Vorbemerkung

Nr.	Anmerkungen	aba-Änderungsvorschlag
10 (neu)	Allgemeine Verweise auf das Proportionalitätsprinzip in der Vorbemerkung 6 sowie die im Konsultationsentwurf als Ergänzung vorgesehene Fußnote sind nicht ausreichend, um offene Fragen zur Umsetzbarkeit der Anforderungen für viele EbAV, insbesondere Unternehmenseinrichtungen, zu beantworten. Aus diesem Grund schlagen wir die Aufnahme einer neu eingefügten Ziffer 10 vor, die auf einer bislang in den Erläuterungen zur Randziffer 1.1 getroffenen Feststellung zur Rolle von Trägerunternehmen als mögliche IT-Dienstleister aufbaut. (Die bisherigen Nr. 10 bis 11 würden zu Nr. 11 bis 12).	*10. IT-Dienstleister im Sinne dieses Rundschreibens können auch die Trägerunternehmen von EbAV sein. Das Rundschreiben berücksichtigt dabei im Sinne des Proportionalitätsprinzips die Situation vieler Einrichtungen, insbesondere von Unternehmenseinrichtungen, die in die IT-Strukturen ihrer Trägerunternehmen eingebunden sind und daher keine eigenständige IT-Struktur haben. Ist die IT von EbAV durch die Ausstattung und die Prozesse ihrer Trägerunternehmen bestimmt, können VAIT-Anforderungen auch durch IT-Standards, sofern deren Zielsetzung und Anforderungen mit VAIT vergleichbar sind, erfüllt werden. Daneben sind die Anforderungen insbesondere in den entsprechenden Ausgliederungsvereinbarungen und sonstigen Verträgen zu berücksichtigen.*

Kapitel 1: IT-Strategie

Rn.	Anmerkungen	aba-Änderungsvorschlag
Übergreifend	Überschriften für die linken und rechten Spalten wären hilfreich, um die unterschiedliche Bedeutung klarzustellen.	Wir regen folgende Überschriften an: • linke Spalte "aufsichtsrechtliche Anforderungen" • rechte Spalte "Erläuterungen".
Übergreifend	Betreffend die Punkte 1.1, 3.5, 3.8, 3.10, 4.4, 4.9., 4.10: Die Anforderung "regelmäßig" in Verbindung mit "anlassbezogen" ist nicht durchgängig eindeutig definiert im Rundschreiben. In 3.10.	

Rn.	Anmerkungen	aba-Änderungsvorschlag
	heißt es "regelmäßig, mindestens jedoch jährlich", in 4.10 "regelmäßig, mindestens vierteljährlich". Hier ist eine Klarstellung für die Praxis wünschenswert, dass "regelmäßig" im Regelfall einen jährlichen Turnus meint, ein anderer Zeitraum hingegen sollte im Rundschreiben in den jeweiligen Abschnitten explizit genannt werden. Die häufig auftretende Bezeichnung "regelmäßig und anlassbezogen" legt die Anforderung "laufend" sehr nahe bzw. permanente Aktivitäten in den IT-Prozessen. Dies ist schwer umsetzbar. Wir bitten darum, die Anforderungen für EbAV so zu fassen, dass sie auch umsetzbar sind.	
1.1	Es handelt sich hier weitgehend um eine neue Anforderung. In der derzeit gültigen Fassung sollte (nur) die IT-Strategie überprüft werden; nun soll ergänzend die Umsetzung der Ziele überwacht und gemessen werden. Für beide Sachverhalte soll ein eigenständiger (gemeinsamer) Prozess eingerichtet werden. Dies kann insbesondere bei komplexen IT-Strategien (dynamisches IT-Umfeld und zahlreiche ggf. auch konträre Ziele) sinnvoll sein. U.E. sollte der Aufwand von EbAV mit einfachen IT-Strategien oder mit einer Strategie, die grundsätzlich der Strategie des Trägerunternehmens folgt, auf prozessualer Ebene möglichst geringgehalten werden. Generell sollte ein eigenständiger Prozess nur erforderlich sein, sofern das Profil dies erfordert. Dies entspricht auch der Anforderung in Rn. 8.3 der MaGo für EbAV in Bezug auf die „Interne Prüfung der Geschäftsorganisation“ (Rz. 49, Satz 3: „Ein gesonderter Prozess ist nicht erforderlich.“).	Der Text der Rn. 1.1 sollte (durch Streichungen und Ergänzungen) wie folgt geändert werden: *Die Geschäftsleitung hat eine mit der Geschäftsstrategie konsistente IT-Strategie festzulegen, in der die Ziele sowie die Maßnahmen zur Erreichung dieser Ziele dargestellt werden. Die Geschäftsleitung muss für die Umsetzung der IT-Strategie Sorge tragen. Sie überprüft diese regelmäßig und anlassbezogen und passt diese erforderlichenfalls an. Die Geschäftsleitung überwacht dabei insbesondere die Umsetzung der Ziele der IT-Strategie. ~~hat zur Überwachung und Messung der Umsetzung der Ziele der Strategie sowie zu ihrer Beurteilung und Anpassung einen Prozess einzurichten. Dieser Prozess ist regelmäßig und anlassbezogen zu überprüfen und erforderlichenfalls anzupassen.~~ Ein gesonderter Prozess ist hierfür bei EbAV nicht erforderlich.* Alternativ könnte eine Formulierung genutzt werden, die einen *„Prozess gemäß bzw. dem Profil/Risikoprofil folgend“* vorsieht.

