Bericht

über die Softwareprüfung nach IDW PS 880

der Software

bit-MaRisk, Version 23.3

für die

bit Informatik GmbH,

Trier

SIGNOS
Singhofen & Gergen Partnerschaftsgesellschaft
Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft

Adelbylund 11 · 24943 Flensburg
Telefon 0461 / 67037-0 · Telefax 0461 / 67037-37
info@signos.de · www.signos.de
Partnerschaftsgesellschaft · Amtsgericht Kiel PR 399

Bedingungen für die Weitergabe des Berichts

Die bit Informatik GmbH, Trier (im Folgenden „Auftraggeber“ oder „bit Informatik“), hat die SIGNOS Singhofen & Gergen Partnerschaftsgesellschaft, Wirtschaftsprüfungsgesellschaft, Steuerberatungsgesellschaft, Flensburg (im Folgenden „SIGNOS“), mit der Prüfung des Softwareproduktes bit-MaRisk, Version 23.3 gemäß dem IDW Prüfungsstandard: Die Prüfung von Softwareprodukten (IDW PS 880) beauftragt. Als Ergebnis der Prüfung hat die SIGNOS den nachfolgenden „Bericht über die Softwareprüfung nach IDW PS 880 der Software bit-MaRisk, Version 23.3 für die bit Informatik“ (im Folgenden „Bericht“) erstattet.

Dieser Bericht ist ausschließlich für den Auftraggeber bestimmt. Durch den Auftraggeber ist die SIGNOS gebeten worden, den Bericht auch Kunden des Auftraggebers oder interessierten Dritten (im Folgenden „Dritte“) zur Verfügung zu stellen.

Der Bericht kann Ihnen als Dritter nur nach Kenntnisnahme und Zustimmung zu den nachfolgenden Bedingungen für die Weitergabe zur Verfügung gestellt werden.

- Der Bericht ist auf Grundlage eines Auftrags zwischen dem Auftraggeber und der SIGNOS erstellt worden. Diesem Auftragsverhältnis liegen die dem Bericht und diesen Weitergabebedingungen beigefügten und von Ihnen zu akzeptierenden Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 1. Januar 2017 zugrunde. Wir möchten Sie insbesondere auf die Haftungsbegrenzung dieser Allgemeinen Auftragsbedingungen hinweisen. Die Haftungssumme steht Dritten (Gesamtgläubiger) als gemeinschaftliche Haftungshöchstgrenze zur Verfügung, kein Dritter kann gegen uns eine weitergehende Haftung geltend machen.
- Die Prüfung beruht auf den vom Auftraggeber erhaltenen Unterlagen und Auskünften und dient ausschließlich für Zwecke des Auftraggebers. Die Prüfungshandlungen und der erstellte Bericht beziehen sich auf die Software bit-MaRisk, Version 23.3 und gibt den Stand unserer Erkenntnisse wieder, die zum Zeitpunkt der Prüfung und der Erstellung des Berichts bestanden haben. Eine laufende Aktualisierung des vorliegenden Prüfungsberichts wurde nicht vereinbart. Für zukünftige Anpassungen der Software treffen wir somit keine Aussagen. Die Verwertung des Berichts durch Dritte erfolgt in der alleinigen Verantwortung des Dritten. Die für Ihre Zwecke notwendigen Entscheidungen auf Basis der Erkenntnisse zu den Feststellungen dieses Berichts treffen Sie vollständig eigenverantwortlich. Wir übernehmen demnach Dritten gegenüber keine Verantwortung dafür, dass unsere Prüfung oder Informationen aus der Berichterstattung für deren Zwecke tauglich oder ausreichend sind.

- Der Bericht ist vertraulich zu behandeln. Eine Weitergabe darf nur in der hier dargelegten Form erfolgen. Die Weitergabe aufgrund gesetzlicher Vorschriften und auf Anordnung eines Gerichts oder einer Aufsichtsbehörde ist hiervon unberührt.
- Es ist bzgl. des Berichts und dessen Weitergabe kein Abschluss eines Auskunftsverhältnisses zwischen den Dritten und der SIGNOS beabsichtigt. Ebenso sind keine Ansprüche von Dritten aus dem Auftragsverhältnis zwischen dem Auftraggeber und der SIGNOS herleitbar. Eine vertragliche Haftung seitens der SIGNOS gegenüber Dritten durch die Verwertung dieses Berichts besteht demnach nicht.
- Die bit Informatik verpflichtet sich, die SIGNOS von jeglicher Inanspruchnahme durch Dritte, die mittelbar oder unmittelbar durch eine bedingungswidrige Weitergabe Kenntnis vom dem Inhalt des Berichts erhalten, freizustellen. Es sei denn, diese Ansprüche beruhen nicht auf der Kenntnis durch die bedingungswidrige Weitergabe.
- Für diese Vereinbarung gilt ausschließlich deutsches Recht. Als Gerichtsstand gilt Flensburg als vereinbart.

Bedingungen akzeptieren und Bericht anzeigen lassen

Inhalt

Anlage

Allgemeine Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 1. Januar 2017

1. Auftrag und Auftragsdurchführung

1 Die Geschäftsführung der

bit Informatik GmbH, Trier (im Folgenden „bit Informatik“),

hat uns beauftragt, eine Softwareprüfung nach IDW PS 880 für die Software bit-MaRisk, Version 23.3 durchzuführen.

2 Die Software bit-MaRisk richtet sich mit ihren verschiedenen Modulen an Institute nach dem Kreditwesengesetz (KWG) zur Erfüllung der gesetzlichen und aufsichtsrechtlichen Anforderungen im Bereich der Informationssicherheit und der damit verbundenen organisatorischen Aspekte nach den Mindestanforderungen an das Risikomanagement (MaRisk), Rundschreiben 05/2023 (BA) vom 18. Oktober 2023 sowie den Bankaufsichtlichen Anforderungen an die IT (BAIT), Rundschreiben 10/2017 (BA) in der Fassung vom 16. August 2021 der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin).

3 Gegenstand der Prüfung sind die im Folgenden beschriebenen Verarbeitungsfunktionen sowie deren Dokumentation und die Softwareentwicklungsumgebung.

Die Prüfung bezieht sich ausschließlich auf die Software bit-MaRisk, Version 23.3 in der grundlegenden Fassung bei Auslieferung vor individuellen Anpassungen (Customizing) durch die Kunden der bit Informatik. Die Ordnungsmäßigkeit der Parametrisierung im Einführungsprozess oder im laufenden Betrieb von bit-MaRisk bei den jeweiligen Kunden der bit Informatik ist ebenfalls nicht Gegenstand der Prüfung.

4 Zu den geprüften Modulen von bit-MaRisk zählen die Module:

- Benutzerverwaltung
- Vertragsverwaltung und Dienstleistersteuerung
- ObjectLifecycle
- Internes Kontrollsystem
- Organisationshandbuch
- Notfallmanagement
- IT-Betrieb
- Projektmanagement.

Die Bereitstellung von bit-MaRisk erfolgt i.d.R. auf Servern des jeweiligen Kunden, die auch zur Archivierung von Dateien verwendet werden. Aufgrund der Abhängigkeit von der Konfiguration der Server beim Kunden der bit Informatik obliegt die revisionssichere Archivierung und die Definition von Aufbewahrungsfristen für Verträge oder anderweitige Dokumente nicht der Prüfung.

5 Art und Umfang der Prüfung sowie unsere Prüfungshandlungen und die daraus resultierenden Feststellungen haben wir in diesem Prüfungsbericht dargestellt.

6 Für den genannten Auftragsumfang und die Auftragsdurchführung haben wir Kriterien auf Basis der folgenden gesetzlichen und regulatorischen Anforderungen sowie Prüfungsstandards zugrunde gelegt, die Maßstab zur Beurteilung der Ordnungsmäßigkeit der Software waren:

- Anforderungen an das Risikomanagement nach § 25a KWG
- Mindestanforderungen an das Risikomanagement (MaRisk), Rundschreiben 05/2023 (BA) der BaFin vom 18. Oktober 2023
- Bankaufsichtliche Anforderungen an die IT (BAIT), Rundschreiben 10/2017 (BA) der BaFin in der Fassung vom 16. August 2021
- Grundsätze ordnungsmäßiger Buchführung gemäß §§ 238 und 239 HGB bzw. die hieraus abgeleiteten regulatorischen Vorschriften zur Rechnungslegung und dem Internen Kontrollsystem.

Neben dem IDW Prüfungsstandard: „Die Prüfung von Softwareprodukten" (IDW PS 880) wurden der IDW Prüfungsstandard: „Abschlussprüfung bei Einsatz von Informationstechnologie (IDW PS 330) und der IDW Prüfungsstandard: „Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken (IDW PS 261)“, soweit für unsere Prüfungshandlungen anwendbar, berücksichtigt.

7 Die Prüfung wurde so geplant und durchgeführt, dass aufgrund der bei der Prüfung gewonnenen Erkenntnisse mit hinreichender Sicherheit beurteilt werden kann, ob die Software bit-MaRisk, Version 23.3 bei sachgerechter Anwendung eine wirkungsvolle Unterstützung einer ordnungsgemäßen Geschäftsorganisation ermöglicht und den im Prüfungsauftrag vereinbarten Kriterien, die die fachliche Anforderungen an eine Software darstellen, entspricht.

8 Grundlage der Prüfung sind die Ordnungsmäßigkeitskriterien Vollständigkeit, Richtigkeit, Zeitgerechtheit, Nachvollziehbarkeit und Unveränderlichkeit, deren Einhaltung unter Voraussetzung der Sicherheit, insbesondere der Integrität der verarbeiteten Daten, beurteilt und bewertet wurden.

Das Kriterium der Unveränderlichkeit sowie die Sicherheitsanforderungen sind durch weiterführende Maßnahmen der Kunden der bit Informatik zu gewährleisten. Insbesondere sind durch die Kunden geeignete Berechtigungen für die Nutzung des Programms zu vergeben. Dieses Kriterium bzw. die Sicherheitsanforderungen für den Zugriffsschutz waren daher nicht Gegenstand der Prüfung.

Es wurden seitens der bit Informatik keine zusätzlichen Kriterien im Sinne des IDW PS 880 zur Beurteilung der Software herangezogen. Unsere Prüfung basiert somit ausschließlich auf den oben beschriebenen gesetzlichen und regulatorischen Anforderungen.

9 Die Prüfung deckte neben den fachlichen Funktionalitäten auch die Wirksamkeit der programminternen Kontrollen ab. Es wurde beurteilt, ob die vorhandenen Funktionen eine vollständige, richtige, nachvollziehbare und sichere Verarbeitung gewährleisten und ob auftretende Fehler in der Verarbeitung zeitnah erkannt werden können. Der Nachweis der Fehlerfreiheit durch geeignete Testfälle kann aufgrund der Vielzahl der möglichen Testdatenkombinationen im Rahmen der Prüfung nicht vollständig erbracht werden. Es war daher nicht Ziel der Prüfung, die Fehlerfreiheit von bit-MaRisk, Version 23.3 zu bestätigen. Wir weisen in diesem Zusammenhang darauf hin, dass wegen der immanenten Grenzen der Softwareprüfung ein unvermeidbares Risiko von unentdeckten selbst wesentlichen Fehlern bzw. Fehlfunktionen besteht.

Eine Beurteilung der Softwareergonomie (Usability bzw. User Experience) von bit-MaRisk in Bezug auf die grafische Gestaltung der Nutzeroberflächen war nicht Gegenstand der Prüfung. Zudem bezogen sich unsere Prüfungshandlungen auf die eigenständige Funktionsfähigkeit der Software. Das Zusammenwirken von bit-MaRisk mit den notwendigen Kernbankverfahren, ERP-Systemen oder anderen benötigten Systemumgebungen wurde nicht untersucht. Hieraus folgt, dass die Import-Funktionen oder auch die Migration von Daten aus anderen Softwareprodukten nicht unserer Prüfung unterlegen haben.

10 Für die Datensicherung und das Wiederanlaufverfahren der Software ist der Kunde der bit Informatik zuständig. Des Weiteren bezogen sich unsere Prüfungshandlungen nicht auf die Feststellung von Unregelmäßigkeiten jeder Art, Computerkriminalität oder sonstigen deliktischen Handlungen.

11 Die gesetzlichen Vertreter der bit Informatik sind für die Software und die Planung, Durchführung und Überwachung der Softwareentwicklung verantwortlich. Diese Verantwortung wird durch unsere Prüfung nicht berührt oder eingeschränkt. Unsere Aufgabe ist es, auf Grundlage der von uns durchgeführten Prüfung eine Beurteilung über die Software abzugeben.

12 Für die Durchführung des Auftrags und unsere Verantwortlichkeit sind, auch im Verhältnis zu Dritten, die als Anlage beigefügten Allgemeine Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 1. Januar 2017 maßgebend.

13 Unsere Berichterstattung dient ausschließlich dem vereinbarten Zweck. Folglich ist unser Bericht allein zur Informationen der gesetzlichen Vertreter der bit Informatik bestimmt und darf zu keinem anderen Zweck verwendet werden. Eine Weitergabe aufgrund gesellschaftsvertraglicher oder gesetzlicher Vorschriften sowie auf Anordnung eines Gerichts oder einer Aufsichtsbehörde bleibt hiervon unberührt.

