Eine Veröffentlichung des ISACA Germany Chapter e.V.

ISACA-Leitfaden

und Nachschlagewerk

IDW PS 330 ↔ DIN ISO/IEC 27001 Referenztabelle

ISACA®
Trust in, and value from, information systems
Germany Chapter

dpunkt.verlag

Impressum

Herausgeber:
ISACA Germany Chapter e.V.
Postfach 18 03 99
60084 Frankfurt/Main
E-Mail: webmaster@isaca.de
http://www.isaca.de

Redaktion: Andreas Teuscher, SICK AG

Verantwortliches Gremium:
ISACA Germany Chapter
Fachgruppe Informationssicherheit
ISO 27xxx

Lektorat: Vanessa Wittmer
Copy-Editing: Ursula Zimpfer, Herrenberg
Satz + Herstellung: komplus GmbH, Heidelberg
Umschlaggestaltung: Helmut Kraus, www.exclam.de
Druck: Wörmann PRODUCTIONCONSULT, Heidelberg

ISACA-Leitfaden und Nachschlagewerk

IDW PS 330 ←→ DIN ISO/IEC 27001

Referenztabelle

Inhaltsübersicht

1 Einleitung

Wissen und Informationen bilden einen erheblichen Teil des immateriellen Vermögens eines Unternehmens. Firmen-Know-how und Unternehmensdaten angemessen zu schützen, sei es vor unerlaubter Manipulation, Diebstahl oder Verlust, liegt im Interesse jedes Unternehmers und wird zunehmend auch von anderen Anteilseignern und Geschäftspartnern (Stakeholdern) eingefordert. Der Schutz und die Prüfung der eingesetzten Informationstechnologie (IT) in einem Unternehmen oder einer Organisation, die zum Speichern und Verarbeiten der Informationen eingesetzt wird, sind hierbei also von besonderer Bedeutung.

Dieser Praxis-Leitfaden stellt eine Zuordnung des ISO/IEC-2700x-Standards zu den Prüfvorschriften des Instituts der deutschen Wirtschaftsprüfer (IDW) her, insbesondere zum Prüfstandard (PS) IDW PS 330. Der Leitfaden wurde strukturell an diesem Prüfstandard ausgerichtet. Die Tabellen beschränken sich auf eine Zuordnung von Prüfkriterien von IDW PS 330 (2002) zu Anforderungen aus der deutschsprachigen DIN ISO/IEC 27001:2008-09. Weitere IDW- und ISO-Standards sind aufgeführt, soweit sie relevant sind. Sie wurden aber nicht detailliert analysiert und in die Analysen oder den Leitfaden einbezogen. Gleiches gilt für Gesetze, Verordnungen oder weitere referenzierte Dokumente. Die Auflistung in den Tabellen erhebt keinen Anspruch auf Vollständigkeit.

Unternehmen, die ihre IT an den Vorgaben der ISO/IEC 27001 ausrichten oder ein entsprechendes Informationssicherheits-Managementsystem (ISMS) aufgebaut haben, bekommen mit diesem Leitfaden eine wertvolle Hilfestellung an die Hand, die sie dabei unterstützt, festzustellen, welche IDW-Grundsätze durch die Umsetzung der für ihre Organisation zutreffenden Vorgaben aus der ISO/IEC 27001 bereits erfüllt werden. Sie erhalten damit einen Überblick, inwieweit die umgesetzten Maßnahmen der ISO/IEC 27001 den Anforderungen des IDW PS 330 genügen.

Der Leitfaden unterstützt sie, den Nachweis zu erbringen, dass ein adäquates, internes Kontrollsystem (IKS) im Bereich der IT nach den Vorgaben des IDW PS 330 existiert, wenn bereits relevante Controls und Prozesse auf Basis von ISO/IEC 27001 in ihrem Unternehmen implementiert wurden. Dazu wurde die Auswahl der IDW-Vorgaben aus PS 330 den Kriterien der ISO/IEC 27001 zugeordnet. Auf einfache Art und Weise kann man so herausfinden, ob Deltas vorhanden sind und wenn ja, in welchen Bereichen. Die Synergien kann man sich außerdem bei der Durchführung von internen und externen Audits und Abschlussprüfungen zunutze machen.

Der Praxis-Leitfaden wurde in erster Linie unter dem Gesichtspunkt »aus der Praxis, für die Praxis« erstellt. Er soll Anwendern eine Hilfestellung bieten und sie in die Lage versetzen, eine Übersicht über die Anforderungen zu bekommen, die sowohl aus der ISO/IEC 27001 als auch aus dem IDW PS 330 an eine Organisation gestellt werden.

Die Ziele der **Fachgruppe Informationssicherheit ISO 27xxx** des ISACA Germany Chapter e.V. sind u.a. das Zuordnen relevanter Standards wie z.B. COBIT, PS 330 u.a. im Hinblick auf die ISO-27000-Normenreihe und die Identifikation von IT-Compliance-Anforderungen, die mit der ISO-27000-Normenreihe angemessen beantwortet werden können.

2 Erläuterungen

Die in diesem Dokument genutzten *Abkürzungen* sind im Abkürzungsverzeichnis zusammengefasst und aufgeschlüsselt.
Fachbegriffe, die in den Standards genutzt werden und in diesem Zusammenhang ggf. eine besondere Bedeutung haben, sind im Glossar erläutert. Die Quelle(n), woher die Erläuterung stammt, ist (sind) dort ebenfalls aufgeführt.
Einige *Begriffe und Abkürzungen*, wie z.B. IT, Tz oder Utilitie sind nicht aufgeschlüsselt bzw. erläutert, wenn davon ausgegangen wird, dass die Abkürzung oder der Begriff ein gebräuchliches »Wort« ist, das in dem hier dargestellten Umfeld bekannt ist und regelmäßig genutzt wird.
Referenzen auf genutzte und weiterführende Dokumente/Standards sind am Ende des Dokumentes zusammen aufgelistet.

Erläuterungen zur Lesart der Referenztabelle

Die Tabellen ab Kapitel 4 sind analog zu der Struktur des IDW PS 330 und numerisch aufsteigend nach den jeweiligen Textziffern (Tz) aufgebaut. Diese Textziffern sind – wie in IDW PS 330 auch – in runden Klammern aufgeführt. Es kann vorkommen, dass in den Tabellen einzelne Textziffern, wie z.B. (1) bis (7), nicht aufgeführt bzw. ausgelassen sind, wenn sie in dem hier betrachteten Zusammenhang als nicht relevant erachtet wurden.

Die Textziffer aus IDW PS 330 steht jeweils links in der grau unterlegten Zeile. Rechts steht eine Zusammenfassung des entsprechenden Textes aus IDW PS 330.

In den folgenden Zeilen der Tabelle sind rechts Kapitel der ISO/IEC 27001 oder eine Maßnahmennummer aus dem Anhang A der ISO/IEC 27001 aufgelistet. Der Bezug zu einem Kapitel aus der ISO/IEC 27001 ist an der entsprechenden Kapitelnummer erkenntlich. Die Referenz auf eine Maßnahme aus dem Anhang beginnt jeweils mit dem Buchstaben »A« gefolgt von der Maßnahmennummer. Wenn auf eine spezielle Anforderung in einem Kapitel der ISO/IEC 27001 verwiesen wird, ist der Kapitelnummer noch ein kleiner Buchstabe angehängt (z.B. 4.2.1g), der auf den entsprechenden Absatz hinweist. Rechts von den jeweiligen Nummern steht entweder die Kapitelüberschrift oder die Anforderung. Die Reihenfolge ist aufsteigend und ohne Wertung.

Soweit relevant sind Referenzen auf weitere Prüfstandards, Gesetze oder internationale Standards aufgeführt. Da der Fokus der Referenztabelle bewusst auf IDW PS 330 und ISO/IEC 27001 beschränkt wurde, sind sie als ergänzende Informationen zu verstehen. Sie sind grau und kursiv gedruckt.

Beispiel

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO/IEC 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
4.3.2	Lenkung von Dokumenten
4.2.1g	Auswahl der Maßnahmenziele und Maßnahmen für die Risikobehandlung
A.7.1.1	Inventar der organisationseigenen Werte (Assets)
Gesetze	*HGB, AO, BDSG, SGB*

Ergänzende Hinweise

Die im Anhang der ISO/IEC 27001 aufgeführten Maßnahmenziele und Maßnahmen wurden direkt aus denen in ISO/IEC 27002, Kapitel 5 bis 15, abgeleitet. Das heißt die Anforderung, die beispielsweise unter A.7.1.1 im Anhang der ISO/IEC 27001 spezifiziert ist, ist in Kapitel 7.1.1 der ISO/IEC 27002 wiederzufinden. In ISO/IEC 27002 sind die im Anhang A der ISO/IEC 27001 spezifizierten Maßnahmen durch Anleitungen zur Umsetzung und weitere Informationen ergänzt.

Zum Teil wurden Passagen aus den referenzierten Unterlagen sinngemäß zusammengefasst und/oder ins Deutsche übersetzt, wenn ein Dokument, wie z.B. ISO/IEC 27006, zurzeit nur in der englischsprachigen Version veröffentlicht ist.

3 Zusammenfassung

Unternehmen sind heutzutage einer Vielzahl von Compliance-Anforderungen ausgesetzt. Viele Personen und Institutionen fordern Prüfungen, Audits und/oder Nachweise. Dazu zählen die interne Revision, der Wirtschaftsprüfer, das Finanzamt genauso wie Kunden und Teilhaber. Auch wenn die Schwerpunkte der jeweiligen Prüfungen unterschiedlich sein mögen: Im Wesentlichen haben sie doch ein gemeinsames Ziel. Durch die Prüfung/das Audit soll nachgewiesen werden, dass das Geprüfte ordnungsgemäß funktioniert.

Für Unternehmen ist erstrebenswert, Synergien zu nutzen und den Gesamtaufwand für Planung, Implementierung und Pflege von Maßnahmen, das Führen von Nachweisen und auch die Anzahl und den Umfang von Prüfungen zu reduzieren.

Hierzulande setzt nahezu jedes Unternehmen Informationstechnologie ein, um seine Geschäftsprozesse abwickeln zu können – auch für die Buchhaltung und das Erstellen der Bilanz. Daher sollten Maßnahmen zur Informationssicherheit und der ordnungsgemäße Betrieb der IT selbstverständlich sein. Ebenso selbstverständlich ist, dass der Abschlussprüfer die IT-Systeme prüft, die rechnungslegungsrelevante Daten verarbeiten.
Gut und nützlich wäre es daher für alle Beteiligten, wenn die erfolgreiche Umsetzung von Maßnahmen zur Informationssicherheit dem Wirtschaftsprüfer als Nachweis für ein wirksam funktionierendes internes Kontrollsystem dienen.
Aus diesem Grund sind der Prüfstandard der Wirtschaftsprüfer und der internationale Standard für Informationssicherheits-Managementsysteme gegenübergestellt worden.

Die Ziele des Leitfadens sind:

- Überschneidungen und Synergien zwischen dem Prüfstandard der Wirtschaftsprüfer und internationalen Normen aufzeigen.
- Einen Ratgeber für Unternehmen und IT-Verantwortliche zur Verfügung stellen, die ein Informationssicherheits-Managementsystem (ISMS) nach ISO/IEC 27001 aufgebaut oder zumindest nach den Vorgaben dieser Norm ausgerichtet haben und wissen wollen, welche Anforderungen der Wirtschaftsprüfungsgesellschaften an die Unternehmens-IT bereits durch die Norm abdeckt werden.
- Tabellarisch darstellen, welche Anforderungen sich aus der ISO/IEC 27001 und dem Prüfstandard des IDW PS 330 überschneiden.
- IT-Compliance-Anforderungen der beiden Standards zu konsolidieren und Interessenten in einer aufbereiteten und praxistauglichen Form zur Verfügung stellen.

Der Vergleich zwischen ISO/IEC 27001 und IDW PS 330 zeigt, dass erhebliche Synergieeffekte genutzt werden können. Das heißt eine Anforderung aus einem der Standards kann als erfüllt bzw. erfüllbar angesehen werden, wenn die zugeordneten Maßnahmen aus dem anderen Standard erfüllt sind – jeweils unter der Voraussetzung, dass der Anwendungsbereich passend ist.
Der Vergleich hat aber auch ergeben, dass ISO/IEC 27001 allein nicht ausreicht, um sämtliche Anforderungen, die IDW PS 330 enthält, abzubilden. Kriterien hinsichtlich Prüfer, Prüfumfang und -durchführung sind in separaten ISO-Normen geregelt.

4 Ziele und Umfang von IT-Systemprüfungen

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
(8)	Scope umfasst die IT-gestützten Rechnungslegungssysteme, die direkt oder als Vorsysteme an der Erstellung des Jahresabschlusses beteiligt sind.
4.2.1	Festlegen des ISMS a) Definition des Anwendungsbereichs und der Grenzen des ISMS j) Erstellung einer Erklärung der Anwendbarkeit
A.7.1.1	Inventar der organisationseigenen Werte (Assets)
A.7.1.2	Eigentum von organisationseigenen Werten
A.7.1.3	Zulässiger Gebrauch von organisationseigenen Werten
A.15.1.1	Identifikation der anwendbaren Gesetze
Gesetze	*HGB, AO, BDSG, SGB*
ISO 38500	*3.2 Prinzipien 1: Verantwortung, Nutzung und zukünftige Nutzung von IT*
ISO 38500	*3.6 Prinzipien 5: Konformität, regelmäßige Untersuchung von regulativen und gesetzlichen Anforderungen*
(9)	IT-Kontrollsystem ist Teil des internen Kontrollsystems – Systemprüfungen haben das Ziel einer Risikobeurteilung.
4.2.2	Umsetzen und Durchführen des ISMS
4.2.3	Überwachen und Prüfen des ISMS
4.2.4	Instandhalten und Verbessern des ISMS
ISO 27005	*7.2 Grundlegende Kriterien, Risiko-Untersuchungskriterien, Risiko-Akzeptanzkriterien*
ISO 38500	*2 Rahmenwerk für »Good Corporate Governance« in der IT*

4.1 Risiken aus dem Einsatz von IT

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
(15)	Durchführen von Risikobeurteilungen zum Einsatz von IT, die die Entwicklung des Unternehmens beeinträchtigen oder der Erreichung der Unternehmensziele entgegenwirken können.
4.2.1	Festlegen des ISMS
4.2.2	Umsetzen und Durchführen des ISMS
A.5	Sicherheitsleitlinie
A.6	Organisation der Informationssicherheit
A.6.2.1	Identifizierung von Risiken in Zusammenhang mit externen Mitarbeitern
ISO 27002	*4.1 Einschätzung der Sicherheitsrisiken*
ISO 27002	*4.2 Umgang mit Sicherheitsrisiken*
ISO 27005	*8.2.1.2 Identifikation von Werten* *8.2.1.3 Identifikation von Bedrohungen* *Annex A, A1 Untersuchung der Organisation* *Annex C, Beispiele für typische Bedrohungen*
ISO 38500	*3.5 Prinzipien 4: Leistung*
(18)	Vernetzung mit anderen Geschäftspartnern und Behörden
A.6.1.6	Kontakt zu Behörden
A.6.1.7	Kontakt zu speziellen Interessengruppen

