KES/KPMG-Sicherheitsstudie 2002

Kapitel 4: Methoden und Instrumente

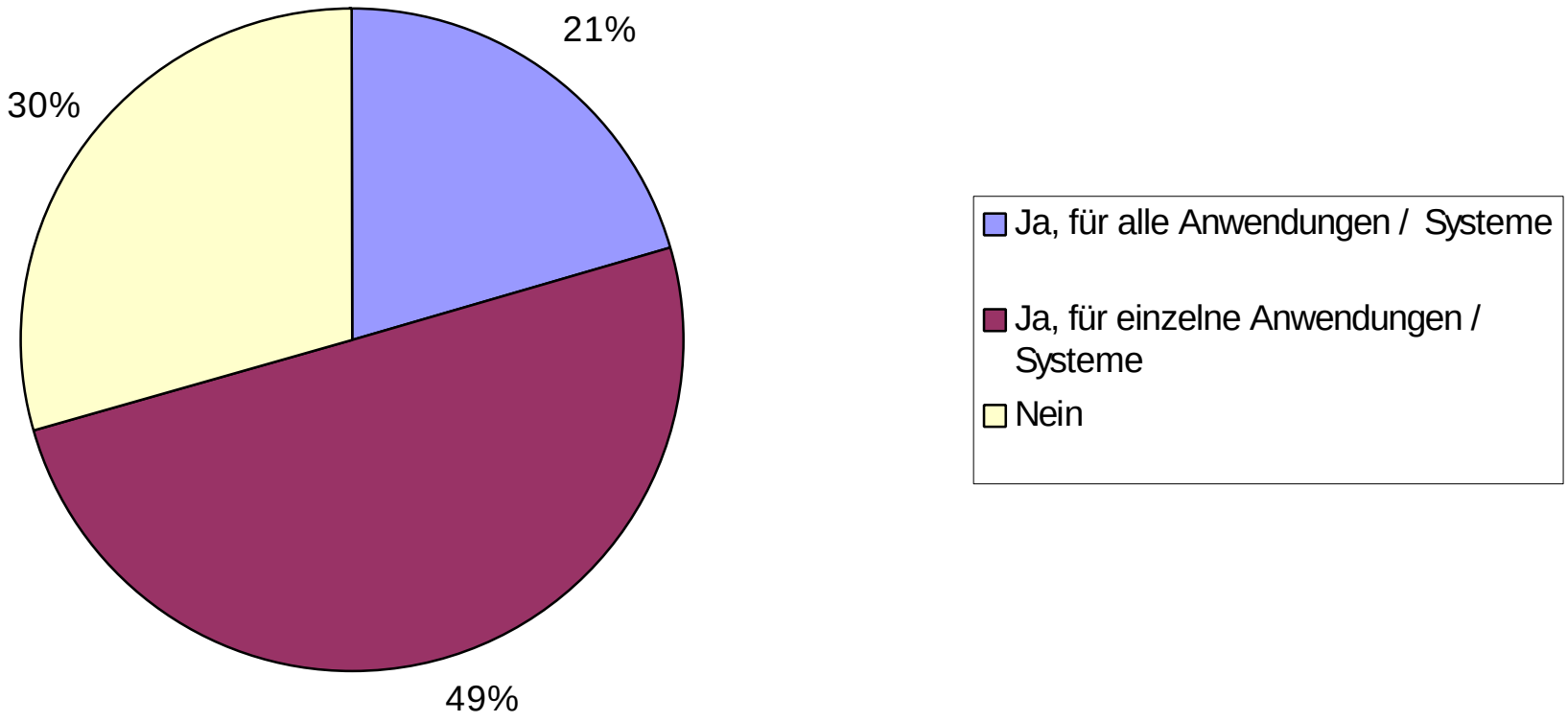
UIMC Dr. Vossbein Gmbh & Co KG, Wuppertal

4.01

Haben Sie in Ihrem Haus die Anwendungen / Systeme hinsichtlich ihrer Bedeutung für die Aufgabenerfüllung (Abhängigkeit, Schutzbedarf) sowie der bestehenden Risiken bewertet und klassifiziert?		
	Anzahl	Prozent
Ja, für alle Anwendungen / Systeme	53	21%
Ja, für einzelne Anwendungen / Systeme	128	49%
Nein	76	30%
Summe	257	
Keine Angaben	3	