Die Weitergabe oder der Verweis auf unsere Berichterstattung bedarf unserer vorherigen Zustimmung. Daher verpflichten sich die gesetzlichen Vertreter der bit Informatik, uns von allen Ansprüchen Dritter, die durch diese ohne unsere Zustimmung von unserer Berichterstattung Kenntnis erhalten haben, freizustellen. Der Weitergabe unseres Berichts an Dritte erteilen wir die Zustimmung unter der Voraussetzung, dass die Weitergabe ausschließlich in der nachfolgenden Form erfolgt.

14 Zur Weitergabe stellen wir Ihnen unseren Bericht als PDF-Datei bereit, welche eine Bestätigung der im Folgenden dargestellten Bedingungen zum Öffnen des Berichts benötigt.

- Der Bericht ist auf Grundlage eines Auftrags zwischen dem Auftraggeber und der SIGNOS erstellt worden. Diesem Auftragsverhältnis liegen die dem Bericht und diesen Weitergabebedingungen beigefügten und von Ihnen zu akzeptierenden Allgemeine Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 1. Januar 2017 zugrunde. Wir möchten Sie insbesondere auf die Haftungsbegrenzung dieser Allgemeinen Auftragsbedingungen hinweisen. Die Haftungssumme steht Dritten (Gesamtgläubiger) als gemeinschaftliche Haftungshöchstgrenze zur Verfügung, kein Dritter kann gegen uns eine weitergehende Haftung geltend machen.
- Die Prüfung beruht auf den vom Auftraggeber erhaltenen Unterlagen und Auskünften und dient ausschließlich für Zwecke des Auftraggebers. Die Prüfungshandlungen und der erstellte Bericht beziehen sich auf die Software bit-MaRisk, Version 23.3 und gibt den Stand unserer Erkenntnisse wieder, die zum Zeitpunkt der Prüfung und der Erstellung des Berichts bestanden haben. Eine laufende Aktualisierung des vorliegenden Prüfungsberichts wurde nicht vereinbart. Für zukünftige Anpassungen der Software treffen wir somit keine Aussagen. Die Verwertung des Berichts durch Dritte erfolgt in der alleinigen Verantwortung des Dritten. Die für Ihre Zwecke notwendigen Entscheidungen auf Basis der Erkenntnisse zu den Feststellungen dieses Berichts treffen Sie vollständig eigenverantwortlich.

- Der Bericht ist vertraulich zu behandeln. Eine Weitergabe darf nur in der hier dargelegten Form erfolgen. Die Weitergabe aufgrund gesetzlicher Vorschriften und auf Anordnung eines Berichts oder einer Aufsichtsbehörde ist hiervon unberührt.
- Es ist bzgl. des Berichts und dessen Weitergabe kein Abschluss eines Auskunftsverhältnisses zwischen den Dritten und der SIGNOS beabsichtigt. Ebenso sind keine Ansprüche von Dritten aus dem Auftragsverhältnis zwischen dem Auftraggeber und der SIGNOS herleitbar. Eine vertragliche Haftung seitens der SIGNOS gegenüber Dritten durch die Verwertung dieses Berichts besteht demnach nicht.
- Die bit Informatik verpflichtet sich, die SIGNOS von jeglicher Inanspruchnahme durch die Dritte, die mittelbar oder unmittelbar durch eine bedingungswidrige Weitergabe Kenntnis vom dem Inhalt des Berichts erhalten, freizustellen. Es sei denn, diese Ansprüche beruhen nicht auf der Kenntnis durch die bedingungswidrige Weitergabe.
- Für diese Vereinbarung gilt ausschließlich deutsches Recht. Als Gerichtsstand gilt Flensburg als vereinbart.

15 Die Programmentwicklung, -wartung und -freigabe erfolgt eigenverantwortlich durch die bit Informatik. Dabei sind nachvollziehbare Entwicklungsrichtlinien festgelegt. Ein Prozess zur angemessenen Programmentwicklung inkl. Test- und Freigabeverfahren (zweistufiges Verfahren) ist eingerichtet. In Bezug auf die Richtigkeit der Verarbeitungsfunktionen verfügt die Gesellschaft über eine Testfallsammlung, die bei jedem Update nachvollziehbar getestet wird.

16 Die Prüfung erfolgte durch Einsichtnahme in die Dokumentationen, Durchführung eigener Testfälle und Befragungen. Die Prüfung fand in Stichproben durch bewusste Auswahl statt. Als Informationsquellen dienten insbesondere die Verfahrensdokumentationen, Protokolle von durch die bit Informatik selbst durchgeführten Tests und die Auskünfte der zuständigen Mitarbeiter sowie eigene Tests in einer uns für die Zwecke der Prüfung zur Verfügung gestellten Testumgebung. Die Ergebnisse unserer Prüfungshandlungen und Kontrolltests haben wir in unseren Arbeitspapieren dokumentiert.

17 Die Prüfungshandlungen zur Prüfung der Programmfunktionen von bit-MaRisk, Version 23.3 erfolgten auf einem Web-Server, der uns von der bit Informatik mit entsprechenden Testdatenbanken zur Verfügung gestellt wurde. Bei der Durchführung der Prüfungshandlungen wurde ausschließlich der Browser Microsoft Edge for Business, Version 121.0.2277.110 (Offizielles Build) (64-Bit) verwendet.

18 Die von der Geschäftsführung der bit Informatik unterzeichnete berufsübliche Vollständigkeitserklärung haben wir zu unseren Arbeitspapieren genommen.

2. Prüfungsfeststellungen

2.1 Beurteilung der Dokumentation

Anforderungen

19 Der Umfang und die Aussagefähigkeit der Dokumentation müssen genügen, um einen sachverständigen Dritten innerhalb angemessener Zeit, die Software und deren Nutzung zu erläutern. Die Verfahrensdokumentation besteht dabei aus einer Systemdokumentation und der Anwenderdokumentation. Diese ist erforderlich für die sachgerechte Handhabung und künftige Fortführung der Software. Eine sachgerechte Dokumentation ist Grundvoraussetzung für die Nachvollziehbarkeit und damit die Prüfbarkeit des Verfahrens.

20 In Anlehnung an den IDW RS FAIT 1 ist folgender Mindestinhalt der Dokumentation vorzusehen:

- Beschreibung der sachlogischen Lösung
- Beschreibung der programmtechnischen Lösung
- Beschreibung zur Wahrung der Programmidentität
- Beschreibung zur Wahrung der Datenintegrität
- Arbeitsanweisungen für den Anwender

Umsetzung

21 Die Dokumentation für bit-MaRisk, Version 23.3 besteht aus einer internen Systemdokumentation zur Erläuterung der Funktionen und der Anwenderdokumentation, die in Form von Benutzerhandbüchern oder Schulungsvideos sowie softwareintegrierten Hilfe-Funktionen bereitgestellt wird.

22 Die interne Systemdokumentation umfasst eine Beschreibung der wesentlichen Funktionen der Software und eine Analyse der zur Umsetzung notwendigen Schritte. Die Dokumentation beruht zu wesentlichen Teilen auf fachlichen und technischen Konzepten, die im Rahmen von Kundenanfragen bzw. der Anpassung an aufsichtsrechtliche Anforderungen erstellt wurden.

23 Die Anwenderdokumentation ist insgesamt sowohl vollständig und aktuell als auch eindeutig. Für den Anwender ist die Dokumentation verständlich und übersichtlich aufbereitet, wobei alle Funktionen der Anwendung systematisch erläutert und die Zusammenhänge zwischen den einzelnen Abschnitten erkennbar werden. Die Beschreibungen werden mit Workflows in den Hilfefunktionen oder durch Videos der entsprechenden Abläufe verdeutlicht.

Prüfung und Ergebnis

24 Wir haben die fachliche Richtigkeit der Verfahrensdokumentation geprüft. Dabei wurden sowohl die geprüften Verarbeitungsregeln anhand der Dokumentation nachvollzogen als auch Testfälle in Stichproben anhand der Dokumentation geprüft.

25 Die Dokumentation in den programmseitig integrierten Hilfefunktionen ist vollständig und aktuell. Es wird die geprüfte Version 23.3 wiedergegeben. Alle notwendigen Informationen sind enthalten. Innerhalb der Dokumentation konnten keine Widersprüche festgestellt werden.

26 Die Systemdokumentation ist geeignet, einem sachverständigen Dritten in angemessener Zeit ein Verständnis für das dokumentierte Verfahren zu geben.

27 Die Anwenderdokumentation ist geeignet, einem sachverständigen Dritten in angemessener Zeit ein Verständnis für das dokumentierte Verfahren zu geben.

2.2 Beurteilung des Softwareentwicklungsverfahrens

Anforderungen

28 Die Anforderungen an die Softwareentwicklung ergeben sich grundsätzlich aus dem IDW PS 880. Es ist insbesondere auf die

- Trennung der Systeme für Entwicklung, Test und Produktion
- Verfahren zur Erstellung der Anforderungen an die Software und deren Änderung
- Einführung von Standards für die Entwicklung und Wartung
- Angemessene Versionsführung
- Ordnungsmäßigkeit der Test- und Abnahmekonzepte

zu achten. Hierdurch sollen die Nachvollziehbarkeit des Entwicklungsverfahrens verbessert und eine prozessintegrierte Qualitätssicherung erreicht werden. Innerhalb der Programmbibliotheken sind die verschiedenen Versionen eindeutig nachzuweisen und Änderungen voneinander abzugrenzen.

29 Die Test- und Abnahmekonzepte müssen insgesamt einen ausreichenden Testumfang der in der Software dargestellten Funktionen und Prozesse ermöglichen. Die abschließende Dokumentation der Testfälle und die hierdurch geprüften Programmfunktionen müssen für sachverständige Dritte nachvollziehbar sein. Durchgeführte Änderungen in der Software sollten des Weiteren bei einer Versionsänderung in der Aktualisierung der Anwender- und Systemdoku-

mentation berücksichtigt werden.

Umsetzung

30 Die bit Informatik verfügt über ein individuell entwickeltes Verfahren zur Entwicklung, Pflege und Freigabe von Software. Das fachliche Konzept beschreibt die fachlichen Detailanforderungen und enthält die Umsetzungsbausteine für das zukünftige Release bzw. Build. Grundlage für das Verfahren sind Organisationsanweisungen, auf dessen Grundlage Prozesse im Rahmen der Entwicklung, Pflege und Freigabe von Software für die jeweiligen Beteiligten beschrieben werden. Ein Internes Kontrollsystem ist implementiert und wird nach unseren Erkenntnissen eingehalten. Die für die Bereitstellung notwendige Software wird über Versionsverwaltungsprogramme verwaltet.

31 Bei der bit Informatik werden die Programmversionen im Quellcode-Format aufbewahrt. Es ist jederzeit ein historischer Versionsstand der einzelnen Releases/Builds reproduzierbar. Vorgenommene Veränderungen gegenüber einer Vorgängerversion werden hinreichend dokumentiert und protokolliert. Ferner wird über die interne Vergabe einer Versionsnummer gesteuert.

32 Die Qualitätssicherung bei der Programmentwicklung erfolgt auf Basis von standardisierten Tests auf Grundlage vordefinierter Prozesse durch Mitarbeitende der Entwicklung.

Prüfung und Ergebnis

33 Zur Beurteilung der Möglichkeiten der zukünftigen Programmentwicklung und -pflege haben wir die softwaretechnischen Werkzeuge und die organisatorischen Maßnahmen bei der Programmentwicklung untersucht. Weiterhin haben wir uns über die Entwicklungsumgebung bzw. über die Bibliothekverwaltungsprogramme für die notwendige Versionsführung informiert und in Stichproben in der Änderungsdokumentation Einblick genommen.

34 Es ergaben sich im Zusammenhang mit der Prüfung des Softwareentwicklungsverfahrens für bit-MaRisk keine Beanstandungen.

2.3 Prüfung der notwendigen Verarbeitungsfunktionen

2.3.1 bit-MaRisk - Administration

Anforderungen

35 Die Anforderungen des Moduls zur Administration von bit-MaRisk („Einstellungen“) von bit-MaRisk lassen sich grundsätzlich aus den allgemeinen organisatorischen Pflichten von Institu-

ten gemäß § 25a KWG ableiten. Hierbei hat ein Institut interne Kontrollverfahren mit einem internen Kontrollsystem, wobei das interne Kontrollsystem insbesondere aufbau- und ablauforganisatorische Regelungen mit klarer Abgrenzung der Verantwortungsbereiche beinhalten soll, einzurichten.

36 Die MaRisk konkretisieren die Anforderungen an ein Internes Kontrollsystem in AT 4.3. In Abhängigkeit von Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten sind durch ein Institut Regelungen zur Aufbau- und Ablauforganisation zu treffen. Miteinander unvereinbare Tätigkeiten sind jeweils durch unterschiedliche Mitarbeiter durchzuführen und Interessenkonflikte sowie Selbstprüfungen zu vermeiden. Prozesse sowie die damit verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege sind gemäß den MaRisk klar zu definieren und aufeinander abzustimmen. Berechtigungen und Kompetenzen sind nach dem Sparsamkeitsgrundsatz zu vergeben und zeitnah anzupassen.

37 Ziel der Prüfung der Differenzierung von Zugangs- und Zugriffsberechtigungen ist die Feststellung, ob die Software über hinreichende Mechanismen zur Identifikation, Autorisierung (Einhaltung der Funktionstrennung) und Authentizität während der Verarbeitung verfügt. Es ist zu prüfen, ob und inwieweit es die Software zulässt, durch Vergabe von Benutzerkennungen (Benutzer-ID) und Passwörtern einen sicheren Zugang zur Software zu realisieren.

