

HANSER



Inhaltsverzeichnis

Klaus Schmidt, Dirk Brand

IT-Revision in der Praxis

nach den Grundsätzen einer ordnungsgemäßen IT

ISBN: 978-3-446-41706-9

Weitere Informationen oder Bestellungen unter

<http://www.hanser.de/978-3-446-41706-9>

sowie im Buchhandel.



Inhalt

Vorwort	XI
Die Autoren	XIII
Teil I: Praxis der IT-Revision	1
1 Grundlagen der IT-Revision	3
1.1 Das Wesen der IT-Revision	3
1.1.1 Ziele der IT-Revision	4
1.1.2 Externe Revision	7
1.1.3 Interne Revisionsarten	8
1.2 Mit der IT-Revision verwandte Funktionen	9
1.3 Die IT-Revision im Unternehmen	11
1.3.1 Position im Unternehmen	11
1.3.2 Befugnisse	11
1.3.3 Mitarbeiter	13
1.3.4 Qualitätssicherung und Leistungsmessung	15
1.3.5 Sicherheit der Revisionsabteilung	18
1.4 Prüfungsaspekte	19
1.4.1 Rechtmäßigkeit	19
1.4.2 Ordnungsmäßigkeit	20
1.4.3 Sicherheit	21
1.4.4 Zweckmäßigkeit/Funktionsfähigkeit	22
1.4.5 Wirtschaftlichkeit	23
1.4.6 Kontrollierbarkeit und Nachvollziehbarkeit	24
2 Prüfungsorganisation und Vorgehen	25
2.1 Prüfungsplanung	25
2.1.1 Strategische Planung (3-Jahres-Plan)	26
2.1.2 Jahresplanung	27
2.1.3 Planung und Vorbereitung einer einzelnen Prüfung	28

2.2	Prüfungsauftrag.....	30
2.3	Vorbereitung der Prüfungsdurchführung	31
2.3.1	Analyse des Prüfobjekts/Voruntersuchung.....	31
2.3.2	Prüfungsankündigung.....	31
2.3.3	Kick-off-Meeting	33
2.4	Prüfungsdurchführung	33
2.4.1	Dokumentensichtung.....	33
2.4.2	Fragebogenerhebung	35
2.4.3	Interviews.....	36
2.4.4	Verifikation der Aussagen.....	40
2.5	Prüfungsbericht.....	43
2.5.1	Dokumentation des Ist-Zustands im Prüfungsbericht.....	43
2.5.2	Bewertung des Ist-Zustands	44
2.5.3	Maßnahmenempfehlungen	47
2.5.4	Entwurf und Abstimmung des Prüfungsberichts	47
2.6	Prüfungsabschluss.....	49
2.6.1	Schlussbesprechung	49
2.6.2	Vollständigkeitserklärung	50
2.6.3	Stellungnahme des geprüften Bereichs.....	51
2.6.4	Verfolgung der Umsetzung der Maßnahmen	51
3	Zusammenspiel mit externen Wirtschaftsprüfern	53
3.1	Aufgabe der externen Wirtschaftsprüfer	53
3.2	Grundlagen der Prüfung durch einen Wirtschaftsprüfer	54
3.3	Vorgehen bei der Prüfung durch externe Wirtschaftsprüfer.....	56
3.4	Ergebnisse der internen Revision verwenden.....	57
4	Relevante Prüfungsgrundlagen.....	61
4.1	Prüfungsgrundlagen für die IT-Revision.....	61
4.2	Gesetze.....	62
4.2.1	Handelsgesetzbuch (HGB).....	63
4.2.2	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG).....	66
4.2.3	Bundesdatenschutzgesetz BDSG.....	67
4.2.4	Telemediengesetz (TMG).....	69
4.2.5	SOX.....	70
4.3	Richtlinien für die IT-Revision	71
4.3.1	Allgemein.....	71
4.3.2	Verlautbarungen des IDW	72
4.3.3	GDPdU.....	73
4.3.4	GoBS.....	74
4.4	Branchenvorschriften	76
4.4.1	Basel II.....	76
4.4.2	MaRisk (Mindestanforderungen an das Risikomanagement).....	77
4.4.3	Solvency II	78