	Gesamt	Höchstens	Durchschnitt	Nennungen
Wenn Ja, welcher Prozentanteil der Anwendungen / Systeme hat einen sehr hohen Schutzbedarf bzw. ein sehr hohes Risiko?	5984	100	41,56	144

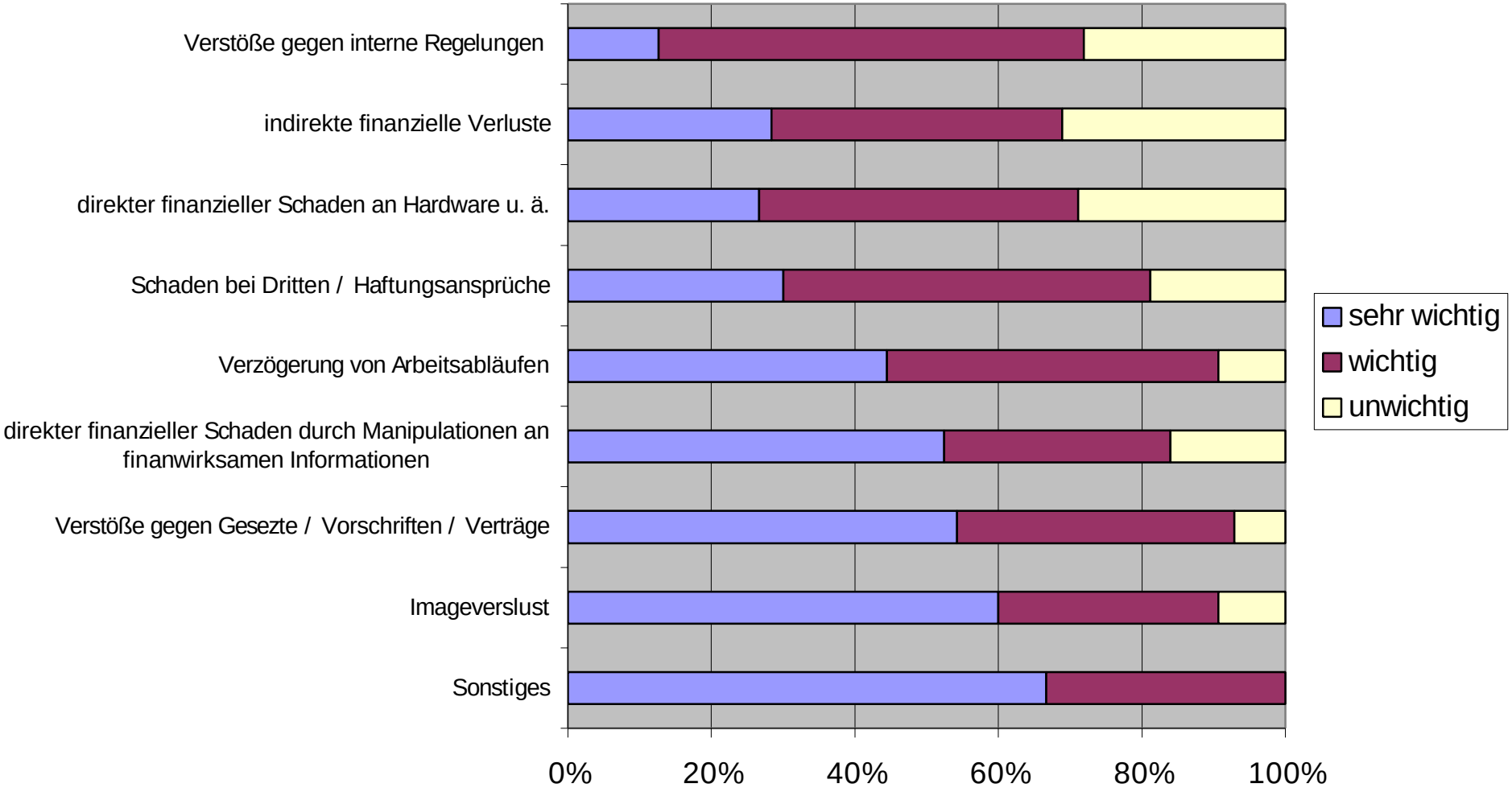
Risikoklassifizierung



4.02

Wie Wichtig sind die folgenden Kriterien für die Klassifizierung von Anwendungen / Systemen in Ihrem Haus?								
	sehr wichtig (2)	wichtig (1)	unwichtig (0)	Summe	sehr wichtig (2)	wichtig (1)	unwichtig (0)	Bedeutungsfaktor
Sonstiges	4	2	0	6	67%	33%	0%	1,67
Imageverslust	135	69	21	225	60%	31%	9%	1,51
Verstöße gegen Gesetze / Vorschriften / Verträge	122	87	16	225	54%	39%	7%	1,47
direkter finanzieller Schaden durch Manipulationen an finanzwirksamen Informationen	118	71	36	225	52%	32%	16%	1,36
Verzögerung von Arbeitsabläufen	100	104	21	225	44%	46%	9%	1,35
Schaden bei Dritten / Haftungsansprüche	67	114	42	223	30%	51%	19%	1,11
direkter finanzieller Schaden an Hardware u. ä.	60	100	65	225	27%	44%	29%	0,98
indirekte finanzielle Verluste	63	90	69	222	28%	41%	31%	0,97
Verstöße gegen interne Regelungen	28	131	62	221	13%	59%	28%	0,85