Über die Zuordnung einzelner System- bzw. Modulberechtigungen soll die Software eine den institutsspezifischen Vorgaben entsprechende Benutzer-Autorisierung in den einzelnen Systemfunktionen bereitstellen. Diese Sicherheitsmechanismen sollen sicherstellen, dass nur befugte Personen auf bestimmte Funktionen zugreifen können.

38 Die Prüfung von Umfang und Wirksamkeit softwareninterner Plausibilitätskontrollen umfasst sowohl Eingabekontrollen als auch maschinelle Kontroll- und Abstimmverfahren im Verarbeitungslauf. Diese sollen als Teil des softwareunterstützten Internen Kontrollsystems zur Sicherstellung einer vollständigen und richtigen Verarbeitung der Daten beitragen.

Umsetzung

39 bit-MaRisk bietet im Bereich der Einstellungen vielfältige Möglichkeiten zur Administration der Software. Zu den Funktionalitäten zählen bspw. ein Monitoring der **Serveraktivitäten**. Diese Aktivitäten können über „Agenten“ gesteuert und überwacht werden.

40 Diese **Agenten** werden u.a. für globale oder modulspezifische Prozesse, wie die laufende Schutzbedarfsvererbung oder zur Archivierung bzw. zur Synchronisation der Organisationsstruktur genutzt. Sie können periodisch oder manuell initiiert werden, ihre Ausführung wird pro-

tokolliert angezeigt.

41 Über den Menüpunkt „**Hintergrundprozesse“** kann die festgelegte automatische Aktualisierung der Daten durch die Agenten pausiert oder erneut aktiviert werden. Ebenso werden die derzeit laufenden oder abgeschlossenen Läufe der oben genannten Agenten protokolliert dargestellt.

42 Sämtliche Aktivitäten der Benutzer werden innerhalb von **Logeinträgen** in bit-MaRisk erfasst und mit den erforderlichen Informationen zum Zeitpunkt, den betreffenden Modulen und deren Aktivitätsbezeichnungen visualisiert.

43 Aufgrund der Komplexität und modularen Struktur der Software besteht eine stark differenzierbare **Zugangsverwaltung** für die Nutzung von bit-MaRisk. Im Standard bietet bit-MaRisk bereits eine Vielzahl von **Zugriffsrollen**, die Berechtigungen vom Administrator für die gesamte Anwendung bis hin zu Nutzern, die lediglich einen lesenden Zugriff für nachgelagerte Kontrolltätigkeiten in den jeweiligen Modulen erhalten, beinhalten. Des Weiteren wird bspw. zwischen Anwendern oder Fachadministratoren auf Modulebene unterschieden.

Ergänzend zu den Zugriffsrollen können Berechtigungen anhand der vorliegenden Organisationsstruktur der Institute anhand von **Gruppen** vergeben werden. Diese Gruppen beziehen sich i.d.R. auf einzelne Organisationseinheiten oder regionale Einheiten anhand der Filialstruktur.

Als weitere Möglichkeit zur Vergabe von Berechtigungen können auf **Benutzerebene** Einzelrechte für bestimmte Personen vergeben werden.

Die An- oder Abmeldung von einzelnen Usern wird fortlaufend durch **Anmeldeprotokolle** protokoliert und kann im Bedarfsfall ausgewertet werden.

44 Innerhalb der **Konfiguration** können global für die gesamte Anwendung oder je Modul verschiedenste Einstellungen hinterlegt werden. Diese betreffen zum einen zentrale Einstellungen zur Funktionsweise der Software und zum anderen Darstellungen von Ansichten oder Berichten. Die Beschreibung der modulspezifischen Konfigurationen erfolgt in den jeweiligen Abschnitten dieses Prüfungsberichts zu den entsprechenden Modulen.

45 Die zentrale Steuerung von Aufgaben und Vorlagen wird über die Konfiguration von **Workflows** vorgenommen. Hierzu können durch die Anwender in den Modulen individuelle Abläufe zur Bearbeitung von Sachverhalten vergeben werden. Die Information, ob neue Vorlagen bzw. Aufgaben für den Benutzer vorliegen, kann durch den Versand von bedarfsgerechten **Mails** an die betreffenden Mitarbeitenden des Instituts durch die Gestaltung von **Vorlagen** erfolgen. Durch die Definition von **Mailtriggern**, also bspw. das Durchlaufen oder der Abbruch eines Workflows,

werden die entsprechenden Mails versendet. Die Übersicht der aktuell zu bearbeitenden Vorlagen durch die Anwender („Eigene Vorlagen“) wird standardmäßig beim Öffnen der Software und in den betreffenden Modulen angezeigt, wodurch eine laufende Erinnerung an zu erledigende Workflows erfolgt. Fachadministratoren oder globale Administratoren können darüber hinaus modulspezifisch bzw. vollumfänglich die noch offenen Vorlagen überwachen.

46 Zur Vorgabe von Auswahlfeldern in den Eingabemasken in bit-MaRisk können **Schlüsselwortlisten** individuell für einzelne Anzeigebereiche in den Modulen gepflegt werden.

47 Des Weiteren können **Textbausteine** mit individuellen Standardformulierungen als Hinweistexte oder als Inhalt für Reportings angelegt werden.

Prüfung und Ergebnis

48 Die Prüfung der programminternen Verarbeitungsregeln basierte auf Testfällen. Die Protokollierung der **Serveraktivitäten** – Agenten, Hintergrundprozesse und Logeinträge – wurde anhand der in der von der bit Informatik bereitgestellten Testumgebung nachvollzogen.

49 Ebenso wurde die **Zugangsverwaltung**, also die Vergabe von Zugriffsrollen, Gruppen oder Benutzerrechten sowie deren Protokollierung – anhand von Testfällen überprüft.

50 **Konfigurationsänderungen** bzw. Neuanlagen/Archivierungen wurden sowohl global für die gesamte Software als auch für einzelne Module sowie für Berichtsauswertungen vorgenommen.

51 Des Weiteren wurden verschiedene Anpassungen von **Workflows** und deren Durchlauf durch das Testinstitut durchgeführt. Ergänzend wurden die bestehenden Mailvorlagen und Mailtrigger auf Angemessenheit überprüft.

Aufgrund der Individualität der Daten in Abhängigkeit von den Spezifikationen des jeweiligen Instituts unterlag die Funktion für den Daten-Import sowie der Versand von spezifischen Mailings oder das Auslösen von Mailtriggern hinsichtlich der Abhängigkeit vom E-Mail-System des jeweiligen Instituts nicht unserer Prüfung.

52 Die Bearbeitung von **Schlüsselwortlisten** und Textbausteinen wurde ebenfalls anhand von Testfällen nachvollzogen.

53 Bei unseren stichprobenweisen Prüfungen ergaben sich keine Beanstandungen. Die beschriebenen Verarbeitungsregeln sind geeignet, eine ordnungsgemäße Administration von bit-MaRisk zu unterstützen.

2.3.2 bit-MaRisk - Benutzerverwaltung

Anforderungen

54 Die Anforderungen des Moduls zur Benutzerverwaltung (Menüpunkte „Benutzerverwaltung“, „Rezertifizierung“ und „Soll-Ist-Abgleich“) von bit-MaRisk lassen sich grundsätzlich aus den allgemeinen organisatorischen Pflichten gemäß § 25a KWG ableiten. Hierbei hat ein Institut interne Kontrollverfahren mit einem internen Kontrollsystem, wobei das interne Kontrollsystem insbesondere aufbau- und ablauforganisatorische Regelungen mit klarer Abgrenzung der Verantwortungsbereiche beinhalten soll, einzurichten.

55 Die MaRisk konkretisieren die Anforderungen an ein Internes Kontrollsystem in AT 4.3. In Abhängigkeit von Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten sind durch ein Institut Regelungen zur Aufbau- und Ablauforganisation zu treffen. Miteinander unvereinbare Tätigkeiten sind jeweils durch unterschiedliche Mitarbeiter durchzuführen und Interessenkonflikte sowie Selbstprüfungen zu vermeiden. Prozesse sowie die damit verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege sind gemäß den MaRisk klar zu definieren und aufeinander abzustimmen. Berechtigungen und Kompetenzen sind nach dem Sparsamkeitsgrundsatz zu vergeben und zeitnah anzupassen.

IT-Berechtigungen sind regelmäßig und anlassbezogen zu überprüfen, wobei sich der Turnus an der Bedeutung der Prozesse und dem Schutzbedarf der zugrunde liegenden Informationen ausrichtet. Berechtigungen, die Schnittstellen zu wesentlichen Auslagerungen betreffen, sind hierbei ebenfalls zu beachten.

56 Die Vorgaben von AT 7.2 MaRisk spezifizieren weiter die Anforderungen an die Berechtigungsvergabe, für die institutsweit angemessene Prozesse einzurichten sind, die gewährleisten, dass nur Berechtigungen an die Mitarbeitenden vergeben werden, die für eine spezifische Tätigkeit notwendig sind. Ermöglicht wird die Zusammenfassung von Berechtigungen zu verschiedenen Rollenkonzepten.

57 Weitreichender gehen die Anforderungen aus Kapitel 6 der BAIT zum Identitäts- und Rechtemanagement, die standardisierte Prozesse und Kontrollen für sämtliche Zugriffs-, Zugangs- und Zutrittsrechte auf die Bestandteile des Informationsverbundes vorsehen. Die vergebenen Berechtigungskonzepte orientieren sich dabei an dem ermittelten Schutzbedarf für die betreffenden IT-Systeme.

58 Genehmigungs- und Kontrollprozesse sollen sicherstellen, dass die Einrichtung, Änderung, Deaktivierung oder Löschung von Berechtigungen den Vorgaben der Berechtigungskonzepte

entsprechen. Fachlich verantwortliche Stellen sind hierbei angemessen entsprechend ihrer Verantwortung einzubinden. Die laufende Überprüfung der noch benötigten Berechtigungen im Sinne eines Rezertifizierungsprozesses hat ebenfalls unter Einbezug der zuständigen Kontrollinstanzen zu erfolgen. Diese Vorgänge sind nachvollziehbar und auswertbar zu dokumentieren.

59 Im Einklang mit dem bestehenden Schutzbedarf und den Soll-Anforderungen haben die Institute durch eine Protokollierung und Überwachung die bedarfsgerechte Nutzung der vergebenen Berechtigungen nachzuweisen. Privilegierte Benutzer- und Zutrittsrechte sind aufgrund der Kritikalität gesondert zu überwachen und protokollieren.

Umsetzung

60 Das Modul „**Benutzerverwaltung**“ (Menüpunkte „Benutzerverwaltung“, „Rezertifizierung“ und „Soll-Ist-Abgleich“) bietet den Anwendern verschiedene Möglichkeiten zur Vergabe von Benutzerrechten und zur Überwachung der vergebenen Rechte. Zu den am Benutzer gepflegten Informationen zählen u.a. allgemeine personenbezogene Daten wie Vor- und Nachname, berufliche oder private Kontaktdaten, Personalnummer oder die E-Mail-Adresse. Darüber hinaus ist es möglich, auch technische User zu definieren.

Zur Abbildung der Organisationsstruktur der jeweiligen Institute werden zudem die Stellenbezeichnungen und die Zuordnungen zur Organisationseinheiten sowie Zugriffsrollen für bit-MaRisk am Benutzer hinterlegt. Eine Historie kann sowohl für die Dimension des Benutzers als auch für die Berechtigung selbst ausgegeben werden.

61 Es bestehen grundlegende **Benutzer**-Funktionen, die eine Neuanlage von neuen Mitarbeitenden bei Eintritt oder eine Änderung von bestehenden Rechten bei einem Stellenwechsel sowie Namensänderungen ermöglichen. Zudem sind Funktionen zur Verwaltung von längerfristigen Abwesenheiten oder beim Wiedereintritt bzw. Austritt vorhanden. Individuelle Aufgaben zur Bearbeitung durch einzelne Mitarbeitende können ebenso vergeben werden.

62 Innerhalb des Moduls „Benutzerverwaltung“ können auch weitere IDs von **Berechtigungen** zu Programmen, die von den jeweiligen Instituten außerhalb von bit-MaRisk betrieben werden und zu denen keine laufende Importschnittstelle existiert, verwaltet werden.

63 Zur Dokumentation von **Kennwortvergaben** oder Entsperrungsvorgängen sowie Anfragen zur Authentifizierung sind ebenfalls weitere Funktionen implementiert. Es handelt sich bei diesen Funktionen um ausschließlich zur Dokumentation der Bearbeitungsschritte programmierte Abläufe, die Kennwortänderungen oder Entsperrungen selbst sind vorrangig in der jeweiligen Software des Instituts in den jeweiligen Abteilungen und/oder der IT durchzuführen.

64 Die **Berechtigungsaktualisierung** ermöglicht es den Nutzern von bit-MaRisk eine Übernahme von bspw. im Windows Active Directory angepassten Änderungen vorzunehmen und diese mit den bestehenden Berechtigungen in bit-MaRisk abzugleichen.

65 Sämtliche der oben beschriebenen Programmfunktionen, bspw. die Neuanlage oder Veränderung von Berechtigungen (**Benutzeraktionen**), werden in bit-MaRisk protokolliert und können über Übersichten dargestellt werden.

66 Mit Bezug zur Darstellung von **Berechtigungen** werden entsprechende Felder für den Status und die Vorlage eines Berechtigungskonzepts für die jeweilige Anwendung des Instituts mit den vergebenen Rechten und deren Gültigkeit vorgehalten. Vergebene Berechtigungen können über einen Stornierungsantrag wieder entzogen werden.

