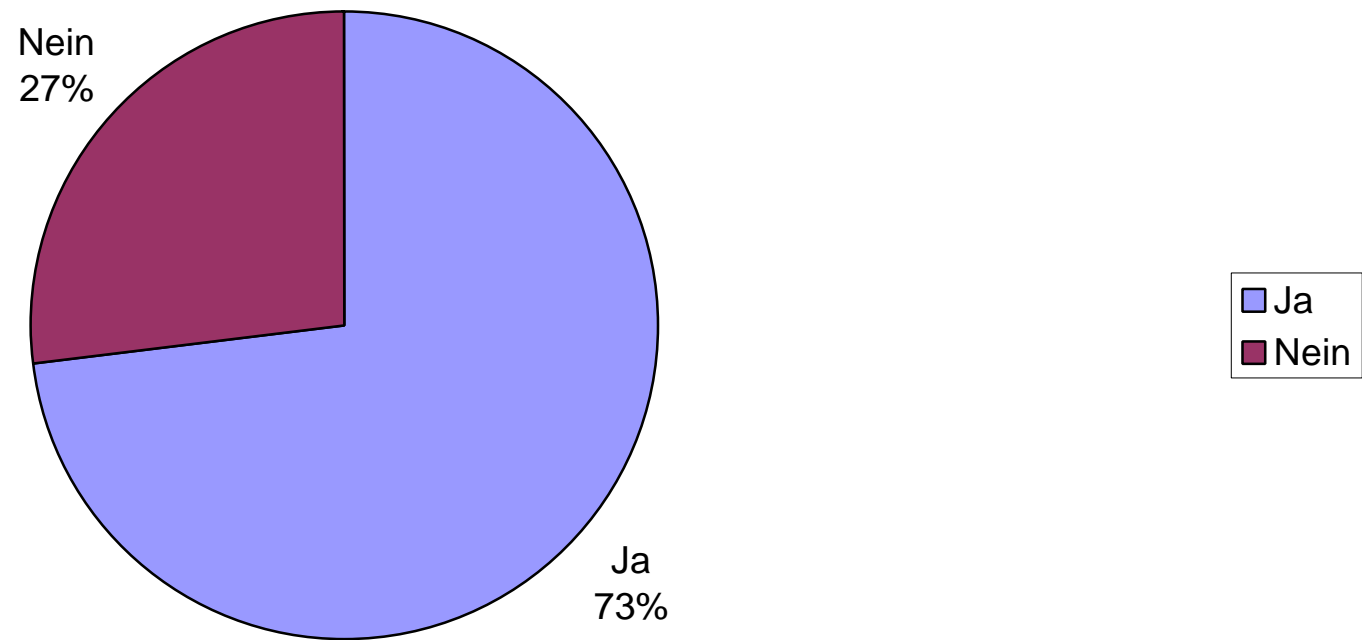
Prüfungsrhythmus bei passiven Kanälen



2.08

Betreiben Sie Outsourcing?		
Ja	Nein	Summe
144	53	197
73%	27%	

Outsourcing



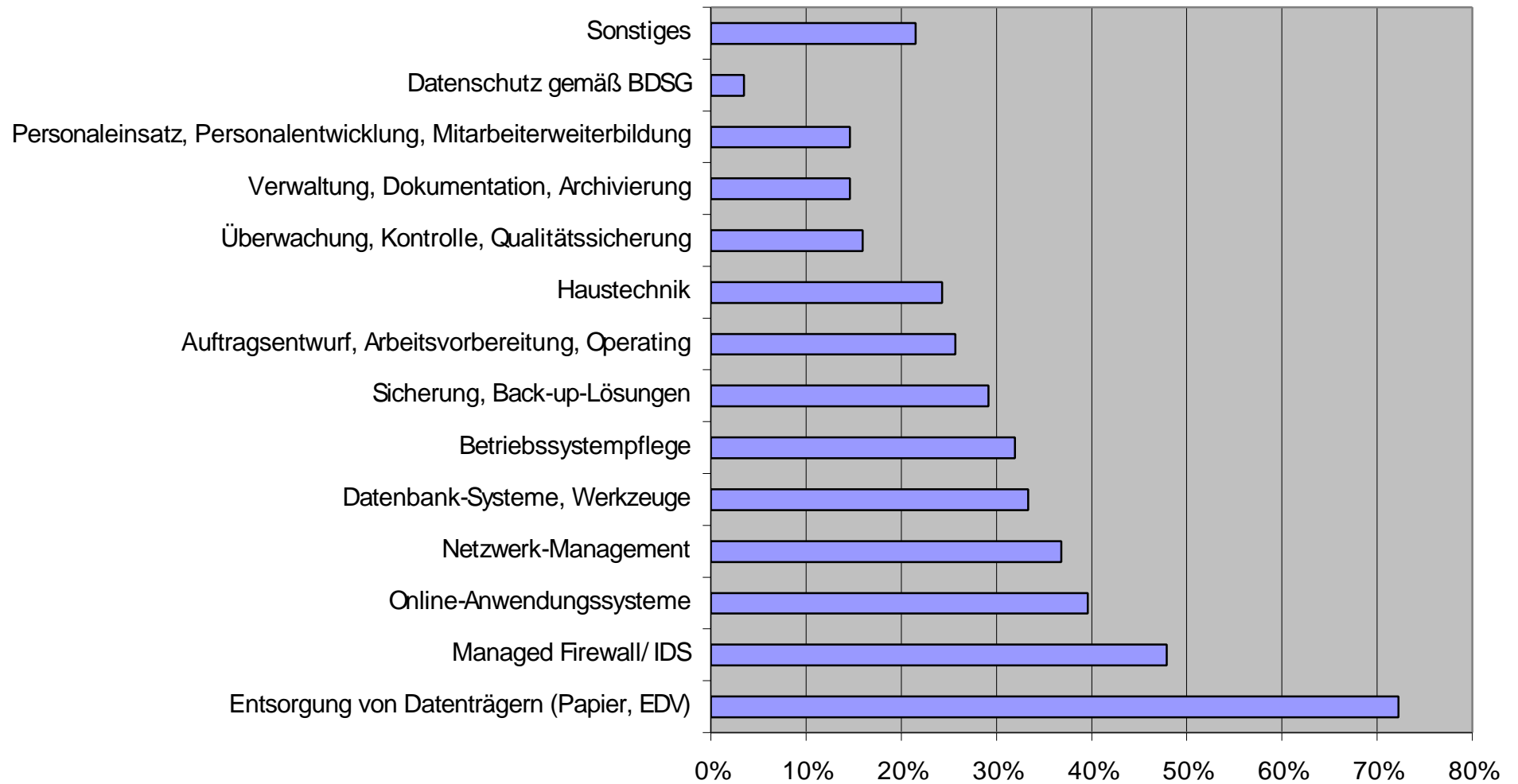
2.08a

Wenn Ja: Welche Funktionen haben Sie ausgelagert?		
Basis der Prozentuierung:	144 Ja-Antworten	
	Nennungen	Prozentual
Entsorgung von Datenträgern (Papier, EDV)	104	72%
Managed Firewall/IDS	69	48%
Online-Anwendungssysteme	57	40%
Netzwerk-Management	53	37%
Datenbank-Systeme, Werkzeuge	48	33%
Betriebssystempflege	46	32%
Sicherung, Back-up-Lösungen	42	29%
Auftragsentwurf, Arbeitsvorbereitung, Operating	37	26%
Haustechnik	35	24%
Überwachung, Kontrolle, Qualitätssicherung	23	16%
Verwaltung, Dokumentation, Archivierung	21	15%
Personaleinsatz, Personalentwicklung, Mitarbeiterweiterbildung	21	15%
Datenschutz gemäß BDSG	5	3%
Sonstiges	31	22%

Liste der Sonstigen:

Entsorgung Datenträgern, nein, Client Installation, Wartung von Firewall, DB-System, Desktopwertung, Produktion, Firewall, CRM, ehemalg Abteilungen werden zu div. GmbH's outgesouret, Beratung allgm., Systemwartung, Internet-Anbindung (plain), IT-Revision, HW, Fibu, Nicht-IT-Angelegenheiten, Desktopwertung

Auslagerung von Funktionen

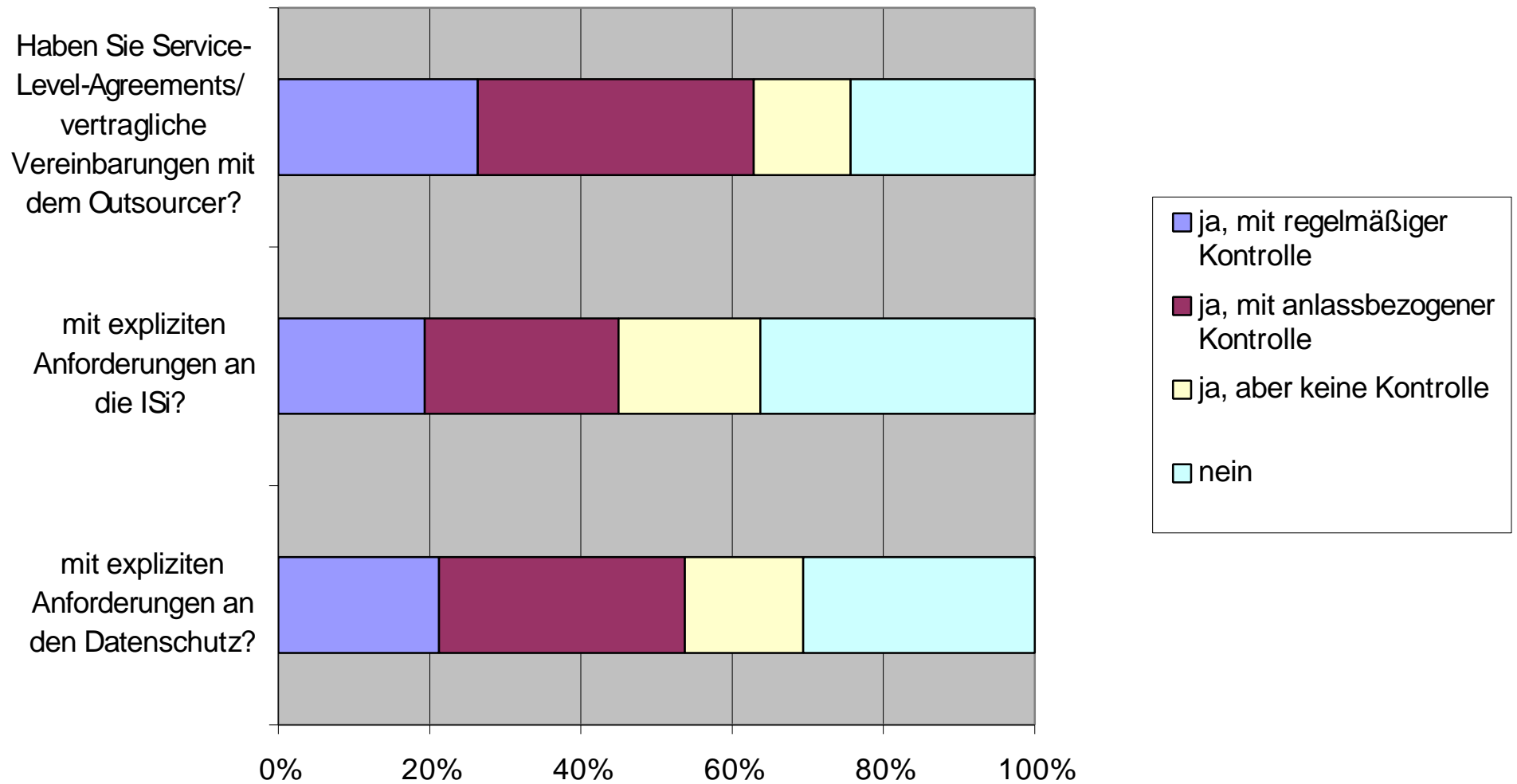


2.08b

Haben Sie Service-Level-Agreements/ vertragliche Vereinbarungen mit dem Outsourcer?					
	ja, mit regelmäßiger Kontrollen	ja, mit anlassbezogener Kontrollen	ja, aber keine Kontrollen	nein	Nennungen
Haben Sie Service-Level-Agreements/ vertragliche Vereinbarungen mit dem Outsourcer?	39	54	19	36	148
mit expliziten Anforderungen an die ISi?	31	41	30	58	160
mit expliziten Anforderungen an den Datenschutz?	34	52	25	49	160

	ja, mit regelmäßiger Kontrollen	ja, mit anlassbezogener Kontrollen	ja, aber keine Kontrollen	nein
Haben Sie Service-Level-Agreements/ vertragliche Vereinbarungen mit dem Outsourcer?	26%	36%	13%	24%
mit expliziten Anforderungen an die ISi?	19%	26%	19%	36%
mit expliziten Anforderungen an den Datenschutz?	21%	33%	16%	31%

