Änderungen der Rechtsgrundlagen zum Thema Access Management / Zugriffsschutzsysteme in rechnungslegungsrelevanten ERP-Systemen // GoBD

Von Dipl.-Betriebswirt Christoph Wildensee, DBA, CISM, CRISC

Am 14.11.2014 veröffentlichte das Bundesministerium der Finanzen (BMF) die „**Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff**“, nachfolgend **GoBD** genannt. Es wird unter Ziffer 183 abschließend festgestellt, dass die GoBD an die Stelle der BMF-Schreiben vom 7.11.1995 (Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme [GoBS] und vom 16.7.2001 mit zusätzlichen Änderungen vom 14.9.2012 (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen [GDPdU]) treten, dies „für Veranlagungszeiträume, die nach dem 31. Dezember 2014 beginnen.“ **Interessant ist, welche Veränderungen sich hinsichtlich der Notwendigkeit und Ausgestaltung von Access Management, also der Anwendung und Gestaltung von Zugriffsschutzsystemen rechnungslegungsrelevanter ERP-Systeme, ergeben**.

Für Betrachtungen bis einschließlich 2014 ergibt sich für diese IT-Systeme das folgende Bild:

Grundlage	Gesetzestext	Bedeutung
§ 238 Abs. 1 HGB	Jeder Kaufmann ist verpflichtet, Bücher zu führen und in diesen seine Handelsgeschäfte und die Lage seines Vermögens nach den Grundsätzen ordnungsmäßiger Buchführung ersichtlich zu machen. Die Buchführung muss so beschaffen sein, dass sie einem sachverständigen Dritten innerhalb angemessener Zeit einen Überblick über die Geschäftsvorfälle und über die Lage des Unternehmens vermitteln kann. Die Geschäftsvorfälle müssen sich in ihrer Entstehung und Abwicklung verfolgen lassen.	Die Grundsätze des ehrbaren Handelns als Kaufmann mit der Darlegung der Unternehmensentwicklung ist zwar unter der gegebenen Fragestellung zunächst nicht wesentlich, der Verweis auf die GoB zeigt jedoch bereits an dieser Eingangsstelle des Gesetzes (3. Buch, 1. Abschnitt, Vorschriften für alle Kaufleute, 1. Unterabschnitt, Buchführung und Inventar) die Wichtigkeit der Verweisung auf die Grundsätze ordnungsmäßiger Buchführung. Verweis auf § 264ff HGB (Jahresabschluss der Kapitalgesellschaft und Lagebericht; Pflicht zur Aufstellung), §§ 297ff HGB (Inhalt und Form des Konzernabschlusses) und §§ 321, 322 HGB (Prüfung; Abschlussprüfer; Prüfungsbericht; Bestätigungsvermerk) ohne gesonderte Erläuterung.

§ 239 Abs. 2 HGB	Die Eintragungen in Büchern und die sonst erforderlichen Aufzeichnungen müssen vollständig, richtig, zeitgerecht und geordnet vorgenommen werden.	Vollständigkeit, Richtigkeit, Zeitgerechtigkeit und Ordnung der Aufzeichnungen sind wesentliche Aspekte der Ordnungsmäßigkeit. Fehlende Aufzeichnungen zu Geschäftsvorfällen, Lücken in den Nummernkreisen der Vorgänge, nicht korrekt darstellbare und zeitlich nicht korrekt zuweisbare Vorgänge sind Aspekte unzureichender Transparenz. Das HGB als eine der tragenden Säulen des kaufmännischen Rechnungswesens und des Jahresabschlusses dient vornehmlich dem Interessenschutz der Kapitalgeber als Gläubigerschutzregeln in Form von Vorgaben zur korrekten Darlegung der Geschäftstätigkeit und der Asset-Entwicklung. Einer Verschleierung von unternehmerisch tadeligem Handeln und der Entwertung des Unternehmens soll vorgebeugt werden.
§ 239 Abs. 3 HGB	Eine Eintragung oder eine Aufzeichnung darf nicht in einer Weise verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist. Auch solche Veränderungen dürfen nicht vorgenommen werden, deren Beschaffenheit es ungewiss lässt, ob sie ursprünglich oder erst später gemacht worden sind.	Diese Regelung ist eine der zentralen Vorgaben, die auf die Ausgestaltung von IT-Systemen mit Datenbank im Hintergrund wirkt. Die Änderung von Inhalten zu Geschäftsvorfällen darf folglich nicht ohne adäquate Protokollierung erfolgen. Änderungsbelege sind zu schreiben, um den ursprünglich erfassten Inhalt nicht zu überschreiben. Aber auch die Protokolldaten sind vor einem manipulierenden Zugriff zu schützen.
§ 239 Abs. 4 HGB	Die Handelsbücher und die sonst erforderlichen Aufzeichnungen können auch in der geordneten Ablage von Belegen bestehen oder auf Datenträgern geführt werden, soweit diese Formen der Buchführung ein-	In dieser Vorschrift wird explizit auf die Möglichkeit der Nutzung von softwarebasierten Lösungen hingewiesen, diese Anwendungen müssen aber den oben beschriebenen gesetzlichen Grund-

	schließlich des dabei angewandten Verfahrens den **Grundsätzen ordnungsmäßiger Buchführung** entsprechen. Bei der Führung der Handelsbücher und der sonst erforderlichen Aufzeichnungen auf Datenträgern muss insbesondere sichergestellt sein, dass die Daten während der Dauer der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb angemessener Frist lesbar gemacht werden können. Absätze 1 bis 3 gelten sinngemäß.	lagen entsprechen. Expliziter Verweis auf die GoB.
§ 243 Abs. 1 HGB	Der Jahresabschluss ist nach den Grundsätzen ordnungsmäßiger Buchführung aufzustellen.	In Verbindung mit § 242ff HGB ergibt sich die Pflicht zur Abschlussaufstellung mit der Darlegung des Verhältnisses von Vermögen und Schulden und der Gewinn- und Verlustrechnung. Die Bewertung erfolgt nach bestimmten Bewertungsmaßstäben, die an dieser Stelle keine Rolle spielen (siehe z.B. auch § 261 AktG und § 256 HGB mit Verweis auf die GoB). Der Verweis auf die GoB ist aber entscheidend, denn hiermit wird auch verweisen auf die Technik des Abschlusses innerhalb der zugrunde liegenden IT-Systeme mit der Zusicherung der Beleg-, Journal- und Kontenfunktion innerhalb der Buchführung.
§ 257 HGB	(1) Jeder Kaufmann ist verpflichtet, die folgenden Unterlagen geordnet aufzubewahren: 1. Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Einzelabschlüsse nach § 325 Abs. 2a, Lageberichte, Konzernabschlüsse, Konzernlageberichte sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen, 2. die empfangenen	Wesentlich ist hier neben der Kategorisierung von Unterlagen die Feststellung, dass sie auf Datenträgern aufbewahrt werden können, wenn sie der GoB entsprechen. Ferner sind die Unterlagen mit einer Aufbewahrungsfrist (und einem Fristbeginn) belegt worden. Dies hat folglich unmittelbar Wirkung auf IT-Systeme. Um die Performance von Applikationen im Zugriff auf die

	Handelsbriefe, 3. Wiedergaben der abgesandten Handelsbriefe, 4. Belege für Buchungen in den von ihm nach § 238 Abs. 1 zu führenden Büchern (Buchungsbelege). (2) Handelsbriefe sind nur Schriftstücke, die ein Handelsgeschäft betreffen. (3) Mit Ausnahme der Eröffnungsbilanzen und Abschlüsse können die in Absatz 1 aufgeführten Unterlagen auch als Wiedergabe auf einem Bildträger oder auf anderen Datenträgern aufbewahrt werden, wenn dies den Grundsätzen ordnungsmäßiger Buchführung entspricht und sichergestellt ist, dass die Wiedergabe oder die Daten 1. mit den empfangenen Handelsbriefen und den Buchungsbelegen bildlich und mit den anderen Unterlagen inhaltlich übereinstimmen, wenn sie lesbar gemacht werden, 2. während der Dauer der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb angemessener Frist lesbar gemacht werden können. Sind Unterlagen auf Grund des § 239 Abs. 4 Satz 1 auf Datenträgern hergestellt worden, können statt des Datenträgers die Daten auch ausgedruckt aufbewahrt werden; die ausgedruckten Unterlagen können auch nach Satz 1 aufbewahrt werden. (4) Die in Absatz 1 Nr. 1 und 4 aufgeführten Unterlagen sind zehn Jahre, die sonstigen in Absatz 1 aufgeführten Unterlagen sechs Jahre aufzubewahren. (5) Die Aufbewahrungsfrist beginnt mit dem Schluss des Kalenderjahrs, in dem die letzte Eintragung in das Handelsbuch gemacht, das Inventar aufgestellt, die Eröffnungsbilanz oder der Jahresabschluss festgestellt, der Einzelabschluss nach § 325 Abs. 2a oder der Kon-	Datenbestände zu erhöhen (nicht selten besonders bei Reportings), können im operativen Betrieb nicht mehr benötigte Unterlagen / Daten archiviert werden. Der Zugriff auf solche Daten muss allerdings im Bedarfsfall ebenso erfolgen wie auf die Daten, die im laufenden Betrieb zur Verfügung stehen.