4.2 Vorgehensweise bei der IT-Systemprüfung

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
(26)	Vorgehensweise bei der IT-Systemprüfung risikoorientiert zur Aufdeckung wesentlicher Fehler in der Rechnungslegung.
A.15.2.1	Einhaltung von Sicherheitsleitlinien und -standards
A.15.2.2	Prüfung der Einhaltung technischer Vorgaben
A.15.3.1	Maßnahmen für Audits von Informationssystemen
(29)	Prüfungsschritte: Aufnahme des IT-Systems, Aufbauprüfung, Funktionsprüfung.
6	Interne ISMS-Audits
A.7.1.1	Inventar der organisationseigenen Werte (Assets)
ISO 17021	*9.2.3.1 Audit der Stufe 1*
ISO 19011	*6.3 Durchführung der Dokumentenprüfung*
ISO 27006	*9.2.3.2 Audit der Stufe 2*
(40)	Abwägung von Wirksamkeit und Wirtschaftlichkeit bei der Verwendung von Arbeiten und Berichten von Dritten (z.B. Interne Revision, Externe Sachverständige).
A.15.3.2	Schutz von Revisionswerkzeugen für Informationssysteme
ISO 17021	*4.2 Unparteilichkeit, 4.2.1-4.2.4*
ISO 19011	*4 Prinzipien der Auditdurchführung*

4.3 Besonderheit des risikoorientierten Prüfungsansatzes

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
(42) – (44)	Ausgestaltung des risikoorientierten Prüfungsansatzes (funktional oder prozessorientiert) für das zu prüfende Unternehmen
4.2.1 a	Festlegen des ISMS – Definition des Anwendungsbereichs
4.2.1 e	Analyse und Bewertung der Risiken
6	Interne ISMS-Audits
A.6.1.8	Unabhängige Überprüfung der Informationssicherheit
ISO 19011	*5.2 Ziele und Umfang des Auditprogramms*

5 Durchführung von IT-Systemprüfungen

5.1 Auftragsannahme und Prüfungsplanung

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
(45) – (46)	Kenntnisse und Erfahrung der Prüfer und der bei der Prüfung eingesetzten fachlichen Mitarbeiter
5.2.2	Schulungen, Bewusstsein und Kompetenz
6	Interne ISMS-Audits
A.6.1.8	Unabhängige Überprüfung der Informationssicherheit
ISO 17021	*4.3 Kompetenz*
ISO 17021	*7.1 Kompetenz der Leitung und des Personals*
ISO 17021	*7.2 Personal, das in die Zertifizierungstätigkeiten einbezogen ist*
ISO 19011	*7.3 Kenntnisse und Fähigkeiten*
ISO 27006	*7.1 Kompetenz von Management und Personal*
ISO 27006	*7.2 Personal, das in die Zertifizierungstätigkeiten einbezogen ist*
(47)	Einbeziehen von Ergebnissen anderer (IT-)Sachverständigen
6	Interne ISMS-Audits
A.6.1.8	Unabhängige Überprüfung der Informationssicherheit
ISO 17021	*9.1.1 Allgemeine Anforderungen*
(48)	Planung der IT-Systemprüfung unter Berücksichtigung der Bedeutung von IT im Unternehmen (Auswirkung des Einsatzes), des Umgangs mit IT-Risiken und der Organisation der IT-gestützten Geschäftsprozesse
4.2.1 a	Festlegen des ISMS – Definition des Anwendungsbereichs
4.2.1 c-g	Methode, Identifizieren von Risiken, Analysieren und Bewerten, Optionen für die Risikobehandlung, Maßnahmen zur Risikobehandlung
6	Interne ISMS-Audits
A.7.1.2	Eigentum von organisationseigenen Werten (Assets)
ISO 27006	*9.1.2 Umfang der Zertifizierung (des Audits)*
ISO 17021	*9.1.2 Allgemeine Anforderungen*

5.2 Erhebung von Informationen

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
(49)	Erheben der rechnungslegungsrelevanten (IT-Systemelemente).
4.2.1 d	Identifizierung der organisationseigenen Werte (Assets) innerhalb des Anwendungsbereichs ...
A.7.1.1	Inventar der organisationseigenen Werte (Assets)
ISO 17021	*9.2.3.1.1 c Identifizierung von Schlüsselleistungen bzw. bedeutsamen Aspekten, Prozessen, …*
(50)	Zugeordnetes IT-Überwachungssystem bestehend aus • IT-Umfeld • IT-Organisation • IT-Infrastruktur • IT-Anwendungen • IT-Geschäftsprozesse
4.2.1 b	ISMS-Leitlinie unter Berücksichtigung der Eigenschaften des Geschäfts
A.10	Betriebs- und Kommunikationsmanagement
A.12	Beschaffung, Entwicklung und Wartung von Informationssystemen
ISO 17021	*9.2.3.1.1 d … notwendige Informationen zu sammeln bezüglich des Geltungsbereichs …*

5.3 Prüfung des IT-Umfelds und der IT-Organisation

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
(51)	Prüfung auf Basis des Sicherheitskonzept, der IT-Strategie, Regelungen, Richtlinien, Prozess- und Funktionsbeschreibungen. Prüfkriterien sind u.a. Vollständigkeit, Aktualität, Organisationsprinzipien (Funktionstrennung etc.).
4.2.3 f	Durchführung einer regelmäßigen Managementbewertung
A.5.1.1	Leitlinie zur Informationssicherheit
A.6.1.1	Engagement des Managements für Informationssicherheit
A.6.1.2	Koordination der Informationssicherheit
A.6.1.3	Zuweisung der Verantwortlichkeiten für Informationssicherheit
A.6.1.4	Genehmigungsverfahren für informationsverarbeitende Einrichtungen
A.6.1.5	Vertraulichkeitsvereinbarungen
A.7.1.2	Eigentum von organisationseigenen Werten (Assets)
A.8.1.1	Aufgaben und Verantwortlichkeiten
A.8.2.1	Verantwortung des Managements
A.10.1.1	Dokumentierte Betriebsprozesse
A.10.1.3	Aufteilung von Verantwortlichkeiten
A.14.1.1	Einbeziehung der Informationssicherheit in den Prozess zur Sicherstellung des Geschäftsbetriebs
A.15.2.1	Einhaltung von Sicherheitsleitlinien und -standards
A.15.2.2	Prüfung der Einhaltung technischer Vorgaben
ISO 17021	*9.2.3.2 Audits der Stufe 2 zur Beurteilung der Umsetzung und Wirksamkeit*
(52)	Prüfung der Wirksamkeit • anhand von Stichproben • Verifizieren von Maßnahmen anhand von Regelungen • Beobachten von Abläufen und Vergleich mit Richtlinien • Vergleich von Richtlinien mit der technischen Umsetzung
6	Interne ISMS-Audits
A.6.1.8	Unabhängige Überprüfung der Informationssicherheit
ISO 17021	*9.2.3.2 Audit der Stufe 2 hinsichtlich Informationen und Nachweisen über die Konformität*
ISO 19011	*6.5.4 Erfassen und Verifizieren von Informationen*
ISO 27006	*9.2.3.2.1 Audit der Stufe 2 um zu bestätigen, dass die Organisation ihre eigenen Richtlinien, Ziele und Verfahren befolgt*
ISO 27006	*9.2.3.2.2 d Audit der Stufe 2 mit Fokus auf die Überprüfung und Bewertung der Wirksamkeit*

5.4 Prüfung der IT-Infrastruktur

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
(54)	Physische Sicherungsmaßnahmen, u.a. bauliche Maßnahmen, Zugangskontrollen, Brandschutz und Sicherheit der Stromversorgung; Gewährleistung der Datensicherheit, des Datenschutzes, der Datenintegrität und der Datenverfügbarkeit
4.2.1 d	Identifizierung der Risiken
4.2.1 e	Analyse und Bewertung der Risiken
A.6.2.1	Identifizierung von Risiken in Zusammenhang mit externen Mitarbeitern
A.6.2.2	Adressieren von Sicherheit im Umgang mit Kunden
A.6.2.3	Adressieren von Sicherheit in Vereinbarungen mit Dritten
A.8.3.3	Aufheben von Zugangsrechten
A.9.1.1	Sicherheitszonen

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
A.9.1.2	Zutrittskontrolle
A.9.1.3	Sicherung von Büros, Räumen und Einrichtungen
A.9.1.4	Schutz vor Bedrohungen von außen und aus der Umgebung
A.9.2.1	Platzierung und Schutz von Betriebsmitteln
A.9.2.2	Unterstützende Versorgungseinrichtungen
A.9.2.3	Sicherheit der Verkabelung
A.9.2.4	Instandhaltung von Gerätschaften
A.10.6.1	Maßnahmen für Netze
A.15.1.4	Datenschutz und Vertraulichkeit von personenbezogenen Daten
ISO 27002	*4.1 Einschätzung der Sicherheitsrisiken*
ISO 27002	*4.2 Umgang mit Sicherheitsrisiken*
IDW RS FAIT	*Tz 23: Sicherheitsanforderungen an IT-Systeme (Vertraulichkeit, Integrität, Verfügbarkeit, Autorisierung, Authentizität, Verbindlichkeit)*
(55)	Beurteilung der Angemessenheit umgesetzter technischer und organisatorischer Sicherheitsmaßnahmen im Hinblick auf den gewählten Geltungsbereich und die definierten Schutzziele
	Wie (54) und zusätzlich:
4.2.1 a	Definition des Anwendungsbereichs und der Grenzen des ISMS
4.2.1 g	Auswahl der Maßnahmenziele und Maßnahmen für die Risikobehandlung
4.2.2 b	Umsetzung des Risikobehandlungsplans
4.2.3	Überwachen und Überprüfen des ISMS
7	Managementbewertung des ISMS
8.2	Korrekturmaßnahmen
8.3	Vorbeugungsmaßnahmen
(56)	Durch eine Vor-Ort-Begehung des Rechenzentrums bzw. des Rechnerraums werden sowohl die Existenz als auch die Funktionsfähigkeit technischer Sicherungsmaßnahmen anhand von Stichproben überprüft.
	Wie (54) und (55) und zusätzlich:
6	Interne ISMS-Audits
7.2 a	Ergebnisse der ISMS-Audits und -Überprüfungen
7.2 d	Status von Korrekturmaßnahmen und Vorbeugungsmaßnahmen
ISO 17021	*9.1.9 Die Zertifizierungsstelle muss über einen Prozess zur Durchführung der Vor-Ort-Audits verfügen …*
ISO 17021	*9.9.2 Aufzeichnungen zu zertifizierten Kunden müssen Folgendes enthalten: c) Begründung für die verwendete Methodik zur Stichprobenprüfung;*
(57)	Ziel ist die Gewährleistung der Vertraulichkeit und Authentizität. Die Beantragung, Genehmigung und Einrichtung von Benutzer-berechtigungen in IT-Systemen, sowohl auf Betriebs-systemebenen und IT-Anwendungen muss durch einen entsprechenden organisatorischen und auditierbaren Prozess geregelt sein. Das Berechtigungskonzept und die Berechtigungsverwaltung müssen im Einklang mit der Risikobeurteilung des Unternehmens stehen. Unberechtigte Datenzugriffe und Datenmanipulationen sind zu verhindern und die Identitäten der Benutzer müssen eindeutig feststellbar sein.
4.2.1 d	Identifizierung der Risiken
4.2.1 e	Analyse und Bewertung der Risiken
4.2.1 f	Identifizierung und Bewertung der Optionen für die Risikobehandlung
4.2.1 g	Auswahl der Maßnahmenziele und Maßnahmen für die Risikobehandlung
4.2.2 b	Umsetzung des Risikobehandlungsplans
A.6.2.3	Adressieren von Sicherheit in Vereinbarungen mit Dritten
A.8.1.1	Aufgaben und Verantwortlichkeiten
A.8.1.2	Überprüfung
A.8.3.1	Verantwortlichkeiten bei der Beendigung

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
A.8.3.3	Aufheben von Zugangsrechten
A.10.1.1	Dokumentierte Betriebsprozesse
A.10.1.2	Änderungsverwaltung
A.10.1.3	Aufteilung von Verantwortlichkeiten
A.10.1.4	Trennung von Entwicklungs-, Test- und Produktiveinrichtungen
A.10.10.1	Auditprotokolle
A.10.10.2	Überwachung der Systemnutzung
A.10.10.3	Schutz von Protokollinformationen
A.10.10.4	Administrator- und Betreiberprotokoll
A.10.10.6	Zeitsynchronisation
A.11.1.1	Regelwerk zur Zugangskontrolle
A.11.2.1	Benutzerregistrierung
A.11.2.2	Verwaltung von Sonderrechten
A.11.2.3	Verwaltung von Benutzerpasswörtern
A.11.2.4	Überprüfung von Benutzerberechtigungen
A.11.3.1	Passwortverwendung
A.11.4.1	Regelwerk zur Nutzung von Netzdiensten
A.11.4.2	Benutzerauthentisierung für externe Verbindungen
A.11.4.5	Trennung in Netzwerken
A.11.4.6	Kontrolle von Netzverbindungen
A.11.4.7	Routingkontrolle für Netze
A.11.5.1	Verfahren für sichere Anmeldung
A.11.5.2	Benutzeridentifikation und Authentisierung
A.11.5.3	Systeme zur Verwaltung von Passwörtern
A.11.5.4	Verwendung von Systemwerkzeugen
A.11.6.1	Einschränkung von Informationszugriffen
A.11.6.2	Isolation sensibler Systeme
A.15.1.4	Datenschutz und Vertraulichkeit von personenbezogenen Informationen
A.15.1.5	Verhinderung des Missbrauchs von informationsverarbeitenden Einrichtungen
ISO 27002	*4.1 Einschätzung der Sicherheitsrisiken*
ISO 27002	*4.2 Umgang mit Sicherheitsrisiken*
IDW RS FAIT	*Tz 23: Sicherheitsanforderungen an IT-Systeme (Vertraulichkeit, Integrität, Verfügbarkeit, Autorisierung, Authentizität, Verbindlichkeit)*
(58)	Überprüfung der Wirksamkeit logischer Zugriffskontrollen. Bei der Benutzeradministration und -pflege werden definierte Verfahren und tatsächliche Abläufe einander gegenübergestellt. Es wird auch geprüft, ob eingerichtete Berechtigungen a) den beantragten Rechten und b) dem tatsächlichen Aufgabengebiet des Mitarbeiters entsprechen.
	Wie (57) und zusätzlich:
6	Interne ISMS-Audits
7.2 a	Ergebnisse der ISMS-Audits und -Überprüfungen
7.2 d	Status von Korrekturmaßnahmen und Vorbeugungsmaßnahmen
ISO 17021	*9.1.9 Die Zertifizierungsstelle muss über einen Prozess zur Durchführung der Vor-Ort-Audits verfügen …*
ISO 17021	*9.9.2 Aufzeichnungen zu zertifizierten Kunden müssen Folgendes enthalten c) Begründung für die verwendete Methodik zur Stichprobenprüfung*
(59)	Datensicherungs- und -auslagerungsverfahren sind eine zentrale Voraussetzung für die Funktionsfähigkeit der Datenverarbeitung sowie der Verfügbarkeit der Daten und Programme.
4.2.1 d	Identifizierung der Risiken
4.2.1 e	Analyse und Bewertung der Risiken