Klassifizierung - Kriterien

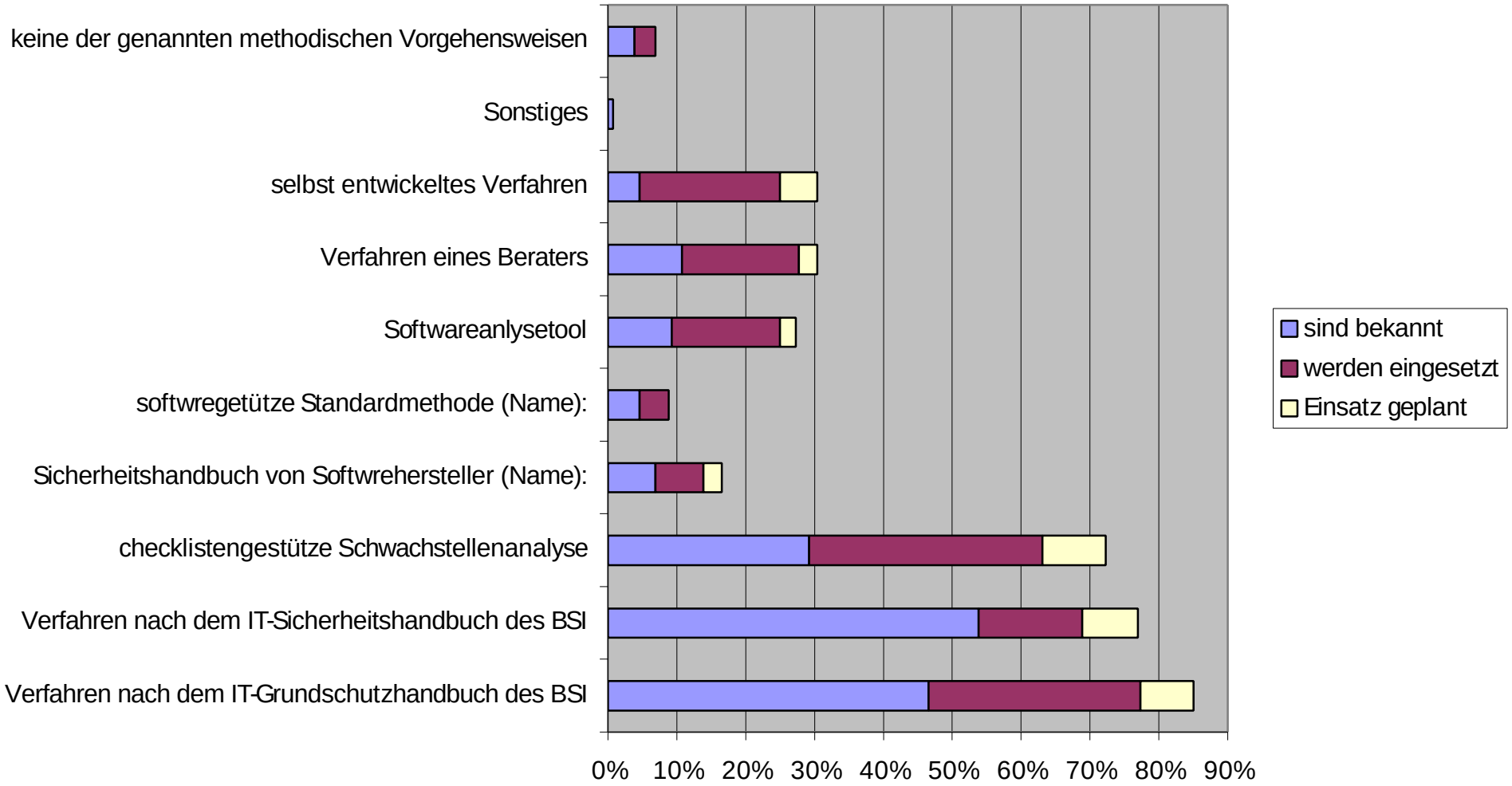


4.03

Die folgenden methodischen Vorgehensweisen und Software-Tools...			
Basis der Prozentuierung:	260		
	sind bekannt	werden eingesetzt	Einsatz geplant
Verfahren nach dem IT-Grundschutzhandbuch des BSI	121	80	20
Verfahren nach dem IT-Sicherheitshandbuch des BSI	140	39	21
checklistengestützte Schwachstellenanalyse	76	88	24
Sicherheitshandbuch von Softwarehersteller	18	18	7
softwaregestützte Standardmethode	12	11	0
Softwareanlysetool	24	41	6
Verfahren eines Beraters	28	44	7
selbst entwickeltes Verfahren	12	53	14
Sonstiges	2	0	0
keine der genannten methodischen Vorgehensweisen	10	8	0

	sind bekannt	werden eingesetzt	Einsatz geplant
Verfahren nach dem IT-Grundschutzhandbuch des BSI	47%	31%	8%
Verfahren nach dem IT-Sicherheitshandbuch des BSI	54%	15%	8%
checklistengestützte Schwachstellenanalyse	29%	34%	9%
Sicherheitshandbuch von Softwarehersteller (Name):	7%	7%	3%
softwregestützte Standardmethode (Name):	5%	4%	0%
Softwareanlysetool	9%	16%	2%
Verfahren eines Beraters	11%	17%	3%