	zernabschluss aufgestellt, der Handelsbrief empfangen oder abgesandt worden oder der Buchungsbeleg entstanden ist.	
§ 91 Abs. 2 AktG	Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.	Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) vom 27.04.1998 trat am 01.05.1998 in Kraft. Die Ergänzung des § 91 AktG (mit Verweis aus § 317 Abs. 4 HGB) um ein gefordertes Risikomanagement, das den Fortbestand der Gesellschaft gefährdende Entwicklungen beobachtet und im Bedarfsfall gegensteuert, war ein Novum mit Signalwirkung auch auf andere Rechtsformen von Unternehmen (siehe BT-Drs. 13/9712, S. 15). Dies korrespondiert auch mit § 289 Abs. 1 HGB (Lagebericht; „[…] In die Analyse sind die für die Geschäftstätigkeit bedeutsamsten finanziellen Leistungsindikatoren einzubeziehen und […] die Beträge und Angaben zu erläutern. Ferner ist im Lagebericht die voraussichtliche Entwicklung mit ihren wesentlichen Chancen und Risiken zu beurteilen und zu erläutern; zugrunde liegende Annahmen sind anzugeben. […]“) und mit dem Artikelgesetz „Gesetz zur Modernisierung des Bilanzrechts“ vom 25.05.2009, Inkrafttreten am 29.05.2009 (Anpassung des § 107 Abs. 3 AktG: „[…] Er kann insbesondere einen Prüfungsausschuss bestellen, der sich mit der Überwachung des Rechnungslegungsprozesses, der Wirksamkeit des internen Kontrollsystems, des Risikomanagementsystems und des internen Revisionssystems sowie der Abschlussprüfung,

		hier insbesondere der Unabhängigkeit des Abschlussprüfers und der vom Abschlussprüfer zusätzlich erbrachten Leistungen, befasst.“) Siehe hierzu z.B. auch §§ 317, 323 HGB und IDW PS 261 als Ersatz für IDW PS 260. Durch den Ausfall von IT-Systemen können immense Schäden entstehen (Forderungen verspätet verbucht, Vertragsstrafen durch verspätete Lieferung oder Zahlung, Imageschaden etc.), die es als Risikowahrnehmung zu behandeln gilt (siehe hierzu auch LÜCK(1998a), S. 9ff und LÜCK(1998b), S. 1924f.). Dies gilt für Handelssysteme ebenso wie für die Buchhaltungssysteme. Ferner ist aber noch wesentlich, dass auch die Archivierung und Datensicherung einbezogen wird in entsprechende Überlegungen, denn auch hier wird mit definierten Berechtigungen zugegriffen. Wesentlich ist außerdem der Einbezug dieser Systeme in Notfall- und Katastrophen-Szenarien und entsprechende Wiederanlaufkonzeptionen. Die Rolle der Internen Revision wird verzahnt über FAIT1.4.2(91) und FAIT1.4.5(112).
§ 146 Abs. 4 AO	Eine Buchung oder eine Aufzeichnung darf nicht in einer Weise verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist. Auch solche Veränderungen dürfen nicht vorgenommen werden, deren Beschaffenheit es ungewiss lässt, ob sie ursprünglich oder erst später gemacht worden sind.	Analog § 239 Abs. 3 HGB. Die Vorgabe unterstreicht, wie wichtig dem Gesetzgeber dieser Aspekt war und ist.

§ 7 Abs. 1 EnWG	Vertikal integrierte Energieversorgungsunternehmen haben sicherzustellen, dass Verteilernetzbetreiber, die mit ihnen im Sinne von § 3 Nummer 38 verbunden sind, hinsichtlich ihrer Rechtsform unabhängig von anderen Tätigkeitsbereichen der Energieversorgung sind.	Die Unabhängigkeit der Gesellschaften führt auch zur Notwendigkeit der Trennung von Systemen, wenn diskriminierungsfrei agiert werden soll.
§ 7 Abs. 2 EnWG	Vertikal integrierte Energieversorgungsunternehmen, an deren Elektrizitätsverteilernetz weniger als 100 000 Kunden unmittelbar oder mittelbar angeschlossen sind, sind hinsichtlich der Betreiber von Elektrizitätsverteilernetzen, die mit ihnen im Sinne von § 3 Nummer 38 verbunden sind, von den Verpflichtungen nach Absatz 1 ausgenommen. Satz 1 gilt für Gasverteilernetze entsprechend.	Die Beschränkung auf 100.000 Kunden verdeutlicht, dass die finanziellen und prozessualen Belastungen des IT-Einsatzes dem Gesetzgeber durchaus bewusst waren. Die Sicherstellung des diskriminierungsfreien Zugangs zu Informationen / Daten bleibt bestehen. Vgl. PWC(2012), S. 22f.
§ 7a Abs. 2 EnWG, § 7a Abs. 3 EnWG	(2) Für Personen, die für den Verteilernetzbetreiber tätig sind, gelten zur Gewährleistung eines diskriminierungsfreien Netzbetriebs folgende Vorgaben: 1. Personen, die mit Leitungsaufgaben für den Verteilernetzbetreiber betraut sind oder die Befugnis zu Letztentscheidungen besitzen, die für die Gewährleistung eines diskriminierungsfreien Netzbetriebs wesentlich sind, müssen für die Ausübung dieser Tätigkeiten einer betrieblichen Einrichtung des Verteilernetzbetreibers angehören und dürfen keine Angehörigen von betrieblichen Einrichtungen des vertikal integrierten Energieversorgungsunternehmens sein, die direkt oder indirekt für den laufenden Betrieb in den Bereichen der Gewinnung, Erzeugung oder des Vertriebs von Energie an Kunden zuständig sind. 2. Personen, die in anderen Teilen des vertikal integrierten Energiever-	Diese konsequent formulierte Leitungsaufgabentrennung und somit der Ausschluss von Aufgabenübernahmen in Personalunion des Stammhauses und des Verteilnetzbetreibers in einer Hand ist wichtig und zeigt, dass dem Gesetzgeber die Abhängigkeit der Leitungsebene des Verteilnetzbetreibers bewusst ist, wenn eine solche Forderung nicht im Gesetz aufgenommen wird. In der Praxis ergeben sich selbstverständlich trotzdem Reibungspunkte, die zu keiner Unabhängigkeit führen, sondern weiterhin gewisse Über- / Unterordnungsverhältnisse zementieren. Vgl. PWC(2012), S. 136.

	sorgungsunternehmens sonstige Tätigkeiten des Netzbetriebs ausüben, sind insoweit den fachlichen Weisungen der Leitung des Verteilernetzbetreibers zu unterstellen. (3) Unternehmen nach § 6 Absatz 1 Satz 1 haben geeignete Maßnahmen zu treffen, um die berufliche Handlungsunabhängigkeit der Personen zu gewährleisten, die mit Leitungsaufgaben des Verteilernetzbetreibers betraut sind.	
§ 7a Abs. 7 EnWG	Vertikal integrierte Energieversorgungsunternehmen, an deren Elektrizitätsverteilernetz weniger als 100 000 Kunden unmittelbar oder mittelbar angeschlossen sind, sind hinsichtlich der Betreiber von Elektrizitätsverteilernetzen, die mit ihnen im Sinne von § 3 Nummer 38 verbunden sind, von den Verpflichtungen nach Absatz 1 bis 6 ausgenommen. Satz 1 gilt entsprechend für Gasverteilernetze.	Siehe § 7 Abs. 2 EnWG
§ 20 Abs. 1 EnWG	Betreiber von Energieversorgungsnetzen haben jedermann nach sachlich gerechtfertigten Kriterien diskriminierungsfrei Netzzugang zu gewähren sowie die Bedingungen, einschließlich möglichst bundesweit einheitlicher Musterverträge, Konzessionsabgaben und unmittelbar nach deren Ermittlung, aber spätestens zum 15. Oktober eines Jahres für das Folgejahr Entgelte für diesen Netzzugang im Internet zu veröffentlichen. Sind die Entgelte für den Netzzugang bis zum 15. Oktober eines Jahres nicht ermittelt, veröffentlichen die Betreiber von Energieversorgungsnetzen die Höhe der Entgelte, die sich voraussichtlich auf Basis der für das Folgejahr geltenden Erlösobergrenze ergeben wird. Sie haben in dem Umfang	Die Diskriminierungsfreiheit im Zugang zu den Netzen ist ein wesentlicher Aspekt in der Ausgestaltung der bilateralen Verhältnisse des Verteilnetzbetreibers zu den vertrieblich aktiven Unternehmen. Dies führt aber auch dazu, dass die ehemals vertikal integrierten Unternehmen IT-Konstrukte schaffen müssen, um die Trennung der Daten des Netzes von denen des Vertriebs zu gewährleisten. Sinnvoll bleibt allerdings eine grundsätzliche Harmonisierung mit einheitlichen Referenzbegriffen. Das Gesetz legt sich nicht fest, ob es in den IT-Systemen ausreicht, lediglich eine Mandantentrennung vorzunehmen, oder ob eine Systemtrennung notwen-