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
4.2.1 f	Identifizierung und Bewertung der Optionen für die Risikobehandlung
4.2.1 g	Auswahl der Maßnahmenziele und Maßnahmen für die Risikobehandlung
A.9.1.1	Sicherheitszonen
A.9.1.2	Zutrittskontrolle
A.9.1.3	Sicherung von Büros, Räumen und Einrichtungen
A.9.1.4	Schutz vor Bedrohungen von außen und aus der Umgebung
A.10.1.1	Dokumentierte Betriebsprozesse
A.10.5.1	Back-up von Informationen
A.10.10.3	Schutz von Protokollinformationen
A.10.10.5	Fehlerprotokolle
A.10.10.6	Zeitsynchronisation
A.14.1.2	Sicherstellung des Geschäftsbetriebs und Risikoeinschätzung
A.14.1.3	Entwickeln und Umsetzen von Plänen zur Sicherstellung des Geschäftsbetriebs, die Informationssicherheit enthalten
A.14.1.4	Rahmenwerk für die Pläne zur Sicherstellung des Geschäftsbetriebs
(60)	Überprüfung der Funktionsfähigkeit des Datensicherungsverfahrens.
	Wie (59) und zusätzlich:
4.2.2 b	Umsetzung des Risikobehandlungsplans
6	Interne ISMS-Audits
7.2 a	Ergebnisse der ISMS-Audits und -Überprüfungen
7.2 d	Status von Korrekturmaßnahmen und Vorbeugungsmaßnahmen
ISO 17021	*9.1.9 Die Zertifizierungsstelle muss über einen Prozess zur Durchführung der Vor-Ort-Audits verfügen …*
ISO 17021	*9.9.2 Aufzeichnungen zu zertifizierten Kunden müssen Folgendes enthalten: c) Begründung für die verwendete Methodik zur Stichprobenprüfung*
(61)	Einhaltung von gesetzlichen Aufbewahrungsfristen.
	Wie (59) und (60) und zusätzlich:
5.2.1 c	Gesetzliche und amtliche Anforderungen und vertragliche Sicherheitsverpflichtungen identifizieren und behandeln
A.15.1.1	Identifikation der anwendbaren Gesetze
A.15.1.3	Schutz von organisationseigenen Aufzeichnungen
A.15.1.4	Datenschutz und Vertraulichkeit von personenbezogenen Informationen
(62)	Maßnahmen für einen geordneten Regelbetrieb der IT sind in Abhängigkeit der Art und Komplexität der eingesetzten Hardware und der Netzwerkkomponenten festzulegen. Dazu gehören organisatorische Anweisungen sowie technische Systeme und Anwendungen.
4.2.1 d	Identifizierung der Risiken
4.2.1 e	Analyse und Bewertung der Risiken
4.2.1 f	Identifizierung und Bewertung der Optionen für die Risikobehandlung
4.2.1 g	Auswahl der Maßnahmenziele und Maßnahmen für die Risikobehandlung
A.7.2.1	Regelungen für die Klassifizierung
A.7.2.2	Kennzeichnung von und Umgang mit Informationen
A.10.1.1	Dokumentierte Betriebsprozesse
A.10.1.2	Änderungsverwaltung
A.10.1.3	Aufteilung von Verantwortlichkeiten
A.10.1.4	Trennung von Entwicklungs-, Test- und Produktiveinrichtungen
A.10.3.2	Systemabnahme
A.10.5.1	Back-up von Informationen
A.10.6.1	Maßnahmen für Netze
A.10.10.2	Überwachung der Systemnutzung
A.10.10.6	Zeitsynchronisation

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
A.11.2.3	Verwaltung von Benutzerpasswörtern
A.11.4.1	Regelwerk zur Nutzung von Netzdiensten
A.11.4.2	Benutzerauthentisierung für externe Verbindungen
A.11.6.1	Einschränkung von Informationszugriffen
A.11.6.2	Isolation sensibler Systeme
A.12.2.2	Kontrolle der internen Verarbeitung
A.12.4.1	Kontrolle von Software im Betrieb
A.12.4.2	Schutz von Testdaten
A.12.4.3	Zugangskontrolle zu Quellcode
A.15.1.4	Datenschutz und Vertraulichkeit von personenbezogenen Informationen
(63) – (64)	Die für den geordneten Regelbetrieb definierten Abläufe müssen hinreichend geregelt, dokumentiert und angemessen sein. Die Abwicklung und Funktionsweise von IT-Anwendungen muss nachvollziehbar sein (z.B. durch Jobprotokolle). Die sachgerechte Umsetzung von Organisationsanweisungen wird durch Einsichtnahme in die Aufzeichnungen der IT-Systeme, durch Abgleich der Anweisungen zur Jobdokumentation mit den tatsächlichen Jobs und durch vorhandene Protokolle überprüft.
	Wie (62) und zusätzlich:
6	Interne ISMS-Audits
7.2 a	Ergebnisse der ISMS-Audits und -Überprüfungen
7.2 d	Status von Korrekturmaßnahmen und Vorbeugungsmaßnahmen
A.10.9.2	Online-Transaktionen
A.10.10.3	Schutz von Protokollinformationen
A.10.10.4	Administrator- und Betreiberprotokolle
A.10.10.5	Fehlerprotokolle
A.12.1.1	Analyse und Spezifikation von Sicherheitsanforderungen
A.12.2.2	Kontrolle der internen Verarbeitung
ISO 17021	*9.1.9 Die Zertifizierungsstelle muss über einen Prozess zur Durchführung der Vor-Ort-Audits verfügen …*
ISO 17021	*9.9.2 Aufzeichnungen zu zertifizierten Kunden müssen Folgendes enthalten: c) Begründung für die verwendete Methodik zur Stichprobenprüfung*
(65)	Es müssen neben dem Regelbetrieb auch Maßnahmen für den Notbetrieb und technische Verfahren zur Wiederherstellung der IT nach teilweisem oder vollständigem Ausfall der IT-Infrastruktur festgelegt werden.
	Wie (63) und zusätzlich:
A.12.6.1	Kontrolle technischer Schwachstellen
A.14.1.1	Einbeziehung der Informationssicherheit in den Prozess zur Sicherstellung des Geschäftsbetriebs
A.14.1.2	Sicherstellung des Geschäftsbetriebs und Risikoeinschätzung
A.14.1.3	Entwickeln und Umsetzen von Plänen zur Sicherstellung des Geschäftsbetriebs, die Informationssicherheit enthalten
A.14.1.4	Rahmenwerk für die Pläne zur Sicherstellung des Geschäftsbetriebs
A.14.1.5	Testen, Instandhaltung und Neubewertung von Plänen zur Sicherstellung des Geschäftsbetriebs
(66) – (69)	Festlegen und Überprüfung der Maßnahmen zur Sicherstellung der Betriebsbereitschaft und Verfügbarkeit der IT, inklusive einer Risikobewertung der IT hinsichtlich unternehmensspezifischer Anforderungen und Abhängigkeiten. Zu prüfende Aspekte sind u.a. Notfallhandbücher, Wiederanlaufpläne, technische Sicherungsmaßnahmen, abgeschlossene Versicherungen, redundante Hardware, Back-up, Ausweichrechenzentrum etc.
4.2.1 d	Identifizierung der Risiken
4.2.1 e	Analyse und Bewertung der Risiken
4.2.1 f	Identifizierung und Bewertung der Optionen für die Risikobehandlung
4.2.1 g	Auswahl der Maßnahmenziele und Maßnahmen für die Risikobehandlung
4.2.2 a	Formulierung eines Risikobehandlungsplans

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
4.2.2 b	Umsetzung des Risikobehandlungsplans
5.2.1 c	Gesetzliche und amtliche Anforderungen und vertraglichen Sicherheitsverpflichtungen identifizieren und behandeln
A.6.2.2	Adressieren von Sicherheit im Umgang mit Kunden
A.6.2.3	Adressieren von Sicherheit in Vereinbarungen mit Dritten
A.7.1.1	Inventar der organisationseigenen Werte (Assets)
A.7.2.1	Regelungen für die Klassifizierung
A.9.2.4	Instandhaltung von Gerätschaften
A.10.1.1	Dokumentierte Betriebsprozesse
A.10.3.1	Kapazitätsplanung
A.10.4.1	Maßnahmen gegen Schadsoftware
A.10.4.2	Schutz vor mobiler Software (mobilen Agenten)
A.10.5.1	Back-up von Informationen
A.13.1.1	Melden von Informationssicherheitsereignissen
A.13.1.2	Melden von Sicherheitsschwachstellen
A.14.1.1	Einbeziehung der Informationssicherheit in den Prozess zur Sicherstellung des Geschäftsbetriebs
A.14.1.2	Sicherstellung des Geschäftsbetriebs und Risikoeinschätzung
A.14.1.3	Entwickeln und Umsetzen von Plänen zur Sicherstellung des Geschäftsbetriebs, die Informationssicherheit enthalten
A.14.1.4	Rahmenwerk für die Pläne zur Sicherstellung des Geschäftsbetriebs
A.14.1.5	Testen, Instandhaltung und Neubewertung von Plänen zur Sicherstellung des Geschäftsbetriebs
A.15.1.1	Identifikation der anwendbaren Gesetze
ISO 27002	*4.1 Einschätzung der Sicherheitsrisiken*
ISO 27002	*4.2 Umgang mit Sicherheitsrisiken*
IDW RS FAIT	*Tz 23: Sicherheitsanforderungen an IT-Systeme (Vertraulichkeit, Integrität, Verfügbarkeit, Autorisierung, Authentizität, Verbindlichkeit)*

5.5 Prüfung der IT-Anwendungen

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
(70)	Folgende Punkte müssen sichergestellt werden: • Verfahrensbezogene Anforderungen gemäß GoB • Anforderungen an die Softwaresicherheit und rechnungslegungsrelevante Verarbeitungsregeln • Einrichtung von anwendungsbezogenen IT-Kontrollen (Eingabe-, Verarbeitungs- und Ausgabekontrollen) • Einrichtung von generellen Kontrollen bezogen auf den Auswahl- und Entwicklungsprozesses sowie Implementierung • Einrichtung von anwendungsbezogenen Zugriffskontrollen im Kontext logischer Zugriffskontrollen
A.6.1.1	Engagement des Managements für Informationssicherheit
A.6.1.3	Zuweisung der Verantwortlichkeiten für Informationssicherheit
A.6.1.4	Genehmigungsverfahren für informationsverarbeitende Einrichtungen
A.6.1.5	Vertraulichkeitsvereinbarungen
A.6.1.8	Unabhängige Überprüfung der Informationssicherheit
A.6.2.1	Identifizierung von Risiken in Zusammenhang mit externen Mitarbeitern
A.11.6	Zugangskontrolle zu Anwendungen und Informationen
A.12.1	Sicherheitsanforderungen von Informationssystemen

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
A.12.2.1	Überprüfung von Eingabedaten
A.12.2.4	Überprüfung von Ausgabedaten
A.12.4	Sicherheit von Systemdateien
A.12.5	Sicherheit bei Entwicklungs- und Unterstützungsprozessen
PS 880	*2.1.2 (23 bis 36)*
(72)	Folgende Punkte müssen sichergestellt werden: Angemessenheit und Funktionsfähigkeit der Programmfunktionen und der programminternen IT-Kontrollen im Hinblick auf GoB
A.7.1.1	Inventar der organisationseigenen Werte (Assets)
A.7.1.2	Eigentum von organisationseigenen Werten (Assets)
Gesetze	*HGB §§ 238, 239, 257* *AO §§ 145, 146, 147* *GoBS*
PS 880	*2.1 Voraussetzung für die Verfahrensprüfung ist die Bestandsaufnahme des Prüfungsobjekts (= Anwendungssoftware) und der Testumgebung*
(73)	Umsetzung der gesetzlichen Anforderungen an Funktionalität, Ordnungsmäßigkeit und Sicherheit; Vorliegen einer vollständigen und aktuellen Verfahrensdokumentation (Anwendungs-dokumentation und technische Systemdokumentation).
4.3	Dokumentationsanforderungen
A.12.1	Sicherheitsanforderungen von Informationssystemen
A.15.1.1	Identifikation der anwendbaren Gesetze
(74)	Angemessenheit der Programmfunktionen; Vorhandensein eines Testsystems
A.10.1.4	Trennung von Entwicklungs-, Test- und Produktiveinrichtungen
A.10.5.1	Back-up von Informationen
A.12.2	Korrekte Verarbeitung in Anwendungen
A.12.2.1	Überprüfung von Eingabedaten
A.12.2.2	Kontrolle der internen Verarbeitung
A.12.2.4	Überprüfung von Ausgabedaten
A.12.2.3	Integrität von Nachrichten
A.15.1	Einhaltung gesetzlicher Vorgaben
PS880	*2.1.1.1 Prüfung der notwendigen Verarbeitungsfunktionen (Tz 9-10)* *Feststellung notwendiger Verarbeitungsfunktionen (Beleg-, Journal- und Kontenfunktion) und ordnungsgemäße Buchungen*
PS880	*2.1.1.1 Prüfung der notwendigen Verarbeitungsfunktionen (Tz 11)* *Integritätsanforderungen* *Sicherung gegen Verlust und unberechtigte Veränderungen von relevanten Informationen durch die Software*
PS880	*2.1.1.1 Prüfung der notwendigen Verarbeitungsfunktionen (Tz 12)* *Erfüllung zwingender gesetzlicher Anforderungen* *Erfüllung der Ordnungsmäßigkeit der Rechnungslegung* *Nachvollziehbarkeit der Buchungen aufgrund der Dokumentation*
PS880	*2.1.1.1 Prüfung der notwendigen Verarbeitungsfunktionen (Tz 13-14)* *Überprüfung der Anwendung anhand der Verfahrensdokumentation und Anforderungen an die Verfahrensdokumentation*
PS880	*2.1.1.2 Prüfung der programmierten Verarbeitungsregeln (Tz 15-22)*
(75)	Für die Programmprüfung können auch weitere Informationen wie Fachkonzepte bzw. Protokolle herangezogen werden.
4.3	Dokumentationsanforderungen
A.10.1.1	Dokumentierte Betriebsverfahren
A.10.10	Überwachung
A.15.1.3	Schutz von organisationseigenen Aufzeichnungen