Rn.	Anmerkungen	aba-Änderungsvorschlag
1.2	Diese Ergänzung dient der Konkretisierung der vorgeschlagenen neuen Vorbemerkung Nr. 9. Sie berücksichtigt die Situation vieler EbAV, insbesondere von Unternehmenseinrichtungen, die über keine eigene IT-Infrastruktur verfügen und die die Auslagerungsentscheidungen als solche als Gegenstand ihrer IT-Strategie betrachten.	In den Erläuterungen zu Rn. 1.2 soll der Satz *IT-Dienstleister in diesem Sinne können auch Trägerunternehmen sein.* wie folgt ergänzt werden: *Dabei kann die Erfüllung der Vorgaben aus diesem Rundschreiben durch angemessene Regelungen in Ausgliederungsvereinbarungen und sonstigen Verträgen sichergestellt werden.*
1.2	Problematisch ist für uns die Abkehr vom Begriff der „*Dienstleistungsbeziehung*“, die regelmäßig insbesondere eine vertragliche Beziehung im IT-Bereich vorausgesetzt hat. Die Formulierung „sonstiger wichtiger Abhängigkeiten“ ist u.E. zu unbestimmt. Sie sollte ergänzt werden um einen Bezug zur „Informationssicherheit“ (also einen Begriff, der weiter gefasst ist als „IT“).	Der Text der Rn. 1.2 sollte (bis zum Aufzählungspunkt a) wie folgt gefasst werden: *Der Detaillierungsgrad der IT-Strategie ist abhängig vom Risikoprofil des Unternehmens. Mindestinhalte sind:* *(a) strategische Entwicklung der IT-Aufbau- und IT-Ablauforganisation des Unternehmens, der Ausgliederungen von IT-Dienstleistungen und sonstige ~~wichtige~~ wesentliche Abhängigkeiten von Dritten mit Bezug zur Informationssicherheit sowie zum isolierten Bezug von Hard- und/oder Software (zusammen auch „isolierter Bezug von IT“);*

Kapitel 2: IT-Governance

Rn.	Anmerkungen	aba-Änderungsvorschlag
2.1	Die Leitlinien sollten nur bei „wesentlichen" Veränderungen „relevanter Aktivitäten und Prozesse zeitnah" anzupassen sein. Für kleinere und normale Veränderungen sollte ein angemessener Zyklus, z.B. im	Der Text der Rn. 2.1 sollte (durch Formulierungsänderungen im letzten Satz) wie folgt gefasst werden:

Rn.	Anmerkungen	aba-Änderungsvorschlag
	Rahmen des regelmäßigen Überprüfungsprozesses genügen, siehe auch Regelungen und Formulierung in 4.2, hier wird auf "wesentliche Veränderungen" abgestellt.	*2. 1 Die IT-Governance im Sinne dieses Rundschreibens ist die Struktur zur Steuerung sowie Überwachung des Betriebs und der Weiterentwicklung der IT-Systeme einschließlich der dazugehörigen IT-Prozesse auf Basis der IT-Strategie. Hierfür maßgeblich sind insbesondere die Vorgaben zur IT- Aufbau- und IT-Ablauforganisation, zum Informationsrisiko- sowie Informationssicherheitsmanagement, zur quantitativ und qualitativ angemessenen Ressourcenausstattung der IT (personelle, finanzielle und sonstige Ressourcen) sowie zum Umfang und zur Qualität der technisch-organisatorischen Ausstattung. Die Leitlinien für die IT-Aufbau- und IT-Ablauforganisation sind bei wesentlichen Veränderungen relevanter ~~der~~ Aktivitäten und Prozesse zeitnah anzupassen.*
2.2	Für EbAV sind Anforderungen an die Interne Revision in den MaGo für EbAV in Rn. 9.3 geregelt. Hier wird die Überprüfung der gesamten Geschäftsorganisation gefordert. Anforderungen an die Interne Revision sollten daher weiterhin im Gesamtzusammenhang und damit ausschließlich in der MaGo für EbAV konkretisiert betrachtet werden.	In der Erläuterung der Rn. 2.2 sollte mit Blick auf die Situation bei EbAV auf die Ergänzung des vorgeschlagenen neuen Satzes 3 verzichtet werden: *Die Geschäftsleitung hat den Leitlinien zur IT-Aufbau- und IT -Ablauforganisation zumindest bei Erstverabschiedung sowie bei nicht geringfügigen Änderungen zuzustimmen. Sollen geringfügige Änderungen vom Zustimmungserfordernis ausgenommen werden, hat das Unternehmen im Vorfeld festzulegen, welche Änderungen als geringfügig einzuschätzen sind. ~~Die Vorgaben zur IT-Governance sind Bestandteil regelmäßiger Überprüfungen durch bezüglich IT hinreichend qualifizierte interne Revisoren.~~*