	zusammenzuarbeiten, der erforderlich ist, um einen effizienten Netzzugang zu gewährleisten. Sie haben ferner den Netznutzern die für einen effizienten Netzzugang erforderlichen Informationen zur Verfügung zu stellen. Die Netzzugangsregelung soll massengeschäftstauglich sein.	dig ist. Wesentliches Merkmal ist aber, dass jede im Unternehmen wahrzunehmende Rolle weiß, welche Daten zur Kenntnis genommen und aufbereitet weitergegeben werden dürfen und welche Daten nicht zur Verfügung zu stellen sind. So ergibt sich, dass auch Shared-Service-Bereiche, die einen Zugriff auf beide Seiten benötigen, ihrer Rolle gerecht werden (Customer Care, IT, Revision, Recht, Personal etc.). Vgl. HODER(2009), S. 24f.
§ 21e und § 21i EnWG	§ 21e EnWG: […] (3) Die an der Datenübermittlung beteiligten Stellen haben dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, die insbesondere die Vertraulichkeit und Integrität der Daten sowie die Feststellbarkeit der Identität der übermittelnden Stelle gewährleisten. Im Falle der Nutzung allgemein zugänglicher Kommunikationsnetze sind Verschlüsselungsverfahren anzuwenden, die dem jeweiligen Stand der Technik entsprechen. […] § 21i EnWG: (1) Die Bundesregierung wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates [<*vornehmlich Definitionen für den Messstellenbetrieb*>…] (2) In Rechtsverordnungen nach Absatz 1 können insbesondere […] 8. die Einzelheiten der technischen Anforderungen an die Speicherung von Daten sowie den Zugriffsschutz auf die im elektronischen Speicher- und Verarbeitungsmedium abgelegten Daten geregelt werden; […]	Es wird die Möglichkeit aufgezeigt, dass Verordnungen erlassen werden, die den Betrieb der Messstellen und entsprechender IT-Systeme bzw. den Umgang mit anfallenden Daten im Bereich der technischen Messeinrichtungen konkretisieren, z.B. im Bereich Smart-Metering und der Erhebung, Übertragung, Speicherung und Verarbeitung von Messdaten. Es sei der Hinweis erlaubt, dass der Gesetzgeber eine weiter gefasste, „mutigere“ Regelung hätte treffen können, um die BNetzA in ihren Befugnissen zur IT-Vorgabensetzung zu stärken. Verordnungen sind ein probates Mittel, alle relevanten Unternehmen zu einem bestimmten Verhalten zu bewegen. Die Umsetzung von Vorgaben in IT-Abbildungen führt z.B. auch im Bereich der Übertragungsformate (EDI) zu Standards, die auch im Bereich des Umgangs mit Datenkonstrukten zu einer Vereinheitlichung hätte führen können. Der § 21e EnWG und die Verpflichtung auf die Sicherstellung von

		Vertraulichkeit und Datenintegrität bzw. der Nutzung von Verschlüsselungstechniken bei Versenden von Daten über das öffentliche Kommunikationsnetz (Internet) zeigt, dass eine konkrete Vorgabe möglich ist. Für die nachfolgende Betrachtung spielen die Punkte der §§ 21e und 21i EnWG eine eher untergeordnete Rolle, da es um technische Messeinrichtungen und deren Datenumgang unter dem Stichwort „Smart Metering“ geht, aber diese Grunddaten sind zur Abwicklung eines Belieferungsvertrags notwendig und insoweit als Vorsystem rechnungslegungsrelevant. In Zukunft wird die Relevanz steigen und dann auch für eine Betrachtung wie vorliegend maßgeblich sein.
Anlage zu § 9 BDSG	Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind, 1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle), 2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle), 3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unter-	Das Bundesdatenschutzgesetz ist eines der wenigen Gesetze in Deutschland, die so konkret eine Berechtigungskonzeption und auch eine Feststellung der Verursacher von Dateneingaben fordern. Das BDSG bezieht sich zunächst zwar nur auf Systeme, die personenbezogene Daten verarbeiten, dies ist allerdings immer dann der Fall, wenn sich in Systemen der Nutzer authentifizieren muss und diese Informationen verwendet werden innerhalb der Funktionalität des Systems, um verursachungsgerechtes Logging der Systemnutzung zu betreiben. Dies ist natürlich der Fall bei Systemen zur Kundenabrechnung und -fakturierung, der Lager- und Materialdisposition, der Personalplanung, der Personalabrech-

	liegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle), 4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle), 5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle), 6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle), 7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle), 8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.	nung, der Personalaktenverwaltung usw. Sofern keine zunächst eindeutige Erlaubnisnorm die Erhebung, Verarbeitung und/oder Nutzung der personenbezogenen oder -beziehbaren Daten erlaubt (gesetzliche oder gesetzeskonforme unternehmensinterne Regelung), ist eine Abwägung mit Erforderlichkeits- und Verhältnismäßigkeitsprüfung und entsprechend aussagekräftiger Dokumentation zum Erwägungsnachvollzug als Möglichkeit der Legitimation vorgesehen. Hier gilt allerdings das „ultima ratio“-Prinzip, d.h. der nachvollziehbaren Abwägung des geringsten probaten Mitteleinsatzes. Vgl. auch ERNESTUS, in: SIMITIS(2011), BDSG, § 9, Rn. 3-9, 23-46.
5.1 GoBS	Die starke Abhängigkeit des Unternehmens von ihren gespeicherten Daten macht ein ausgeprägtes Datensicherheitskonzept für	Es ist erkennbar, dass dem Bundesministerium der Finanzen durchaus die Brisanz der Datensicherheit i.e.S. / IT-

	das Erfüllen der GoBS unabdingbar. Dabei muss dem Unternehmen bewusst und klar sein, dass Datensicherheit nur dann hergestellt und auf Dauer gewährleistet werden kann, wenn bekannt ist, was, wogegen, wie lange und wie zu sichern ist und geschützt werden soll.	Sicherheit i.w.S. und speziell die Frage der Güte des Nachvollzugs auch nach längerer Zeit bekannt ist
5.5.1 GoBS	Der Schutz der Informationen gegen unberechtigte Veränderungen ist durch wirksame Zugriffs- bzw. Zugangskontrollen zu gewährleisten. Dies sind einmal die Zugriffsberechtigungskontrollen, die so zu gestalten sind, dass nur berechtigte Personen in dem ihrem Aufgabenbereich entsprechenden Umfang auf Programme und Daten zugreifen können. Es sind zum anderen die Zugangskontrollen zu den Räumen, in denen die Datenträger aufbewahrt werden. Diese Zugangskontrollen müssen verhindern, dass unberechtigte Personen Zugang zu Datenträgern haben. Sie müssen insbesondere auch für die Räumlichkeiten gelten, in die die Datenträger der Datensicherung ausgelagert sind.	Die Feststellung, dass das Zugriffsberechtigungsverfahren und der Nachweis der sachgerechten Vergabe von Zugriffsberechtigungen ebenfalls zur GoB gehören, um sicherzustellen, dass nicht von Unbekannten / Unbefugten Daten und Programme geändert werden können, ist wesentlich bei der Beurteilung von IT-Systemen. Zu erkennen ist deutlich, dass das Spektrum durchaus weiter zu fassen ist, wenn sogar der Zugangsschutz Erwähnung findet. Diese Vorschrift ist als zentral zu nennen. Sie korrespondiert mit der Vorschrift 6.2.4 GoBS.
5.7 GoBS	Das Datensicherungskonzept des Unternehmens ist zu dokumentieren. Dies gilt insbesondere für das Verfahren / die Prozeduren der Datensicherung […].	Die Prüfbarkeit ist nur gewährleistet, wenn das Ist der Datensicherheit dem Soll entspricht. Das Soll ist entsprechend detailliert zu beschreiben.
6.2.4 GoBS	Als Maßnahmen zur Wahrung der Datenintegrität sind alle Vorkehrungen zu beschreiben, durch die erreicht wird, dass Daten und Programme nicht von Unbefugten geändert werden können. Hierzu gehören neben der Beschreibung des Zugriffsberechtigungsverfahrens der Nachweis der sachgerechten Vergabe von Zugriffsberechtigungen.	Diese Feststellung zementiert, dass das Zugriffsberechtigungsverfahren und der Nachweis der sachgerechten Vergabe von Zugriffsberechtigungen wesentlich sind bei der Beurteilung von IT-Systemen. Diese Vorschrift ist ebenfalls als zentral zu nennen.