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
(76)	Geprüft wird: • Organisation der Systementwicklung • Auswahlprozess von Standardsoftware • Change-Managementprozess von IT-Anwendungen
A.12	Beschaffung, Entwicklung und Wartung von Informationssystemen
A.12.5.1	Änderungskontrollverfahren
(77) – (78)	Folgende Regelungen und Verfahren werden geprüft: • Entwicklung von Individualsoftware (Prüfung von Grob- u. Feinkonzepten, Projektmanagement, QM-Management, Richtlinien, Dokumentation, Test und Freigabe, Einsatz von Entwicklungstools, Change-Management, Versionsmanagement) • Auswahl, Beschaffung, Anpassung und Einführung von Standardsoftware • Test- u. Freigabeverfahren • Change-Management Bezogen auf den Entwicklungs- und Beschaffungsprozess werden z.B. Pflichtenhefte herangezogen und die Einhaltung von rechtlichen, fachlichen und sicherheitsrelevanten Anforderungen geprüft.
A.6.1.1	Engagement des Managements für Informationssicherheit
A.6.1.2	Koordination der Informationssicherheit
A.6.1.3	Zuweisung der Verantwortlichkeiten für Informationssicherheit
A.6.1.4	Genehmigungsverfahren für informationsverarbeitende Einrichtungen
A.10.1.2	Änderungsverwaltung
A.10.1.3	Aufteilung von Verantwortlichkeiten
A.10.1.4	Trennung von Entwicklungs-, Test- und Produktiveinrichtungen
A.12.1.1	Analyse und Spezifikation von Sicherheitsanforderungen
A.12.5.1	Änderungskontrollverfahren
(81)	Prüfung der Regelungen und Maßnahmen bei Implementierung und Anpassungen. Prüfung, ob Dokumentation und Einhaltung der Ordnungsmäßigkeits- und Sicherheitskriterien bei der Anpassung von IT-Anwendungen gewährleistet sind.
A.6.1.1	Engagement des Managements für Informationssicherheit
A.6.1.2	Koordination der Informationssicherheit
A.6.1.3	Zuweisung der Verantwortlichkeiten für Informationssicherheit
A.6.1.4	Genehmigungsverfahren für informationsverarbeitende Einrichtungen
A.12.5.1	Änderungskontrollverfahren
A.12.5.3	Einschränkung von Änderungen an Softwarepaketen
A.15.2.2	Prüfung der Einhaltung technischer Vorgaben
(82)	Funktionsprüfung der Implementierung, Einzelfallprüfung der Parametrisierung durch Testfälle.
A.10.1.1	Dokumentierte Betriebsprozesse
A.10.1.2	Änderungsverwaltung
(83)	Prüfung auf korrekte Übernahme von Altdaten.
A.10.1.2	Änderungsverwaltung
A.12.2.2	Kontrolle der internen Verarbeitung

5.6 Prüfung IT-gestützter Geschäftsprozesse

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
(84)	Die Aufbauprüfung … umfasst Prozessaufnahmen, die dokumentieren … • in welchen Prozessschritten IT-Anwendungen integriert sind und/oder manuelle Tätigkeiten ausgeführt werden, • wie und welche rechnungslegungsrelevanten Daten aus dem Geschäftsprozess in die Rechnungslegung übergeleitet werden, • welche anwendungs- und prozessbezogenen Kontrollen bei der Erfassung und Verarbeitung von Geschäftsvorfällen bestehen.
A.10.1	Verfahren und Verantwortlichkeiten
A.12.2.1	Überprüfung von Eingabedaten
A.12.2.2	Kontrolle der internen Verarbeitung
A.12.2.4	Überprüfung von Ausgabedaten
(85)	Anwendungsbezogene Kontrollen (manuelle als auch programmseitige):
A.10.1.2	Änderungsverwaltung
A.10.10.5	Fehlerprotokolle
A.12.2.1	Überprüfung von Eingabedaten
A.12.2.2	Kontrolle der internen Verarbeitung
A.12.2.4	Überprüfung von Ausgabedaten
(86)	Im Rahmen der Aufbauprüfung hat der Abschlussprüfer die Zielsetzung der IT zu beurteilen.
A.5.1.1	Leitlinie zur Informationssicherheit
A.5.1.2	Überprüfung der Informationssicherheitsleitlinie
A.6.1.2	Koordination der Informationssicherheit
A.6.1.3	Zuweisung der Verantwortlichkeiten für Informationssicherheit
(87)	Bei der Beurteilung der Angemessenheit der prozessintegrierten Kontrollen steht der Kontrollzweck »Gewährleistung der Ordnungsmäßigkeit und Sicherheit der rechnungsrelevanten Daten« im Vordergrund.
4.2.3	Überwachen und Überprüfen des ISMS
A.9.1	Sicherheitsbereiche
A.9.2.1	Platzierung und Schutz von Betriebsmitteln
A.9.2.2	Unterstützende Versorgungseinrichtungen
A.9.2.3	Sicherheit der Verkabelung
A.9.2.4	Instandhaltung von Gerätschaften
A.9.2.6	Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln
A.10.1.3	Aufteilung von Verantwortlichkeiten
A.12.2.1	Überprüfung von Eingabedaten
A.12.2.2	Kontrolle der internen Verarbeitung
A.12.2.3	Integrität von Nachrichten
A.12.2.4	Überprüfung von Ausgabedaten
(88)	Funktionsprüfungen zur Verifizierung der Wirksamkeit der IT-Kontrollen in den IT-gestützten Geschäftsprozessen.
A.11.2.1	Benutzerregistrierung
A.11.2.2	Verwaltung von Sonderrechten
A.11.2.3	Verwaltung von Benutzerpasswörtern
A.11.4.6	Kontrolle von Netzverbindungen
A.11.6.1	Einschränkung von Informationszugriffen
A.12.2.1	Überprüfung von Eingabedaten
A.12.2.2	Kontrolle der internen Verarbeitung
A.12.2.4	Überprüfung von Ausgabedaten

5.7 Prüfung des IT-Überwachungssystems

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
(89)	Es ist das IT-Überwachungssystem stichprobenartig zu überprüfen. Dies kann auch durch Revisionsmechanismen bzw. durch Externe erfolgen.
4.2.2	Umsetzen und Durchführen des ISMS
4.2.3	Überwachen und Prüfen des ISMS
A.6.1.8	Unabhängige Überprüfung der Informationssicherheit
A.15.2.2	Prüfung der Einhaltung technischer Vorgaben
A.15.3.1	Maßnahmen für Audits von Informationssystemen
PS 320	*Prüfungsstandard: Verwendung der Arbeit eines anderen externen Prüfers*

5.8 Prüfung des IT-Outsourcings

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
(90)	Beurteilung der Auslagerung des Bereiches sowie der Einbindung des IKS
A.10.1.1	Dokumentierte Betriebsprozesse
A.10.1.2	Änderungsverwaltung
A.10.1.3	Aufteilung von Verantwortlichkeiten
A.10.2.1	Erbringung von Dienstleistungen
A.10.2.2	Überwachung und Überprüfung der Dienstleistungen von Dritten
A.10.2.3	Management von Änderungen an Dienstleistungen von Dritten
A.14.1.2	Sicherstellung des Geschäftsbetriebs und Risikoeinschätzung
A.15.2.2	Prüfung der Einhaltung technischer Vorgaben
(91)	Bei wesentlicher Auswirkung auf die Abschlussprüfung ist die Überprüfung auszuweiten und das IKS auf Kontrollrisiken zu überprüfen.
4.2.2	Umsetzen und Durchführen des ISMS
4.2.3	Überwachen und Prüfen des ISMS
A.6.2.1	Identifizierung von Risiken in Zusammenhang mit externen Mitarbeitern
PS 951	*Prüfungsstandard: Die Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen für auf das Dienstleistungsunternehmen ausgelagerte Funktionen*
(92)	Bei Auslagerung von Systemen der Buchführung ist die Art der Auslagerung zu prüfen sowie die Anforderungen der GoBS zu beurteilen.
–	
(93)	Bei Einbeziehung von Prüfergebnissen von Sachverständigen sowie Ergebnissen der Abschlussprüfer des Dienstleisters sind IDW PS 320 und PS 322 einzubeziehen.
A.15.3.1	Maßnahmen für Audits von Informationssystemen
PS 322	*Auswertung von Sachverständigen-Unterlagen*

6 IT-gestützte Prüfungstechniken

6.1 Einsatzbereiche

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
(94)	Einführung zur Verwendung IT-gestützter Prüfungstechniken. Sie sind insbesondere dort empfehlenswert, wo nur in elektronischer Form verarbeitet wird oder eine sehr große Zahl von Geschäftsvorfällen vorliegt.
A.10.2	Management der Dienstleistungserbringung von Dritten
(95)	Erläuterung der Vorgehensweise zur Entscheidungsfindung über Art und Umfang IT-gestützter Prüfungshandlungen unter Berücksichtigung der aufgeführten Faktoren
A.6.2.3	Adressieren von Sicherheit in Vereinbarungen mit Dritten
A.10.2	Management der Dienstleistungserbringung von Dritten
A.15.3.1	Maßnahmen für Audits von Informationssystemen
(97)	Vorschlag zur Nutzung von Inventarisierungs- und Überwachungsprogrammen des Unternehmens zur Ermittlung von Informationen über das IT-System
A.6.2.1	Identifizierung von Risiken in Zusammenhang mit externen Mitarbeitern
A.6.2.3	Adressieren von Sicherheit in Vereinbarungen mit Dritten
A.7.1.1	Inventar der organisationseigenen Werte (Assets)
A.7.1.2	Eigentum von organisationseigenen Werten (Assets)
A.7.1.3	Zulässiger Gebrauch von organisationseigenen Werten (Assets)
A.10.1.1	Dokumentierte Betriebsprozesse
(98)	Erläuterung des Einsatzes von IT-gestützten Prüfungstechniken bei Aufbauprüfungen und Funktionsprüfungen mit Auflistung der Werkzeugeigenschaften
A.15.2.2	Prüfung der Einhaltung technischer Vorgaben
(100)	Auflistung der Fälle, in denen Einzelfallprüfungen durch IT-gestützte Prüfungstechniken unterstützt werden können.
A.7.1.3	Zulässiger Gebrauch von organisationseigenen Werten (Assets)
A.10.7.4	Sicherheit der Systemdokumentation

6.2 IT-gestützte Prüfungsdurchführung

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
(101)	Vorschlag des Einsatzes von Standardprüfungsprogrammen, die als integrierte Softwarelösungen eine Unterstützung bei einer Vielzahl von Tätigkeiten im Rahmen der Durchführung von Abschlussprüfungen anbieten. Vorschlag des Einsatzes von nicht integrierten Softwarelösungen zur Unterstützung bei der Prüfungsdurchführung.
A.11.6.1	Einschränkung von Informationszugriff
A.12.1.1	Analyse und Spezifikation von Sicherheitsanforderungen

6.3 Verwendung des IT-Systems des Unternehmens für Prüfzwecke

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
(102)	Neben dem Einsatz eigener Programme auf der Hardware des Abschlussprüfers kann auch die Verwendung des IT-Systems des Mandanten für Prüfungszwecke erforderlich sein.
A.10.3.1	Kapazitätsplanung
A.11.1.1	Regelwerk zur Zugangskontrolle
A.11.2	Benutzerverwaltung
(103)	Der Abschlussprüfer kann die auf der Hardware des Unternehmens installierten Programme mit nutzen. Auflistung verschiedener Einsatzmöglichkeiten für Prüfungszwecke.
A.11.1.1	Regelwerk zur Zugangskontrolle
A.11.6	Zugangskontrolle zu Anwendungen und Informationen
(104)	Vorgehensweise zum Einsatz eigener Programme des Abschlussprüfers auf dem IT-System des Unternehmens
A.7.1.3	Zulässiger Gebrauch von organisationseigenen Werten (Assets)
A.10.1.2	Änderungsverwaltung
A.10.2	Management der Dienstleistungserbringung von Dritten
A.10.3	Systemplanung und Abnahme
A.10.3.2	Systemabnahme
A.10.4	Schutz vor Schadsoftware und mobilem Programmcode
A.10.7.3	Umgang mit Informationen
A.10.8.5	Geschäftsinformationssysteme
A.11.6	Zugangskontrolle zu Anwendungen und Informationen
A.11.6.1	Einschränkung von Informationszugriffen
A.12.1.1	Analyse und Spezifikation von Sicherheitsanforderungen
A.12.2	Korrekte Verarbeitung in Anwendungen
A.12.2.1	Überprüfung von Eingabedaten
A.12.2.4	Überprüfung von Ausgabedaten
A.15.3	Überlegungen zu Revisionsprüfungen von Informationssystemen
A.15.3.1	Maßnahmen für Audits von Informationssystemen
A.15.3.2	Schutz von Revisionswerkzeugen für Informationssysteme
(105)	Auflistung der beim Einsatz von Testdatensätzen zur Prüfung der Verarbeitungsergebnisse von IT-Anwendungen einzuhaltenden Randbedingungen
A.10.1.2	Änderungsverwaltung
A.10.8.1	Leitlinien und Verfahren zum Austausch von Informationen
A.10.8.5	Geschäftsinformationssysteme
A.12.4.2	Schutz von Testdaten
A.12.4.3	Zugangskontrolle zu Quellcode
A.12.5.1	Änderungskontrollverfahren

6.4 Besonderheiten beim Einsatz IT-gestützter Prüfungstechniken

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
(106)	Auflistung der Bereiche, in denen sich Besonderheiten bei der Planung und Durchführung des Einsatzes IT-gestützter Prüfungstechniken ergeben.
A.10.1.1	Dokumentierte Betriebsprozesse
A.10.2	Management der Dienstleistungserbringung von Dritten
A.10.3.2	Systemabnahme
A.10.7.3	Umgang mit Informationen
A.10.8.5	Geschäftsinformationssysteme
A.11.1.1	Leitlinie zur Zugangskontrolle
A.11.6.1	Einschränkung von Informationszugriffen
(107)	Überwachung der Prüfungsdurchführung und der Ableitung der Prüfungsergebnisse
A.10.3.2	Systemabnahme
A.10.6.1	Maßnahmen für Netze
A.10.8	Austausch von Informationen
A.12.4.1	Kontrolle von Software im Betrieb
A.12.5	Sicherheit bei Entwicklungs- und Unterstützungsprozessen
A.12.5.1	Änderungskontrollverfahren
A.12.5.3	Einschränkung von Änderungen an Softwarepaketen