Kapitel 3: Informationsrisikomanagement

Rn.	Anmerkungen	aba-Änderungsvorschlag
3.4	Die vorgeschlagene Ergänzung dient der Klarstellung und Eingrenzung der Erläuterung zu dieser Anforderung.	Die Erläuterungen zu Rn. 3.4 sollten (am Satzende von Satz 2) wie folgt ergänzt werden: *Zu einem Informationsverbund gehören beispielsweise geschäftsrelevante Informationen, Geschäfts- und Unterstützungsprozesse, IT-Systeme und die zugehörigen IT-Prozesse sowie Netz- und Gebäudeinfrastrukturen. Abhängigkeiten und Schnittstellen berücksichtigen auch die Vernetzung des Informationsverbundes mit Dritten, die einen IT-Bezug aufweisen.*
3.5	Mit der vorgeschlagenen Neufassung der Rn. 3.5 soll das Proportionalitätsprinzip auch bei der Feststellung des Schutzbedarfs verankert werden. Die Schutzbedarfsanalyse ist ein wesentlicher Bestandteil der VAIT, der mit einem hohen Aufwand verbunden ist. U.E. sollten insbesondere Bestandteile des Informationsverbundes mit hohem bzw. sehr hohem Schutzbedarf regelmäßig überprüft werden („Kronjuwelen“). Bei der Konkretisierung von „regelmäßig“ soll die Situation von Unternehmen berücksichtigt werden, die ein „stabiles“ Geschäftsfeld bedienen, da hier nicht „jeden Monat neue Kronjuwelen“ eintreffen. Für den aba-Änderungsvorschlag spricht auch die Anforderung in Rn. 3.6, in der eine angemessene Überprüfung durch das Informationsrisikomanagement gefordert wird.	Im Text der Rn. 3.5 sollte (durch Streichungen bzw. einen ergänzten Satz) wie folgt gefasst werden: *Das Unternehmen hat ~~regelmäßig und anlassbezogen~~ den Schutzbedarf für die Bestandteile seines definierten Informationsverbundes, insbesondere im Hinblick auf die Schutzziele „Integrität“, „Verfügbarkeit“, „Vertraulichkeit“ und „Authentizität" zu ermitteln.* *Der Turnus der Überprüfung folgt dabei dem Risikoprofil des Unternehmens und dem Schutzbedarf der einzelnen Bestandteile des Informationsverbundes oder anlassbezogen.*
3.5	Die im Konsultationsdokument neu vorgesehene Formulierung *„Die Eigentümer der Informationen bzw. die Fachbereiche, die verantwortlich für die Geschäftsprozesse sind, verantworten die Ermittlung des*	Im Text der Rn. 3.5 bitten wir außerdem darum, auf den vorgeschlagenen, neuen Satz 2 zu verzichten:

Rn.	Anmerkungen	aba-Änderungsvorschlag
	Schutzbedarfs.“ ist u.E. nicht verhältnismäßig, da diesen Organisationseinheiten regelmäßig die dafür nötigen Fachkenntnisse fehlen. Sie sollte daher gestrichen werden.	~~*Die Eigentümer der Informationen bzw. die Fachbereiche, die verantwortlich für die Geschäftsprozesse sind, verantworten die Ermittlung des Schutzbedarfs.*~~
3.8	Ein Governance-Rahmen regelt klar auch die Verantwortlichkeiten für den Umgang mit Risiken, was unmittelbar auch die Abgrenzung von Kompetenzen beinhaltet. Wir regen daher an, auf die Aussage, dass die Risikoanalyse zu koordinieren ist, ebenfalls zu verzichten. Der letzte Satz stiftet Verwirrung und sollte ebenfalls gestrichen werden.	Der Text der Rn. 3.8 sollte wie folgt gefasst werden (Straffungs- und Streichungsvorschlag): *3. 8 Das Unternehmen hat auf Basis der festgelegten Risikokriterien regelmäßig eine Risikoanalyse durchzuführen und die Ergebnisse zu dokumentieren. ~~Die Risikoanalyse ist zu koordinieren und zu dokumentieren~~. Risikoreduzierende Maßnahmen aufgrund unvollständig umgesetzter Sollmaßnahmen sind wirksam zu koordinieren, zu dokumentieren, zu überwachen und zu steuern. Die Ergebnisse der Risikoanalyse sind in den Prozess des Managements der operationellen Risiken zu überführen. ~~Die Behandlung der Risiken ist kompetenzgerecht zu genehmigen~~*
3.9	Die Formulierungsänderungen trägt der von der aba vorgeschlagenen Vorbemerkung 9 Rechnung. Viele EbAV, insbesondere Unternehmenseinrichtungen, sind häufig an die Träger-IT angeschlossen und übernehmen diese Aufgabe nicht selbst als Einrichtung. Das sollte in der Ausformulierung der VAIT in dem Sinne Berücksichtigung finden, dass bspw. eine Befassung mit Cyber-Crime durch das Trägerunternehmen als ausreichend betrachtet werden kann.	Im Text der Rn. 3.9 sollte die Aussage *Das Unternehmen informiert sich laufend über Bedrohungen und Schwachstellen seines Informationsverbundes, prüft ihre Relevanz, bewertet ihre Auswirkung und ergreift, sofern erforderlich, geeignete technische und organisatorische Maßnahmen.* wie folgt ergänzt werden: *Unternehmen ohne eigene IT-Infrastruktur können dies durch angemessene Regelungen in Ausgliederungsvereinbarungen und sonstigen Verträgen sicherstellen.*