SLA's / vertragliche Vereinbarungen

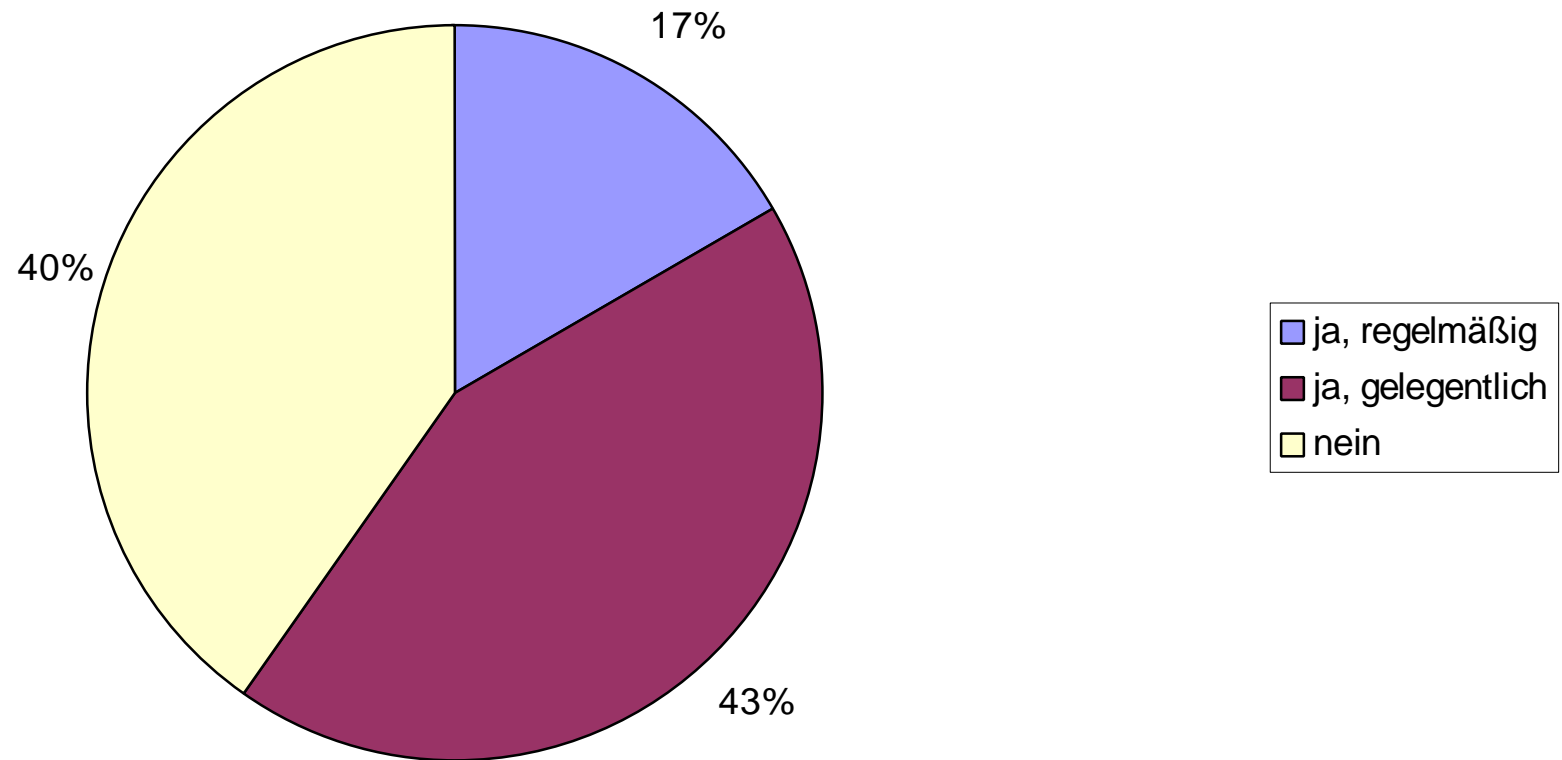


2.09

Nutzt Ihr Haus externe ISi-Beratung ...?			
	Nennungen	Prozent	Ja-Gesamt
ja, regelmäßig	43	17%	154
ja, gelegentlich	111	43%	
nein	104	40%	
Summe	258		