7 GoBS	Daten mit Belegfunktion sind grundsätzlich sechs Jahre, Daten und sonst erforderliche Aufzeichnungen mit Grundbuch- oder Kontenfunktion sind grundsätzlich zehn Jahre aufzubewahren.	Dies korrespondiert mit § 257 HGB.
9 GoBS	Für die Einhaltung der GoB – und damit auch der GoBS – ist auch bei einer DV-Buchführung allein der Buchführungspflichtige verantwortlich. Die Verantwortlichkeit erstreckt sich dabei auf den Einsatz sowohl von selbst- als auch fremderstellter DV-Buchführungssysteme. Wird die DV-Buchführung im Auftrag durch Fremdfirmen durchgeführt, obliegt die Einhaltung der GoB/GoBS ebenfalls dem auftraggebenden Buchführungspflichtigen.	Es ist wesentlich, dass das Unternehmen die Verantwortung für den Nachweis des ordnungsgemäßen Handelns nicht abgeben kann.
FAIT1.3.1(23)	[…] 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. Daher sind z.B. geeignete Back-up-Verfahren zur Notfallvorsorge einzurichten. Maßnahmen zur Sicherung der Verfügbarkeit sind erforderlich, um den Anforderungen nach Lesbarmachung der Buchführung gerecht zu werden. 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	Die Konkretisierung der Begriffe Verfügbarkeit, Autorisierung und Authentizität ist kein Kann-Anspruch, sondern unterstreicht, dass in Verbindung mit der GoB / GoBS zum einen ein Nachvollzug möglich ist, wenn der Verursacher eines Vorganges ermittelbar ist, und zum anderen, dass geeignete Backup- und Notfallkonzepte für eine „Langlebigkeit“ zu implementieren sind. Die Formulierung zur genehmigten Abbildung von Geschäftsvorfällen im System, zu den Zugriffsschutzmaßnahmen und zum Berechtigungsverfahren inkludiert eine Anmeldeprozedur und ein verursachungsgerechtes Logging.

	Löschen von Daten oder die Administration eines IT-Systems. Dadurch soll ausschließlich die genehmigte Abbildung von Geschäftsvorfällen im System gewährleistet werden. Geeignete Verfahren hierfür sind physische und logische Zugriffsschutzmaßnahmen (z.B. Passwortschutz). Organisatorische Regelungen und technische Systeme zum Zugriffsschutz sind die Voraussetzung zur Umsetzung der erforderlichen Funktionstrennungen. Neben Identitätskarten werden zukünftig biometrische Zugriffsgenehmigungsverfahren an Bedeutung gewinnen. […] Authentizität ist gegeben, wenn ein Geschäftsvorfall einem Verursacher eindeutig zuzuordnen ist. Dies kann bspw. über Berechtigungsverfahren geschehen. […]	
FAIT1.3.2(32)	Nach dem Buchungszeitpunkt darf entsprechend dem Grundsatz der Unveränderlichkeit eine Eintragung oder Aufzeichnung nicht so verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist (§ 239 Abs. 3 HGB). Daher sind spätere Eintragungen oder Aufzeichnungen ausschließlich so vorzunehmen, dass sowohl der ursprüngliche Inhalt als auch die Tatsache, dass Veränderungen vorgenommen wurden, in einer für einen sachverständigen Dritten in angemessener Zeit nachvollziehbaren Form erkennbar bleiben. Bei programmgenerierten bzw. programmgesteuerten Buchungen (automatisierte Belege bzw. Dauerbelege) sind Änderungen an den der Buchung zu Grunde liegenden Generierungs- und Steuerungsdaten ebenfalls aufzuzeichnen. Dies betrifft insbesondere die Protokollierung von Änderungen in	Die Vorschrift korrespondiert mit dem HGB und der GoB, insoweit ist erkennbar, dass sich bestimmte Inhalte wiederholen, aber auch in Nuancen angepasst werden. Der Hinweis auf die Aufzeichnungsnotwendigkeit von Generierungs- und Steuerungsdaten ist ebenfalls relevant. Der Aspekt der Protokollierung von Änderungen in rechnungslegungsrelevanten Einstellungen und Parametern der Software zeigt, dass erkannt wurde, wie Software mit darunterliegender Datenbank arbeitet. Die Praxis der Veränderungsbelegerzeugung auch bei Stammdatenänderungen ist ebenfalls hier begründet.

	rechnungslegungsrelevanten Einstellungen oder die Parametrisierung der Software und die Aufzeichnung von Änderungen an Stammdaten.	
FAIT1.3.2.2(40)	Die Autorisierung (Freigabe) der Buchung kann abhängig von der Entstehung des Belegs auf unterschiedliche Weise dokumentiert werden. […] Automatisch mit der Erfassung erstellte Belege […] werden durch die Benutzeridentifikation des verantwortlichen Mitarbeiters in Verbindung mit einem entsprechend ausgestalteten Zugriffsberechtigungsverfahren freigegeben. […]	Die Mitgabe von Benutzerkennzeichen zur Identifizierung der auslösenden Person bei Buchungen ist ein wesentliches Merkmal in den IT-Anwendungen.
FAIT1.3.2.6(62)	Zu den zum Verständnis der Buchführung erforderlichen Unterlagen zählen bei Individualsoftware neben der Anwenderdokumentation der Programm-Quellcode, der in maschinenlesbarer Form aufzubewahren ist, und die technische Systemdokumentation, soweit die entsprechenden Programme rechnungslegungsrelevant und somit für die Erfüllung der Beleg-, Journal- oder Kontenfunktion von Bedeutung sind.	Bei Individualsoftware gehören der Programmquellcode und die technische Systemdokumentation (sofern notwendig für die Erfüllung der Beleg-, Journal- oder Kontenfunktion) zu den aufbewahrungspflichtigen Unterlagen.
FAIT1.3.2.6(66)	Bei der Auslagerung von IT-Systemen und -Anwendungen muss der Servicegeber vertraglich verpflichtet werden, die für die Erfüllung der Buchführungspflichten des Servicenehmers erforderlichen Unterlagen aufzubewahren und auf Verlangen auszuhändigen. Hierzu zählen u.a. die Dokumentation der Programmablaufsteuerung (Job-Prozeduren) und die Dokumentation von Änderungen.	Auch hier wird wieder auf eine Facette hingewiesen. Obwohl die Verantwortung für den Buchführungspflichtigen und die Dokumentationspflichten bereits feststeht, sind vertragliche Zusicherungen möglich. Zu den Dokumenten zählen auch Programmablaufsteuerungen und die Dokumentation von Änderungen.
FAIT1.4.1(78)	[…] Die Anforderungen an die Gestaltung der IT-Organisation betreffen die Aufbau-	Die Abgrenzung der Organisation ist zunächst zwar nur mittelbar relevant für

	und Ablauforganisation. 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. 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.	die Definition von Berechtigungen. Jedoch ist die Definition einer adäquaten IT-Organisation mit der Bereitstellung von festgelegten Aufgaben, Kompetenzen und Verantwortung des IT-Betriebs eines der zentralen Glieder des Internen Kontrollsystems, wenn hier auch die Verantwortungsübernahme der Fachbereiche fehlt. Üblicherweise werden aufgabenbezogene Arbeitsplatzbeschreibungen (APBs) als Sollprofil hergestellt. Ein Stelleninhaber soll die dort formulierten Anforderungen möglichst vollumfänglich erfüllen. Enthalten ist auch die durch den Stelleninhaber bereitzustellende Kompetenz (Ausbildung etc.). Festgelegt wird auch die Verantwortung und zusätzlich, ob es sich um ein besonderes Maß der Verantwortung handelt wie Führungs- oder dezidierte Ergebnisverantwortung (Umsatzziele und andere quantitativen, aber auch qualitativen Zieldefinitionen). Hieraus ergibt sich in einem späteren Schritt die Festlegung von aufgaben- / rollenbasierten Berechtigungen. Dieser Punkt gilt aber grundsätzlich für alle Bereiche des Unternehmens und nicht nur für die IT.
FAIT1.4.2(84)	Durch logische Zugriffskontrollen z.B. unter Verwendung von Benutzer-ID und Passwörtern ist die Identität der Benutzer von IT-Systemen eindeutig festzustellen, um damit nicht autorisierte Zugriffe zu verhindern. Mitarbeitern sind nur die Berechtigungen zu erteilen, die zur Wahrnehmung ihrer Aufgaben erforderlich sind.	Die detaillierte Darlegung der Nutzung von Benutzer-IDs und Passwörtern zur Verhinderung unautorisierter Zugriffe zeigt, wie wichtig die Executive diese Punkte erachtet. Die Forderung der Darlegung von Prozessteilen in organisatorischen Grundsätzen / Reglungen unterstreicht den Grundsatz, dass im