5	Prüfung von IT-Verfahren.....	79
5.1	Das Wesen eines IT-Verfahrens.....	79
5.2	Fragmentierung von Verfahrensprüfungen.....	81
5.3	Prüfung der IT-Verfahrensplanung.....	83
5.3.1	Anforderungen an das neue IT-Verfahren.....	83
5.3.2	Einsatzplanung.....	84
5.3.3	Einbettung in Geschäftsprozesse.....	85
5.3.4	Einbettung in die IT.....	86
5.4	Prüfung der Verfahrensdokumentation.....	87
5.4.1	Das Wesen der Verfahrensdokumentation.....	87
5.4.2	Beschreibung der sachlogischen Lösung.....	89
5.4.3	Beschreibung der technischen Lösung.....	90
5.4.4	Programmidentität.....	93
5.4.5	Datenintegrität.....	94
5.4.6	Arbeitsanweisungen für den Anwender.....	94
5.4.7	Prüfen der Verfahrensdokumentation.....	95
5.5	Berechtigungskonzept.....	97
5.6	Prüfung der Verfahrensdaten.....	99
5.6.1	Anforderungen an Daten in der Planungsphase.....	99
5.6.2	Dateneingabe, -verarbeitung und -ausgabe.....	100
5.6.3	Datentransfer.....	101
5.6.4	Datensicherung und Archivierung.....	101
5.6.5	Datenmigration.....	102
5.6.6	Datenlöschung und -entsorgung.....	103
6	Besondere Prüfungsgebiete.....	105
6.1	Prüfungsgebiet Bundesdatenschutzgesetz.....	105
6.1.1	BSI Grundschutzstandards und -kataloge.....	106
6.1.2	Vorgehen nach BSI Grundschutz.....	107
6.1.3	Umsetzung der Vorgaben anhand eines Sicherheitsrahmenkonzeptes.....	117
6.1.4	Audit eines Informationssicherheitsmanagementsystems (ISMS) nach BSI Grundschutz.....	118
6.2	Prüfungsgebiet Dokumentenmanagement.....	120
6.2.1	Welche Rahmenbedingungen gibt es?.....	120
6.2.2	Bewertungsbereiche.....	122
6.2.3	Prüfung und Zertifizierung.....	122
7	CobIT-Prüfungen.....	125
7.1	Bestimmung des Prüfungsziels.....	125
7.2	Aufnahme der bestehenden Situation.....	127
7.3	Feststellung der CobIT-Erfüllung.....	128
7.4	Ermittlung des Reifegrades.....	128
7.5	Prüfung des Ziel- und Kontrollsystems.....	131

8	Tools zur Prüfungsunterstützung	135
8.1	Wie alles begann.....	135
8.2	Warum überhaupt Tools?.....	136
8.3	Welche Werkzeugarten gibt es?.....	136
8.4	Prüfungsbegleitende Werkzeuge.....	137
8.4.1	Ablauf einer tool-unterstützten Prüfung.....	138
8.5	Prüfende Werkzeuge.....	147
Teil II: Grundsätze einer ordnungsgemäßen Informationstechnik (GoIT)		149
Einleitung.....		151
Gliederung der IT in den GoIT.....		152
IT-Strukturierungsmodell.....		152
Fokus		154
IT-Lebenszyklusphasen in den GoIT.....		155
Prüfungsaspekte in den GoIT		156
Vorgehen bei der Anwendung der GoIT		157
A	Physikalische Ebene	159
A.1	Planungsphase.....	160
A.1.1	Bei der Planung einer physischen Einrichtung sind Sicherheitsmaßnahmen berücksichtigt worden.....	160
A.1.2	Bei der Planung sind einschlägige Normen berücksichtigt worden.....	161
A.1.3	Schützenswerte Gebäudeteile sind deklariert worden.....	162
A.1.4	Elektroversorgungsleitungen und Datenleitungen sind zukunftsorientiert geplant.	163
A.1.5	Versorgungsleitungen sind redundant ausgelegt.	164
A.2	Entwicklungsphase	164
A.3	Implementierungsphase	165
A.3.1	Bei der Realisierung sind die Anforderungen der Planungsphase berücksichtigt worden.....	165
A.3.2	Beim Einzug in eine gemietete Einrichtung sind Sicherheitsmaßnahmen geprüft worden.....	166
A.4	Betriebsphase.....	167
A.4.1	Der Zutritt zum Gebäude wird kontrolliert.....	167
A.4.2	Es sind Schutzmaßnahmen gegen Bedrohungen von außen und aus der Umgebung getroffen worden.....	168
A.4.3	Öffentliche Zugänge, Anlieferungs- und Ladezonen werden kontrolliert.	169
A.4.4	Die Arbeit in Sicherheitszonen ist geregelt.	170
A.4.5	Betriebsmittel sind vor unerlaubtem Zugriff physisch gesichert.	171
A.4.6	Bei physischen Einrichtungen mit Publikumsverkehr sind die Informationsträger gesondert zu sichern.	172
A.4.7	Physische Einrichtungen, in denen sich Mitarbeiter aufhalten, sind gegen unbefugten Zutritt gesichert.	173
A.4.8	Physische Sicherheitsmaßnahmen sind dokumentiert.	174
A.4.9	Notfallmaßnahmen für physische Einrichtungen sind definiert.....	175