Ergänzend kann noch die hierarchische Berechtigungsstruktur inklusive der untergeordneten Berechtigungen und deren Herkunft visualisiert werden. Die hinterlegten Berechtigungen können zudem um Beschreibungen konkretisiert werden.

67 Zur Erleichterung der Anlage von neuen Benutzern oder der Replizierung von bereits bestehenden Berechtigungen können **Sammelvorlagen** angelegt werden. Falls die Bezeichnung von Berechtigungen von den extern übernommenen Werten abweicht, können durch das Institut auch **interne Zuordnungen** vergeben werden.

68 Im Workflow befindliche oder bereits abgeschlossene **Berechtigungsanträge** werden gesondert dargestellt. Innerhalb dieses Dialogs können die noch offenen Anträge umfassend bearbeitet oder neue Anträge gestellt werden.

69 Die jeweils in den Instituten gewählte **Organisationsstruktur** kann eigenständig in bit-MaRisk verwaltet werden. Hierzu sind Funktionen enthalten, die auf Stellen oder auf Ebene der Organisationseinheit eine entsprechende Pflege der benötigten Daten ermöglichen.

70 Eine **Organisationseinheit** erhält neben einem definierten Schlüssel, eine Bezeichnung der Ebene, eine eigenständige E-Mail-Adresse, personelle Verantwortlichkeiten (Rezertifizierung) und die Einordnung in die Organisationsstruktur des Instituts. Hierüber lässt sich bspw. die Vererbung von Berechtigungen von einer übergeordneten Ebene auf eine untergeordnete Ebene steuern. Jede Organisationseinheit kann mit individuellen Berechtigungen in Form von Paketen, Kompetenzen, Profilen, Rollen oder Rollengruppen verknüpft werden.

Innerhalb der Organisationseinheiten lassen sich jederzeit die effektiven Rechte und die zugeordneten Benutzer anzeigen. Den Organisationseinheiten werden ebenso Stellen zugeordnet.

Die Anzahl der Benutzer, die der Organisationseinheit zugeordnet sind, wird zur Plausibilisierung der vorhandenen Strukturen ausgegeben.

Anpassungen der Organisationseinheit werden über den entsprechenden Dialog initiiert. Es lassen sich zusätzlich ein Vergleich der Organisationseinheiten oder Mehrfach-/ Massenänderungen von Rechten oder Paketen vornehmen.

71 Die Verwaltung von **Stellen** folgt einer ähnlichen Logik und lässt ebenfalls einen Vergleich der vergebenen Stellen und Mehrfach-/ Massenänderungen von Rechten zu. Die Stellenstruktur unterstützt durch eine grafische Darstellung der Vorgesetztenstruktur und von rezertifizierenden Stellen die Analysen zur Berechtigungsvergabe und deren Überwachung. Jeder Stelle sind ein Besitzer und die gültigen Berechtigungen in Form von Paketen, Kompetenzen, Profilen, Rollen und Rollengruppen zugeordnet. Darüber hinaus werden die übergeordneten Stellen dargestellt.

72 Die Funktionalitäten zur Steuerung der **Berechtigungsstruktur** unterscheidet grundsätzlich nach

- Paketen
- Berechtigungskonzepten
- Kompetenzen
- Profilen
- Rollen
- Rollengruppen
- Feindefinitionen.

Wie oben bei den Organisationseinheiten und Stellen beschrieben, sind auf jeder Ebene Mehrfach-/ Massenänderungen sowie Vergleiche von bestehenden Berechtigungen möglich. Ebenso können die globalen Funktionen für die Neuanlage, Kopie, Änderung oder Archivierung in den jeweiligen Kategorien der Berechtigungsstruktur genutzt und die Anzahl der zugeordneten Benutzer angezeigt werden.

73 Unter **Paketen** werden die gesammelten, für einen Aufgabenbereich im Institut relevanten Berechtigungen zu den benötigten Programmen, zusammengefasst. Ein Berechtigungs-„Paket“ kann bspw. für einen Arbeitsplatz in der Internen Revision oder in der Organisation eines Instituts angelegt werden.

74 **Berechtigungskonzepte** beziehen sich vornehmlich auf einzelne Anwendungen oder Notes-Datenbanken. Innerhalb der Berechtigungskonzepte werden u.a. die Verantwortlichkeiten – auch für deren Rezertifizierung – festgelegt und die bei Freigabe oder Entzug zu informierenden Personen definiert. Des Weiteren werden dort die zentralen Konfigurationen für Berechtigungs-

vorlagen, die Kennwortverwaltung, Berechtigungsanträge und den Soll-Ist-Abgleich sowie den Informationsverbund getroffen.

75 Als Ebene unterhalb der Berechtigungskonzepte werden **Kompetenzen** in den jeweiligen Anwendungen vergeben. Die Kompetenzen sind grundsätzlich analog zu den Berechtigungskonzepten konfigurierbar. Es ist jedoch zusätzlich möglich, Rechte zusammenzuführen oder Sensibilitäten im Rahmen der IKS-Relevanz zu berechnen. Auf Kompetenzebene besteht zudem die Möglichkeit, Rechte als Belehrung zu interpretieren.

76 Alternativ können als weitere Ebene unterhalb der Berechtigungskonzepte **Profile** auf Personenebene vergeben werden. Bei den Profilen lassen sich ebenfalls Rechte zusammenführen oder Sensibilitäten anhand der IKS-Relevanz bestimmen. Die Konfiguration von Profile entspricht der Vorgehensweise bei den Kompetenzen.

77 Vollkommen identisch zur Funktionsweise der Profile sind die **Rollen** und **Rollengruppen** zu betrachten, die allerdings keine eigenständige Schnittstellenfunktion besitzen.

78 **Feindefinitionen** ermöglichen als weitere Ebene unterhalb der Kompetenzen bspw. eine differenziertere Unterscheidung von Lese- und Schreibrechten oder Zugriffen auf gewisse Wertebereiche von individuell festgelegten Parametern.

Über die Anlage von **Abhängigkeits-** und **Sperrlisten** können zusätzliche Einschränkungen von Berechtigungen definiert werden. Diese Abhängigkeiten oder Sperren werden individuell anhand von für die Durchführung der Aktion benötigten Parametern, bspw. das Vorliegen von gewissen Fortbildungszertifikaten, festgelegt. So wird sichergestellt, dass nur Personen mit der notwendigen fachlichen Kompetenz die parametrisierten Berechtigungen erhalten. Durch diese Funktionalitäten wird ebenso die Umsetzung einer Funktionstrennungs-Matrix („Segregation of Duties“, SoD) unterstützt. Die Abhängigkeits- und Sperrlisten können jederzeit außer Kraft gesetzt werden.

79 Als weiterer Funktionsumfang des Moduls „Benutzerverwaltung“ können **IDs**, welche in anderen Softwarenanwendungen Verwendung finden, in bit-MaRisk konfiguriert werden. Hierbei kann zwischen eindeutigen IDs und Pool-IDs unterschieden werden.

80 Zur individuellen Bearbeitung von anfallenden Tätigkeiten in der Benutzerverwaltung können, losgelöst von den bestehenden Workflows, einmalig oder wiederholend zu erledigende **Aufgaben** unter Berücksichtigung von Fristen vergeben werden. Als Nachweis von erfolgten Rezertifizierungen können über das Programm auch **Quittungen** in Form von vorformulierten Bestätigungen an die betroffenen Mitarbeitenden des Instituts zur Kenntnisnahme und Bestätigung des

Erhalts des Schreibens versendet werden. Sowohl die Aufgaben als auch die Quittungen lassen sich über entsprechende Vorlagen und Bedingungen konfigurieren.

81 Die Benutzerverwaltung von Instituten wird ebenfalls durch die Funktionen der **Rezertifizierung** in einem separaten Menüpunkt unterstützt. Innerhalb dieser Funktionen werden die verschiedenen Vorgänge der Rezertifizierung nach Typen und Zeitpunkten ausgegeben. Ebenso lassen sich die **Rezertifizierungsdokumente** nach diversen Filterlogiken sortieren.

82 Grundlegende **Rezertifizierungskonfigurationen** ermöglichen des Weiteren eine Parametrisierung von Rezertifizierungsläufen, bspw. anhand von verschiedenen Rezertifizierungstypen. Darüber hinaus können **Ad-hoc Rezertifizierungen** durchgeführt oder auch ausgewählte Benutzer individuell rezertifiziert werden.

83 Weitere Unterstützungsfunktionen zur Benutzerverwaltung bietet bit-MaRisk im Zusammenhang mit dem **Soll-Ist-Abgleich** von Berechtigungen. Im Listenformat werden **Abgleichsanforderungen** bezogen auf die relevanten Berechtigungskonzepte je Anwendung definiert und mit den Parametern einer **Abgleichskonfiguration** für diese Anwendung verglichen. Die Abgleichskonfigurationen beinhalten allgemeine Informationen wie die Bezeichnung, aber auch die Einstellungen aus der Benutzerverwaltung bzgl. der Rechte, Kompetenzen, Profile, Rollen und Rollengruppen. Ebenso werden an dieser Stelle die Eigenschaften der zu erwartenden Import-Datei festgelegt. Wesentlicher Faktor für einen korrekten Abgleich der Berechtigungen ist das in der Konfiguration festgelegte Mapping der Datenfelder im Livesystem (Ist) und der Benutzerverwaltung (Soll). Eine Historie zeigt die Veränderungen der Konfiguration auf.

84 Zur Parametrisierung der Konfigurationen können die tatsächlich vergebenen **Berechtigungen** aus den betreffenden Anwendungen (Ist-Berechtigungen) direkt eingelesen und den Berechtigungen aus der Benutzerverwaltung von bit-MaRisk (Soll-Berechtigungen) gegenübergestellt werden. Eine Aktualisierungsfunktion der Standardkonfigurationen gewährleistet die Aktualität der jeweiligen Parameter. Ein **Abgleich** von Berechtigungen ist sowohl auf Ebene von Benutzern als auch auf Berechtigungsebene jederzeit möglich und wird grafisch mit Hervorhebungen von Abweichungen in tabellarischer Form durch die Software ausgegeben.

85 Diverse Bearbeitungswerkzeuge lassen die Anwender Such- und Ersetz-Funktionen, oder Black- und Whitelisten simulieren sowie Massenänderungen in den Listen der Soll- und Ist-Berechtigungen vornehmen. Zudem können aus den Abgleichslisten zur einzelne Datensätze aus den Ansichten entfernt oder als bearbeitet markiert werden.

Prüfung und Ergebnis

86 Die Prüfung der programminternen Verarbeitungsregeln basierte auf Testfällen. Die durchgeführten Tests fanden auf der von der bit Informatik bereitgestellten Testumgebung statt.

87 Die Mitarbeiterstammdaten können aus den Systemen, also bspw. dem Windows Active Directory des Kunden der bit Informatik übernommen werden. Aufgrund der vielfältigen Importmöglichkeiten und der Abhängigkeit von den Systemen der Kunden unterlag der Import von Stammdaten nicht der Prüfung.

Die Funktion „Weitere ID ändern“ (**Benutzer**) wurde aufgrund der individuellen Anforderungen an die dort verwalteten IDs in anderen Softwarewareanwendungen des jeweiligen Instituts nicht nachvollzogen.

Die Funktionen zur Kennwortvergaben (**Benutzer**) unterlag aufgrund der alleinigen Betrachtung der Programmfunktionen von bit-MaRisk nur insoweit der Prüfung, als diese in bit-MaRisk anhand der vorliegenden Dokumentation validiert werden konnte. Die tatsächliche Durchführung von Kennwortänderungen oder Entsperrungen in den von den jeweiligen Instituten noch betriebenen Anwendungen und die Übertragung nach bit-MaRisk war nicht Gegenstand der Prüfung.

Ebenso wenig konnte die Funktion zur Berechtigungsaktualisierung (**Benutzer**) aufgrund der benötigten Daten aus Fremdsystemen getestet werden, da diese Fremdsysteme und deren individuellen Datenformate nicht Gegenstand der Prüfung waren.

Die Schnittstellen-Funktion bei den **Profilen** wurde aufgrund der Abhängigkeit von anderen Softwarelösungen nicht in die Prüfung einbezogen.

88 Bei unseren stichprobenweisen Prüfungen der verbleibenden Verarbeitungsfunktionen ergaben sich keine Beanstandungen. Die beschriebenen Verarbeitungsregeln sind geeignet, eine ordnungsgemäße Benutzerverwaltung zu unterstützen.

2.3.3 bit-MaRisk - Vertragsverwaltung und Dienstleistersteuerung

Anforderungen

89 Die Anforderungen an das Modul „Vertragsverwaltung und Dienstleistersteuerung“ von bit-MaRisk lassen sich grundsätzlich aus den organisatorischen Verpflichtungen gemäß § 25a KWG herleiten. Hierbei hat ein Institut interne Kontrollverfahren mit einem internen Kontrollsystem, wobei das interne Kontrollsystem insbesondere aufbau- und ablauforganisatorische Regelungen mit klarer Abgrenzung der Verantwortungsbereiche beinhalten soll, einzurichten. Zudem

ist eine vollständige Dokumentation der Geschäftstätigkeit sicherzustellen.

90 Die MaRisk konkretisieren die Anforderungen an ein Internes Kontrollsystem in AT 4.3. In Abhängigkeit von Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten sind durch ein Institut Regelungen zur Aufbau- und Ablauforganisation zu treffen. Prozesse sowie die damit verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege sind gemäß den MaRisk klar zu definieren und aufeinander abzustimmen.