	In organisatorischen Grundsätzen sind die Einrichtung, Änderung und Entziehung sowie die Sperrung von Berechtigungen, die Protokollierung aller Aktivitäten im Bereich der Berechtigungsverwaltung, die Gestaltung des Passwortes z.B. hinsichtlich Mindestlänge und Ablaufdatum und die Festlegung von aufgabenbezogenen Berechtigungsprofilen festzulegen.	Nachhinein ein Nachvollzug wesentlich ist.
FAIT1.4.2(91)	Katastrophenfall-Szenarien reichen von räumlich entfernten Rechenzentren, die (gegenseitig) die vollständige Rechenlast übernehmen können, über Backup-Rechner innerhalb oder außerhalb des Unternehmens bis zu Servicevereinbarungen zwischen Unternehmen und speziellen Backup-Dienstleistern oder Hardware-Herstellern und Lieferanten. Die Entscheidung des Unternehmens für ein spezifisches Szenario wird maßgeblich von der Abhängigkeit des Unternehmens von der Verfügbarkeit der IT-Anwendungen und der Art der eingesetzten IT-Infrastruktur bestimmt. Die Maßnahmen zum Notbetrieb bzw. zum Wiederanlauf sind entsprechend dem Sicherheitskonzept festzulegen, zu dokumentieren (Notfall- / Katastrophenhandbuch) und an die betroffenen Mitarbeiter zu kommunizieren. Die Wirksamkeit der umgesetzten Maßnahmen ist in regelmäßigen Zeitabständen zu trainieren und zu testen.	Hier wird explizit ein Backup- und ein Notfall- / Katastrophen- / Wiederanlauf-Konzept gefordert. Wesentlich bei einem Wiederanlauf-Konzept ist auch, dass die Systemabhängigkeiten beachtet werden, d.h. die Notwendigkeit des sequenziellen Anlaufs von IT-Systemen, die aufgrund von Schnittstellen u.Ä. ineinandergreifen und folglich nicht losgelöst voneinander wieder anstarten können, sondern ggf. auf den Start bzw. die Dienstebereitstellung bestimmter Systeme warten müssen.
FAIT1.4.3(104)	Voraussetzung für die Freigabe sind sowohl die erfolgreich getesteten Verarbeitungsfunktionen und -regeln der IT-Anwendung als auch das Vorliegen angemessener aktueller Anwender- und Verfah-	Neben den Freigabevoraussetzungen *bei Auswahl, Einführung, Implementierung und laufendem Betrieb mit Änderungsdienst* wird nochmals auf die Schnittstellenproblematik zu vor- und

	rensdokumentationen sowie die Funktionsfähigkeit von Schnittstellenprozessen zu vor- und nachgelagerten Anwendungen.	nachgelagerten Anwendungen hingewiesen. Dies ist wesentlich, denn die Transferdateien und -verzeichnisse bergen die Gefahr, dass aufgrund weitreichender Zugriffsrechte Manipulationen in den Dateien erfolgen können. Es ist ersichtlich, dass auch die Ebene des Betriebssystems (und der Datenbanken) folglich in die Betrachtung einzubeziehen ist (sind), denn hierüber können privilegierte Benutzer Manipulationen durchführen.
FAIT1.4.4(109)	Damit im Zusammenhang kann auch eine mangelnde Berücksichtigung der systemtechnischen Zusammenhänge stehen. Sie beinhaltet die Gefahr, dass bspw. Zugriffsrechte, Datensicherungsmaßnahmen etc. lediglich bezüglich der einzelnen IT-Teilsysteme wirksam sind und damit hinsichtlich des Teilprozesses, jedoch nicht hinsichtlich des Gesamtprozesses. Zugriffsschutz- oder Datensicherungsverfahren, die auf eine einzelne im Geschäftsprozess integrierte IT-Anwendung durch Manipulation in den vor- oder nachgelagerten IT-Teilsystemen reagieren, könnten gezielt umgangen werden.	In den heutigen Unternehmens-IT-Umgebungen ist eine isolierte Betrachtung von IT-Systemen in ihrer Risikoanfälligkeit unzureichend, denn über Schnittstellen werden übergreifend Daten / Informationen zusammengetragen, um betriebswirtschaftlich fundierte Aussagen herzustellen oder auch nur Daten analog der gesetzlichen Vorgaben zu konsolidieren. Die Manipulierbarkeit von IT-Systemen bei isolierter Betrachtung wird herausgestellt und die Wichtigkeit einer solchen Sicht unterstrichen.
FAIT1.4.5(112)	In zahlreichen Unternehmen wird neben prozessintegrierten Überwachungsmaßnahmen das IT-Kontrollsystem von der internen Revision überwacht. Zu den Aufgaben der internen Revision zählt die Beurteilung der Wirksamkeit des eingerichteten IT-Kontrollsystems sowie die Überwachung der Einhaltung der Regelungen und Anforderungen der gesetzlichen Vertreter und der Ordnungsmäßigkeit z.B. durch eine	Mit Verweis auf den IDW- Prüfungsstandard PS 321 (Interne Revision und Abschlussprüfung) wird hier die Rolle der Internen Revision herausgestellt bei der Beurteilung der Wirksamkeit der „Internal Controls“ und der Einhaltung von Regelungen.

	regelmäßige Überwachung sensitiver IT-gestützter Geschäftsprozesse.	
FAIT2.1(2)	Rechnungslegungsrelevante E-Commerce-Systeme lassen Daten über betriebliche Aktivitäten entweder direkt (d.h. ohne manuelle Eingaben) in die IT-gestützte Rechnungslegung einfließen oder stellen diese Daten in elektronischer Form als Grundlagen für Buchungen im Rechnungslegungssystem zur Verfügung.	E-Commerce-Systeme als Vor- oder Nebensysteme des Buchhaltungshauptsystems.
FAIT2.2.2.1(12)	Neben den rechnungslegungsspezifischen Vorschriften des HGB (§§ 238f. HGB) und den Grundsätzen ordnungsmäßiger Buchführung (GoB) bestehen beim Einsatz von E-Commerce zahlreiche weitere rechtliche Anforderungen. Diese betreffen beispielsweise den Schutz von personenbezogenen Daten oder - bei Rechtsgütern wie Urheberschutzrechten - das anzuwendende Vertragsrecht. Darüber hinaus sorgt die Internationalität des Internets und damit verbunden die grenzüberschreitende Geschäftsabwicklung für weitere rechtliche Problemstellungen. Diese betreffen z.B. nationale und internationale Rechtsfragen des Handelsrechts, des Steuerrechts, des Strafrechts, des Zivilrechts oder des Datenschutzes.	Rechtsnormerweiterung bei E-Commerce.
FAIT2.5.1(32)	Die Autorisierung soll sicherstellen, dass keine unberechtigten bzw. keine fiktiven Geschäftsvorfälle in das System eingehen. Es muss festgelegt sein, wann, wie und durch wen die Autorisierung erfolgt.	Die Mitgabe von Benutzerkennzeichen zur Identifizierung der auslösenden Person bei Buchungen und der Zeitstempel mit der auslösenden Funktion / Transaktion ist ebenfalls ein wesentliches Merkmal in den IT-Anwendungen.
FAIT2.Anh.1.1.4	Zur Risikoreduzierung werden nachfolgend Maßnahmen genannt, die jedoch nicht isoliert, sondern als Teil eines umfassen-	Der explizite Verweis auf verlässliche Zugriffsschutzverfahren und Benutzerberechtigungskonzepten sowie einem