Rn.	Anmerkungen	aba-Änderungsvorschlag
3.10	Die vorgeschlagene Formulierung in den Erläuterungen ist unklar. „Potenzielle Bedrohungen“ können nur beschrieben werden, wenn sie bekannt sind.	In den Erläuterungen der Rn. 3.10 bitten wir darum, auf den vorgeschlagenen neuen Satz 2 zu verzichten: *Der Statusbericht enthält beispielsweise die Bewertung der Risikosituation im Vergleich zum Vorbericht*. ~~*Die Risikosituation enthält auch externe potenzielle Bedrohungen.*~~

Kapitel 4: Informationssicherheitsmanagement

Rn.	Anmerkungen	aba-Änderungsvorschlag
4.2	Die Beschreibung des Umfangs der Informationssicherheitsleitlinie geht für die meisten EbAV über einen sinnvollen und leistbaren Umfang weit hinaus.	In den Text der Rn. 4.2 sollte folgender Satz eingefügt werden. *Die Geschäftsleitung hat eine schriftliche Informationssicherheitsleitlinie zu beschließen und innerhalb des Unternehmens zu kommunizieren.* *Hat eine EbAV keine eigene IT-Infrastruktur, weil sie z.B. jene des Trägerunternehmens nutzt, kann es als proportional angesehen werden, wenn eine solche, inhaltlich vergleichbare Leitlinie des Trägerunternehmens in entsprechender Weise gilt.* Alternativ könnte die Situation vieler EbAV auch durch „vor die Klammer gezogene“ Ausführungen zu Ausgliederungsvereinbarungen aufgegriffen und damit für EbAV angemessene und umsetzbare Anforderungen formuliert werden, zum Beispiel: *Unternehmen ohne eigene IT-Infrastruktur können dies durch angemessene Regelungen in Ausgliederungsvereinbarungen und sonstigen Verträgen sicherstellen.*

Rn.	Anmerkungen	aba-Änderungsvorschlag
4.2	Die in der Kommentierung geforderten „Eckpunkte“ (also „Maßnahmen“) zum Schutz der VIVA-Ziele (Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität) bewirken aus unserer Sicht eine spürbare Erweiterung der Anforderungen des VAIT-Rundschreibens. Zuvor ging es „nur“ um die „Ziele“ der Informationssicherheit. Um den Dokumentationsaufwand zu begrenzen bzw. sicherzustellen, dass der Mehraufwand auch einen praktischen Mehrwert hat, sprechen wir uns für eine Klarstellung zu Gunsten „relevanter“ Rahmenbedingungen aus.	Der von der BaFin ergänzte Satz im Text der Rn. 4.2 sollte durch eine sprachliche Konkretisierung wie folgt gefasst werden: *Die Leitlinie ist bei wesentlichen Veränderungen ~~der~~ relevanter Rahmenbedingungen zu prüfen und bei Bedarf zeitnah anzupassen.*
4.3	Bei einer vollständigen Ausgliederung der IT, z.B. auf ein Trägerunternehmen, existieren solche Anforderungen und Regelungen (Informationssicherheitsrichtlinien und Informationssicherheitsprozesse) auf der Ebene des Trägerunternehmens und werden von der EbAV nicht spezifisch gestaltet. Dies sollte in der endgültigen Formulierung klar benannt und berücksichtigt werden.	
4.4	U.E. ist diese Anforderung insbesondere für Unternehmenseinrichtungen überzogen, unnötig und unpraktikabel. Die Anforderung kann in solchen Fällen nicht von der EbAV selbst erfüllt werden. Es muss ausreichen, dass sie Test- und Prüfaktivitäten *gewährleistet*, etwa durch die Ausgestaltung von Ausgliederungsvereinbarungen. Auf diese Weise wären im Falle von Unternehmenseinrichtungen auch die vom Trägerunternehmen geleisteten Test- und Prüfungsaktivitäten der EbAV *zurechenbar*.	Im Text der (insgesamt neu vorgeschlagenen) Rn. 4.4 sollte Satz 1 wie folgt gefasst werden: *Das Unternehmen führt eine Richtlinie über das Testen und Überprüfen der Maßnahmen zum Schutz der Informationssicherheit ein oder gewährleistet das Vorhandensein oder die Anwendung einer solchen Richtlinie über die Ausgliederungsvereinbarung. Die Richtlinie ist regelmäßig und anlassbezogen zu überprüfen und bei Bedarf anzupassen.*
4.4	Die Gewährleistung der Qualifikation von Testern ist eine Selbstverständlichkeit. Als ausformulierte Anforderung des VAIT-Rundschreibens	Im Text der (insgesamt neu vorgeschlagenen) Rn. 4.4 bitten wir daher auf Satz 2 zu verzichten:

Rn.	Anmerkungen	aba-Änderungsvorschlag
	kann dies aber unnötigen Dokuments- und Mehraufwand verursachen.	~~*Die ausreichende Qualifikation der Tester ist zu gewährleisten.*~~
4.5	Die Überwachung von IT-Projekten durch den ISB sollte sich auf Aspekte der Informationssicherheit beschränken. Dies sollte bei der Aufzählung klargestellt werden.	In den Erläuterungen zu Rn. 4.5 sollte im Aufzählungspunkt zu IT-Projekten die folgende Streichung vorgenommen werden. *… angemessene Beteiligung bei Projekten und Beschaffungen mit IT-Relevanz (je nach Einzelfall kann eine angemessene Beteiligung reichen von der Information des Informationssicherheitsbeauftragten über das IT-Projekt bis hin dazu, dass der Informationssicherheitsbeauftragte* ~~*das IT-Projekt überwacht und*~~ *auf Einhaltung der Informationssicherheit hinwirkt …,*
4.5	Der ergänzte Satz am Ende der Erläuterungen *(„Der Informationssicherheitsbeauftragte kann durch ein Informationssicherheitsmanagement-Team unterstützt werden.“)* ist für die meisten EbAV realitätsfern. Auch in der Ausformulierung als Kann-Bestimmung lehnen wir daher dieses „Angebot“ ab. Für viele EbAV, insbesondere Unternehmenseinrichtungen, ist ein zusätzliches Team unrealistisch und unter dem Gesichtspunkt der kostenmäßigen Attraktivität von EbAV verfehlt.	In den Erläuterungen zu Rn. 4.5 sollte auf den im Konsultationsdokument neu vorgeschlagenen letzten Satz verzichtet werden: ~~*Der Informationssicherheitsbeauftragte kann durch ein Informationssicherheitsmanagement-Team unterstützt werden.*~~
4.6	Die vorgeschlagene Formulierung in den Erläuterungen unterstellt implizit, dass die Position eines (Stell-)Vertreters definiert werden muss. Auch diese Anforderung ist aus Sicht vieler EbAV als überzogen abzulehnen.	In den Erläuterungen zu Rn. 4.6 sollte daher folgende Änderungen vorgenommen werden: *Funktions- und Stellenbeschreibung für den Informationssicherheitsbeauftragten, seinen möglichen Vertreter und ggf. weitere Stellen.* Dieser Vorschlag gilt entsprechend auch für weitere Aufzählungspunkte, in denen die Rede von dem „Vertreter“ ist.

Rn.	Anmerkungen	aba-Änderungsvorschlag
4.10	Wir verweisen hier auf unsere auf Seite 1 gemachte Anregung, den Begriff „regelmäßig“ konsistent zu verwenden.	Im Text der Rn. 4.10 sollte daher die folgende Streichung vorgenommen werden. *Der Informationssicherheitsbeauftragte hat der Geschäftsleitung, ggf. dem zuständigen Geschäftsleiter, ~~regelmäßig~~, mindestens vierteljährlich, und ggf. ad hoc, über den Status der Informationssicherheit zu berichten.*