91 In AT 9 der MaRisk werden die grundlegenden Anforderungen an die Analyse von Vertragsverhältnissen bzgl. der Beurteilung, ob die in Anspruch genommene Dienstleistungen eine nicht wesentliche oder wesentliche Auslagerung bzw. einen sonstigen Fremdbezug darstellt, gestellt. Hierzu ist durch die Institute eine umfassende Risikoanalyse zu implementieren. Ebenso sind bereits bei der Vertragsgestaltung die Anforderungen von AT 9.7 zu beachten, die konkrete vertragliche Bestandteile wie bspw. die Nennung der Standorte der Dienstleistungserbringung, die vereinbarten Service Level, uneingeschränkte Informations- und Prüfungsrechte oder Regelungen zur Weiterverlagerungen von Tätigkeiten sowie ein Notfallkonzept umfassen.

92 Die laufende Überwachung von wesentlichen Auslagerungen und die damit verbundene Risikosteuerung regelt AT 9.9 MaRisk mit Bezug zu den vereinbarten Gütekriterien sowie den durch den Dienstleister bereitgestellten Informationen zur Beurteilung der Leistungserbringung. Im Rahmen dieser Tätigkeiten sind Verantwortlichkeiten für den Kontroll- und Überwachungsprozess zu regeln und eine Dokumentation im Sinne eines Auslagerungsregisters mit entsprechenden Nachweisen der Kontrollverantwortlichen zu erstellen.

93 Das Kapitel 9 der BAIT konkretisiert die Vorgaben aus AT 9 MaRisk hinsichtlich der Implikationen der Dienstleistungsvereinbarungen auf die Informationssicherheit von Instituten. Insbesondere wird dort der Umfang der Risikoanalyse auf den sonstigen Fremdbezug von IT-Dienstleistungen unter Einbindung des Informationssicherheits- und Notfallbeauftragten ausgeweitet. Analog zur Steuerung der Auslagerungen ist der sonstige Fremdbezug von IT-Dienstleistungen ebenfalls einer laufenden Überwachung und Risikobeurteilung zu unterziehen. Die BAIT weisen, wie auch die MaRisk, auf die vertraglichen Anpassungen hinsichtlich der Aufnahmen von Regelungen zum Informationsrisiko- und -sicherheitsmanagement durch den Dienstleister hin.

94 Neben den bankaufsichtlichen Anforderungen sind für die Vertragsverwaltung die Regelungen der §§ 238 ff. HGB und § 257 HGB relevant, die die geordnete Aufbewahrung und Archivierung von rechnungslegungsrelevanten Unterlagen, im vorliegenden Fall für Dauerschuldverhältnisse, kodifizieren. Im Wesentlichen sind hier die Verfügbarkeit und die Lesbarkeitmachung der Unterlagen innerhalb der Aufbewahrungsfrist von i.d.R. zehn Jahren zu nennen.

Umsetzung

95 Das Modul „**Vertragsverwaltung und Dienstleistersteuerung**“ gliedert sich in Funktionalitäten zur Verwaltung von Vertragsdaten, wie den Vertrags- und Ansprechpartnern bei den Lieferanten oder Dienstleistern sowie zur Archivierung der zugrundeliegenden Verträge. Neben diesen Funktionen zum Vertragsmanagement existieren weitreichende Möglichkeiten zur Unterstützung der laufenden Dienstleisterüberwachung über die Ablage von verschiedenen Begleitdokumenten.

96 Wesentlicher Bestandteil ist die Vertragsverwaltung gegliedert nach **Vertragspartnern**. Diese werden standardmäßig in Kategorien von

- Direkten Vertragspartnern
- Weiterverlagerungsunternehmen
- Verbundpartnern
- Herstellern
- Lieferanten und
- Supportanbietern

klassifiziert und grafisch in der Listendarstellung hervorgehoben. Neben individuellen Änderungen der Unternehmensdaten von Vertragspartnern sind Massenänderungen von Datensätzen der Vertragspartner analog zu den Funktionalitäten der anderen Module möglich.

97 Für jeden Vertragspartner können eine Vielzahl von **Begleitdokumenten**, bspw. der abgeschlossene Vertrag, Berichtsauswertungen von erhaltenen Prüfungsberichten des Vertragspartners oder Beurteilungsbögen sowie Überwachungsergebnisse von Service Level Agreements (SLA) angelegt werden.

98 Neben der Gliederung nach Vertragspartnern können die Dienstleister zur Vereinfachung der Kommunikation auch nach **Ansprechpartnern**, deren Kontaktdaten unter diesem Menüpunkt gepflegt werden können**,** sortiert angezeigt werden.

99 Die **Vertragsübersichten** geben eine Darstellung der abgeschlossenen Verträge nach Vertragsarten und den Vertragslaufzeiten wieder. Des Weiteren werden grafische Hervorhebungen für die Klassifikation eines Vertrags als Rahmenvertrag oder als untergeordneter Vertrag innerhalb einer Rahmenvereinbarung, die Eigenschaft der Weiterverlagerung und dem Vorliegen von Begleitdokumenten dargestellt. Innerhalb des Menüs „Begleitdokumente“ besteht neben dem Aufruf der jeweilig zugeordneten Dokumente zudem eine Import-Funktion von Risikoermittlungen für den Dienstleistungsbezug zur Verfügung.

100 In der jeweiligen Vertragsansicht sind die allgemeinen Vertragsdaten, wie die internen Zuständigkeiten für den Dienstleister, Laufzeiten und Kündigungsfristen, Kosten oder die aufsichtsrechtlichen Anforderungen, zu hinterlegen. Die Steuerung der aufsichtsrechtlichen Anforderungen betrifft Datenfelder für die vertraglichen Mindestanforderungen nach AT 9 MaRisk, datenschutzrechtliche Anforderungen, Compliance-Anforderungen nach dem GwG oder WpHG und vom Institut individuell angelegte Vorgaben.

Darüber hinaus werden in der Vertragsverwaltung die Verknüpfungen zu bestehenden Geschäftsprozessen erstellt und die Ergebnisse der Schutzbedarfsanalyse sowie bestehende Berechtigungskonzepte dargestellt.

Über die Vertragsansicht können zudem die Weiterverlagerungskette und die Bedeutung des Vertrags für die betroffenen Geschäftsprozesse in der Hierarchie des Informationsverbunds visualisiert sowie die Historie des Vertrags angezeigt werden.

101 Auf einer weiteren Ebene können die **Begleitdokumente** in Listenform aufgerufen werden. Je Begleitdokument können die Historie des Dokuments abgerufen oder Wiedervorlagen zur workflowgestützten Bearbeitung erzeugt werden.

Die Begleitdokumente sind wesentlicher Bestandteil der Instrumente zur Dienstleistersteuerung nach AT 9 MaRisk. Neben der initialen Auslagerungs- bzw. Risikoanalyse bis hin zur Erstellung des Jahresberichts des zentralen Auslagerungsmanagements stehen diverse Dokumentenklassen zum Nachweise der Tätigkeiten mit Bezug zur Dienstleistersteuerung zur Verfügung.

Prüfung und Ergebnis

102 Die Prüfung der programminternen Verarbeitungsregeln basierte auf Testfällen. Die Testfälle wurden mit selbst erstellen Testdaten bzw. Demo-Daten der bit Informatik durchgeführt. Die durchgeführten Tests fanden auf der von der bit Informatik bereitgestellten Testumgebung statt. Die Tests umfassten die Kontrolle der Benachrichtigungen, die Konfiguration der Vertragsparameter, die Ansichten zur Vertragsverwaltung und laufende Überwachung der Dienstleister über die Bearbeitung von Begleitdokumenten sowie die Erstellung der relevanten Auswertungen für dieses Modul, insbesondere das Auslagerungsregister.

103 Bei unseren stichprobenweisen Prüfungen ergaben sich keine Beanstandungen. Die beschriebenen Verarbeitungsregeln sind geeignet, eine ordnungsgemäße Vertragsverwaltung und Dienstleistersteuerung zu unterstützen.

2.3.4 bit-MaRisk - ObjectLifecycle

Anforderungen

104 Die Anforderungen an das Modul „ObjectLifecycle“ (Menüpunkte „Anwendungsverwaltung“, „Strukturanalyse“ und „Geschäftsprozesse“) von bit-MaRisk lassen sich grundsätzlich aus den organisatorischen Verpflichtungen gemäß § 25a KWG herleiten. Hierbei hat ein Institut interne Kontrollverfahren mit einem internen Kontrollsystem, wobei das interne Kontrollsystem insbesondere aufbau- und ablauforganisatorische Regelungen mit klarer Abgrenzung der Verantwortungsbereiche beinhalten soll, einzurichten. Zudem ist eine vollständige Dokumentation der Geschäftstätigkeit sicherzustellen.

105 Die MaRisk konkretisieren die Anforderungen an ein Internes Kontrollsystem in AT 4.3. In Abhängigkeit von Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten sind durch ein Institut Regelungen zur Aufbau- und Ablauforganisation zu treffen. Prozesse sowie die damit verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege sind gemäß den MaRisk klar zu definieren und aufeinander abzustimmen.

106 Die Vorgaben von AT 7.2 MaRisk verlangen eine Ausrichtung des Umfangs und der Qualität der technisch-organisatorischen Ausstattung an den betriebsinternen Erfordernissen, den Geschäftsaktivitäten sowie der Risikosituation des Instituts. Hierzu sind die IT-Systeme und IT-Prozesse sowie weitere Bestandteile des Informationsverbundes unter Berücksichtigung der Schutzziele Integrität, Verfügbarkeit, Authentizität und Vertraulichkeit zu analysieren.

IT-Risiken sind innerhalb eines angemessenen Überwachungs- und Steuerungsprozesses darzulegen, wobei diese Prozesse anhand von festgelegten IT-Risikokriterien, die Identifikation von IT-Risiken, die Festlegung des Schutzbedarfs, daraus abgeleitete Schutzmaßnahmen für den IT-Betrieb sowie Maßnahmen zu Risikobehandlung und -minderung ermöglichen sollen. Dies schließt den Softwarebezug mit ein. Im Institut entwickelte oder betriebene Anwendungen, die der individuellen Datenverarbeitung zuzuordnen sind, werden ebenfalls in diese Betrachtungsweise einbezogen.

107 Das Kapitel 3 der BAIT zum Informationsrisikomanagement gibt weitere Erläuterungen zur Darstellung des Informationsverbundes, welcher einen Überblick über die jeweiligen Bestandteile und die Abhängigkeiten sowie Schnittstellen geben soll. Der Schutzbedarf anhand der oben genannten Schutzziele ist dabei regelmäßig oder anlassbezogen zu ermitteln. Die Verantwortung hierfür liegt bei den Eigentümern der Information, i.d.R. bei den Prozess- oder Risikoverantwortlichen. Die Überprüfung der Schutzbedarfsfeststellung hat durch das Informationsrisikomanagement zu erfolgen. Zur Erreichung des jeweiligen Schutzbedarfs sind Anforderungen im

Form eines Sollmaßnahmenkatalogs zu definieren, der regelmäßig mit den umgesetzten Maßnahmen (Ist-Zustand) abgeglichen wird.

108 Koordiniert und überwacht wird die Risikoanalyse über das Informationsrisikomanagement. Die Ergebnisse sollen hiernach in die Prozesse zur Steuerung der operationellen Risiken übergeben werden. Die Behandlung der Risiken unterliegt einer kompetenzgerechten Genehmigung.

109 Laufende Bedrohungen für den Informationsverbund sind durch das Institut auf Relevanz zu überprüfen und deren Auswirkungen zu bewerten. Sofern erforderlich, sind geeignete technische und organisatorische Maßnahmen zu ergreifen. Die Geschäftsleitung ist regelmäßig, mindestens vierteljährlich, über die Ergebnisse der Risikoanalyse sowie Veränderungen der Risikosituation zu informieren.

110 Die Einbindung des Informationssicherheitsbeauftragten wird in Kapitel 4 der BAIT zum Informationssicherheitsmanagement geregelt, diese unabhängige Stelle ist ebenso verpflichtet, einen regelmäßigen, mindestens vierteljährlichen Bericht der Geschäftsleitung zum Status der Informationssicherheit vorzulegen.

111 In Abhängigkeit von in der Informationssicherheitsleitlinie und in den aus dieser abgeleiteten Richtlinien definierten institutsindividuellen Vorgaben sind gemäß Kapitel 5 BAIT zur operativen Informationssicherheit angemessene Sicherheitsmaßnahmen und Prozesse zu implementieren, die möglichst frühzeitig Gefährdungen des Informationsverbundes identifizieren.

Umsetzung

112 Das Modul ObjectLifecycle von bit-MaRisk setzt sich aus den drei separaten Menüpunkten „Anwendungsverwaltung“, „Strukturanalyse“ und „Geschäftsprozesse“ zusammen.

113 Die **Anwendungsverwaltung** gibt einen Überblick über die durch das Institut genutzten **Anwendungen**, die nach Programmarten, Versionsständen, Verantwortlichkeiten und den Ergebnissen der Schutzbedarfsanalyse strukturiert dargestellt werden können.

114 Innerhalb der Anwendungsverwaltung werden bereits standardmäßig diverse Workflows (**Vorgänge**) zur Softwarebeschaffung/-ablösung, dem Programmeinsatzverfahren (PEV), von Auswertungen zur individuellen Datenverarbeitung (IDV) sowie zu Updates oder jährlichen Überprüfungen von Anwendungen angeboten. Ebenso wie bei den anderen Modulen sind Massenänderungen für eine Vielzahl von Anwendungen durchführbar.