	den Systems zur Vermeidung von IT-Risiken unter Einbeziehung der E-Commerce-Risiken zu betrachten sind. Voraussetzung für die Wirksamkeit der im Weiteren dargestellten Maßnahmen ist die Einrichtung von generellen IT-Kontrollen, insbesondere von verlässlichen Zugriffsschutzverfahren (Benutzerberechtigungskonzepten) sowie effektiven Change Management-Verfahren.	effektiven Change-Management unterstreicht die Wesentlichkeit von Kontrollen auch im Bereich der Berechtigungsvergabe.
FAIT3.7.2(53)	Durch physische Sicherungsmaßnahmen sind die IT-Infrastruktur beim Einsatz von Archivierungsverfahren und die Speichermedien vor Verlust, Zerstörung oder unberechtigter Veränderung zu schützen.	Diese Regelung für Archivierungssysteme korrespondiert mit §§ 239, 257 HGB, § 146 AO, FAIT1.3.2(32).
FAIT3.7.2(54)	Neben den Zugriffsschutzmechanismen der Rechnungslegungssysteme muss zum Schutz der archivierten Daten und Dokumente auch im Archivierungssystem ein geeignetes Berechtigungskonzept implementiert werden. Dies kann auch durch ein anwendungsübergreifendes Berechtigungskonzept gewährleistet werden.	Der Verweis auf ein dezidiertes Berechtigungskonzept auch im Archivierungssystem mit dem Hinweis auf eine anwendungsübergreifende Konzeption ist wesentlich und hebt dies nochmals heraus.
FAIT3.7.3(62)	An die Funktionalitäten der Archivierungssoftware sind folgende Mindestanforderungen zu stellen: - Protokollierung der durchgeführten Archivierung - Sicherstellung der Datenkonsistenz durch Plausibilitätskontrollen - Differenziertes Berechtigungskonzept.	Die Funktionsbereitstellung innerhalb eines Archivierungssystems beinhaltet nochmals den Grundsatz des „Need-to-Know“-Prinzips, ausgedrückt als „Differenziertes Berechtigungskonzept“.
FAIT3.7.4.3(74)	Häufig werden die zu archivierenden Daten und Dokumente vor der Speicherung auf einem Langzeitmedium zwischengespeichert. Darüber hinaus werden Zwischenspeicher für die Optimierung des Zugriffs	Der Einbezug von Zwischenspeicher (auch im Sinne von Schnittstellenbelieferungen und Transferdateien / -verzeichnissen) ist wesentlich zur Gewährleistung einer Gesamtbetrachtung der

	auf archivierte Daten und Dokumente eingesetzt. Daher müssen geeignete Berechtigungskonzepte gewährleisten, dass Daten im Zwischenspeicher des Archivierungssystems nicht verändert werden können. Zugriffe der für die Systemverwaltung verantwortlichen Mitarbeiter müssen anhand entsprechender Protokollierungen nachvollziehbar sein.	Funktionalitäten.
FAIT4.3(15)	Voraussetzung für eine Reduzierung der Risiken aus IT-gestützten Konsolidierungsprozessen ist die Wirksamkeit von generellen IT-Kontrollen. Zu den generellen IT-Kontrollen gehören insb. Kontrollen für eine konsistente Berechtigungsvergabe, Kontrollen zur Stammdatenänderung sowie Kontrollen im Bereich des Changemanagements und des IT-Betriebs.	Eine konsistente Berechtigungsvergabe bei Konsolidierungsprozessen, Kontrollen zur Stammdatenänderung und Kontrollen im Bereich des Change-Managements und des IT-Betriebs sind Aufgaben des Internen Kontrollsystems der einsetzenden Fachbereiche, aber auch Prüfobjekte der Internen Revision.
FAIT4.4.1(19)	[…] Autorisierung bedeutet, dass nur im Voraus festgelegte Personen auf Daten zugreifen können […] und dass nur sie die für das System definierten Rechte wahrnehmen können. Dadurch soll ausschließlich die genehmigte Abbildung von konsolidierungsbedingten Anpassungsmaßnahmen im IT-System gewährleistet werden. Geeignete Verfahren hierfür sind physische Zugriffsschutzmaßnahmen und Berechtigungskonzepte. Authentizität ist gegeben, wenn eine konsolidierungsbedingte Anpassungsmaßnahme einem Verursacher eindeutig zuzuordnen ist. Dies kann bspw. über Berechtigungs- und Protokollierungsverfahren geschehen. […]	Auch in Konsolidierungsprozessen sind die Vorgaben der Berechtigungs- und Protokollierungsverfahren wesentlich. Ansonsten weitgehend analoge Formulierungen aus der GoBS und FAIT1.
FAIT4.4.2(26)	Abhängig von dem eingesetzten Verfahren kann die Autorisierung gemeldeter Daten auf unterschiedliche Weise dokumentiert	Analog zuvor.

	werden: […] Bei der elektronischen Übernahme von Meldedaten kann die Autorisierung durch die Benutzeridentifikation des für die Meldedaten verantwortlichen Mitarbeiters in Verbindung mit einem entsprechend ausgestalteten Zugriffsberechtigungsverfahren erfolgen. Bei programmintern generierten Vorgängen erfolgt die Autorisierung durch die IT-Anwendung. Aus der Verfahrensdokumentation müssen die Regeln für Generierung und Kontrolle der maschinell generierten Vorgänge eindeutig erkennbar sein. Die freigegebenen Programme müssen gegen unautorisierte und undokumentierte Änderungen geschützt sein.	
FAIT4.5.1(35)	Im IT-Umfeld und in der IT-Organisation sind generelle IT-Kontrollen vorzusehen, die sicherstellen, dass die IT-Anwendung zur Konzernrechnungslegung sowie die verarbeiteten rechnungslegungsrelevanten Daten den zu stellenden Ordnungsmäßigkeits- und Sicherheitsanforderungen entsprechen. Generelle IT-Kontrollen im Zusammenhang mit IT-gestützten Konsolidierungsprozessen betreffen insbesondere: - Kontrollen für eine konsistente Berechtigungsvergabe - Kontrollen zur Stammdatenänderung - logische Zugriffskontrollen sowie - Kontrollen im Bereich des Changemanagements im Zusammenhang mit der Entwicklung, Einführung und Änderung von IT-Anwendungen (Programmänderungen).	Analog zuvor.
FAIT4.5.1(36)	Für eine konsistente und adäquate Berechtigungsvergabe ist es notwendig, dass Be-	An dieser Stelle wird explizit vermerkt, dass kritische Berechtigungen und Be-

	nutzern keine kritischen Berechtigungen und Berechtigungskombinationen zugewiesen werden (bspw. Änderungen der Stammdaten und deren Freigabe). Ferner ist sicherzustellen, dass die eingerichteten logischen Zugriffskontrollen wirksam sind und damit die Beachtung der Ordnungsmäßigkeits- und Sicherheitsanforderungen an die IT-gestützte Konzernrechnungslegung sicherstellen.	rechtigungskombinationen (Kollisionen) auszuschließen sind. In einer solchen Detaillierung findet sich eine IT- / berechtigungsbezogene Vorgabe nicht. Zutreffend für SAP SEM BCS (Business Consolidation).
GDPdU.I.1	Das Recht auf Datenzugriff beschränkt sich ausschließlich auf Daten, die für die Besteuerung von Bedeutung sind (steuerlich relevante Daten). Die Daten der Finanzbuchhaltung, der Anlagenbuchhaltung und der Lohnbuchhaltung sind danach für den Datenzugriff zur Verfügung zu halten. Soweit sich auch in anderen Bereichen des Datenverarbeitungssystems steuerlich relevante Daten befinden, sind sie durch den Steuerpflichtigen nach Maßgabe seiner steuerlichen Aufzeichnungs- und Aufbewahrungspflichten zu qualifizieren und für den Datenzugriff in geeigneter Weise vorzuhalten.	Das Recht auf Ausübung des Datenzugriffs in seinen drei Varianten zeigt deutlich, welche Anforderungen an IT-Anwendungen und den darunter liegenden Datenbanken gestellt werden. Spätestens bei der Überlassung von Daten in Form von auswertbaren Tabellenstrukturen mit Cross-Referenzierung ergeben sich erhebliche Aufwände für die Unternehmen. Softwareprodukte wie SAP ERP haben entsprechende Objekte definiert, die bei der Generierung von Datenextrakten helfen. Auch Fremdanbieter liefern Software zur GDPdU-konformen Generierung von Datenextrakten.
GDPdU.I.1	Bei der Ausübung des Rechts auf Datenzugriff stehen der Finanzbehörde nach dem Gesetz drei Möglichkeiten zur Verfügung. Die Entscheidung, von welcher Möglichkeit des Datenzugriffs die Finanzbehörde Gebrauch macht, steht in ihrem pflichtgemäßen Ermessen; falls erforderlich, kann sie auch mehrere Möglichkeiten in Anspruch nehmen:	
GDPdU.I.2	[…] Beim unmittelbaren Datenzugriff […] Die Zugangsberechtigung muss so ausgestaltet sein, dass dem Prüfer dieser Zugriff	Details zu I.1.a)

	auf alle steuerlich relevanten Daten eingeräumt wird. Sie umfasst u.a. auch die Nutzung der im DV-System vorhandenen Auswertungsprogramme. Enthalten elektronisch gespeicherte Datenbestände andere, z.B. steuerlich nicht relevante personenbezogene oder dem Berufsgeheimnis (§ 102 AO) unterliegende Daten, so obliegt es dem Steuerpflichtigen oder dem von ihm beauftragten Dritten, **durch geeignete Zugriffsbeschränkungen sicherzustellen**, dass der Prüfer nur auf steuerlich relevante Daten des Steuerpflichtigen zugreifen kann. Die Zugangsberechtigung hat auch die Nutzung der im DV-System vorhandenen Auswertungsprogramme zu umfassen. Das Datenverarbeitungssystem muss die Unveränderbarkeit des Datenbestandes gewährleisten […].	