Kapitel 5: Operative Informationssicherheit

Rn.	Anmerkungen	aba-Änderungsvorschlag
5 übergreifend	Die Ausformulierung der Randnummern 5.1 und 5.2 zielt u.E. darauf ab, einheitliche Marktstandards zu implementieren. Dabei wird weder den Besonderheiten der bAV noch dem Proportionalitätsprinzip Rechnung getragen. Viele EbAV, insbesondere Unternehmenseinrichtungen, nutzen häufig die bestehenden IT-Infrastruktur und -Prozesse ihrer Trägerunternehmen, die – in vielen Fällen als weltweit tätige Großunternehmen – in der Regel ein äußerst starkes Eigeninteresse an einer funktionierenden und sicheren IT haben. Auch wenn die Qualität der IT von der EbAV überwacht wird, hat diese doch keinen direkten Einfluss auf die Ausgestaltung der operativen Prozesse im Detail. Daher droht für die genannten Einrichtungen das gesamte neue Kapitel 5 an der Praxis vorbeizugehen. Eine allgemeine Regelung mit Verweis auf das VAIT-Rundschreiben in seiner jeweils gültigen Fassung im Ausgliederungsvertrag hierzu sollte ausreichend sein.	Wir bitten daher darum, im Hinblick auf EbAV auf die Randziffern 5.1 und 5.2 komplett zu verzichten oder zumindest angemessen zu formulieren. Dabei sollte im Text der Rn. 5.1 zumindest folgende Ergänzung vorgenommen werden: *Hat eine EbAV keine eigene IT-Infrastruktur, weil sie z.B. jene des Trägerunternehmens nutzt, gewährleistet die Einrichtung die Einhaltung der Bestimmungen dieses Kapitels durch eine entsprechende Ausgestaltung der Ausgliederungsvereinbarung.*

Rn.	Anmerkungen	aba-Änderungsvorschlag
5.2	Die Formulierung "dem Stand der Technik entsprechende" ist sehr weit gefasst und bedarf u.E. der Präzisierung.	Im Text der Rn. 5.2 sollte folgende Ergänzung vorgenommen werden: *Das Unternehmen hat auf Basis der Informationssicherheitsleitlinie und Informationssicherheitsrichtlinien angemessene, dem Stand der Technik bei Anwendungen und IT-Systemen entsprechende, operative Informationssicherheitsmaßnahmen und Prozesse zu implementieren.*
5.3	Diese Regelung würde u.U. massive Änderungen in Bestandssystemen erfordern.	Wir schlagen vor, im Hinblick auf EbAV auf Rn. 5.3 komplett zu verzichten. ~~5.3 Gefährdungen des Informationsverbundes sind möglichst frühzeitig zu identifizieren. Potentiell sicherheitsrelevante Informationen sind angemessen zeitnah, regelbasiert und zentral auszuwerten. Diese In formationen müssen bei Transport und Speicherung geschützt wer- den und für eine angemessene Zeit zur späteren Auswertung zur Verfügung stehen~~
5.3 bis 5.5	Die zur Streichung vorgeschlagene Formulierung wäre der Aufforderungen gleichzusetzen, dass Auswertungen über teure und aufwendig zu betreibende SIEM-Lösungen vorgenommen werden müssen. Das Kosten-Nutzen-Verhältnis solcher Systeme ist umstritten. Es sollte stattdessen im Risiko-Ermessen des Unternehmens liegen, wie die geeignete regelbasierte Auswertung vorgenommen wird. Generell basieren die Anforderungen in den Randziffern 5.3 bis 5.5 auf der Annahme, dass es sinnvoll ist, "sich anbahnende Bedrohungen" zu beobachten. Die Wirksamkeit einer solchen Maßnahme ist fraglich. Das Regelwerk für solche Auswertungen zu erstellen ist aufwändig und fehlerträchtig. Der Trend geht hier daher zu KI-basierten Lösungen, die meist beinhalten, dass sämtlichen Daten in die Cloud des Lösungsanbieter transferiert werden, um eine größere Lernbasis	Im Text der Erläuterung zu Rn. 5.3 sollte außerdem folgende Formulierung gestrichen werden: ~~*Die regelbasierte Auswertung (z. B. über Parameter, Korrelationen von Informationen, Abweichungen oder Muster) großer Datenmengen erfordert in der Regel den Einsatz automatisierter IT-Systeme.*~~

Rn.	Anmerkungen	aba-Änderungsvorschlag
	für die KI zu haben. Bei so einer Lösung entsteht zusätzlicher Aufwand für Compliance (welche Daten dürfen überhaupt transferiert werden.) Insgesamt sind solche Lösungen (SIEM) daher umstritten. In der VAIT sollte hier die Risiko-Angemessenheit angemessen berücksichtigt werden. Versicherungen und EbAV betreiben in der Regel keine Systeme die 24/7 die Möglichkeit anbieten, durch Kunden Zahlungen auszulösen.	

