

IT-Revision

**Ergänzbarer Leitfaden zur Durchführung
von Prüfungen der Informationsverarbeitung**

Erarbeitet in den Arbeitskreisen
„IT-Revision“
und „IT-Revision in Kreditinstituten“
des
DEUTSCHEN INSTITUTS
FÜR INTERNE REVISION e.V.

ERICH SCHMIDT VERLAG

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über dnb.ddb.de abrufbar.

Weitere Informationen zu diesem Titel finden Sie im Internet unter
[ESV.info/3 503 05910 5](http://ESV.info/3_503_05910_5)

Das Werk erschien bis zur 6. Lieferung unter dem Titel „DV-Revision“.

ISBN-13: 3 503 05910 2

ISBN-10: 3 503 05910 5

ISSN 1615-8091

Alle Rechte vorbehalten

Erich Schmidt Verlag GmbH & Co., Berlin 2006

www.ESV.info

Satz: multitext, Berlin

Druck: Zimmermann, Balve

Inhaltsverzeichnis

	Kennz.	Seite
Vorwort	010	1
Inhaltsverzeichnis	030	1
Abkürzungsverzeichnis	050	1
Stichwortverzeichnis	080	1
Einführung	100	1
1. Zielsetzung und Aufgabe der DV-Revision	100	1
2. Revisionsfeld	100	2
3. Prüfkriterien	100	3
4. Externe und interne Anforderungen	100	5
5. Planung und Steuerung	100	5
6. Arbeitsweise	100	6
7. Anforderungsprofil	100	7
Risikoorientierte Prüfungsplanung der IT-Revision	110	1
1. Vorbemerkung	110	1
2. Risikoorientierte Prüfungsplanung als Basis der IT-Prüfung	110	1
Revision der IT-Stellen (Struktur)	200	1
DV-Gesamtplanung	210	1
1. DV-Strategie	210	1
2. DV-Organisation	210	3
3. DV-Projekte	210	5
4. DV Bedarfs- und Kapazitätsplanung	210	6
5. DV-Sicherheit	210	7
6. DV Kosten- und Leistungsrechnung	210	7
Projektentwicklung	230	1
1. Methoden, Tools, Standards	230	1
2. Basisverfahren	230	2
3. Planung, Steuerung und Kontrolle der Ressourcen für die Projektentwicklung	230	3
4. Projektdurchführung	230	4
5. Qualitätssicherung	230	5
6. DV-Aus- und -Fortbildung	230	6
Anforderungen an das IT-Controlling	240	1
1. Bedeutung und Ziele des IT-Controllings	240	1
2. Abgrenzung IT-Controlling und IT-Revision	240	1

	Kennz.	Seite
3. Strategisches IT-Controlling	240	2
4. Projekt-Controlling	240	2
5. Controlling Anwendungsbetrieb und IT-Infrastruktur	240	4
6. Leistungskontrolle (Kennzahlen-/Frühwarnsysteme)	240	6
7. Interne Leistungsverrechnung	240	9
8. Handlungsfelder und Fazit	240	10
Rechenzentrum	250	1
1. Vorbemerkungen	250	1
2. Risikomanagement (KonTraG)	250	1
3. Administration	250	2
4. Budget- und Investitionsanalyse	250	20
5. Sicherheit	250	22
6. Katastrophenfall(Wiederanlauf)-Planung	250	28
Ansätze zur Prüfung von IT-Netzwerken	260	1
1. Einleitung	260	1
2. Planung der IT-Infrastruktur und der Installation	260	1
3. Netz- und Systemmanagement	260	4
4. Sicherheit	260	7
5. Wirtschaftlichkeitsaspekte	260	15
Sicherheit im Funk-Lan	261	1
1. Einleitung	261	1
2. Architekturen	261	1
3. Sicherheitsprobleme	261	2
4. Maßnahmen	261	5
5. Literatur	261	7
6. Glossar	261	7
DV-Archivierungsverfahren	270	1
1. Prüfung der eingesetzten Speichermedien	270	1
2. Zusammenfassende Merkmale von Archivierungsverfahren auf digitalen Systemen	270	9
Revision der Software-Entwicklung	300	1
Entwicklung eines DV-Verfahrens	330	1
1. Vorstudie/Voruntersuchung	330	1
2. Fachkonzept	330	2
3. DV-Konzept	330	5
4. Programmierung/Test	330	8
5. Freigabeverfahren	330	11
6. Einführung des DV-Verfahrens	330	14
7. Pflege des DV-Verfahrens	330	16