7 Dokumentation und Berichterstattung

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
(108)	Dokumentation während der Prüfung und Prüfungsbericht
A.6.2.3	Adressieren von Sicherheit in Vereinbarungen mit Dritten
A.15.1.3	Schutz von organisationseigenen Aufzeichnungen
A.15.3.2	Schutz von Revisionswerkzeugen für Informationssysteme
ISO 17021	*9.1.10 Allgemeine Anforderungen. Für jedes Audit ist ein schriftlicher Bericht zu erstellen.* *9.2.4 Das Auditteam muss alle während der Audits der Stufe 1 und der Stufe 2 erfassten Informationen und Auditnachweise analysieren, um die Auditfeststellungen zu bewerten und sich auf Auditschlussfolgerungen zu einigen.*
ISO 19011	*6.6.1 Vorbereitung des Auditberichts* *6.6.2 Genehmigung & Verteilung des Auditberichts*
ISO 27006	*9.1.6 Zertifizierung Auditbericht* *9.1.6.2 Auditbericht* *9.1.6.3 Bericht über Abweichungen (Abweichungsprotokoll)*
(109)	Art und Umfang der Dokumentation der Prüfung
A.6.1.8	Unabhängige Überprüfung der Informationssicherheit
ISO 17021	*9.1.10 Die Zertifizierungsstelle muss für jedes Audit einen schriftlichen Bericht erstellen. Dieser Bericht muss sich auf die relevanten Leitlinien in ISO 19011 beziehen.*
(110)	Hinweise zur Handhabung des Bestätigungsvermerks.
A.6.1.8	Unabhängige Überprüfung der Informationssicherheit
ISO 17021	*9.1.14 Die Zertifizierungsstelle muss sicherstellen, dass die Personen oder Ausschüsse, die die Entscheidung über die Zertifizierung oder Rezertifizierung treffen, andere sind als die, die die Audits durchgeführt haben.* *9.1.15 Bevor sie eine Entscheidung trifft, muss die Zertifizierungsstelle die Unabhängigkeit (siehe a bis c) bestätigen.*
(111)	Hinweise zur Handhabung von entdeckten Verstößen gegen Gesetze zum Schutz personenbezogener Daten.
A.15.1.4	Datenschutz und Vertraulichkeit von personenbezogenen Informationen
ISO 17021	*9.1.15 Bevor sie eine Entscheidung trifft, muss die Zertifizierungsstelle bestätigen, ….*
ISO 19011	*6.5.5 Treffen von Auditfeststellungen.*
(112)	Hinweis zur Ordnungsmäßigkeit der Buchführung, Sicherheit der rechnungslegungsrelevanten Daten.
4.3.3	Lenkung von Aufzeichnungen
A.15.1.3	Schutz von organisationseigenen Aufzeichnungen
ISO 17021	*9.1.15 Bevor sie eine Entscheidung trifft, muss die Zertifizierungsstelle bestätigen, ….*
ISO 19011	*6.5.5 Treffen von Auditfeststellungen.*
(113)	Darstellung von festgestellten Mängeln, die nicht direkt für die Rechnungslegung relevant sind.
A.6.1.8	Unabhängige Überprüfung der Informationssicherheit
ISO 17021	*Bevor sie eine Entscheidung trifft, muss die Zertifizierungsstelle die Unabhängigkeit (siehe a bis c) bestätigen.*
ISO 19011	*6.5.5 Treffen von Auditfeststellungen*
ISO 27006	*9.1.6.3 Bericht über Abweichungen (Abweichungsprotokoll), Beobachtungen (z.B. positiv/negativ aufgefallen, mögliche Quelle für Abweichungen)*
(114)	Darstellung wesentlicher Schwächen des IT-Systems.
A.6.1.8	Unabhängige Überprüfung der Informationssicherheit
ISO 19011	*6.5.5 Treffen von Auditfeststellungen*

PS 330	Zusammenfassung der Anforderung aus PS 330
ISO 27001	Kapitel und/oder Anforderung aus ISO 27001
Referenzen	*Ergänzende Quellen und/oder Spezifikationen aus Standards*
ISO 27006	*9.1.6.3 Bericht über Abweichungen (Abweichungsprotokoll), Beobachtungen (z.B. positiv/negativ aufgefallen, mögliche Quelle für Abweichungen)*
(115)	Darstellung von Verbesserungspotenzialen
8	Verbesserung des ISMS
A.6.1.8	Unabhängige Überprüfung der Informationssicherheit
ISO17021	*9.1.10 …Das Auditteam darf Verbesserungsmöglichkeiten aufzeigen, aber keine zielgerichteten Lösungen empfehlen.*
ISO 19011	*6.5.5 Treffen von Auditfeststellungen* *6.5.6 c Empfehlungen zu erarbeiten, …*
ISO 27006	*9.1.6.3 Bericht über Abweichungen (Abweichungsprotokoll), Beobachtungen (z.B. positiv/negativ aufgefallen, mögliche Quelle für Abweichungen)*

8 Fazit

Standards und Regelwerke bilden die Grundlage für ein einheitliches Verständnis und Wertesystem. Mit ihnen ist es möglich, Anforderungen nach allgemeingültigen branchen-, fach- oder aufgabenspezifischen, nationalen oder sogar internationalen Vorgaben zu planen, umzusetzen, zu messen und zu verbessern. Darüber hinaus ermöglichen sie die einheitliche Prüfung und Bewertung der Umsetzung dieser Anforderungen und helfen somit, den Reifegrad der Umsetzung bestimmen zu können.

Normen sollen auch dazu dienen, substanzielle Werte zu schützen und Compliance-Vorgaben nach erprobten Methoden zu erfüllen. Wie immer gibt es auch hier zwei Seiten einer Medaille, die erwähnenswert sind. Der zuvor beschriebene Vorteil einer Norm »international verständlich und anerkannt zu sein« wurde mit der ISO/IEC 27001 – der Norm für Informationssicherheit – sicherlich erreicht. Mit ihr werden die Grundwerte Verfügbarkeit (also das Sicherstellen der jederzeitigen Verfügbarkeit von Informationen), Integrität (also die Sicherung der Richtigkeit und Unveränderlichkeit der Informationen) und Vertraulichkeit (also Sicherstellung der korrekten Zugriffsberechtigungen) festgelegt und geregelt. Die Beschreibungen wurden dabei generisch gehalten und beschreiben das »Was«, aber nicht das »Wie«.

Es gibt Vorwürfe, dass die Einigung hier nur auf dem kleinsten gemeinsamen Nenner erfolgte und spezifische fachliche und gesetzliche Anforderungen wie z.B. aus dem Standard IDW PS 330 oder an Gesetzen in Teilen oder gar nicht abgedeckt sind. Dies ist aber bei näherer Betrachtung genau der Charakter einer international gültigen Norm, die Informationssicherheit in der Breite beschreibt und für die unterschiedlichsten Anwendungsgebiete und Gesetze genügend Freiheit in der Praxis lässt.

Der Vergleich zwischen ISO/IEC 27001 und IDW PS 330 hat aufgezeigt, dass viele Übereinstimmungen bestehen und erhebliche Synergieeffekte genutzt werden können. Ziel des Arbeitskreises des ISACA Germany Chapter war es, über die Vergleichstabelle Gemeinsamkeiten festzustellen und darüber hinaus Hinweise auf weitere Standards zu geben, die für den umfassenden Abgleich relevant sind.

9 Danksagung

Die erste Version des Leitfadens und Nachschlagewerks »IDW PS 330 ←→ DIN ISO/IEC 27001 – Referenztabelle« entstand durch die enge Zusammenarbeit zwischen ISACA und dem Fachausschuss Informationstechnik des IDW.
Unser besonderer Dank gilt den Autoren der ersten Version des Leitfadens für das kontinuierliche Interesse am Thema sowie die zahlreichen Textbeiträge, die diesen umfassenden Leitfaden erst ermöglichten:

Andreas Teuscher (SICK AG)
Rainer Nuss (Voith AG)
Werner Syndikus (Tobaccoland Automatengesellschaft)
Holger Anspach (Computacenter AG & Co. oHG)
Oliver Knörle (ditis Systeme, Niederlassung der JMV GmbH und Co. KG)
Ingrid Dubois (dubois it-consulting GmbH)
Gerhard Funk (Freiberufler)
Oliver Töpfer (SICK AG)
Gerd Niehuis (BDO Deutsche Warentreuhand AG)
Mustafa Topal (BDO Deutsche Warentreuhand AG)

Für das Korrekturlesen, die Koordination der Treffen der Fachgruppe und die Bereitstellung von bibliografischen Angaben geht unser Dank an:

Andrea Nöthen (SICK AG)
Michael Neuy (ISACA Germany Chapter)
CIA-Arbeitskreis Süd des DIIR
CIA-Arbeitskreis Süd-West des DIIR

10 Anhang

10.1 Glossar

Begriff aus PS 330	Erläuterung	Quelle(n)
Ablauforganisation	Die Ablauforganisation regelt sowohl die Organisation der Entwicklung, Einführung und Änderung als auch die Steuerung des Einsatzes von IT-Anwendungen. Auch im Rahmen des IT-Betriebs müssen Aufgaben, Kompetenzen und Verantwortlichkeiten der IT-Mitarbeiter klar definiert sein. Übliche Instrumente hierfür sind Prozess- und Funktionsbeschreibungen oder Organisationshandbücher.	RS FAIT 1 (78)
Abschlussprüfung	Prüfungen von Jahres-, Konzern- und Zwischenabschlüssen. Wirtschaftszweigspezifische und sonstige Besonderheiten, die im Einzelfall zusätzlich zu berücksichtigen sind, bleiben außer Betracht. Ggf. sind auch die im Dienstleistungsunternehmen eingerichteten organisatorischen Regelungen und die dort vorgehaltenen Aufzeichnungen für die Abschlussprüfung zu beurteilen.Die Aufdeckung von sonstigen Gesetzesverstößen, die nicht zu falschen Angaben im Abschluss oder Lagebericht führen, ist nicht Gegenstand der Abschlussprüfung.	PS 330 (2), (3), (90) PS 210 (5), (46)
Änderungen an IT-Anwendungen	Sie sind nur auf der Basis eines geregelten Verfahrens vorzunehmen. Auch für Änderungen sind festgelegte Anforderungen an Programmierung, Dokumentation und Tests zu beachten. Voraussetzung für die ordnungsgemäße Integration von Änderungen in das Gesamtsystem ist die Einführung eines geeigneten Change- und Konfigurationsmanagements, das Verfahren zur Installation und Überwachung von Änderungen innerhalb von definierten Releasekonzepten oder Versionsführungen beinhaltet.	RS FAIT 1 (105)
Angemessenheit	Der Kontrollzweck »Gewährleistung der Ordnungsmäßigkeit und Sicherheit der rechnungslegungsrelevanten Daten« steht im Vordergrund. Neben anwendungsbezogenen Kontrollen sind auch integrierte IT-Kontrollen (Gewährleisten der vollständigen und richtigen Verarbeitung, Schnittstellenimplementierung, Funktionstrennung) zu beurteilen.	PS 330 (87)
Aufbauorganisation	Die Aufbauorganisation regelt die Einordnung des IT-Bereichs in die Organisationsstruktur des Gesamtunternehmens und den Aufbau des IT-Bereichs selbst. Geregelt werden die Verantwortlichkeiten und Kompetenzen im Zusammenhang mit dem IT-Einsatz.	RS FAIT 1 (78)
Aufbauprüfung	Beurteilung der Angemessenheit der personellen, organisatorischen und technischen Maßnahmen bzgl. IT-Umfeld, IT-Organisation, IT-Betrieb, Sicherung der Verfügbarkeit, Gewährleistung der Sicherheit (Umsetzung des Sicherheitskonzeptes), Funktionalität der IT-Anwendungen, Wirksamkeit der Kontrollmaßnahmen (Überwachungssystem). Sie erfolgt auf Basis des Sicherheitskonzeptes, der IT-Strategie, der Regelungen sowie Prozess- und Funktionsbeschreibungen. Ziel der Aufbauprüfung ist eine Beurteilung, ob das angewiesene IT-Kontrollsystem (Sollzustand) des Unternehmens, unter Berücksichtigung der prüffeldspezifischen inhärenten Risiken, und die festgelegten Sicherheitsmaßnahmen im Hinblick auf die eingesetzte Technik und den gewünschten Schutzzweck angemessen und im geplanten Umfang wirksam sind.	PS 330 (32), (33), (51), (55)
Aufnahme des IT-Systems	Hard- und Softwarekomponenten wie auch die vorgesehenen IT-Kontrollen und damit der von der Unternehmensleitung angewiesene Sollzustand des IT-Systems.	PS 330 (30)
Aufrechterhaltung des Geschäftsbetriebs	Die jederzeitige Verfügbarkeit des IT-Systems ist eine wesentliche Voraussetzung für die Aufrechterhaltung des Geschäftsbetriebs. Deshalb sind Vorkehrungen für einen Notbetrieb zu treffen. Ein Ausfall wesentlicher IT-Anwendungen, ohne kurzfristige Ausweichmöglichkeit, kann materielle und immaterielle Vermögensschäden nach sich ziehen und stellt einen wesentlichen Mangel der Buchführung dar.	RS FAIT 1 (88)

Begriff aus PS 330	Erläuterung	Quelle(n)
Ausgabekontrolle	Stellt die vollständige und richtige Erstellung und Verteilung von Verarbeitungsergebnissen in lesbarer Form sicher.	RS FAIT 1 (95)
Authentizität	Authentizität ist gegeben, wenn ein Geschäftsvorfall einem Verursacher eindeutig zuzuordnen ist.	RS FAIT 1 (23)
Autorisierung	Autorisierung bedeutet, dass nur im Voraus festgelegte Personen auf Daten zugreifen können (autorisierte Personen) und dass nur sie die für das System definierten Rechte wahrnehmen können. Diese Rechte betreffen das Lesen, Anlegen, Ändern und Löschen von Daten oder die Administration eines IT-Systems (aber auch: Freigabe einer Buchung).	RS FAIT 1 (23), (40)
Bestätigungsvermerk	Feststellung zur Gesetzmäßigkeit von Buchführung, Jahres-/ Konzernabschluss und Lagebericht/Konzernlagebericht. Der Bestätigungsvermerk ist nur einzuschränken oder zu versagen, wenn sich die Unrichtigkeit oder der Verstoß wesentlich auf den Abschluss auswirkt und der Mangel im Zeitpunkt des Abschlusses der Prüfung noch vorliegt und nicht zutreffend im Abschluss dargestellt ist. Sofern das Unternehmen den Abschlussprüfer daran hindert, Untersuchungen zur Aufdeckung von möglicherweise für den Abschluss wesentlichen Unrichtigkeiten und Verstößen anzustellen, hat der Abschlussprüfer den Bestätigungsvermerk einzuschränken oder zu versagen und dies entsprechend zu begründen.	PS 210 (59), (61), (62)
Datensicherung, Datensicherungs- und Auslagerungs-verfahren	Voraussetzungen für die Funktionsfähigkeit der Datenverarbeitung und zudem Voraussetzung zur Sicherung der Vollständigkeit und Verfügbarkeit der Daten und Programme. Sie sind erforderlich, um den Anforderungen nach Lesbarmachung der Daten – auch i.S. ein ordnungsmäßigen Buchführung – gerecht zu werden. Stellt die jederzeitige Verfügbarkeit und Lesbarkeit der Daten sicher. Geeignete Verfahren sind hinreichend gestaffelte Tages-, Monats- und Jahressicherungen, die Inventarisierung aller Sicherungsmedien einschließlich der Führung von Datenträgerverzeichnissen sowie die Auslagerung wichtiger Sicherungsbestände außerhalb des Rechnerbereichs. Die Durchführung regelmäßiger Datensicherungen ist im Allgemeinen Voraussetzung für die Rekonstruktion historischer Bestände (Programme und Daten) und die Rekonstruktion aktueller Software- und Datenbestände bei Funktionsstörungen der Hardware.	PS 330 (59) RS FAIT 1 (85), (86)
Eingabekontrolle	Die Richtigkeit und Vollständigkeit der in IT-Anwendungen übernommenen Daten sind sichergestellt.	RS FAIT 1 (95)
Einrichtung eines IT-Systems	Sicherstellen der Anforderungen der Grundsätze ordnungsmäßiger Buchführung an eine ordnungsmäßige IT-gestützte Rechnungslegung für alle Elemente des IT-Systems.	PS 330 (28) RS FAIT 1 (76)
Einsatz von IT im Unternehmen	Die gesetzlichen Vertreter haben die Verantwortung dafür, dass die Unternehmensziele in Übereinstimmung mit der von ihnen festgelegten Geschäftspolitik des Unternehmens im Rahmen der gesetzlichen Vorschriften erreicht werden. Soweit hierfür IT eingesetzt wird, haben sie geeignete Regelungen einzuführen, um die Risiken aus dem Einsatz von IT zu bewältigen. Das Zusammenwirken der Elemente eines IT-Systems (IT-gestützte Geschäftsprozesse, IT-Anwendungen, IT-Infrastruktur) wird durch das IT-Kontrollsystem bestimmt, das von dem IT-Umfeld und der IT-Organisation abhängt.	PS 330 (7) RS FAIT 1 (7)
Entdeckungsrisiko	Die Beurteilung der sich aus inhärenten und den Kontrollrisiken zusammensetzenden Fehlerrisiken hat eine unmittelbare Auswirkung auf die Bestimmung des von Art, Umfang und zeitlichem Ablauf der aussagebezogenen Prüfungshandlungen abhängigen Entdeckungsrisikos.	PS 260 (74)
Fehlerrisiken, IT-Fehlerrisiken	Wesentliche Fehler für die Rechnungslegung verursacht durch die konkrete Ausgestaltung des IT-Systems. Sie setzen sich aus inhärenten Risiken und Kontrollrisiken zusammen.	PS 260 (24) PS 330 (9), (16)