A.4.10	Notfallübungen werden durchgeführt.....	176
A.5	Migration.....	176
A.6	Roll-Off.....	177
A.6.1	Der Auszug aus physischen Einrichtungen ist geregelt.....	177
A.6.2	Betriebsmittel werden ordnungsgemäß entsorgt.....	178
A.6.3	Bestandsverzeichnisse sind auf dem aktuellen Stand.....	179
B	Netzwerkebene.....	181
B.1	Planungsphase.....	182
B.1.1	Eine geeignete Netzwerksegmentierung ist geplant.....	182
B.1.2	Bei der Planung sind Sicherheitsmaßnahmen zum Schutz des Netzwerkes getroffen worden.....	183
B.1.3	Das physische Netzwerk ist vor unbefugten Zugängen geschützt.....	184
B.1.4	Ein Netzwerkrealisierungsplan ist vorhanden.....	185
B.1.5	Eine geeignete Netzkopplung ist eingeplant.....	186
B.2	Entwicklungsphase.....	186
B.3	Implementierungsphase.....	187
B.3.1	Das Netzwerk ist auf Engpässe überprüft.....	187
B.3.2	Die Verwaltung der Netzkomponenten ist zentral gesteuert.....	188
B.3.3	Eine vollständige Netzdokumentation ist vorhanden.....	189
B.3.4	Mit Netzwerkbetreibern sind geeignete Verträge abgeschlossen.....	190
B.3.5	Netzkomponenten sind sicher zu konfigurieren.....	191
B.4	Betriebsphase.....	192
B.4.1	Der Netzwerkverkehr wird protokolliert.....	192
B.4.2	Die Protokolle werden regelmäßig ausgewertet und auf Unregelmäßigkeiten geprüft.....	193
B.4.3	Ein Monitoring ist eingerichtet.....	194
B.4.4	Das Verhalten bei Zwischenfällen ist definiert.....	195
B.4.5	Netzwerkadministratoren sind sorgfältig ausgewählt worden.....	196
B.4.6	Netzwerkspezifische Sicherheitsmaßnahmen sind dokumentiert.....	197
B.4.7	Notfallmaßnahmen für das Netzwerk sind definiert.....	198
B.4.8	Notfallübungen werden durchgeführt.....	199
B.5	Migrationsphase.....	199
B.6	Roll-Off.....	200
B.6.1	Inhalte auf aktiven Netzwerkkomponenten sind ordentlich gelöscht worden.....	200
B.6.2	Protokolle werden nach gesetzlichen Vorgaben vernichtet.....	201
C	Systemebene.....	203
C.1	Planungsphase.....	204
C.1.1	Der Schutzbedarf des Systems ist ermittelt.....	204
C.1.2	Die sich aus dem Schutzbedarf ableitenden Sicherheitsanforderungen und -maßnahmen sind definiert.....	205
C.1.3	Leistungs- und Kapazitätsanforderungen an das System sind definiert.....	206
C.1.4	Die Dimensionierung des Systems entspricht der zu erbringenden Leistung.....	207
C.1.5	Die Systeme folgen definierten Unternehmensstandards.....	208
C.2	Entwicklungsphase.....	208