Kapitel 6: Identitäts- und Rechtemanagement

Rn.	Anmerkungen	aba-Änderungsvorschlag
6.1	Eine Anforderung, grundsätzlich immer standardisierte Prozesse und Kontrollen vorzusehen, kann sich u.E. in Einzelfällen für EbAV als schwierig oder ggf. sogar nachteilig erweisen. Eine der Anforderung an Ausgliederungsvereinbarungen in Rz. 207 der MaGo für EbAV lautet: *„die Verpflichtung des Dienstleisters, der EbAV sowie deren Abschlussprüfer und der Aufsichtsbehörde den Zugang zu Informationen über die ausgelagerten Funktionen oder Tätigkeiten zu gewähren sowie vor Ort Prüfungen zu ermöglichen,“*. Wir gehen daher davon aus, dass EbAV diese Anforderung auch über die Ausgliederungsvereinbarung erfüllen können, und halten daher auch eine diesbezügliche Klarstellung im Text des Rundschreibens für wünschenswert.	Wir schlagen daher vor, den Text von Kapitel 6.1 (durch die Ersetzung eines Worts und die Ergänzung eines Satzes) abzuändern. *6. 1 Das Unternehmen hat ein Identitäts- und Rechtemanagement einzurichten, welches sicherstellt, dass den Benutzern eingeräumte Berechtigungen so ausgestaltet sind und genutzt werden, wie es den organisatorischen und fachlichen Vorgaben des Unternehmens entspricht. Bei der Ausgestaltung des Identitäts- und Rechtemanagements sind die Anforderungen an die Ausgestaltung der Prozesse (siehe 2.2 und 2.10) entsprechend zu berücksichtigen. Jegliche Zugriffs-, Zugangs- und Zutrittsrechte auf Bestandteile bzw. zu Bestandteilen des Informationsverbundes müssen ~~standardisierten~~ angemessene Prozessen und Kontrollen unterliegen.* *Diese Anforderungen können im Falle einer Ausgliederung, von einer EbAV auch über die Ausgliederungsvereinbarung (siehe R. 207 MaGo für EbAV) erfüllen werden.*

Rn.	Anmerkungen	aba-Änderungsvorschlag
6.2	Bzgl. der vorgesehenen Ergänzung: *„Berechtigungskonzepte sind regelmäßig und anlassbezogen zu überprüfen und ggf. zu aktualisieren“*: Die Umsetzung von Anforderungen darf nicht dazu führen, dass IT-Abteilungen ganze Wochen im Jahr dafür „exklusiv“ tätig sind. Das scheint weder zielführend noch wirtschaftlich zu sein.	Wir bitten daher darum, auf die vorgesehene Verschärfung der Rn. 6.2 zu verzichten.

Kapitel 7: IT-Projekte und Anwendungsentwicklung

Rn.	Anmerkungen	aba-Änderungsvorschlag
7.1 und weitere Rn.	Die Anforderung "wesentlich" findet sich mehrfach im Dokument (wesentliche Berechtigungen, wesentliche IT-Projekte, wesentliche Veränderungen in den IT- Systemen). Hier sollte die EbAV eigenverantwortlich und prinzipienorientiert den Begriff – analog zu den Bestimmungen in den MaGo für EbAV in Rn. 43 – festlegen und im Betrieb analysieren. Wir regen daher eine entsprechende Ergänzung für eine übergreifende Reglung an.	Der Text von Rn. 7.1 sollte um folgenden Satz ergänzt werden: *Unternehmen und EbAV legen eigenverantwortlich und nachvollziehbar fest, welche IT-Projekte und Änderungen von IT-Systemen und Anwendungen und -Projekte als wesentlich einzustufen sind.* Aufbauend auf dieser Ergänzung des Texts der Rn. 7.1 sollte außerdem die Erläuterungen um folgenden Satz ergänzt werden: *Von wesentlichen Veränderungen kann dann ausgegangen werden, wenn Teile des IT- Systems vollständig ersetzt oder ergänzt werden oder durch Anpassungen der Architektur gesamthafte Auswirkungen auf wesentliche Geschäftsprozesse zu erwarten sind.*
7.5	Die Formulierung "entsprechende Änderungsanträge" ist unklar. Es sollte in der Erläuterungsspalte präzisiert werden, dass damit Änderungsanträge im Rahmen von Change-Management-Prozessen gemeint sind. Sinnvoll wäre auch, diesen wichtigen Aspekt in Rn. 7.8 als	In der Erläuterungsspalte zu Rn. 7.5 sollte präzisiert werden: *Der Begriff „Änderungsanträge“ bezieht sich auf Änderungsanträge im Rahmen von Change-Management-Prozessen (z.B. nach ITIL).*