Begriff aus PS 330	Erläuterung	Quelle(n)
Funktionsprüfung	Ziel der Funktionsprüfung ist, ob die eingerichteten IT-Kontrollen wirksam sind und damit zur Begrenzung der IT-Fehlerrisiken beitragen. Die Funktionsprüfungen sind auf die prüffeldspezifischen Kontrollrisiken auszurichten. Funktionsprüfungen betreffen die Art der Anwendung bestimmter organisatorischer Regelungen, die Kontinuität in der Anwendung im abgelaufenen Geschäftsjahr und die Frage, welche Personen für die Durchführung bestimmter Maßnahmen verantwortlich waren und wer diese tatsächlich durchgeführt hat.	PS 260 (66), (67) PS 330 (35)
Generelle Kontrollen	Kontrollen für Entwicklung von Individualsoftware, Auswahl, Beschaffung und Einführung von Standardsoftware, Test- und Freigabeverfahren, Verfahren zur Änderung von IT-Anwendungen (Change-Management)	RS FAIT 1 (96)
Gesamturteil einer IT-Systemprüfung	Das Gesamturteil fasst Erkenntnisse über das eingesetzte IT-System, vorläufige Beurteilung aus der Aufbauprüfung, abschließende Würdigung der Ergebnisse der Funktionsprüfung (Wirksamkeit) und der Prüfung der Überwachung des IT-Kontrollsystems (z.B. durch die Interne Revision) zusammen.	PS 330 (41)
Implementierung rechnungslegungs-relevanter Software	Spezifische Anpassungen der IT-Anwendung. Regelungen und Maßnahmen für die Implementierung wie Parameter zum Steuern der Anwendung (automatische Kontenfindungen und Buchungen, die Gestaltung von Bewertungsverfahren in der Materialwirtschaft, die Ausgestaltung des Zugriffsschutzsystems, die Erstellung unternehmensindividueller Auswertungen, Übernahme von Altdaten, Systemwechsel etc.	PS 330 (81), (83)
Implementierung von Standardsoftware	Anpassungen und Einstellungen (Customizing), die der konkreten Ausgestaltung der Standardsoftware in der Rechnungslegung des Unternehmens dienen. Sie unterliegen den Anforderungen der Ordnungsmäßigkeit und Sicherheit.	RS FAIT 1 (100)
Indizien für Risiken	Folgende Sachverhalte können Indizien für solche Risiken sein: - Zweifel an der Integrität oder Kompetenz der Unternehmensleitung - kritische Unternehmenssituationen - ungewöhnliche Geschäfte - Schwierigkeiten mit der Erlangung von Prüfungsnachweisen - sonstige Umstände - fehlende oder veraltete Dokumentation des Aufbaus der Dateien oder der Programme - zahlreiche nicht genehmigte, nicht getestete oder nicht dokumentierte Änderungen	PS 210 (30)
Informations-technologie	Die Gesamtheit der im Unternehmen zur elektronischen Datenverarbeitung eingesetzten Hard- und Software	PS 330 (7) RS FAIT 1 (2)

Begriff aus PS 330	Erläuterung	Quelle(n)
Inhärente Risiken	Durch den Einsatz eines IT-Systems können Fehler auftreten, die Auswirkungen auf die Ordnungsmäßigkeit der Rechnungslegung haben (korrekte Ausgestaltung des Buchführungsverfahrens, Richtigkeit der rechnungslegungsrelevanten Programmabläufe und Verarbeitungsregeln, Sicherheit der rechnungslegungsrelevanten Daten etc.). Es sind unternehmensinterne und unternehmensexterne Faktoren zu beachten: - Integrität und Kompetenz der Unternehmensleitung - ungünstige Entwicklungen im Unternehmen - Art und Umfang der Geschäftstätigkeit - Besonderheiten der Geschäftsentwicklung - branchenspezifische Faktoren - neue fachliche Standards oder gesetzliche Regelungen - fachliche Kompetenz bzgl. Rechnungslegung Folgende Aspekte sind für die prüffeldspezifische Beurteilung von Bedeutung: - Fehleranfälligkeit von Posten des Jahresabschlusses - Komplexität der Geschäftsvorfälle - Beurteilungsspielräume (Schulden, Vermögensgegenstände) - Gefahr von Verlust oder Unterschlagung von Vermögenswerten - Abschluss ungewöhnlicher Geschäfte - Geschäftsvorfälle, die nicht routinemäßig verarbeitet werden	PS 260 (28), (29) PS 330 (17)
Integrität	Die Integrität von IT-Systemen ist gegeben, wenn die Daten und die IT-Infrastruktur sowie die IT-Anwendungen vollständig und richtig zur Verfügung stehen und vor Manipulation und ungewollten oder fehlerhaften Änderungen geschützt sind.	RS FAIT 1 (23)
Interne Revision	Prozessunabhängige Institution, die innerhalb eines Unternehmens Strukturen und Aktivitäten prüft und beurteilt. Dieser unternehmensinterne Überwachungsträger darf weder in den Arbeitsablauf integriert noch für das Ergebnis des überwachten Prozesses verantwortlich sein.	PS 260 (6)
Internes IT-Kontroll-system, IT-Über-wachungssystem	siehe IT-Kontrollsystem	
Internes Kontrollsystem	Unter einem internen Kontrollsystem werden die von der Unternehmensleitung im Unternehmen eingeführten Grundsätze, Verfahren und Maßnahmen (Regelungen) verstanden, die gerichtet sind auf die organisatorische Umsetzung der Entscheidungen der Unternehmensleitung zur Sicherung der Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit, zur Ordnungsmäßigkeit und Verlässlichkeit der internen und externen Rechnungslegung und zur Einhaltung der für das Unternehmen maßgeblichen rechtlichen Vorschriften. Das interne Kontrollsystem besteht aus Regelungen zur Steuerung der Unternehmensaktivitäten (internes Steuerungssystem) und Regelungen zur Überwachung der Einhaltung dieser Regelungen (internes Überwachungssystem).Ein internes Kontrollsystem ist aus Sicht des Abschlussprüfers dann wirksam, wenn es mit hinreichender Sicherheit verhindert, dass sich Unternehmensrisiken wesentlich auf die Ordnungsmäßigkeit des Jahresabschlusses oder des Lageberichts auswirken.	PS 260 (5), (39) PS 330 (89)
IT-Anwendungen	Anwendungen, Funktionen in Anwendungen, Verfahrensregelungen und -beschreibungen, verfahrens-bezogene Anforderungen der Grundsätze ordnungsmäßiger Buchführung, Verarbeitungskontrollen, Zugriffsberechtigung, Datensicherung, Wiederanlaufverfahren. Auswahl, Entwicklung, Wartung, Freigabe, Dokumentation, Klassifizierung (Batch/Dialog), Typ (Individual-, Standard-, modifizierte Standardsoftware, Hersteller, Version), Programmiersprachen, Datenhaltung (Datenbank, Dateiorganisation)	PS 330 (22), (70) RS FAIT 1 (95)

Begriff aus PS 330	Erläuterung	Quelle(n)
IT-Betrieb	Der IT-Betrieb umfasst sowohl Verfahren für einen geordneten Regelbetrieb von IT-Anwendungen als auch Verfahren für den Notbetrieb, Organisation, Systemverwaltung, Produktionsabwicklung, Ressourcen-, Change- und Problemmanagement.	PS 330 (59) RS FAIT 1 (87)
IT-gestützte Geschäftsprozesse, IT-Geschäftsprozesse	IT-Sicherheit bezieht sich in diesem Kontext auf die Ordnungsmäßigkeit der Geschäftsprozesse; Datenaustausch, Transparenz, Integration, Abstimm- und Kontrollverfahren. Unternehmensabläufe (funktions- oder prozessorientiert), dazu eingesetzte IT-Infrastruktur und IT-Anwendungen und relevante Schnittstellen, Datenfluss, Verbindung zur Buchführung, anwendungs- und prozessbezogene Kontrollen (manuelle, programmseitige Kontrollen), (zeitnahe) Bearbeitung von Fehlermeldungen und -protokollen. Geschäftsprozesse, die das Geschäftsmodell des Unternehmens angemessen abbilden, d.h., die Zielsetzung des Unternehmens steht in Übereinstimmung mit ihrer organisatorischen Ausgestaltung.	PS 330 (50), (84), (85), (86) RS FAIT 1 (14)
IT-gestützte Prüftechniken	Computer-Assisted Audit Techniques (CAAT): - IT-gestützte Erhebung von Informationen über das IT-System, automatisierte Checklisten zur Prüfungsdurchführung, durch Expertensysteme unterstützte Anwendungen zur Dokumentation und Beurteilung von internem Kontrollsystemen und Geschäftsprozessen - Programme zur Beurteilung der Wirksamkeit (Prüfung der Konfiguration von Betriebssystemen, Beurteilung von Zugriffsrechten etc.) Programmgesteuertes Generieren von Testfällen zur Prüfung der Eingabe-, Verarbeitungs- und Ausgabekontrollen - Analytische Prüfungshandlungen (Ermitteln von Kennzahlen, Verhältniszahlen, Trends, Abweisungen, Schwankungen, Zusammenhänge, Widersprüche etc.) - Einzelfallprüfungen - Automation von wiederkehrenden Aufgaben (Projekt/Prüfungsplanung, Datenanalyse, grafische Darstellung, Dokumentation etc.)	PS 330 (94), (98), (99), (100), (101)
IT-Infrastruktur	Hardware, Betriebssysteme, Middleware, Netzwerke, IT-Betrieb, Sicherheitsmaßnahmen/-systeme (Zugriffskontrollsysteme, Firewall, Datensicherung)	PS 330 (21), (59)
IT-Kontrollsystem	Das IT-Kontrollsystem ist Bestandteil des internen Kontrollsystems (IKS). Es umfasst diejenigen Grundsätze, Verfahren und Maßnahmen (Regelungen), die zur Bewältigung der Risiken aus dem Einsatz von IT eingerichtet werden. Hierzu gehören Regelungen zur Steuerung des Einsatzes von IT im Unternehmen (internes Steuerungssystem) und Regelungen zur Überwachung der Einhaltung dieser Regelungen (internes Überwachungssystem). Das IT-Kontrollsystem ist integraler Bestandteil des internen Kontrollsystems eines Unternehmens. Es stellt die angemessene Reaktion eines Unternehmens auf die festgestellten inhärenten Risiken des IT-Systems dar. Ein IT-Kontrollsystem ist aus Sicht des Abschlussprüfers dann wirksam, wenn es mit der erforderlichen Sicherheit gewährleistet, dass inhärente Risiken des IT-Systems, die zu wesentlichen Fehlern in der Rechnungslegung führen, verhindert bzw. aufgedeckt und korrigiert werden.	PS 330 (9), (26) RS FAIT 1 (8)
IT-Organisation	Organigramme, Verantwortlichkeiten, Kompetenzen, Regelungen, Verfahren, Maßnahmen und Regelungen für Entwicklung, Einführung und Änderungen von IT-Anwendungen	PS 330 (50)
IT-Outsourcing	- Auslagern von IT-Systemen oder IT-gestützten, betrieblichen Funktionen - Auslagern des Rechnungswesens ganz oder teilweise (Buchführung außer Haus, Shared Services) - Auslagerung (IT-Outsourcing) von Prozessen und Funktionen auf Provider und andere externe Dienstleister, wie z.B. Übertragung von Rechenzentrums-Dienstleistungen, Einschaltung von Providern z.B. bei Geschäftsprozessen, die das Internet nutzen, sowie Administration von (Standard-) Software durch externe Dienstleister.	PS 330 (90) RS FAIT 1 (113)