Keine
Angaben: 2

Externe ISI-Beratung



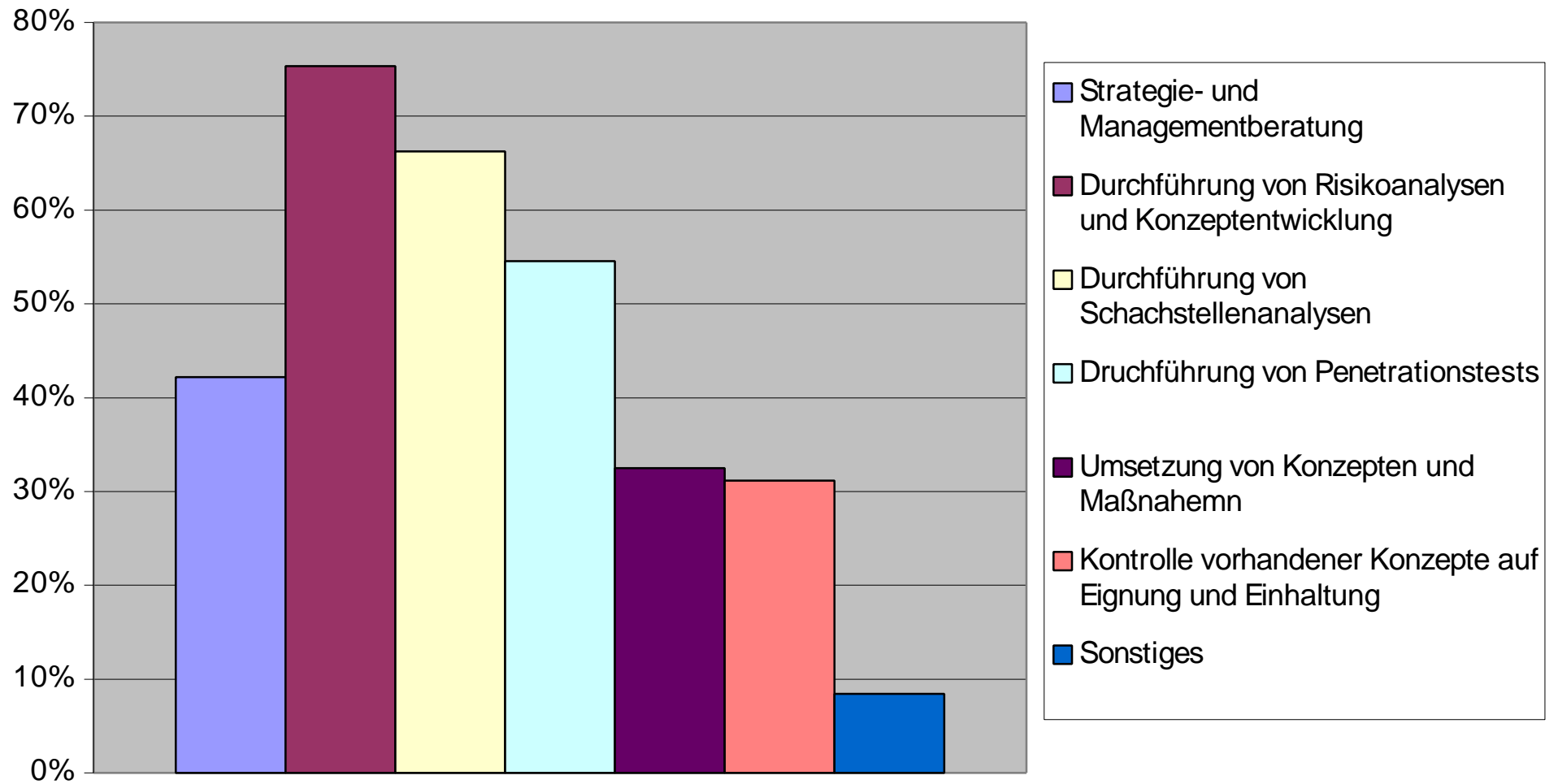
2.09a

Wenn Ja, in welcher Form? (Mehrfachnennungen möglich)		
Basis der Prozentuierung:	154	
	Nennungen	Prozentua 1
Strategie- und Managementberatung	65	42%
Durchführung von Risikoanalysen und Konzeptentwicklung	116	75%
Durchführung von Schachstellenanalysen	102	66%
Druchführung von Penetrationstests	84	55%
Umsetzung von Konzepten und Maßnahemn	50	32%
Kontrolle vorhandener Konzepte auf Eignung und Einhaltung	48	31%
Sonstiges	13	8%

Lister der Sonstigen:

Notfallplanung, Hard- und Software, Jahresabschlussprüfer, Anbieter von Systemen, Projekte IT-Optimierung, Backup-Support, Softwarelieferant