	Kennz.	Seite
Revision eines eingesetzten Verfahrens	350	1
1. Verfahrensdokumentation	350	1
2. Einsatz in der Fachabteilung	350	3
3. Einsatz im Rechenzentrum	350	7
4. Anwender-Software	350	10
5. Schnittstellen zu anderen Verfahren	350	11
 Auswahl von Standard-Anwender-Software	 370	 1
1. Prüfung des Pflichtenheftes	370	1
2. Dokumentationsprüfung	370	2
3. Qualitätsanforderungen	370	2
4. Sicherheitsanforderungen	370	2
5. DV-technische Anforderungen	370	3
6. Wirtschaftlichkeitsbetrachtung	370	3
7. Bonität des Herstellers	370	4
8. Vertrag/Wartungsvertrag	370	4
 Einsatz von Systemsoftware bzw. systemnaher Software	 390	 1
1. Prüfungsgebiet Systemsoftware	390	1
2. Beschaffung von Systemsoftware	390	2
3. Eingesetzte Systemsoftware	390	4
 Revision der Prozesse	 400	 I
Prüfung von Geschäftsprozessen	410	1
1. Ziel des Kapitels	410	1
2. Grundlagen der Prüfung von Geschäftsprozessen	410	1
3. Prüfbarkeit des Geschäftsprozesses / Geschäftsprozessdokumentation	410	2
4. Prüfungsaspekte zu Sicherheit und Ordnungsmäßigkeit des Geschäftsprozesses	410	4
 Prüfung des Systementwicklungsprozesses	 420	 1
1. Ziel dieses Kapitels	420	1
2. Prüfungsfragen zum Systementwicklungsprozess	420	1
3. Prüfungsfelder des Systementwicklungsprozesses	420	2
 Revision der dezentralen IT	 500	 I
Client/Server-Betrieb		
Grundsatzfragen zur strategieorientierten Revision von Client/Server-Architekturen	505	1
1. Einführung	505	1
2. Zusammenhang zwischen Geschäft und Informationsverarbeitung	505	3
3. Organisation	505	6

	Kennz.	Seite
4. Administration	505	7
5. Migration	505	7
6. Standardsoftware	505	8
7. Sicherheit	505	9
8. Wirtschaftlichkeit	505	11
Absicherung von Serversystemen (speziell: UNIX, Windows NT) .	507	1
1. Ziel des Kapitels	507	1
2. Grundlagen des Zugriffsschutzes	507	1
3. Prüfungsfelder und prinzipielle Schwachstellen	507	2
4. Prüfungsaspekte und Prüfungsfragen	507	3
Einsatz der individuellen Datenverarbeitung (IDV)	510	1
1. Definition, Anforderungen und mögliche Maßnahmen	510	1
2. Prüfung der grundlegenden Anforderungen	510	4
3. Autorisierte DV-Verfahren (ADV)	510	12
4. Einhaltung des Datenschutzes (BDSG) und Schutz von Mitarbeiterdaten	510	16
5. Notfallkonzept	510	17
6. Wirtschaftlichkeit	510	17
7. Datenaustausch	510	18
8. Literaturhinweise	510	20
Prüfung des Email-Systems	520	1
1. Sicherheit	520	1
2. Verfügbarkeit	520	4
3. Ordnungsmäßigkeit	520	6
Internet/Firewall	530	1
1. Einführung	530	1
2. Prüfungsfragen	530	8
3. Literaturverzeichnis	530	11
Kontrolle und Sicherheitsaspekte bei E-Commerce	540	1
1. Einführung	540	1
2. E-Commerce in der Praxis	540	1
3. Risiken, Gefahren und Maßnahmen	540	2
4. Rechtliche Aspekte bei E-Commerce	540	7
Revision des IT-Einsatzes Externer	600	1
DV-Leistungen durch Fremdfirmen	610	1
Outsourcing	620	1
1. Begriff Outsourcing	620	1
2. Prüffelder in den Phasen des Outsourcingprozesses	620	4

