

Revision von IT-Verfahren in öffentlichen Institutionen

Praxisleitfaden für den Prüfungsprozess

Herausgegeben vom DIIR – Deutsches Institut für Interne Revision e.V.
Erarbeitet im Arbeitskreis „Interne Revision in öffentlichen Institutionen“

ERICH SCHMIDT VERLAG

Inhaltsverzeichnis

Vorwort	5
Inhaltsverzeichnis	7
Abbildungsverzeichnis	11
Tabellenverzeichnis	13
1 Einleitung	15
2 Prüfungsansatz	19
3 Vorgehensweise zur Durchführung der Prüfung	21
4 Kurzcheck IT-Verfahren und Überblick über Prüfungshandlungen	23
5 Rahmenvorgaben für IT-Verfahren	27
6 Revision von IT-Verfahren	33
6.1 Überprüfung/Ermittlung der Grundgesamtheit	33
6.1.1 Überprüfung/Ermittlung der Grundgesamtheit über die Zuständigkeiten	33
6.1.2 Überprüfung/Ermittlung der Grundgesamtheit über die Haushalts- und Wirtschaftspläne	35
6.1.3 Überprüfung/Ermittlung der Grundgesamtheit über die Abbildung der Geschäftsprozesse	36
6.1.4 Zukünftige Sicherstellung der Vollständigkeit	36
6.2 Durchführung Bestandsaufnahme	36
6.2.1 Allgemeine Angaben zum IT-Verfahren	37
6.2.2 Unterstützte Prozesse	39
6.2.3 IT-Verfahren – Entwicklung	42
6.2.4 IT-Verfahren – Weiterentwicklung	49
6.2.5 IT-Infrastruktur	49
6.2.6 Beziehung zum ERP-System	51
6.2.7 Schnittstellen zum ERP-System	51
6.2.8 Maschinelle Schnittstellen zum ERP-System	52
6.2.9 Finanzieller Beitrag	53
6.3 Risikoanalyse	55
6.3.1 Allgemeine Risikoanalyse	55
6.3.2 Spezifische Risikoanalyse für rechnungslegungs- relevante IT-Verfahren (z.B. ERP-System)	57
6.3.3 Spezifische Risikoanalyse für nicht-rechnungslegungs- relevante IT-Verfahren	61

6.4	Revision der IT-Infrastruktur	62
6.4.1	Physische Sicherungsmaßnahmen.	63
6.4.2	Logische Zugriffskontrollen	63
6.4.3	Datensicherungs- und Auslagerungsverfahren	67
6.4.4	Maßnahmen für den geordneten Regelbetrieb	68
6.4.5	Verfahren für den Notbetrieb.	68
6.4.6	Sicherung der Betriebsbereitschaft	69
6.4.7	Besonderheiten der Internet-Nutzung	69
6.5	Revision der IT-Anwendungen.	70
6.5.1	Auswahl-, Entwicklungs- und Änderungsprozess sowie Implementierung (Change Management)	70
6.5.2	Programmfunktionen	72
6.5.2.1	Allgemeine Fragen zu Programmfunktionen	72
6.5.2.2	Belegfunktion	73
6.5.2.3	Journalfunktion (Protokollierungsfunktion)	74
6.5.2.4	Kontenfunktion	75
6.6	Revision IT-gestützter Geschäftsprozesse.	75
6.6.1	Geschäftsprozesse	76
6.6.2	Prozessintegrierte Kontrollen	77
6.6.3	Vollständige Verarbeitung	78
6.6.4	Abstimmungsverfahren	78
6.7	Revision des IT-Outsourcings.	79
6.7.1	IT-Outsourcing	80
6.7.2	IKS für den Rechenzentrumsbetrieb	80
6.7.3	Prozess Outsourcing	81
6.7.4	IKS bei Prozess Outsourcing	81
6.8	Revision der Schnittstellen.	81
6.8.1	Verarbeitung der Schnittstellendaten im Sendersystem	83
6.8.2	Extraktion der Schnittstellendaten aus dem Sendersystem	83
6.8.3	Übergabe der Schnittstellendaten an das Empfängersystem	85
6.8.4	Aufbereitung der Schnittstellendaten für das Empfängersystem	85
6.8.5	Verarbeitung der Schnittstellendaten im Empfängersystem	87
6.8.6	Fehlerbeseitigung innerhalb der Schnittstellen- verarbeitung	88
6.8.7	Dokumentation der Schnittstellenverarbeitung.	88
6.9	Revision der Einhaltung des BSI IT-Grundschutzes	91
6.10	Revision der Einhaltung des Datenschutzes.	94

6.11	Zusammenfassung und Darstellung der Prüfungsergebnisse	96
7	Ansatzpunkte aus den Prüfungsergebnissen	99
7.1	Zu 5 Rahmenvorgaben für IT-Verfahren (Berechtigungsrahmenkonzept)	99
7.2	Zu 5 Rahmenvorgaben für IT-Verfahren (Wirtschaftlichkeitsuntersuchungen)	100
7.3	Zu 6.2.3 IT-Verfahren – Entwicklung	101
7.4	Zu 6.2.6 Beziehung zum ERP-System	104
7.5	Zu 6.3.1 Allgemeine Risikoanalyse	104
7.6	Zu 6.4.2 Logische Zugriffskontrollen	105
7.7	Zu 6.7 Revision des IT-Outsourcings	105
7.8	Zu 6.8.2 Extraktion der Schnittstellendaten aus dem Sendersystem	107
	Abkürzungsverzeichnis	109
	Literaturverzeichnis	111
Anlage 1	Kopiervorlage Grundgesamtheit	119
Anlage 2	Kopiervorlage Bestandsaufnahme/Risikoanalyse	120
Anlage 3	Checkliste zur Prüfung der Rechnungslegungsrelevanz.	125
Anlage 4	Kopiervorlage Revision der IT-Infrastruktur	127
Anlage 5	Kopiervorlage Revision der IT-Anwendungen	129
Anlage 6	Kopiervorlage Revision IT-gestützter Geschäftsprozesse	131
Anlage 7	Kopiervorlage Revision des IT-Outsourcings	132
Anlage 8	Kopiervorlage Revision der Schnittstellen	133
Anlage 9	Kopiervorlage Revision der Einhaltung des BSI IT-Grundschutzes	137
Anlage 10	Kopiervorlage Revision der Einhaltung des Datenschutzes	138