115 Bezogen auf die Anwendungen lassen sich die dazugehörigen Geschäftsprozesse, deren Schutzbedarf und Schutzniveau, Schutzobjektzuordnungen sowie die eingeleiteten Maßnahmen zur Risikosteuerung anzeigen oder ändern. In Verbindung mit den übrigen Modulen von bit-MaRisk bestehen des Weiteren Verknüpfungen zu den jeweiligen Verträgen, Dokumentationen im Organisationshandbuch und Berechtigungs-/ Protokollauswertungskonzepten. Des Weiteren können die gesetzlichen, fachlichen und technischen Anforderungen, Parameter zu den Verantwortlichkeiten und Schnittstellen hinterlegt sowie Auswirkungen auf das Notfallmanagement konfiguriert werden.

Ergänzt werden diese Angaben durch Informationen zu den Freigaben der Anwendung innerhalb des Programmeinsatzverfahrens und Prüfungsintervallen sowie weiteren Informationen zu Herstellern und den mit der Anwendung verbundenen Kosten.

116 Abschließend kann festgelegt werden, ob die Anwendung in das **Verzeichnis der Verarbeitungstätigkeiten** übernommen wird, welches sich aus dem entsprechenden Menüpunkt öffnen lässt.

117 Standardmäßig können die Historie und die laufenden Vorgänge einer Anwendung angezeigt und Wiedervorlagen erstellt werden. Grafisch lassen sich der über- und untergeordnete Informationsverbund in Abhängigkeit von der Ebene der Anwendung visualisieren.

118 Hinsichtlich der vergleichbaren Anforderungen an die Informationssicherheit lassen sich auch aus dem Menüpunkt **Strukturanalyse** die verwalteten **Anwendungen** öffnen und bearbeiten. Wesentliche Funktionen zur Unterstützung der Strukturanalyse finden sich in der Darstellung der im Institut vorhandenen IT-Systeme, Verbindungen, Räume und sonstigen Objekte. Darüber hinaus werden Funktionen zur Auswertung von Protokollen zur Überprüfung der Schutzobjekte angeboten.

119 In Analogie zu den Informationen der Anwendungen werden bei den **IT-Systemen**, die für ein Informationssicherheitsmanagementsystem (ISMS) notwendigen Informationen zusammengetragen. Zu diesen Informationen zählen sowohl allgemeine Angaben zu Herstellern oder Inventarnummern als auch die Verknüpfungen zu bestehenden Geschäftsprozessen und den hierarchischen Ebenen im Informationsverbund. Ebenso werden je IT-System die aktuellen Schutzbedarfseinschätzungen über den Vererbungsstatus im Verhältnis zum tatsächlichen Schutzniveau unter Hervorhebung von möglichen Abweichungen dargestellt. Wie in den anderen Menüpunkten stehen in der Ansicht der Strukturanalyse die verknüpften Verträge und Berechtigungskonzepte sowie die Überprüfungsintervalle zur Verfügung.

120 Die Menüpunkte der **Verbindungen, Räume** und **sonstigen Objekte** orientieren sich ebenfalls an dem oben beschriebenen Schema und ermöglichen eine Auswertung der Verbindungen, Räume und sonstigen Objekte im Zusammenhang mit den verknüpften Geschäftsprozessen, den festgestellten Schutzbedarf bzw. Schutzniveau sowie zu den betroffenen Verträgen und Berechtigungskonzepten.

121 Im Unterpunkt der **Protokollauswertungskonzepte** können die Kontrollverantwortlichen ihre Tätigkeiten hinsichtlich der Überprüfung von Protokollen aus IT-Verfahren – bspw. zur Aktualität von Programmversionen – dokumentieren, den Turnus der Überwachungen und Auswirkungen auf Berechtigungskonzepte steuern.

122 Im Menüpunkt der **Geschäftsprozesse** befinden sich die Konfiguration der **Datenklassen** sowie die Funktionalitäten zur regelmäßigen Überprüfung der Schutzbedarfsfeststellungen. Die Datenklassen werden an dieser Stelle zentral parametrisiert und einer Schutzbedarfsanalyse mit Bezug zu den relevanten Schutzzielen unterzogen. Darüber hinaus wird festgelegt, welchen Geschäftsprozessen die Datenklassen zuzuordnen sind. Zur Visualisierung der Resultate steht wiederum die Darstellung des Informationsverbundes zur Verfügung.

123 Zentrales Element dieses Menüpunktes ist die Dokumentation der im Institut gelebten **Geschäftsprozesse**. Die Funktionen erlauben die Durchführung einer Risikobewertung des Geschäftsprozesses mit einer Verknüpfung zum Modul Internes Kontrollsystem und die Festlegung, ob der betreffende Prozess als wesentlicher Geschäftsprozess für das Institut zu werten ist. Zusätzlich können die Prozessschritte individuell definiert, der Prozess als für das Notfallmanagement unter Berücksichtigung von Business Impact Analysen (BIA) relevant und in Abhängigkeit der verknüpften Notfallszenarien klassifiziert werden.

Der oben beschriebenen Logik folgend, können die Datenklassen sowie der Schutzbedarf des Geschäftsprozesses angezeigt und bearbeitet werden. Zur Verdeutlichung der Abhängigkeiten mit den Schutzobjekten können die verknüpften vor- und nachgelagerten Geschäftsprozesse und Anwendungen sowie Verträge aufgerufen werden.

124 Zur Unterstützung der Vollständigkeit können die entsprechenden Geschäftsprozesse dem datenschutzrechtlichen **Verzeichnis der Verarbeitungstätigkeiten** zugewiesen werden. Innerhalb dieses Menüs können die Zwecke und Zulässigkeit der Datenverarbeitung, die Klassen der personenbezogenen Daten, Empfängerkategorien und die Datenübermittlung an Dritte sowie die technischen und organisatorischen Maßnahmen dokumentiert und die Ergebnisse von Datenschutz-Folgenabschätzung abgelegt werden.

Prüfung und Ergebnis

125 Die Prüfung der programminternen Verarbeitungsregeln basierte auf Testfällen. Die Testfälle wurden mit selbst erstellten Testdaten und Demo-Daten der bit Informatik durchgeführt. Die durchgeführten Tests fanden auf der von der bit Informatik bereitgestellten Testumgebung statt. Die Tests umfassten die Erstellung, Bearbeitung und Verwaltung von Anwendungen, Schutzobjekten der Strukturanalyse und von Geschäftsprozessen.

126 Bei unseren stichprobenweisen Prüfungen ergaben sich keine Beanstandungen. Die beschriebenen Verarbeitungsregeln sind geeignet, eine ordnungsgemäße Verwaltung eines ISMS zu unterstützen.

2.3.5 bit-MaRisk - Internes Kontrollsystem

Anforderungen

127 Die Anforderungen für das Modul „Internes Kontrollsystem“ von bit-MaRisk lassen sich grundsätzlich aus den organisatorischen Verpflichtungen gemäß § 25a KWG herleiten. Hierbei hat ein Institut interne Kontrollverfahren mit einem internen Kontrollsystem, wobei das interne Kontrollsystem insbesondere aufbau- und ablauforganisatorische Regelungen mit klarer Abgrenzung der Verantwortungsbereiche beinhalten soll, einzurichten. Zudem ist eine vollständige Dokumentation der Geschäftstätigkeit sicherzustellen.

128 Die MaRisk konkretisieren die Anforderungen an ein Internes Kontrollsystem in AT 4.3. In Abhängigkeit von Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten sind durch ein Institut Regelungen zur Aufbau- und Ablauforganisation zu treffen. Miteinander unvereinbare Tätigkeiten sind jeweils durch unterschiedliche Mitarbeiter durchzuführen und Interessenkonflikte sowie Selbstprüfungen zu vermeiden.

129 Prozesse sowie die damit verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege sind gemäß den MaRisk klar zu definieren und aufeinander abzustimmen, Berechtigungen und Kompetenzen nach dem Sparsamkeitsgrundsatz zu vergeben.

Umsetzung

130 Das Modul Internes Kontrollsystem orientiert sich bei den dortigen Funktionalitäten an den grundsätzlich vorhandenen **Geschäftsprozessen** im Institut. Die Geschäftsprozesse werden im Wesentlichen einer Risikoeinstufung unterworfen, die zwischen einer Brutto- und Nettobetrachtungsweise unterscheidet. Die Risikoeinstufung erfolgt anhand der im Institut vorherrschenden Risikomatrix. Jedem Geschäftsprozess ist folglich ein Brutto- und Nettoschadenspotenzial zu-

geordnet. Die Risikobewertung kann, wie bereits oben bei der Beschreibung des Moduls zu den Geschäftsprozessen dargelegt, turnusmäßig überprüft und aktualisiert werden.

131 Wesentlicher Bestandteil dieses Moduls ist die Dokumentation der **Risikobewertung** auf Prozessebene. Die in der Risikobewertung beinhalteten Risikokategorien werden zentral administriert und an den Bedarf des jeweiligen Instituts angepasst, beispielhaft genannt sein hier die Risiken aus der internen Infrastruktur und den Verfahren, in Bezug auf das Verhalten von Mitarbeitenden oder juristische und regulatorische Einflüsse. Jeder Kategorie sind eine Vielzahl von Einzelrisiken zugewiesen, die einem Risikoeigner und verschiedenen Brutto- und Nettorisikowerte zugeordnet sein können. Als Ergebnis ergibt sich jeweils ein Brutto- oder Nettoschadenspotenzial anhand der Mittelwerte der Risiken gemessen in EUR und in einer farblichen Risikoeinstufung („Ampel-Logik“) gegliedert.

132 Den erfassten Risiken kann durch die Implementierung von **Kontrollen** begegnet werden. Hierzu gibt das Modul „Internes Kontrollsystem“ eine Kontrollübersicht aus, die sämtliche dem Geschäftsprozess zugeordnete Kontrollen zusammenfasst. Diese Kontrollen werden Verantwortlichen zugewiesen und unterscheiden sich nach Kontrollarten/-typen sowie nach der Eigenschaft als Schlüsselkontrolle.

133 Die Wirksamkeit der definierten Kontrollen kann im Rahmen von **Kontrolltests** validiert und über entsprechende Eingabemasken dokumentiert werden. Zur Dokumentation der Kontrolltests sind allgemeine Informationen wie der Zeitpunkt der Prüfungshandlung und die Verantwortlichkeiten sowie der Stichtags- oder Zeitraumbezug der Kontrolle einzugeben. Des Weiteren können die Art der Prüfungshandlung (Befragung, Beobachtung, Durchsicht, Nachvollzug), ergänzende Dokumente und das entscheidende Ergebnis der Prüfung angegeben werden.

In Checklistenform können Fragen zur Angemessenheit und Wirksamkeit sowie zur vorgesehenen Durchführung der Kontrolltests unter Berücksichtigung von Empfehlungen beantwortet werden. Analog zur Festlegung eines Intervalls zur Risikobewertung kann auch ein Turnus für die Durchführung des Kontrolltests vergeben werden.

Prüfung und Ergebnis

134 Die Prüfung der programminternen Verarbeitungsregeln basierte auf Testfällen. Die Testfälle wurden mit selbst erstellten Testdaten und Demo-Daten der bit Informatik durchgeführt. Die durchgeführten Tests fanden auf der von der bit Informatik bereitgestellten Testumgebung statt. Die Tests umfassten die Erstellung, Bearbeitung und Verwaltung des Internen Kontrollsystems, den Nachvollzug der Prüfungs- und Freigabeworkflows im Zusammenhang mit der Durchführung der Kontrollen bzw. Kontrolltests und die relevanten Benachrichtigungsfunktionen.

135 Bei unseren stichprobenweisen Prüfungen ergaben sich keine Beanstandungen. Die beschriebenen Verarbeitungsregeln sind geeignet, eine ordnungsgemäße Überwachung des Internen Kontrollsystems zu unterstützen.

2.3.6 bit-MaRisk - Notfallmanagement

Anforderungen

136 Die zentralen Anforderungen für das Modul „Notfallmanagement“ von bit-MaRisk ergeben sich aus AT 7.3 MaRisk. Grundlage eines aufsichtlichen Notfallmanagements sind die Festlegung von Zielen und den hieraus abgeleiteten Prozessen des Notfallmanagements. Für die identifizierten zeitkritischen Prozesse des Instituts ist ein Notfallkonzept zu erstellen, welches anlassbezogen oder jährlich zu aktualisieren bzw. zu überprüfen sowie angemessen zu kommunizieren ist. Innerhalb des Notfallkonzeptes sind für die zeitkritischen Prozesse Geschäftsfortführungs- und Wiederherstellungspläne festzulegen. Im Notfall sind diese Pläne ebenfalls angemessen intern und extern zu kommunizieren.

137 Wechselwirkungen zum Auslagerungsmanagement nach AT 9 MaRisk ergeben sich bei der Auslagerung von zeitkritischen Prozessen an Dienstleister. In diesem Fall haben das Institut und der Dienstleister aufeinander abgestimmte Notfallkonzepte zu definieren.

138 Eine regelmäßige, mindestens jährliche bzw. anlassbezogene, Überprüfung der für das Institut relevanten Notfallszenarien für die zeitkritischen Prozesse auf Angemessenheit und Wirksamkeit ist durchzuführen. Die Ergebnisse der Überprüfung der Szenarien sind zu dokumentieren, auf Verbesserungspotenzial zu untersuchen und den Verantwortlichen schriftlich vorzulegen. Zudem sollen die Erkenntnisse aus der Überprüfung in die Risikosteuerung des Instituts eingebracht werden.