C.3	Implementierungsphase	209
C.3.1	Bei erhöhtem Schutzbedarf wird das System gehärtet.	209
C.3.2	Die Erfüllung der Leistungs- und Kapazitätsanforderungen wird nachgewiesen.	210
C.3.3	Die Systemfunktionen und -komponenten sind ausführlich getestet.	211
C.4	Betriebsphase	212
C.4.1	Alle Lizenzvereinbarungen werden eingehalten.	212
C.4.2	Das System ist vor zu langen Ausfällen geschützt.	213
C.4.3	Die Wiederherstellung des Systems ist in der erforderlichen Zeit möglich.	214
C.4.4	Das System wird durch Updates auf dem neuesten Stand gehalten.	215
C.4.5	Das System ist vor unberechtigten Zugriffen geschützt.	216
C.4.6	Die Erfüllung der Leistungs- und Sicherheitsanforderungen wird regelmäßig analysiert und ggf. angepasst.	217
C.4.7	Das System ist angemessen dokumentiert.	218
C.5	Migrationsphase	219
C.5.1	Die Systemfunktion bleibt zu jedem Zeitpunkt der Migration erhalten.	219
C.5.2	Für einen möglichen Fehlschlag von Änderungen/Migrationen ist ein Rollback vorhanden.	220
C.5.3	Systemänderungen werden auf Seiteneffekte hin geprüft.	221
C.5.4	Es gibt eine Übersicht, welche Systemeigenschaften des Altsystems denen des Neusystems entsprechen.	222
C.5.5	Änderungen und Migrationen unterliegen einem definierten und kontrollierten Change-Management-Prozess.	223
C.6	Roll-Off	224
C.6.1	Alle Systemfunktionen werden nicht mehr benötigt.	224
C.6.2	Alle Systemlizenzen erlöschen.	225
C.6.3	Vor dem Roll-Off wird sichergestellt, dass ein zu entsorgendes, physisches System keine vertraulichen Daten mehr enthält.	226
C.6.4	Das physische IT-System wird de-inventarisiert und die Entsorgung protokolliert.	227
D	Applikationsebene	229
D.1	Planungsphase	230
D.1.1	Die Ziele und Aufgaben, welche die Anwendung erfüllen soll, sind definiert worden.	230
D.1.2	Die Anforderungen sind in einem Lastenheft/Anforderungskatalog konkretisiert worden.	231
D.1.3	Für die Entwicklung/Implementierung werden geeignete Ressourcen bereitgestellt.	232
D.1.4	Die Daten, die verarbeitet werden sollen, sind klassifiziert und definiert worden.	233
D.1.5	Eine geeignete Infrastruktur für den Betrieb wurde ausgewählt.	234
D.2	Entwicklungsphase	235
D.2.1	Geeignete Vorgehensweisen zur Entwicklung sind mit den Anforderungen verglichen worden.	235
D.2.2	Die Entwicklung wird konform zur Vorgehensweise dokumentiert.	236
D.3	Implementierungsphase	237
D.3.1	Quellcode ist gegen unbefugte Veränderung gesichert.	237