Tab. 1: Beispiele rechtlicher Grundlagen und deren Bedeutung für die Beurteilung von IT-Systemen (ohne MaRisk).

Es ist unproblematisch zu erkennen, dass durch die Substitution der Bestimmungen der GoBS und GDPdU durch die **GoBD** zunächst auch ohne inhaltliche Betrachtung der GoBD gar nicht wesentlich in die Regulation eingegriffen wurde, denn auch weiterhin sind konkrete Vorgaben z.B. aus dem BDSG und vornehmlich aus **FAIT-Verlautbarungen** maßgeblich, um feststellen zu können, dass **abgestufte und legitimierende Zugriffsschutzsysteme zu implementieren** sind, wo dies möglich ist.

Was bedeutet aber die Neufassung der verabschiedeten GoBD mit Wirkung ab 2015 ? Nachfolgende Tabelle erläutert wesentliche Aspekte der GoBD.

GOBD.6(100)	Für die Einhaltung der Ordnungsvorschriften des § 146 AO (siehe unter 3.) hat der Steuerpflichtige **Kontrollen einzurichten, auszuüben und zu protokollieren**. Hierzu gehören beispielsweise • **Zugangs- und Zugriffsberechtigungs-**	Dieser Bereich sagt bereits sehr viel aus über die Notwendigkeit der Ausgestaltung von Schutzsystemen und der notwendigen Prüfungen und internen Kontrollen. Die Frage steht aber auch im Raum, welche Konsequenzen

	kontrollen, auf Basis entsprechender Zugangs- und Zugriffsberechtigungskonzepte (z. B. spezifische Zugangs- und Zugriffsberechtigungen), **• Funktionstrennungen,** • Erfassungskontrollen (Fehlerhinweise, Plausibilitätsprüfungen), • Abstimmungskontrollen bei der Dateneingabe, • Verarbeitungskontrollen, **• Schutzmaßnahmen gegen die beabsichtigte und unbeabsichtigte Verfälschung von Programmen, Daten und Dokumenten.** Die konkrete Ausgestaltung des Kontrollsystems ist abhängig von der Komplexität und Diversifikation der Geschäftstätigkeit und der Organisationsstruktur sowie des eingesetzten DV-Systems.	drohen bei Nichtbeachtung.
GOBD.6(101)	Im Rahmen eines funktionsfähigen IKS muss auch anlassbezogen (z. B. Systemwechsel) geprüft werden, **ob das eingesetzte DV-System tatsächlich dem dokumentierten System entspricht** […]	Soll-Ist-Abgleich, aber nur anlassbezogen. Der Begriff Anlass wird nicht konkretisiert und ist somit nach Maßgabe der Unternehmensinteressen zu sehen.
GOBD.6(102)	Die Beschreibung des IKS ist Bestandteil der Verfahrensdokumentation (siehe unter 10.1).	Eine Verfahrensdokumentation ist selbstverständlich auch weiterhin notwendig und vom Steuerpflichtigen für den IT-Einsatz zu erstellen.
GOBD.7(103)	Der Steuerpflichtige hat sein DV-System gegen Verlust (z. B. Unauffindbarkeit, Vernichtung, Untergang und Diebstahl) zu sichern **und gegen unberechtigte Eingaben und Veränderungen (z. B. durch Zugangs- und Zugriffskontrollen) zu schützen.**	Eindeutig notwendige Schutzmaßnahmen sind zu ergreifen gegen unberechtigte / unbefugte Manipulation.

GOBD.7(104)	Werden die Daten, Datensätze, elektronischen Dokumente und elektronischen Unterlagen **nicht ausreichend geschützt und können deswegen nicht mehr vorgelegt werden, so ist die Buchführung formell nicht mehr ordnungsmäßig.**	**Die Konsequenz: Verlust des Status „ordnungsmäßig“.**
GOBD.7(106)	Die Beschreibung der Vorgehensweise zur Datensicherung ist Bestandteil der Verfahrensdokumentation (siehe unter 10.1). Die konkrete Ausgestaltung der Beschreibung ist abhängig von der Komplexität und Diversifikation der Geschäftstätigkeit und der Organisationsstruktur sowie des eingesetzten DV-Systems.	
GOBD.8(107)	Nach § 146 Absatz 4 AO darf eine Buchung oder Aufzeichnung nicht in einer Weise verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist. Auch solche Veränderungen dürfen nicht vorgenommen werden, deren Beschaffenheit es ungewiss lässt, ob sie ursprünglich oder erst später gemacht worden sind.	Verweis auf Abgabenordnung. Eindeutiges Verfahren zum Replace in Tabellen durch Edit oder Programmen ist notwendig.
GOBD.8(108)	Das zum Einsatz kommende DV-Verfahren muss die Gewähr dafür bieten, dass alle Informationen (Programme und Datenbestände), die einmal in den Verarbeitungsprozess eingeführt werden (Beleg, Grundaufzeichnung, Buchung), nicht mehr unterdrückt oder ohne Kenntlichmachung überschrieben, gelöscht, geändert oder verfälscht werden können. Bereits in den Verarbeitungsprozess eingeführte Informationen (Beleg, Grundaufzeichnung, Buchung) dürfen nicht ohne Kenntlichmachung durch neue Daten ersetzt werden.	Gleiches gilt dann auch für Veränderungsbelegdaten, da diese als Ergebnis des hier Gesagten zu sehen sind.

GOBD.8(109)	Beispiele 7 für unzulässige Vorgänge: • Elektronische Grund(buch)aufzeichnungen aus einem Kassen- oder Warenwirtschaftssystem **werden über eine Datenschnittstelle in ein Office-Programm exportiert, dort unprotokolliert editiert und anschließend über eine Datenschnittstelle reimportiert**. **• Vorerfassungen, Stapelbuchungen werden bis zur Erstellung des Jahresabschlusses und darüber hinaus offen gehalten. Alle Eingaben können daher unprotokolliert geändert werden.**	
GOBD.8(110)	Die Unveränderbarkeit der Daten, Datensätze, elektronischen Dokumente und elektronischen Unterlagen (vgl. Rzn. 3 bis 5) kann sowohl hardwaremäßig (z. B. unveränderbare und fälschungssichere Datenträger) als auch softwaremäßig (z. B. Sicherungen, Sperren, Festschreibung, Löschmerker, automatische Protokollierung, Historisierungen, Versionierungen) als auch organisatorisch (**z. B. mittels Zugriffsberechtigungskonzepten**) gewährleistet werden. Die Ablage von Daten und elektronischen Dokumenten in einem Dateisystem erfüllt die Anforderungen der Unveränderbarkeit regelmäßig nicht, soweit nicht zusätzliche Maßnahmen ergriffen werden, die eine Unveränderbarkeit gewährleisten.	
GOBD.8(111)	Spätere Änderungen sind ausschließlich so vorzunehmen, dass sowohl der ursprüngliche Inhalt als auch die Tatsache, dass Veränderungen vorgenommen wurden,	Wieder Verweis auf AO.

	erkennbar bleiben. Bei programmgenerierten bzw. programmgesteuerten Aufzeichnungen (automatisierte Belege bzw. Dauerbelege) sind Änderungen an den der Aufzeichnung zugrunde liegenden Generierungs- und Steuerungsdaten ebenfalls aufzuzeichnen. Dies betrifft insbesondere die Protokollierung von Änderungen in Einstellungen oder die Parametrisierung der Software. Bei einer Änderung von Stammdaten (z. B. Abkürzungs- oder Schlüsselverzeichnisse, Organisationspläne) muss die eindeutige Bedeutung in den entsprechenden Bewegungsdaten (z. B. Umsatzsteuerschlüssel, Währungseinheit, Kontoeigenschaft) erhalten bleiben. Ggf. müssen Stammdatenänderungen ausgeschlossen oder Stammdaten mit Gültigkeitsangaben historisiert werden, um mehrdeutige Verknüpfungen zu verhindern. **Auch eine Änderungshistorie darf nicht nachträglich veränderbar sein.**	[GOBD.8(108)]
GOBD.8(112)	**Werden Systemfunktionalitäten oder Manipulationsprogramme eingesetzt, die diesen Anforderungen entgegenwirken, führt dies zur Ordnungswidrigkeit der elektronischen Bücher und sonst erforderlicher elektronischer Aufzeichnungen.**	**Die Konsequenz: Verlust des Status „ordnungsmäßig“.**
GOBD.10(146)	Auch an die DV-gestützte Buchführung wird die Anforderung gestellt, dass **Geschäftsvorfälle für die Dauer der Aufbewahrungsfrist retrograd und progressiv prüfbar bleiben müssen**.	
GOBD.10(148)	Von einem sachverständigen Dritten kann zwar Sachverstand hinsichtlich der Ordnungsvorschriften der §§ 145 bis 147 AO	So ist also folglich die Bereitstellung von Informationen und Zugriffen auszulegen und auszugestalten.