139 Konkretisierende Vorgaben zu AT 7.3 MaRisk finden sich in Kapitel 10 der BAIT zum IT-Notfallmanagement, insbesondere für die in den IT-Notfallplänen zu definieren Parameter der Wiederanlaufzeit, des maximal tolerierbaren Zeitraums, in dem Datenverlust hingenommen werden kann, und zur Konfiguration des Notbetriebs. Des Weiteren sind u.a. die Abhängigkeiten zwischen vor- und nachgelagerten Geschäftsprozessen, den eingesetzten IT-Systemen sowie den Dienstleistern und Priorisierungen von Prozessen bei der Wiederherstellung zu analysieren. Diese Analyse beinhaltet die Betrachtung der notwendigen Ressourcen zur Fortführung der Geschäftsprozesse.

140 Wesentliche Anforderung aus Kapitel 10 BAIT ist der Nachweis durch das Institut, dass bei den Tests der IT-Notfallpläne sämtliche IT-Systeme (bspw. Komponenten, Anwendungen), die die

zeitkritischen Prozesse unterstützen, einbezogen werden. Dabei sind Abhängigkeiten zwischen den IT-Systemen oder gemeinsam genutzten IT-Systemen zu berücksichtigen.

Umsetzung

141 Das Modul Notfallmanagement bietet Funktionalitäten zur Erstellung eines Notfallhandbuchs und zur Dokumentation von Übungs-/Notfällen sowie der Business Impact Analyse (BIA).

142 Innerhalb des **Notfallhandbuchs** werden die zentralen Notfallszenarien hinterlegt und die dazugehörige Notfall- und Übungsdokumentation abgelegt. Diesen Szenarien sind wiederum Überprüfungsintervalle zugeordnet. Innerhalb der Szenarien lassen sich die allgemeinen Informationen zu den Kategorien und Verantwortlichkeiten sowie die verbale Beschreibung des Szenarios bzw. Konzepts hinterlegen. Zu den Informationen zählen auch die schrittweise anzulegenden Geschäftsfortführungs- und Wiederherstellungspläne. Ergänzend kann ein Übungsplan für das betreffende Notfallszenario definiert werden. Eine Exportfunktion zur papierhaften Aufbewahrung des Notfallhandbuchs ist ebenso enthalten.

143 Die **Übungs-/Notfalldokumentation** bietet verschiedene Möglichkeiten zur Beschreibung des Ablaufs des Übungs- bzw. Notfalls unter Einbezug der teilnehmenden Personen (Leitungsfunktion, Protokollführung oder Beobachtende) und eines festgelegten Zeitplans. In ausführlicher Schriftform kann das Protokoll des Vorfalls gespeichert werden. Die einzelnen Schritte des Ablaufs sind hierbei dezidiert als Dokumentationseinträge erfassbar.

144 Die laufende Überwachung der kritischen Geschäftsprozesse kann im Rahmen der Funktionen für die **Business Impact Analyse** dokumentiert werden. Hierzu sind wesentliche Parameter für das Notfallmanagement, wie die maximale Wiederanlaufzeit, die maximal tolerierbare Ausfallzeit und die maximale Wiederherstellungszeit des Normalbetriebs zu definieren.

145 Die Bewertung der Kritikalität von Geschäftsprozessen differenziert in das Schutzziel der Verfügbarkeit und dem untergeordneten Schutzziel der Datenverfügbarkeit in Abhängigkeit der festgelegten Ausfallkategorien, die wiederum in zeitliche Intervalle nach Stunden vergeben werden. Für jedes Notfallszenario sind anhand einer Skala die Auswirkungen auf die Verfügbarkeit bzw. Datenverfügbarkeit innerhalb der Ausfallkategorien zu bestimmen („Ampel-Logik“).

Jedes Szenario erhält dabei eine numerische Gewichtung, wobei sich aus der Summe über alle Szenarien ein Scoring-Wert ergibt, der dem determinierten Schwellenwert für nennenswerte Schäden, Datenverluste und dem maximal tolerierbaren Schaden für den Geschäftsprozess gegenübergestellt wird. Diese Schwellenwerte sind hierbei systemisch mit einer Ausfallkategorie verknüpft, für welche ein Ausfallzeitraum – in Tagen bzw. Stunden - hinterlegt wurde.

146 Die Ergebnisse der Business Impact Analyse werden zusammengefasst für die oben genannten Parameter zur Beurteilung der Verfügbarkeit bzw. Datenverfügbarkeit in bit-MaRisk dargestellt, verbale Begründungen und kritische Termine können ergänzt werden. Wie in den anderen Modulen von bit-MaRisk, kann zur laufenden Überprüfung der Business Impact Analyse ein Intervall zur Aktualisierung im Rahmen eines Workflows eingerichtet werden.

147 Um auftretende Auswirkungen aus der Business Impact Analyse auf die Notfalldokumentation umgehend zu dokumentieren, besteht die Möglichkeit, aus der Analyse eine Aktualisierung der Notfallszenarien anzustoßen. Zur visuellen Unterstützung der Business Impact Analyse kann jederzeit der Informationsverbund innerhalb der Bearbeitung der Analyse aufgerufen werden.

Prüfung und Ergebnis

148 Die Prüfung der programminternen Verarbeitungsregeln basierte auf Testfällen. Die Testfälle wurden mit selbst erstellten Testdaten und Demo-Daten der bit Informatik durchgeführt. Die durchgeführten Tests fanden auf der von der bit Informatik bereitgestellten Testumgebung statt. Die Tests umfassten die Erstellung, Bearbeitung und Verwaltung von Dokumenten des Notfallmanagements, den Nachvollzug der Prüfungs- und Freigabeworkflows und die in diesem Zusammenhang stehenden Benachrichtigungsfunktionen.

149 Bei unseren stichprobenweisen Prüfungen ergaben sich keine Beanstandungen. Die beschriebenen Verarbeitungsregeln sind geeignet, eine ordnungsgemäßes Notfallmanagement zu unterstützen.

2.3.7 bit-MaRisk - Organisationshandbuch

Anforderungen

150 Die Anforderungen des Moduls „Organisationshandbuch“ von bit-MaRisk lassen sich grundsätzlich aus den allgemeinen organisatorischen Pflichten gemäß § 25a KWG ableiten. Hierbei hat ein Institut interne Kontrollverfahren mit einem internen Kontrollsystem, wobei das interne Kontrollsystem insbesondere aufbau- und ablauforganisatorische Regelungen mit klarer Abgrenzung der Verantwortungsbereiche beinhalten soll, einzurichten. Zudem ist eine vollständige Dokumentation der Geschäftstätigkeit sicherzustellen.

151 Die MaRisk konkretisieren die Anforderungen an ein Internes Kontrollsystem in AT 4.3. In Abhängigkeit von Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten sind durch ein Institut Regelungen zur Aufbau- und Ablauforganisation zu treffen. Miteinander unvereinbare Tätigkeiten sind jeweils durch unterschiedliche Mitarbeiter durchzuführen und Interessenkonflikte sowie Selbstprüfungen zu vermeiden.

Prozesse sowie die damit verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege sind gemäß den MaRisk klar zu definieren und aufeinander abzustimmen, Berechtigungen und Kompetenzen nach dem Sparsamkeitsgrundsatz zu vergeben.

152 In AT 5 und AT 6 der MaRisk werden die zentralen Anforderungen an Organisationsrichtlinien und die allgemeine Dokumentation der Institute gestellt. Demnach sind die Richtlinien schriftlich zu fixieren und den betroffenen Mitarbeitern in der jeweils aktuellen Fassung zur Verfügung zu stellen und bei Veränderungen der Aktivitäten und Prozesse zeitnah anzupassen. Die allgemeinen Geschäfts-, Kontroll- und Überwachungsunterlagen sind des Weiteren systematisch und für sachkundige Dritte nachvollziehbar zu erstellen und aufzubewahren, dabei ist die Aktualität und Vollständigkeit der Dokumentation zu gewährleisten.

Umsetzung

153 Das Modul „Organisationshandbuch“ ermöglicht eine strukturierte, hierarchische Ablage von **Dokumenten** mit Weisungscharakter. Die entsprechenden Dokumente sind hierfür mit einer Nummerierung, Bezeichnung und Verantwortlichkeiten sowie Gültigkeits- und Ablaufdaten zu versehen. Innerhalb der Dokumente sind allgemeine Informationen zur hierarchischen Gliederung und deren Inhalte festzulegen. Verknüpfungen zu anderen Dokumenten können für den Verweis auf weitere verwandte Quellen verwendet werden.

154 Neben der Vergabe von Veröffentlichungs-/Gültigkeitsdaten und Ablauffristen/-daten können wahlweise Benachrichtigungen über die Veröffentlichung von Dokumenten bzw. Lesebestätigungen angefordert oder Einschränkungen bei den Leseberechtigungen sowie der Erstellung von untergeordneten Dokumenten vergeben werden. Zu den übergeordneten Dokumenten lassen sich die spezifischen untergeordneten Dokumente anzeigen, eine grafische Dokumentenstruktur unterstützt ebenfalls bei der Visualisierung der organisatorischen Strukturen. Eine Historisierung der Dokumente verdeutlicht zudem die Veränderungen zwischen den verschiedenen Versionen des betreffenden Dokuments.

155 Als weitere Kategorie neben den Dokumenten können **Vorstandsbeschlüsse** im Modul „Organisationshandbuch“ verwaltet werden. Die Konfiguration der Vorstandsbeschlüsse unterscheidet sich nicht bedeutend von den Informationen, die bei den Dokumenten zu pflegen sind. Im Wesentlichen können zusätzlich das Entscheidungsdatum und der betroffene Fachbereich durch den Beschluss nebst Verteilerkreis sowie die Genehmigenden mit deren Unterschriften als „Zeitstempel" hinterlegt werden. Wie auch bei den Dokumenten, besteht eine Funktion zur Anzeige der Historie der Beschlüsse.

Prüfung und Ergebnis

156 Die Prüfung der programminternen Verarbeitungsregeln basierte auf Testfällen. Die Testfälle wurden mit selbst erstellten Testdaten und Demo-Daten der bit Informatik durchgeführt. Die durchgeführten Tests fanden auf der von der bit Informatik bereitgestellten Testumgebung statt. Die Tests umfassten die Erstellung, Bearbeitung und Verwaltung von Dokumenten des Organisationshandbuchs und der Vorstandsbeschlüsse, den Nachvollzug der Prüfungs- und Freigabeworkflows und die in diesem Zusammenhang stehenden Benachrichtigungsfunktionen.

157 Bei unseren stichprobenweisen Prüfungen ergaben sich keine Beanstandungen. Die beschriebenen Verarbeitungsregeln sind geeignet, ein ordnungsgemäßes Organisationshandbuch zu unterstützen.

2.3.8 bit-MaRisk - IT-Betrieb

Anforderungen

158 Die Anforderungen für das Modul „IT-Betrieb“ von bit-MaRisk lassen sich grundsätzlich aus den allgemeinen organisatorischen Pflichten gemäß § 25a KWG ableiten. Hierbei hat ein Institut interne Kontrollverfahren mit einem internen Kontrollsystem, wobei das interne Kontrollsystem insbesondere aufbau- und ablauforganisatorische Regelungen mit klarer Abgrenzung der Verantwortungsbereiche beinhalten soll, einzurichten.

159 Die MaRisk konkretisieren die Anforderungen an ein Internes Kontrollsystem in AT 4.3. In Abhängigkeit von Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten sind durch ein Institut Regelungen zur Aufbau- und Ablauforganisation zu treffen. Miteinander unvereinbare Tätigkeiten sind jeweils durch unterschiedliche Mitarbeiter durchzuführen und Interessenkonflikte sowie Selbstprüfungen zu vermeiden.

Prozesse sowie die damit verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege sind gemäß den MaRisk klar zu definieren und aufeinander abzustimmen.

160 Die Vorgaben von AT 7.2 MaRisk stellen weitere Anforderungen an den Einsatz von IT-Systemen und deren Tests sowie fachlichen Abnahmen durch die zuständigen Mitarbeitenden beim erstmaligen Einsatz und nach wesentlichen Änderungen. Für diese Tätigkeiten ist durch die Institute ein Regelprozess zu implementieren. Des Weiteren sollen die IT-Risiken einer angemessenen Überwachung und Steuerung unterliegen.

161 Die wesentlichen Anforderungen an den IT-Betrieb ergeben sich aus Kapitel 8 der BAIT, die eine Verwaltung der Komponenten von IT-Systemen unter Berücksichtigung der Beziehungen dieser Komponenten miteinander und eine regelmäßige bzw. anlassbezogene Aktualisierung der Bestandsangaben vorsehen.

Hierunter fällt auch ein entsprechendes Lebenszyklus-Management des Portfolios aus den IT-Systemen zur frühzeitigen Erkennung von veralteten oder nicht mehr unterstützten IT-Systemen in Form einer geordneten und strukturierten Aufnahme und Dokumentation von Änderungen unter Beachtung von zeitkritischen Änderungen.