Begriff aus PS 330	Erläuterung	Quelle(n)
IT-Strategie	Strategie, die mittel- bis langfristig ausgerichtet, dokumentiert, von der Unternehmensleitung genehmigt ist und konkrete Maßnahmen beinhaltet. Die geschäftlichen Anforderungen und die Anwenderbedürfnisse müssen klar definiert sein und über IT-Funktionalitäten bzw. -Prozesse weitgehend abgedeckt werden. Zudem sind rechtliche Rahmenbedingungen – auch außerhalb des Handelsrechts – zu beachten.	PS 330 (18), (27) RS FAIT 1 (76)
IT-System	System zur Verarbeitung von Daten. Es beinhaltet IT-gestützte Geschäftsprozesse, IT-Anwendungen und IT-Infrastruktur.	RS FAIT 1 (7)
IT-Umfeld	Unternehmensleitlinien, IT-Sicherheitskonzept, IT-Sicherheitshandbuch, IT-Strategie etc.	PS 330 (50)
Komplexität	- Größe und Komplexität des Unternehmens - Komplexität und Diversifikation der Geschäftstätigkeit - Komplexität der Geschäftsvorfälle - Komplexität des eingesetzten IT-Systems, die insbesondere von dem Grad der Integration in umfassende EDV-Lösungen abhängt - Komplexität der eingesetzten IT - Komplexität der IT-Systeme, die häufig ganze Prozessketten unterstützen - Komplexität der eingesetzten Hardware und der Netzkomponenten - Komplexität der IT-Anwendung	PS 260 (13), (29) PS 330 (10), (12), (18), (62) RS FAIT 1 (57)
Kontrollaktivitäten	Der Abschlussprüfer hat die Kontrollaktivitäten des Unternehmens zu beurteilen, um festzustellen, ob sie geeignet sind, wesentliche Fehler in der Rechnungslegung zu verhindern bzw. aufzudecken und zu korrigieren. Erfolgen diese Kontrollaktivitäten durch das Unternehmen nicht, kann sich der Abschlussprüfer insoweit nicht auf das interne Kontrollsystem stützen.	PS 260 (50), (51)
Kontrollrisiko	Hält der Abschlussprüfer das interne Kontrollsystem ganz oder teilweise für unwirksam, ist dementsprechend in einzelnen Prüffeldern von einem hohen Kontrollrisiko auszugehen.	PS 260 (64)
Logische Zugriffskontrollen	Unter Verwendung von Benutzer-ID und Passwörtern ist die Identität der Benutzer von IT-Systemen eindeutig festzustellen, um damit nicht autorisierte Zugriffe zu verhindern.	RS FAIT 1 (84)
Nachvollziehbarkeit	Ein sachverständiger Dritter muss in der Lage sein, sich in angemessener Zeit einen Überblick über die Geschäftsvorfälle und die Lage des Unternehmens zu verschaffen.	RS FAIT 1 (31)
Notbetrieb	Die Maßnahmen für den Notbetrieb ergänzen die Maßnahmen für den Regelbetrieb um organisatorische Regelungen und technische Verfahren zur Wiederherstellung der IT nach teilweisem oder vollständigem Ausfall der IT-Infrastruktur. Die Verfahren für den Notbetrieb umfassen organisatorische Regelungen zur Wiederherstellung der Betriebsbereitschaft und reichen von Maßnahmen bei Systemstörungen (Wiederanlaufkonzepte) bis hin zu Konzepten bei einem vollständigen Ausfall des IT-Systems (Katastrophenfallkonzept).	PS 330 (65) RS FAIT 1 (87)
Ordnung	Die Buchungen können sowohl in zeitlicher Ordnung (Journalfunktion) als auch in sachlicher Ordnung (Kontenfunktion) dargestellt werden.	RS FAIT 1 (30)
Ordnungsmäßigkeit, Kriterien für Ordnungsmäßigkeit	Bei Verarbeitung, Ausgabe und Aufbewahrung sind folgende Kriterien zu gewährleisten: Vollständigkeit, Richtigkeit, Zeitgerechtheit (Zeitgerechtigkeit), Ordnung, Nachvollziehbarkeit, Unveränderlichkeit.	PS 330 (8) RS FAIT 1 (25)
Organisatorische Sicherungsmaßnahmen	Organisatorische Sicherungsmaßnahmen werden durch laufende, automatische Einrichtungen wahrgenommen. Sie umfassen fehlerverhindernde Maßnahmen, die sowohl in die Aufbau- als auch die Ablauforganisation eines Unternehmens integriert sind und ein vorgegebenes Sicherheitsniveau gewährleisten sollen (z.B. Funktionstrennung, Zugriffsbeschränkungen im EDV-Bereich, Zahlungsrichtlinien).	PS 260 (6)

Begriff aus PS 330	Erläuterung	Quelle(n)
Physische Sicherungs-maßnahmen	Dienen dem Schutz der Hardware sowie der Programme und Daten vor Verlust, Zerstörung und unberechtigter Veränderung. Hierzu zählen bauliche Maßnahmen, Zugangskontrollen, Feuerschutzmaßnahmen und Maßnahmen zur Sicherung der Stromversorgung, die zur Sicherung der Funktionsfähigkeit der IT erforderlich sind.	PS 330 (54), (56) RS FAIT 1 (83)
Programmfunktion	- Funktionsfähigkeit der Programmfunktionen sowie der im Programm vorhandenen IT-Kontrollen im Hinblick auf die Einhaltung der Grundsätze ordnungsmäßiger Buchführung (Softwarebescheinigungen) - Funktionalität, Ordnungsmäßigkeit und Sicherheit - Vorliegen einer vollständigen und aktuellen Verfahrensdokumentation (Anwenderdokumentation, technische Systemdokumentation), - Weitere Informationen, die bei Programmprüfungen berücksichtigt werden können, sind u.a. Fachkonzepte, Berichtsprotokolle, Revisionsberichte, Dokumentation der Anwender- und Integrationstests sowie Abnahmeprotokolle.	PS 330 (72), (75) RS FAIT 1 (25)
Prüfbericht	Umfasst Arbeitspapiere und Prüfbericht. Art und Umfang sind abhängig von der Komplexität des geprüften IT-Systems und dem Umfang der Prüfung. Enthält eine Aussage zum Bestätigungsvermerk (erteilt, eingeschränkt erteilt, verweigert). Enthält Angaben zu - Ordnungsmäßigkeit der Buchführung - Sicherheit der rechnungslegungsrelevanten Daten - bestehende Mängel des IT-Kontrollsystems (auch wenn nicht rechnungslegungsrelevant) - soweit festgestellt: Verstöße gegen Datenschutzgesetze - Weist hin auf Systemschwächen von nicht rechnungslegungsrelevanten Bereichen. - Informiert über Verbesserungspotenziale.	PS 330 (108) bis (115)
Prüfung des internen Kontrollsystems	Entspricht der IT-Systemprüfung. Prüfung des IT-Überwachungssystems: - Prüfung des internen Kontrollsystems durch die Interne Revision - Prüfung des internen Kontrollsystems durch einen anderen externen Prüfer	PS 330 (29), (89)
Prüfungsplanung	Berücksichtigung der Auswirkungen des Einsatzes von IT im Unternehmen.Die Prüfungsplanung umfasst die Entwicklung einer Prüfungsstrategie und darauf aufbauend ein Prüfungsprogramm, da die im Einzelnen durchzuführenden Prüfungshandlungen enthält. Im Rahmen der Entwicklung der Prüfungsstrategie ist die Beurteilung der inhärenten IT-Risiken auf Unternehmensebene vorzunehmen.	PS 330 (48)
Prüfungsrisiko	Risiko der Abgabe eines positiven Prüfungsurteils trotz vorhandener Fehler in der Rechnungslegung. Das Risiko der Abgabe eines positiven Prüfungsurteils muss trotz vorhandener Fehler in der Rechnungslegung (Prüfungsrisiko) auf ein akzeptables Maß reduziert werden. Fehler können hierbei sowohl unabsichtlich als auch absichtlich entstanden sein. Der Abschlussprüfer muss die einzelnen Komponenten des Prüfungsrisikos kennen und analysieren. Das Prüfungsrisiko setzt sich aus den Fehlerrisiken und dem Entdeckungsrisiko zusammen. Fehlerrisiken beinhalten inhärente Risiken und Kontrollrisiken.	PS 260 (23), (24)
Prüfungswerkzeuge	Dienstprogramme, Utilities, in IT-Anwendungen eingebettete Prüfwerkwerkzeuge (Embedded Audit Routines), kontinuierliche Verarbeitung von Testfällen (Integrated Test Facility)	PS 330 (103)
Rechnungslegung	Umfasst die Buchführung, den Jahresabschluss und den Lagebericht bzw. auf Konzernebene den Konzernabschluss und den Konzernlagebericht.	PS 330 (8)
Rechnungslegungs-relevante Daten	Das sind Daten über Geschäftsvorfälle oder betriebliche Aktivitäten, die entweder direkt in die IT-gestützte Rechnungslegung einfließen oder als Grundlage für Buchungen im Rechnungslegungssystem dienen.	PS 330 (8)

Begriff aus PS 330	Erläuterung	Quelle(n)
Regelbetrieb	Der geordnete Regelbetrieb von IT-Anwendungen setzt dokumentierte Verfahrensabläufe für die Arbeitsvorbereitung, die Programmeinsatzplanung, den Betrieb von IT-Anwendungen und Netzwerken und für die Arbeitsnachbereitung voraus. Er umfasst sowie detaillierte organisatorische Anweisungen zur Abwicklung der Datenverarbeitung (z.B. RZ-Handbuch, Administratorenanweisungen) als auch technische Systeme zur Steuerung des Rechnerbetriebs (Jobsteuerungssysteme, Überwachungssysteme, Verfahren zur Gewährleistung eines operatorlosen RZ-Betriebs etc.).	PS 330 (62) RS FAIT 1 (87)
Richtigkeit	Die Belege und Bücher haben die Geschäftsvorfälle inhaltlich zutreffend abzubilden.	RS FAIT 1 (27)
Risiko	Risiko ist die Einwirkung von Unsicherheit auf die Erreichung der Unternehmensziele. Unrichtigkeiten (unbeabsichtigte Fehler) und Verstöße (Täuschungen, Vermögensschädigungen und Gesetzesverstöße) führen zu falschen Angaben im Abschluss (Verlust und Verfälschung von Buchungsstoff).	PS 210 (6), (22), (33)
Risikobeurteilung	Beurteilungen, um Risiken festzustellen und zu analysieren, die die Entwicklung des Unternehmens beeinträchtigen oder der Erreichung der Unternehmensziele entgegenstehen können. Das Verfahren und die Ergebnisse der Risikobeurteilungen des Unternehmens im Bereich Rechnungslegung stellen den Ausgangspunkt für die Risikobeurteilungen im Rahmen der risikoorientierten Prüfungsplanung des Abschlussprüfers dar. Umfasst alle wesentlichen Regelungen, die der Feststellung und Analyse von für die Rechnungslegung relevanten IT-Risiken (Auswirkung auf Ordnungsmäßigkeit und Verlässlichkeit der Rechnungslegung, Eintrittswahrscheinlichkeit, quantitative Auswirkungen) dienen (siehe auch Unternehmensrisiko)	PS 330 (15), (28)
Risikoindikatoren	Abhängigkeit, Änderungen, Know-how und Ressourcen, geschäftliche Ausrichtung	PS 330 (18)
Risikomanagement-system	Teilbereich des internen Kontrollsystems. Nach § 317 Abs. 4 HGB hat der Abschlussprüfer bei börsennotierten Aktiengesellschaften bei der Abschlussprüfung auch zu beurteilen, ob der Vorstand im Rahmen des Risikomanagements geeignete Maßnahmen getroffen hat, insbesondere ein Überwachungssystem eingerichtet hat, damit die Entwicklung den Fortbestand des Unternehmens gefährden, früh erkannt werden (Risikofrüherkennungssystem), und ob dieses Risikofrüherkennungssystem seine Aufgaben erfüllen kann.	PS 260 (10)
Risikoorientierter Prüfungsansatz	Eine risikoorientierte Prüfung kann an der Systematik der Rechnungslegung ansetzen oder von den Unternehmensfunktionen und -prozessen ausgehen. Bei einer Ausgestaltung des risikoorientierten Prüfungsansatzes, die sich an der Systematik der Rechnungslegung orientiert, werden die Prüffelder in Anlehnung an die Posten und Angaben der Rechnungslegung und deren Zusammenhänge untereinander bestimmt. Bei funktionsorientierter Ausgestaltung des Prüfungsansatzes werden die Prüffelder in Anlehnung an die betrieblichen Funktionen des Unternehmens bestimmt (z.B. Einkauf, Verkauf, Materialwirtschaft). Dieser Ansatz kann erweitert werden zu einer Orientierung an den Geschäftsprozessen des Unternehmens, bei dem die Prüffelder prozessorientiert festgelegt werden. Im Mittelpunkt stehen in diesem Falle z.B. finanzwirtschaftliche, personalwirtschaftliche oder Produktionsprozesse, die sich auf unterschiedliche betriebliche Funktionen auswirken.	PS 260 (23), (37) PS 330 (42)
Sicherheits-anforderungen	Authentizität, Autorisierung, Vertraulichkeit, Verbindlichkeit, Integrität, Verfügbarkeit	RS FAIT 1 (23)

Begriff aus PS 330	Erläuterung	Quelle(n)
Sicherheitskonzept	Umfasst technische und organisatorische Kontrollen. Das Sicherheitskonzept beinhaltet die Bewertung der Sicherheitsrisiken aus dem Einsatz von IT aus Sicht der gesetzlichen Vertreter und daraus abgeleitet die technologischen und organisatorischen Maßnahmen, um eine angemessene IT-Infrastruktur für die IT-Anwendungen zu gewährleisten sowie die ordnungsmäßige und sichere Abwicklung der IT-gestützten Geschäftsprozesse sicherzustellen. Die aus dem Sicherheitskonzept abgeleiteten Sicherungsmaßnahmen umfassen physische Sicherungsmaßnahmen und logische Zugriffskontrollen, Datensicherungs- und Auslagerungsverfahren.	PS 330 (21) RS FAIT 1 (22), (82)
Sicherung der Betriebsbereitschaft	Organisatorische Regelungen (Katastrophenfall-Handbuch) und technische Sicherungsmaßnahmen (z.B. redundante Auslegung der Hardware, vertragliche Back-up-Vereinbarungen, Ausweich-Rechenzentrum)	PS 330 (67)
Systemprüfung, IT-Systemprüfung	Prüfung der Elemente des IT-Systems eines Unternehmens, die dazu dient, Daten über Geschäftsvorfälle oder betriebliche Aktivitäten zu verarbeiten, die entweder direkt in die IT-gestützte Rechnungslegung einfließen oder als Grundlage für Buchungen im Rechnungslegungssystem in elektronischer Form zur Verfügung gestellt werden (rechnungslegungsrelevante Daten). Sie kann sich grundsätzlich auf die Elemente des IT-Systems beschränken, die für die IT-gestützte Rechnungslegung von wesentlicher Bedeutung sein können. Sie stellt einen Teilausschnitt aus der Prüfung des internen Kontrollsystems dar. Die IT-Systemprüfung setzt sich zusammen aus: - Aufnahme des IT-Systems - Aufbauprüfung - Funktionsprüfung Ziel der IT-Systemprüfung ist die Beurteilung der IT-Fehlerrisiken, d.h. des Risikos wesentlicher Fehler im IT-System, soweit diese rechnungslegungsrelevant sind. Der Abschlussprüfer hat die IT-Systemprüfung so zu planen und durchzuführen, dass die IT-Fehlerrisiken des im Unternehmen eingesetzten IT-Systems zutreffend beurteilt werden.	PS 330 (8) bis (11), (25), (29)
Test- und Freigabeverfahren	Trennung von Entwicklungs- und Testsystem von dem produktiv eingesetzten System (für den laufenden Geschäftsbetrieb eingesetztes System). Das Verfahren zur technischen Übergabe von Programmen muss gewährleisten, dass nur autorisierte und freigegebene Programme aus den Entwicklungs- bzw. Testbibliotheken in die Produktionsbibliotheken eingestellt werden können.	RS FAIT 1 (102)
Überwachung des internen Kontrollsystems, Überwachung des IT-Kontrollsystems	Beurteilung der Wirksamkeit des internen Kontrollsystems durch Mitarbeiter des Unternehmens. Dabei ist zu beurteilen, ob das interne Kontrollsystem sowohl angemessen ist als auch kontinuierlich funktioniert. Darüber hinaus hat die Unternehmensleitung dafür Sorge zu tragen, dass festgestellte Mängel im internen Kontrollsystem in geeigneter Weise abgestellt werden.	PS 260 (29) RS FAIT 1 (110), (112)
Überwachungstätigkeit	Beinhaltet im Einzelfall Aktivitäten, die durch die gesetzlichen Vertreter selbst ergriffen bzw. beauftragt werden und eine Beurteilung erlauben, ob die Strategien (Unternehmensstrategie und IT-Strategie), die daraus abgeleiteten Grundsätze, Verfahren und Maßnahmen (Regelungen) in Übereinstimmung mit den Unternehmenszielen umgesetzt wurden, ob das eingerichtete Kontrollsystem angemessen und wirksam ist und ob die umgesetzten Maßnahmen die Erreichung der Unternehmensziele sicherstellen.	RS FAIT 1 (111)
Unternehmensrisiko	Identifikation sämtlicher Risiken im Unternehmen, die sich auf die Ordnungsmäßigkeit und Verlässlichkeit der Rechnungslegung auswirken können und die Beurteilung von deren Tragweite in Bezug auf die Eintrittswahrscheinlichkeit und auf die quantitativen Auswirkungen.	PS 260 (47)