Rn.	Anmerkungen	aba-Änderungsvorschlag
	Bestandteil der Prozesse zu integrieren und entsprechen zu benennen.	
7.11	Die beschriebenen Anforderungen dürften bei den meisten EbAV durch den IT-Dienstleister erfolgen. Daher betrachten wir die Regelungsdichte an dieser Stelle als zu hoch.	Wir schlagen vor, auf die geplante Änderung des Texts der Rn. 7.11 im Hinblick auf EbAV zu verzichten. Alternativ bitten wir darum, die Anforderung so zu formulieren, dass sie auch für EbAV umsetzbar ist.
7.13	Tests zum Schutz von Informationen sollten u.E. überhaupt nur dann durchzuführen sein, wenn diese von den Anwendungen überhaupt betroffen sind. Sonst ist übermäßiger Testaufwand die Konsequenz, ohne jeglichen Mehrwert.	Im Text der Erläuterung zu Rn. 7.13 soll der in der Konsultationsfassung als Ergänzung vorgeschlagene Satz 2 *Der Schutzbedarf der zum Testen verwendeten Daten ist zu berücksichtigen.* wie folgt formuliert werden: *In Entscheidungen über die Durchführung und Ausgestaltung von Tests fließt insbesondere der Schutzbedarf der von der betreffenden Anwendung verarbeiteten Daten mit ein.*

Kapitel 8: IT-Betrieb

Rn.	Anmerkungen	aba-Änderungsvorschlag
8.1	Begründung: Siehe aba-Anmerkungen zu Kapitel 5	Der Text von Rn. 8.1 sollte um folgenden Satz ergänzt werden: *Unternehmen ohne eigene IT-Infrastruktur können dies durch angemessene Regelungen in Ausgliederungsvereinbarungen und sonstigen Verträgen sicherstellen.*

Rn.	Anmerkungen	aba-Änderungsvorschlag
8.3	Wir regen an, die geforderte Aktualisierung in einer Weise zu konkretisieren, die den Unternehmen mehr Spielräume verschafft.	Der Text von Rn. 8.3 sollte um folgende Konkretisierungen ergänzt werden: *Das Portfolio aus IT-Systemen bedarf der Steuerung. IT-Systeme sollten regelmäßig entsprechend der technischen Entwicklung dieser Systeme und daraus resultierenden Sicherheitserfordernissen aktualisiert werden. Risiken aus veralteten ~~bzw.~~ (bspw. nicht mehr vom Hersteller unterstützten) IT-Systemen sind zu steuern (Lebenszyklus-Management). Nicht mehr verwendete Hardwarekomponenten sind sicher zu entsorgen.*
8.8.	Die vorgeschlagenen Änderungen etablieren einen formellen, dokumentationspflichtigen Prozess zu Kapazitätsgesichtspunkten, die in der Praxis von Unternehmen bzw. ihren IT-Dienstleistern selbstverständlich und implizit beachtet werden. In dieser Form ist die ergänzte Rn. 8.8 insbesondere für viele EbAV unproportional und ohne Mehrwert.	Wir schlagen daher vor, auf die Anwendung der neuen Rn. 8.8 zumindest im Hinblick auf EbAV zu verzichten.

Kapitel 9: Ausgliederungen von IT-Dienstleistungen und sonstige Dienstleistungsbeziehungen im Bereich IT-Dienstleistungen

Rn.	Anmerkungen	aba-Änderungsvorschlag
9.4	Wir weisen darauf hin, dass dies („*Risikoanalyse in Bezug auf sonstige Dienstleistungsbeziehungen im Bereich der IT-Dienstleistungen“* und daraus abgeleitete Maßnahmen*)* in Dienstleistungsverträgen allenfalls allgemein und abstrakt geregelt werden kann.	

Kapitel 10: IT-Notfallmanagement

Rn.	Anmerkungen	aba-Änderungsvorschlag
10	Für das gesamte Kapitel 10 gilt folgende Anmerkung: Für viele EbAV, insbesondere Unternehmenseinrichtungen, die ihre IT auf Trägerunternehmen ausgelagert haben und in komplexe IT-Landschaften eingebunden sind, über die sie nicht die alleinige und vollständige Kontrolle haben, ist die Umsetzung des in Kap. 10 niedergelegten Notfallmanagements in dieser Form nicht möglich. Es muss in diesem Falle ausreichen, wenn beim Trägerunternehmen oder Dienstleister ein wirksames Notfallmanagement existiert.	*Der Text von Rn. 10.1 sollte um folgenden Satz ergänzt werden.* *Unternehmen ohne eigene IT-Infrastruktur können dies durch angemessene Regelungen in Ausgliederungsvereinbarungen und sonstigen Verträgen sicherstellen.*
10.7	Wir plädieren für eine Formulierungsänderung, da unklar ist, wie der Nachweis über die in 10.6 benannten Anforderungen hinaus erbracht werden soll.	Der Text von Rn. 10.7 sollte um folgenden Satz ergänzt werden. *Das Unternehmen hat ~~nachzuweisen~~ sicherzustellen, dass bei Ausfall eines Rechenzentrums die zeitkritischen Aktivitäten und Prozesse aus einem ausreichend entfernten Rechenzentrum und für eine angemessene Zeit sowie für die anschließende Wiederherstellung des ordentlichen IT-Betriebs erbracht werden können.*