	und allgemeiner DV-Sachverstand erwartet werden, nicht jedoch spezielle, produktabhängige System- oder Programmierkenntnisse.	
GOBD.10(150)	Für die Prüfung ist eine aussagefähige und aktuelle Verfahrensdokumentation notwendig, die alle System- bzw. Verfahrensänderungen inhaltlich und zeitlich lückenlos dokumentiert.	Verfahrensdokumentation inkl. Zugriffsschutzsystem
GOBD.10.1(151)	Da sich die Ordnungsmäßigkeit neben den elektronischen Büchern und sonst erforderlichen Aufzeichnungen auch auf die damit in Zusammenhang stehenden Verfahren und Bereiche des DV-Systems bezieht (siehe unter 3.), muss für jedes DV-System eine übersichtlich gegliederte Verfahrensdokumentation vorhanden sein, aus der Inhalt, Aufbau, Ablauf und Ergebnisse des DV-Verfahrens vollständig und schlüssig ersichtlich sind. Der Umfang der im Einzelfall erforderlichen Dokumentation wird dadurch bestimmt, was zum Verständnis des DV-Verfahrens, der Bücher und Aufzeichnungen sowie der aufbewahrten Unterlagen notwendig ist. Die Verfahrensdokumentation muss verständlich und damit für einen sachverständigen Dritten in angemessener Zeit nachprüfbar sein. Die konkrete Ausgestaltung der Verfahrensdokumentation ist abhängig von der Komplexität und Diversifikation der Geschäftstätigkeit und der Organisationsstruktur sowie des eingesetzten DV-Systems.	Nicht wesentlich anders zur GoBS.
GOBD.10.1(152)	Die Verfahrensdokumentation beschreibt den organisatorisch und technisch gewollten Prozess, z. B. bei elektronischen Dokumenten von der Entstehung der Informa-	Natürlich auch das Zugriffsschutzsystem

	tionen über die Indizierung, Verarbeitung und Speicherung, dem eindeutigen Wiederfinden und der maschinellen Auswertbarkeit, **der Absicherung gegen Verlust und Verfälschung** und der Reproduktion.	
GOBD.11.2(174)	Beim unmittelbaren Datenzugriff hat der Steuerpflichtige dem Prüfer die für den Datenzugriff erforderlichen Hilfsmittel zur Verfügung zu stellen und ihn für den Nur-Lesezugriff in das DV-System einzuweisen. **Die Zugangsberechtigung muss so ausgestaltet sein, dass dem Prüfer dieser Zugriff auf alle aufzeichnungs- und aufbewahrungspflichtigen Daten eingeräumt wird. Sie umfasst die im DV-System genutzten Auswertungsmöglichkeiten (z. B. Filtern, Sortieren, Konsolidieren) für Prüfungszwecke, (z. B. in Revisionstools, Standardsoftware, Backofficeprodukten)**. In Abhängigkeit vom konkreten Sachverhalt kann auch eine vom Steuerpflichtigen nicht genutzte, aber im DV-System vorhandene Auswertungsmöglichkeit verlangt werden. Eine Volltextsuche, eine Ansichtsfunktion oder ein selbsttragendes System, das in einer Datenbank nur die für archivierte Dateien vergebenen Schlagworte als Indexwerte nachweist, reicht regelmäßig nicht aus. Eine Unveränderbarkeit des Datenbestandes und des DV-Systems durch die Finanzbehörde muss seitens des Steuerpflichtigen oder eines von ihm beauftragten Dritten gewährleistet werden.	Ehemals GDPdU

Tab. 2: Ausgesuchte Grundlagen der GoBD für rechnungslegungsrelevante ERP-Systeme mit Wirkung ab 2015.

Fazit

Aus profunder Sicht ergeben sich keine negativen Veränderungen der GoBD (für steuerliche Veranlagungszeiträume ab 2015) gegenüber der GoBS und GDPdU (für steuerliche Veranlagungszeiträume bis einschließlich 2014). Im Gegenteil. Es sind eher übersteigerte Erwartungen seitens des BMF, die über das Machbare in Unternehmen hinausgehen. [THELEN(2015), S. 142] Es werden aber an einigen Stellen konkrete Formulierungen gewählt, die keine Interpretation zulassen, dass bei bestimmten Inhalten bzw. Manipulationen der Verlust des Status „ordnungsmäßig gefahrenes rechnungslegungsrelevantes IT-System“ droht. An zwei Stellen wird dies besonders deutlich. Der Verlust von Daten durch nicht ausreichenden Schutz dieser führt nach GOBD.7(103) und (104) zur Zuerkennung des Status „**formell nicht mehr ordnungsmäßig**“. Werden Systemfunktionen oder Manipulationsprogramme nach GOBD.8(112) verwendet, die die Anforderungsumsetzungen nach GOBD.8(111) terminieren bzw. diesen entgegenstehen, führt dies ebenso zur Attributzuweisung „**Ordnungswidrigkeit der elektronischen Bücher** […]“. [THELEN(2015), S. 142] Der Wirtschafts- / Abschlussprüfer findet folglich an dieser Stelle eine Eindeutigkeit vor, die bisher so klar kaum formuliert war.

Entsprechend sollten sich zumindest die Bereiche Finanz- und Rechnungswesen, SAP-Betrieb und Interne Revision gemeinsam einem unsachgemäßen Fahren des produktiven SAP ERP-Systems entgegenstellen. Dies gilt insbesondere für den Bereich der Eigenentwicklung und auch des hierfür oft genutzten externen Dienstleistereinsatzes. Es ist ferner zu bedenken, dass eine solche Wirkung auch über ein unsachgemäßes Fahren von Vor- und Nebensystemen erfolgen kann, so dass eine übergreifende Betrachtung dieser Problematik notwendig ist.

Literatur

GOBD(2014), Schreiben des Bundesministeriums der Finanzen vom 14.11.2014, IV A 4 - S 0316/13/10003, http://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/Datenzugriff_GDPdU/2014-11-14-GoBD.pdf?__blob=publicationFile&v=1 .

GOBS(1995), Schreiben des Bundesministeriums der Finanzen vom 7.11.1995, IV A 8 - S 0316 - 52/95 - BStBl 1995 I S. 738, http://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Betriebspruefung/015.pdf?__blob=publicationFile&v=3 .

GM(1984), Verwendung von Mikrofilmaufnahmen zur Erfüllung gesetzlicher Aufbewahrungspflichten, IV A 7- S 0318-1/84, BStBl I S. 155, http://dms-portal.net/wp-content/uploads/2015/01/BMF-Schr-Microfilm_Erlass-1984.pdf .

GDPDU(2001), Schreiben des Bundesministeriums der Finanzen vom 16.7.2001, IV D 2 - S 0316 - 136/01 - BStBl I S. 415, http://www.baron-consult.de/Archiv/GDPdU.pdf .

GDPDU(2012), Änderung des BMF-Schreibens „Grundsätze zum Datenzugriff und zur Prüfung digitaler Unterlagen (GDPdU)“ IV A4 - S 0316/12/10001, http://www.cdh.de/user/eesy.de/cdh.de/dwn/bmf_13_datenzugriff.pdf .

HODER(2009), Kerstin Hoder, Analyse von Dienstleistungen und Shared-Service-Gesellschaften in der Energiewirtschaft, Diplomarbeit 2009, TU München, http://www.suportica.de/download/diplomarbeit-suportica.pdf.

LÜCK(1998a), Elemente eines Risikomanagementsystems, in: DB, 51(1998), S. 8-14.

LÜCK(1998b), Der Umgang mit unternehmerischen Risiken durch ein Risikomanagementsystem und durch ein Überwachungssysten, in: DB, 51(1998), S. 1925-1930.

PWC(2012), PricewaterhouseCoopers (Hrsg.), Entflechtung und Regulierung in der deutschen Energiewirtschaft, 3. Auflage, Freiburg 2012.

SIMITIS(2011), Simitis (Hrsg.), Bundesdatenschutzgesetz, 7. Auflage 2011.

THELEN(2015), GoBD - Die Büchse der Pandora? in: PRev Revisionspraxis, 3/2015, S. 140-144.

FAIT1-3: http://www.beidatsch.net/wp-content/uploads/gobs_0**x**_idw_rs_fait**y**.pdf (x=2-4; y=x-1).

GoBS, GDPdU, BMF: http://www.elektronische-steuerpruefung.de/rechtsgrund/a_rechtsgrund.htm ,

http://www.elektronische-steuerpruefung.de/bmf/a_bmf.htm .