Begriff aus PS 330	Erläuterung	Quelle(n)
Unveränderlichkeit	Eine Eintragung oder Aufzeichnung darf nicht so verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist.	RS FAIT 1 (32)
Verantwortlichkeit des Prüfers bei IT-Systemprüfungen	Sie erstreckt sich in jedem Fall auf das gesamte rechnungslegungsrelevante IT-System (eigenständiger Rechenzentrumsbetrieb im Unternehmen und/oder ganz oder teilweise ausgelagert).	PS 330 (13)
Verarbeitungs-kontrolle	Die Daten durchlaufen den Verarbeitungsprozess vollständig und richtig.	RS FAIT 1 (95)
Verbindlichkeit	Unter Verbindlichkeit wird die Eigenschaft von IT-gestützten Verfahren verstanden, gewollte Rechtsfolgen bindend herbeizuführen.	RS FAIT 1 (23)
Verfahrens-dokumentation	Beschreibung, die alle zum Verständnis der Rechnungslegung erforderlichen Verfahrensbestandteile enthält. Die Verfahrensdokumentation in einer IT-gestützten Rechnungslegung besteht aus der Anwenderdokumentation und der technischen Systemdokumentation sowie der Betriebsdokumentation.	RS FAIT 1 (53), (54)
Verfügbarkeit	Verfügbarkeit verlangt zum einen, dass das Unternehmen zur Aufrechterhaltung des Geschäftsbetriebs die ständige Verfügbarkeit der IT-Infrastruktur, der IT-Anwendungen sowie der Daten gewährleistet. Zum anderen müssen die IT-Infrastruktur, die IT-Anwendungen und Daten sowie die erforderliche IT-Organisation in angemessener Zeit funktionsfähig bereitstehen.	RS FAIT 1 (23)
Verhaltensregeln, -anweisungen, Kodizes	Verständnis für eine verantwortungsvolle Führung der Geschäfte und für ethische Grundsätze an die Belegschaft	PS 210 (26)
Vertraulichkeit	Vertraulichkeit, dass von Dritten erlangte Daten nicht unberechtigt weitergegeben oder veröffentlicht werden.	RS FAIT 1 (23)
Vollständigkeit	Lückenlose Erfassung aller rechnungslegungsrelevanten Geschäftsvorfälle	RS FAIT 1 (26)
Wesentlichkeit	Die Wesentlichkeit des IT-Systems für die Rechnungslegung bzw. für die Beurteilung der Ordnungsmäßigkeit der Rechnungslegung. Die Wesentlichkeit kann in der absoluten Höhe oder in der Bedeutung der Angabe für die Rechnungslegung sowie darin begründet sein, dass die falsche Angabe zusammen mit anderen falschen Angaben wesentlich wird.	PS 260 (25) PS 330 (10)
Wiederherstellen der Betriebsbereitschaft	- Vorkehrungen gegen den Ausfall von IT - Gestaltung der organisatorischen Regelungen (Katastrophenfall-Handbuch) und der technischen Sicherungsmaßnahmen (z.B. redundante Auslegung der Hardware, vertragliche Back-up-Vereinbarungen, Ausweich-Rechenzentrum) - Zeitraum vom Eintreten eines Schadensfalls bis zur Wiederherstellung der Programmfunktionen und Programmabläufe	PS 330 (67)
Wirksamkeit	Wesentliche Fehler (in der Rechnungslegung) werden verhindert bzw. aufgedeckt und korrigiert. Die Beurteilung der Wirksamkeit der IT-Organisation kann beispielsweise anhand des Vergleichs der Arbeitsergebnisse der jeweiligen IT-Organisation mit branchentypischen Ausgestaltungen oder mit Best Practices vorgenommen werden. Weiterhin können Plausibilitätsbeurteilungen durch Verprobungen von kumulierten Verkehrszahlen oder Mengenströmen zwischen IT-Systemen oder deren Teilsystemen stattfinden. Die Prüfung der Wirksamkeit erstreckt sich zum einen auf die Übereinstimmung von definierten Verfahren mit den tatsächlichen Abläufen. Zum anderen ist in Stichproben zu prüfen, ob die eingerichteten Maßnahmen den tatsächlichen Aufgaben/ Anforderungen entsprechen.	PS 330 (26), (38), (58)
Zeitgerechtheit	Zuordnung der Geschäftsvorfälle zu Buchungsperioden sowie die Zeitnähe der Buchungen	RS FAIT 1 (28)
Zugriff, Zugriffskontrollen	Notwendige Maßnahme(n), um Autorisierung und Authentisierung sicherstellen zu können.	PS 330 (57) RS FAIT 1 (23)

10.2 Abkürzungsverzeichnis

Abkürzung	Langform
AO	**A**bgaben**o**rdnung
BDSG	**B**undes**d**atenschutz**g**esetz
BITKOM	**B**undesverband **I**nformationswirtschaft, **T**elekommuni**k**ati**o**n und neue **M**edien e.V.
BSI	**B**undesamt für **S**icherheit in der **I**nformationstechnik
CAAT	**C**omputer-**A**ssisted **A**udit **T**echniques
COBIT	**C**ontrol **Ob**jectives for **IT** and related **T**echnology
DIN	**D**eutsches **I**nstitut für **N**ormung
DIIR	**D**eutsches **I**nstitut für **I**nterne **R**evision e.V.
GoB	**G**rundsätze **o**rdnungsgemäßer **B**uchführung
GoBS	**G**rundsätze **o**rdnungsgemäßer DV-gestützter **B**uchführungs-**S**ysteme
HGB	**H**andels**g**esetz**b**uch
IDW	**I**nstitut **D**er **W**irtschaftsprüfer
IEC	**I**nternational **E**lectrotechnical **C**omitee
IKS	**I**nternes **K**ontrollsystem
ISACA	The **I**nformation **S**ystems **A**udit and **C**ontrol **A**ssociation
ISMS	**I**nformations**s**icherheits-**M**anagement**s**ystem
ISO	**I**nternational **O**rganization for **S**tandardization
ISO 27001	ISO/IEC 27001
ISO nnnnn	analog für andere Standards von ISO und ISO/IEC
IT	**I**nformations**t**echnologie
PS	**P**rüfungs**s**tandard
NIA	**N**ormenausschuss **I**nformationstechnik und **A**nwendungen
PS 330	IDW PS 330
PS nnn	analog für andere Standards des IDW
RS FAIT 1	**R**echnungslegungs**s**tandard **F**ach**a**usschuss **IT**
RZ	**R**echen**z**entrum
SGB	**S**ozial**g**esetz**b**uch
QM	**Q**ualitäts**m**anagement

10.3 Quellenverzeichnis

Internationale Normen

DIN EN ISO/IEC 17021:2006
Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren
Diese Norm beschreibt die Anforderungen zur Konformitätsbewertung.

DIN EN ISO 19011:2002
Leitfaden für Audits von Qualitätsmanagement- und/oder Umweltmanagementsystemen

ISO/IEC 27000:2009
Overview and vocabulary
Beschreibt Grundlagen von Managementsystemen für die Informationssicherheit, die Gegenstand der ISMS-Normenfamilie sind, und definiert zugehörige Begriffe.

DIN ISO/IEC 27001:2008
Informationssicherheits-Managementsysteme – Anforderungen
Beschreibt Anforderungen an die wirksame Planung, Umsetzung und Dokumentation eines ISMS. Dieses Dokument ist die Prüfungsgrundlage, nach der ein Unternehmen zertifiziert wird oder interne Audits durchgeführt werden können.

DIN ISO/IEC 27002:2008
Leitfaden für das Informationssicherheits-Management
Referenzdokument zur Errichtung eines Informationssicherheits-Managementsystems (kurz ISMS). Der Standard ist ein Leitfaden zur Implementierung eines ISMS.

ISO/IEC 27006:2007
Requirements for bodies providing audit and certification of information security management systems.
Diese Norm ergänzt ISO/IEC 17021 hinsichtlich der Beschreibung der Anforderungen für die Zertifizierung und Akkreditierung.

ISO/IEC 27014
Information security governance framework »Working draft Information security governance framework« verweist auf ISO/IEC 38500 IT-Governance. Diese Norm beschreibt, wie Managementsysteme auditiert werden.

ISO/IEC 38500:2008
Corporate Governance of Information Technology. Diese Norm beschreibt Führungsgrundsätze zur nachhaltigen Unternehmensführung in der IT.

IDW-Prüfungsstandards

IDW-EPS 210 (Stand: 2002)
Entwurf: Zur Aufdeckung von Unregelmäßigkeiten im Rahmen der Abschlussprüfung

IDW PS 240 (Stand: 2006)
IDW-Prüfungsstandard: Grundsätze der Planung von Abschlussprüfungen

IDW PS 260 (Stand: 2001)
IDW-Prüfungsstandard: Das interne Kontrollsystem im Rahmen der Abschlussprüfung

IDW PS 261 (Stand: 2006)
IDW-Prüfungsstandard: Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken

IDW PS 300 (Stand: 2006)
IDW-Prüfungsstandard: Prüfungsnachweise im Rahmen der Abschlussprüfung

IDW PS 312 (Stand: 2001)
IDW-Prüfungsstandard: Analytische Prüfungshandlungen

IDW PS 320 (Stand: 2004)
IDW-Prüfungsstandard: Verwendung der Arbeit eines anderen externen Prüfers

IDW PS 321 (Stand: 2002)
IDW-Prüfungsstandard: Interne Revision und Abschlussprüfung

IDW PS 322 (Stand: 2002)
IDW-Prüfungsstandard: Verwertung der Arbeit von Sachverständigen

IDW PS 330 (Stand: 2002)
IDW-Prüfungsstandard: Abschlussprüfung bei Einsatz von Informationstechnologie

IDW PS 340 (Stand: 2000)
IDW-Prüfungsstandard: Die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB

IDW PS 951 (Stand: 2007)
IDW-Prüfungsstandard: Die Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen für auf das Dienstleistungsunternehmen ausgelagerte Funktionen

IDW PS 880 (Stand: 1999)
IDW-Prüfungsstandard: Erteilung und Verwendung von Softwarebescheinigungen

IDW RS FAIT 1 (Stand: 2002)
IDW-Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Informationssicherheit – Ein Vergleich von Standards und Rahmenwerken

BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS), Version 1.5

BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, Version 2.0

BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz, Version 2.5

BSI-Standard 100-4: Notfallmanagement, Version 1.0

IT-Grundschutz-Kataloge, 11. Ergänzungslieferung, November 2009

Informationssicherheitsrevision
Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz, 2008

ISACA Reference

Val IT – »Getting Started With Value Management«

The Val IT Framework 2.0

The Val IT Framework 2.0 Extract

An Executive View of IT Governance

An Executive Primer on the Critical Role of IT Governance

ITGI Enables, ISO/IEC 38500:2008 Adaption

IT Governance and Process Maturity

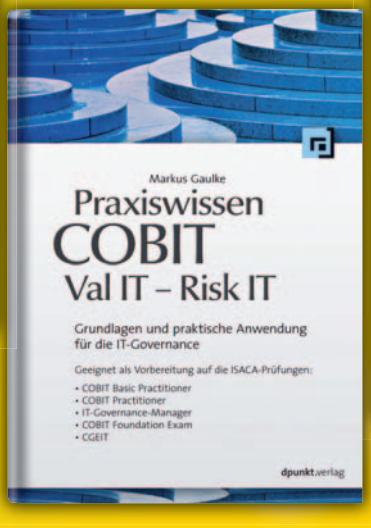
BITKOM

Leitfaden »Kompass der IT-Sicherheitsstandards« Version 2

dpunkt.it & business

dpunkt.verlag

2011, 356 Seiten
2. Auflage
€ 44,90 (D)
ISBN 978-3-89864-616-1



2010, 314 Seiten
€ 46,00 (D)
ISBN 978-3-89864-655-0

2010, 282 Seiten
€ 39,90 (D)
ISBN 978-3-89864-651-2

2010, 152 Seiten
€ 39,90 (D)
ISBN 978-3-89864-667-3

2011, 360 Seiten
4. Auflage
€ 42,90 (D)
ISBN 978-3-89864-703-8

2010, 218 Seiten
€ 36,00 (D)
ISBN 978-3-89864-647-5

2011, 256 Seiten
€ 29,90 (D)
ISBN 978-3-89864-654-3

2011, 157 Seiten
€ 19,90 (D)
ISBN 978-3-89864-717-5

dpunkt.verlag GmbH · Ringstraße 19 B · D-69115 Heidelberg
fon: 0 62 21 / 14 83 40 · fax: 14 83 99 · e-mail: bestellung@dpunkt.de

www.dpunkt.de

COBIT- und IT-Governance-Zertifikate des ISACA Germany Chapters

ISACA
Trust in, and value from, information systems
Germany Chapter

Der deutsche Berufsverband ISACA Germany Chapter e.V. hat ein Zertifikatsprogramm für Fachkräfte entwickelt, die sich auf dem Gebiet der **IT-Governance** und **IT-Compliance** weiterbilden und darüber einen anerkannten Nachweis erhalten wollen.

bereits über 1.600 Zertifikatsinhaber

Die COBIT-Zertifikate können beim ISACA Germany Chapter oder bei akkreditierten Schulungsanbietern erworben werden. Die Zertifikate IT-Governance- und IT-Compliance-Manager sind duale Zertifikate und werden ausschließlich in Zusammenarbeit mit dem ISACA Germany Chapter bei der Frankfurt School of Finance & Management angeboten.

Sie stellen auch eine ideale Vorbereitung für die internationale ISACA-Zertifizierung CGEIT dar.

Weitere Informationen zu den Zertifikaten erhalten Sie unter: www.isaca.de