D.3.2	Applikationstests werden nach den Vorgaben der Planung umgesetzt.	238
D.4	Betriebsphase	239
D.4.1	Anforderungen der Applikation an den Betrieb sind dokumentiert.	239
D.4.2	Prozesse zur sicheren Applikationsverwaltung sind beschrieben.	240
D.4.3	Integritäts- und vertraulichkeitssichernde Maßnahmen sind für den Betrieb beschrieben und umgesetzt.	241
D.4.4	Etwaige Verschlüsselungsverfahren sind beschrieben.	242
D.4.5	Prozesse für die Benutzerverwaltung innerhalb der Anwendung sind dem Betrieb bekannt und dokumentiert.	243
D.4.6	Eine Testumgebung der Applikation ist vorhanden.	244
D.5	Migrationsphase	245
D.5.1	Der im Falle einer Migration durchzuführende Prozess ist definiert und dokumentiert.	245
D.5.2	Eine Migration erfolgt geplant.	246
D.6	Roll-Off.	247
D.6.1	Die Benutzerverwaltung ist auch über die End-of-Life-Phase hinaus geregelt.	247
D.6.2	Betriebsmittel werden ordnungsgemäß entsorgt.	248
D.6.3	Durch die Anwendung mitgenutzte Ressourcen sind durch Befugte freigegeben.	249
E	Inhaltsebene	251
E.1	Planungsphase	252
E.1.1	Es werden die und nur die Daten vorgesehen, die für den Geschäftszweck benötigt werden.	252
E.1.2	Die Gewährleistung der Datenkonsistenz ist in der Planung berücksichtigt.	253
E.1.3	Die Gewährleistung der Datenqualität ist in der Planung berücksichtigt.	254
E.1.4	Die Daten werden hinsichtlich der Kritikalität bewertet.	255
E.2	Entwicklungsphase.	256
E.2.1	Es werden möglichst keine Produktionsdaten in Entwicklungs- oder Testumgebungen verwendet.	256
E.2.2	Für Tests werden möglichst geeignete Testdaten verwendet.	257
E.2.3	Testdaten werden möglichst automatisiert generiert.	258
E.2.4	Die Daten, die durch das entwickelte System entstehen, werden dokumentiert.	259
E.3	Implementierungsphase	260
E.3.1	Es ist transparent, welche Daten in welchen Speicherorten geführt und auf welchen Datenträgern archiviert werden.	260
E.3.2	Es wird kontrolliert, dass die Daten gemäß ihrer Spezifikation implementiert werden.	261
E.4	Betriebsphase	262
E.4.1	Buchführungsrelevante Daten sind nach der Eingabe nicht mehr änderbar.	262
E.4.2	Wichtige Daten werden vor der Speicherung validiert bzw. plausibilisiert.	263
E.4.3	Wichtige, kritische oder sensible Daten sind vor Verlust geschützt.	264
E.4.4	Vertrauliche Daten sind nur den Personen zugänglich, für die sie bestimmt sind.	265
E.4.5	Vertrauliche bzw. personenbezogene Daten dürfen nur Personen zugänglich sein, die eine Verpflichtungserklärung zu Vertraulichkeit und Datenschutz abgegeben haben.	266
E.4.6	Der Zugriff auf vertrauliche/sensible Daten wird protokolliert.	267

E.5	Migrationsphase.....	268
E.5.1	Die Verfügbarkeit und Vertraulichkeit der Daten ist auch bei Änderungen und Migrationen zu jedem Zeitpunkt sichergestellt	268
E.5.2	Die Datensemantik wird von einer Migration nicht ungewollt verändert.....	269
E.5.3	Datenänderungen werden in einem geordneten Prozess durchgeführt	270
E.5.4	Datenänderungen werden protokolliert	271
E.6	Roll-Off	272
E.6.1	Vorgeschriebene Aufbewahrungsfristen werden gewährleistet.....	272
E.6.2	Es ist definiert, wann und durch wen Daten gelöscht werden dürfen	273
E.6.3	Sensible Daten werden sicher, zuverlässig, dauerhaft und nachweisbar gelöscht ..	274
E.6.4	Die Vernichtung von Datenträgern mit sensiblen Daten wird geprüft und protokolliert.....	275
F	Personelle Ebene	277
F.1	Planungsphase.....	278
F.1.1	Aufgaben und Verantwortung von Angestellten sind definiert.	278
F.1.2	Stellenbeschreibungen werden verwendet.....	279
F.1.3	Anforderungen an besondere Stellen sind definiert	280
F.1.4	Eine Überprüfung der Angestellten fand im Einklang mit den Gesetzen statt.....	281
F.2	Entwicklungsphase	281
F.3	Implementierungsphase	282
F.3.1	Sicherheitsrichtlinien für Angestellte sind durch das Management in Kraft gesetzt worden.....	282
F.3.2	Angestellte sind Ihren Aufgaben entsprechend sensibilisiert.	283
F.3.3	Sensible Posten sind mit vertrauenswürdigen Angestellten besetzt.....	284
F.3.4	Angestellte haben den vertraglichen Vereinbarungen ihrer Posten zugestimmt.	285
F.4	Betriebsphase	286
F.4.1	Angestellte werden regelmäßig über die geltenden Regelungen informiert.	286
F.4.2	Sanktionen sind definiert.....	287
F.4.3	Mitarbeiter sind ausreichend geschult.	288
F.5	Roll-Off	289
F.5.1	Die Verantwortlichkeiten für das Ausscheiden der Angestellten sind geregelt	289
F.5.2	Alle organisationseigenen Wertgegenstände sind zurückgenommen worden.	290
	Literaturhinweise	291
	Register.....	293