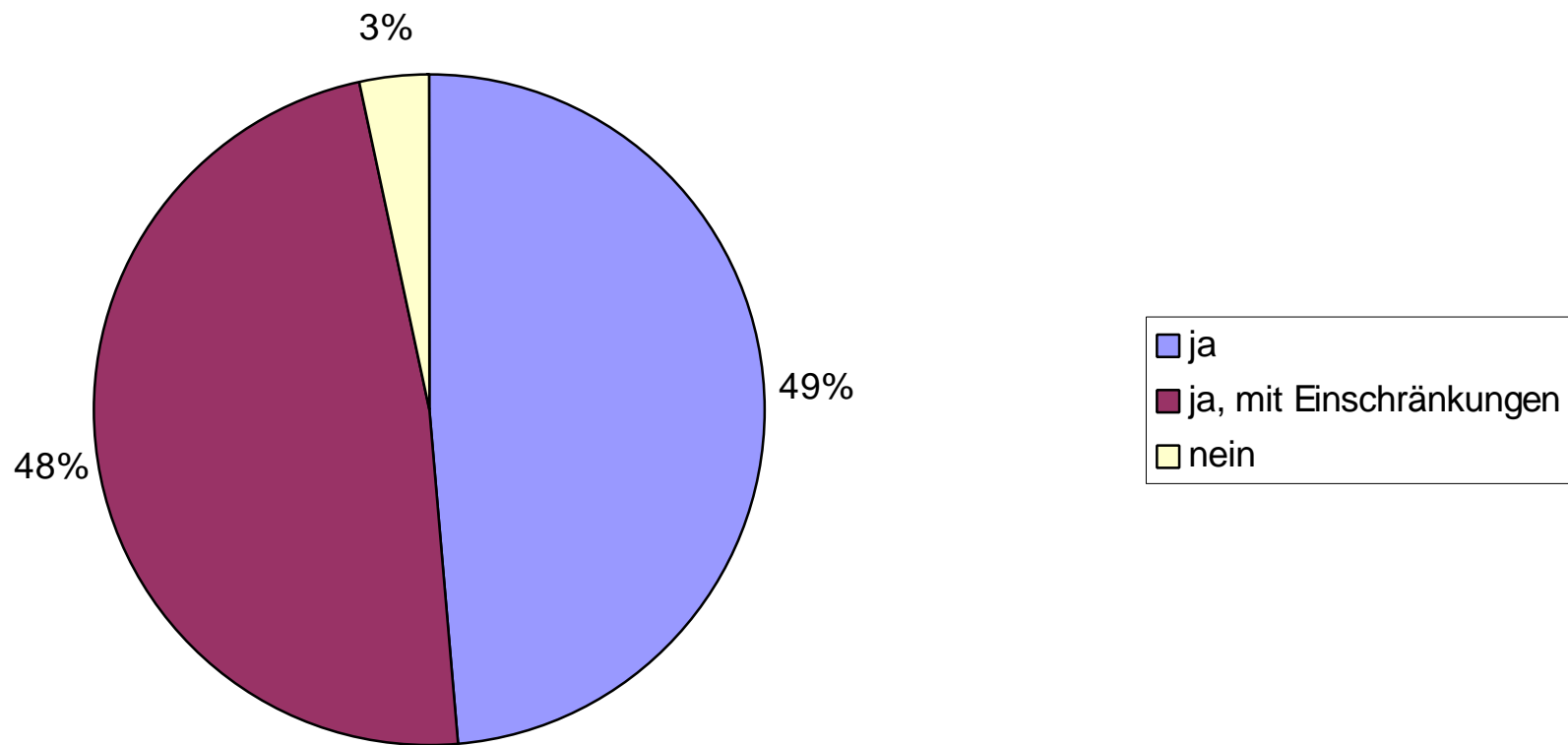
Art der ISi-Beratung



2.09b

Waren Sie mit der Beratung zufrieden?		
	Nennungen	Prozentua l
ja	75	49%
ja, mit Einschränkungen	74	48%
nein	5	3%
Summe	154	

Zufriedenheit mit ISi-Beratung



2.10

**Welche Versicherung aus dem Bereich ISi haben Sie abgeschlossen?
 (Mehrfachnennungen möglich)**

Basis der Prozentuierung:		235			
	abgeschlo ssen			in Anspruch genomme n	
Elektronikversicherung	202	86%		69	34%
- Sachversicherung	194	83%		60	31%
-	69	29%		4	6%
Datenversicherung/Softwareversicherung					
- Erweiterte Datenversicherung (inkl. Schäden durch Viren, fehlerhaftes Programmieren, versehentliches Löschen)	23	10%		11	48%
- Mehrkostenversicherung	26	11%		6	23%
- Elektronik- Betriebsunterbrechungsversicherung	65	28%		3	5%
Feuerversicherung	188	80%		10	5%
"Technologie-Police" o. ä. (Kombination von Elektronik- u. Maschinenversicherung)	23	10%		3	13%
Vertrauensschaden-Versicherung	36	15%		4	11%
- computermisbrauch-Versicherung	36	15%		4	11%
- Datenmissbrauch-Versicherung	18	8%		4	22%
Datenschutzversicherung	29	12%		6	21%
- Datenhaftpflicht-Versicherung	29	12%		3	10%
- Datenrechtsschutz-Versicherung	12	5%		4	33%
Keine der genannten	22	9%		11	1%

} Von abgeschlossen

} Von allen abgeschlossenen

Keine Angaben: 25