	Kennz.	Seite
Wartung von DV-Hard- und Software	630	1
1. Wartungskonzepte	630	1
2. Wartungsverträge	630	2
3. Hardware und DV-Infrastruktur	630	5
4. Software	630	8
Revision mit IT	700	I
Einsatz von Software für Revisionszwecke	710	1
1. DV prüft DV	710	1
2. Prüfplanung	710	1
3. Datenanalyse	710	2
4. Systemgebundene Werkzeuge (Host, Client/Server)	710	4
5. Generelle Prüfsoftware	710	7
6. Universelle Programme (PC)	710	8
7. Host Connection	710	9
8. Übertragung zwischen PC	710	10
9. SAP-Analyse-Tools	710	10
10. Virenschutz	710	10
11. Internet	710	10
12. Präsentation	710	11
13. Groupware-Produkte	710	11
14. Hardware-Anforderungen	710	12
Grundsatzbeiträge	800	I
Bundesdatenschutzgesetz (BDSG)	810	1
1. Abgrenzung der durch das BDSG geschützten Daten und Begriffsbestimmungen	810	4
2. Bestellung eines Beauftragten für den Datenschutz (§ 4f)	810	6
3. Aufgaben des Datenschutzbeauftragten (§ 4g)	810	8
4. Datenvermeidung und Datensparsamkeit (§ 3a BDSG)	810	12
5. Rechte des Betroffenen (§§ 6, 19, 33ff.)	810	15
6. Verarbeitung oder Nutzung personenbezogener Daten im Auftrag (§ 11)	810	16
7. Besondere Maßnahmen zur Datensicherung nach § 9 BDSG	810	18
8. Schadensersatz (§ 7)	810	20
9. Bußgeld- und Strafvorschriften (§§ 43, 44)	810	21
Beiträge zu Sicherheitsanforderungen	830	1
Beiträge zu Anforderungen an die Ordnungsmäßigkeit der Datenverarbeitung	840	1
Problematik der ex ante-Revision	850	1
1. Definition	850	1
2. Voraussetzungen	850	1

	Kennz.	Seite
3. Probleme während der ex ante-Revision	850	2
4. Problematik bei nachgelagerten Prüfungen	850	3
5. Schlussfolgerungen	850	4
6. Prüf-Checklisten	850	4
Prüfung zur Qualitätssicherung nach DIN ISO 9000:2000 ff.	860	1
Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU).....	870	1
1. Vorbemerkungen.....	870	1
2. Checkliste	870	2
Grundlagen	900	1
Stellungnahme FAMA 1/1987 (Nachdruck): Grundsätze ordnungsmäßiger Buchführung bei computerunter- stützten Verfahren und deren Prüfung	910	1
Stellungnahme FAMA 1/1995 (Nachdruck): Aufbewahrungspflichten beim Einsatz von EDI.....	911	1
Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme GoBS (Nachdruck).....	920	1
Verzeichnis wesentlicher Dokumentationskomponenten im Rah- men einer ordnungsmäßigen Buchführung bei Einsatz von Infor- mationstechnologie in Finanzinstituten, Prüfungsverband deut- scher Banken e.V. (Nachdruck)	930	1
Informationsquellen zu Revisionsprüfungen der Standardsoftware SAP	960	1
1. SAP Online Support System (OSS).....	960	1
2. SAP-Arbeitskreis Revision	960	1
3. Internetadressen und News-Groups	960	3
4. Seminare und Literatur	960	3