selbst entwickeltes Verfahren	5%	20%	5%
Sonstiges	1%	0%	0%
keine der genannten methodischen Vorgehensweisen	4%	3%	0%

Vorgehensweisen



4.04

Im Rahmen von Prüfungen (z. B. durch interne Revision, Wirtschaftsprüfer) werden unter ISi-Aspekten geprüft:		
Basis der Prozentuierung:	254	
	Nennungen	Prozentual
Datenklassifizierung und Zugriffsrechte	144	57%
Ablauforganisation (z. B. für einzelne Vorgänge, Verfahren)	141	56%
Software-Einsatz	135	53%
Software-Entwicklung (inkl. Test- und Freigabeverfahren)	107	42%
Konzeption und Zielsetzung	104	41%
Software (Korrektheit, Fehlerfreiheit usw.)	103	41%
Change Management (z. B. Änderungshistorie)	102	40%
Aufbauorganisation	99	39%
Virenschutz	97	38%
Übereinstimmung der System-Konfiguration mit Vorgaben	89	35%
nichts Derartiges	55	22%
Sonstiges	19	7%
Keine Angaben:	6	

Liste der Sonstigen
Zugriffsschutz, Verschlüsselungstechnologie, Sicherstellung der Verfügbarkeit, phy-sische Sicherheit, FW, einzelne Projkte je nach Bedeutung/Größe, EDV Notfall-Konzept, Dokumentation, Datenschutz (BayDSG)

ISi-Aspekte bei der Prüfung