162 Meldungen über Störungen des IT-Betriebs und deren Ursachen sind zu erfassen, zu bewerten und zu priorisieren sowie im entsprechenden Fall anhand eines Kriterienkatalogs einem Eskalationsprozess zuzuführen. Diese Vorgehensweise soll getroffene Maßnahmen, Kommunikationswege und definierte Zuständigkeiten beinhalten. Die Bearbeitung, Ursachenanalyse, Lösungsfindung und Nachverfolgung ist zu dokumentieren. Zusammenhänge zwischen Störungen und deren Ursachen sind zu beachten. Der Bearbeitungsstand von offenen Meldungen über Störungen ist nachvollziehbar zu überwachen und zu steuern. Anhand von geeigneten Kriterien ist die Information der beteiligten Personen im Institut über die vorherrschenden Störungen sicherzustellen.

Umsetzung

163 Die Modul „IT-Betrieb“ stellt ein **Ticketsystem** zur Annahme und Bearbeitung von internen oder externen Anfragen dar. Die Anfragen können hierbei mit einer Ticketnummer, Kurzbezeichnung, einem Erstellungszeitpunkt und der von der Anfrage betroffenen Personengruppe sowie dem derzeitigen Bearbeitungsstatus versehen werden. Sollte ein Zusammenhang zwischen mehreren Tickets bestehen, können diese in ein Ticket zusammengeführt werden.

164 Innerhalb des Tickets sind Informationen zum internen Support mit ergänzenden Prioritäten, Status und Kategorien sowie einer Problembeschreibung hinterlegt. Des Weiteren kann bei der Anzeige eines Tickets dieses als globales Ticket, welches für sämtliche Personen sichtbar ist, definiert werden. Mit dem Ticket kann wiederum eine betroffene Ressource verknüpft werden. Die Einbindung des externen Supports, bspw. des Herstellers einer Ressource, kann ebenfalls im Ticket vermerkt werden.

165 Nach erfolgreicher Behebung einer Störung kann der Lösungsweg und der Zeitpunkt des Endes der Störung im Ticket dokumentiert werden. Zur Dokumentation der Bearbeitung von Anfragen können sämtliche Kommunikationen mit Eingangszeitpunkt bzw. dem Beginn und dem Betreff sowie dem entsprechenden Benutzer/Ansprechpartner am Ticket festgehalten werden.

166 Eine Historie zur Bearbeitung des Tickets ermöglicht den Nachvollzug der Änderungen, und die Erstellung einer zusammenfassenden Dokumentation gibt einen Überblick über den Verlauf der Bearbeitung der Anfrage.

167 Zur Erläuterung von wiederkehrend auftretenden Störungen besteht die Möglichkeit, in diesem Modul zentrale **Dokumentationen** in Form von Anleitungen zu hinterlegen. Diesen Dokumentationen sind Kategorien und Verantwortlichkeiten zuzuordnen und Leseberechtigungen zu vergeben. Die Verknüpfung zu den betroffenen Ressourcen erläutert den Anwendungsbereich der Dokumentationen. Wie bei den Tickets, stellt eine Historisierung der Dokumentationen den Nachvollzug von Änderungen sicher.

168 Das Modul bietet die Möglichkeit der Verwaltung von vorhandenen technischen Systemen über eine Inventarisierung dieser Systeme anhand von Inventarnummern. Das Inventar enthält Informationen zum Typ, der Seriennummer und dem Standort des Systems. Für inventarisierte Systeme können individuelle Aufgaben bzw. ein Überprüfungsintervall vergeben oder auch Massenänderungen vorgenommen werden.

169 Für jedes verwaltete **System** können die spezifischen Angaben zu Verantwortlichkeiten, Hersteller- und Lieferantenangaben, Supportanbietern, dem Status sowie die Kategorie gepflegt werden. Zur betriebswirtschaftlichen Betrachtung können die Erwerbsart (Kauf, Miete, Leasing) und die Kosten (netto/brutto) sowie Daten zur Bestellung (Datum, Nummer), Rechnung (Datum, Nummer) und Lieferung (Datum, Nummer) erfasst werden. Bestehende Garantien, Wartungsverträge und Nutzungsdauern mit Restbuchwerten können ebenfalls am System hinterlegt werden. In Abhängigkeit der Kategorie des Systems sind im technischen Datenblatt Angaben zu den Netzwerk- (bspw. Host, Domäne, IP-/MAC-Adressen) und Softwaredaten (Firmware) zu tätigen. Zur differenzierten Betrachtung des Systems können diesem noch weitere Komponenten zugeordnet werden. Ebenso können Verknüpfungen zu existierenden Dokumentationen, Verträgen und der Objektbezeichnung im Rahmen der Strukturanalyse für das betrachtete Systeme erstellt werden. Die grafische Darstellung des Informationsverbundes verdeutlicht dabei die hierarchische Struktur des Systems. Die Inbetrieb- oder Entgegennahme des Systems kann durch ein schriftliches Übergabeprotokoll erläutert werden.

170 Die Administration von **Komponenten** verhält sich analog zur Verwaltung der Systeme. Neben den allgemeinen und betriebswirtschaftlichen Angaben sich auch hier technische Informationen sowie Verknüpfungen zur Abbildung des Informationsverbunds – insbesondere die Zuordnung zu einem System - zu pflegen.

171 Die **Prüfungsliste** gibt einen Überblick über die zu erledigenden turnusmäßigen oder anlassbezogenen Überprüfungen bzw. Wartungen von Systemen.

172 Wie im Modul zur Vertragsverwaltung und Dienstleistersteuerung, wird eine Liste der **Unternehmen** und **Ansprechpartner**, mit denen Verträge zur Lieferung oder Support der inventarisierten Systeme besteht, im Modul „IT-Betrieb“ angezeigt. Die Ansichten der Unternehmensdaten und Ansprechpartner entsprechen den oben beschriebenen Informationen zum Modul „Vertragsverwaltung und Dienstleistersteuerung“ und sollen an dieser Stelle nicht erneut beschrieben werden. Insofern wird auf die Ausführungen in Abschnitt 2.3.3 verwiesen.

Prüfung und Ergebnis

173 Die Prüfung der programminternen Verarbeitungsregeln basierte auf Testfällen. Die Testfälle wurden mit selbst erstellten Testdaten und Demo-Daten der bit Informatik durchgeführt. Die durchgeführten Tests fanden auf der von der bit Informatik bereitgestellten Testumgebung statt. Die Tests umfassten die Erstellung, Bearbeitung und Verwaltung von Dokumenten zum IT-Betrieb, den Nachvollzug der Prüfungs- und Freigabeworkflows und die in diesem Zusammenhang stehenden Benachrichtigungsfunktionen.

174 Bei unseren stichprobenweisen Prüfungen ergaben sich keine Beanstandungen. Die beschriebenen Verarbeitungsregeln sind geeignet, eine ordnungsgemäßen IT-Betrieb zu unterstützen.

2.3.9 bit-MaRisk - Projektmanagement

Anforderungen

175 Die Anforderungen an das Projektmanagement lassen sich für die betroffenen Institute grundsätzlich aus den allgemeinen organisatorischen Pflichten gemäß § 25a KWG ableiten. Hierbei hat ein Institut interne Kontrollverfahren mit einem internen Kontrollsystem, wobei das interne Kontrollsystem insbesondere aufbau- und ablauforganisatorische Regelungen mit klarer Abgrenzung der Verantwortungsbereiche beinhalten soll, einzurichten. Zudem ist eine vollständige Dokumentation der Geschäftstätigkeit sicherzustellen.

176 Die MaRisk konkretisieren die Anforderungen an ein Internes Kontrollsystem in AT 4.3. In Abhängigkeit von Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten sind durch ein Institut Regelungen zur Aufbau- und Ablauforganisation zu treffen. Miteinander unvereinbare Tätigkeiten sind jeweils durch unterschiedliche Mitarbeiter durchzuführen und Interessenkonflikte sowie Selbstprüfungen zu vermeiden.

Prozesse sowie die damit verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege sind gemäß den MaRisk klar zu definieren und aufeinander abzustimmen, Berechtigungen und Kompetenzen nach dem Sparsamkeitsgrundsatz zu vergeben.

177 In AT 8 der MaRisk werden weitere Anforderungen an die Dokumentation von Anpassungsprozessen genannt, die für die das Modul „Projektmanagement“ von bit-MaRisk herangezogen werden können. Insbesondere AT 8.1 MaRisk stellt umfassende Anforderungen an die Dokumentation des Neu-Produkt-Prozesses, der Erstellung von Konzepten sowie der Beschreibung von Geschäftsaktivitäten oder den Ergebnissen von Testphasen.

178 Wesentliche Veränderungen von betrieblichen Prozessen oder Strukturen sind nach AT 8.2 MaRisk einer gesonderten Analyse der Auswirkungen auf die Kontrollverfahren und die Kontrollintensität zu unterziehen.

179 Speziell für IT-Projekte und die Anwendungsentwicklung geben die BAIT in Kapitel 7 zusätzliche Vorgaben in Bezug auf die Veränderungen von IT-Systemen, die ebenfalls eine Auswirkungsanalyse der wesentlichen Veränderungen auf die IT-Aufbau- und Ablauforganisation fordern. Insbesondere die Steuerung von Projektrisiken – auch deren Abhängigkeiten im Projektportfolio -, die Umsetzung von Qualitätssicherungsmaßnahmen und die Implikationen für den Informationsverbund werden durch die BAIT hervorgehoben. Des Weiteren soll eine Aufarbeitung der gewonnenen Erkenntnisse (im Sinne von „Lessons Learned“) durch die Institute erfolgen.

Umsetzung

180 Das Modul "Projektmanagement" unterscheidet grundsätzlich in Projekte und Aktivitäten. Für ein Projekt können individuelle Verantwortlichkeiten und hierarchische Zuordnungen von Projekten in über- oder untergeordnete Projektteile vergeben werden. Des Weiteren können zur zeitlichen Steuerung diverse Zeitpunkte- oder räume (früheste und späteste Start- und Endtermine) vergeben werden.

181 Die Überwachung der Projektstände erfolgt über die grafische Anzeige von verschiedenen Projektstatus (in Arbeit, geplant, abgeschlossen, abgebrochen). Zusätzlich ist es auch möglich, ein Gantt-Diagramm zur Visualisierung des zeitlichen Verlaufs eines Projekts zu erstellen. Eine Historie des Verlaufs sichert den Nachvollzug von Änderungen innerhalb des Projekts.

182 Als wesentliche Projektparameter sind die Kategorie und die Priorität eines Projektes neben einer allgemeinen Beschreibung und den geschätzten Kosten zu pflegen. Im Rahmen der vereinfachten oder erweiterten Zeitplanung (Angabe von Zeitpunkten oder Zeiträumen in Soll-/Ist-Dauern in Tagen) besteht zudem die Möglichkeit, freie Pufferzeiten bzw. einen Gesamtpuffer in Tagen berechnen zu lassen.

183 Wesentlicher Bestandteil des Moduls „Projektmanagement“ ist die Verknüpfung der geplanten Tätigkeiten in einem Projekt mit den bspw. hiervon betroffenen Geschäftsprozessen, Anwen-

dungen oder Organisationseinheiten (Informationsverbund). Hierbei wird zwischen benötigten Ressourcen und betroffenen Ressourcen unterschieden.

184 Innerhalb von Projekten können wiederum einzelne Aktivitäten geplant werden, die ebenso die gleichen zeitlichen oder kostenseitigen Parameter zur Steuerung der Aktivitäten beinhalten und in eine chronologische Abfolge gegliedert sind.

185 Die Aggregation von zeitlichen und kostenseitigen Auswirkungen aus untergeordneten Projekten auf Ebene der übergeordneten Projekten zeigt frühzeitig den Verbrauch von zeitlichen oder monetären Ressourcen des Gesamtprojektes an. Abhängigkeiten zwischen sequenziell verlaufenden Projekten werden über die Parametrisierung von Projekten als vor- und nachgelagerte Projekte zum betrachteten Hauptprojekt dargestellt.

Prüfung und Ergebnis

186 Die Prüfung der programminternen Verarbeitungsregeln basierte auf Testfällen. Die Testfälle wurden mit selbst erstellten Testdaten und Demo-Daten der bit Informatik durchgeführt. Die durchgeführten Tests fanden auf der von der bit Informatik bereitgestellten Testumgebung statt. Die Tests umfassten die Bearbeitung von Projekten und Aktivitäten, den Nachvollzug der Workflows für die laufende Projektüberwachung und die in diesem Zusammenhang stehenden Benachrichtigungsfunktionen.

187 Bei unseren stichprobenweisen Prüfungen ergaben sich keine Beanstandungen. Die beschriebenen Verarbeitungsregeln sind geeignet, ein ordnungsgemäßes Projektmanagement zu unterstützen.

3. Zusammenfassung des Prüfungsergebnisses

188 Im Ergebnis unserer Prüfung der Software bit MaRisk, Version 23.3 ergaben sich keine Beanstandungen.

Wir fassen das Ergebnis unserer Prüfung wie folgt zusammen:

Die Software bit-MaRisk, Version 23.3 ermöglicht bei sachgerechter Anwendung eine wirkungsvolle Unterstützung einer ordnungsgemäßen Geschäftsorganisation und entspricht den für die Prüfung relevanten Ordnungsmäßigkeitskriterien.

4. Bescheinigung

189 Basierend auf unseren Prüfungsfeststellungen, den vorgelegten Unterlagen, den erhaltenen Auskünften sowie der Einsichtnahme in Systeme erteilen wir folgende Bescheinigung:

„An die bit Informatik GmbH, Trier:

Die bit Informatik GmbH hat uns beauftragt, eine Softwareprüfung nach IDW PS 880 für die Software bit-MaRisk, Version 23.3 durchzuführen.

Gegenstand der Prüfung waren die Verarbeitungsfunktionen zur Erfüllung der Ordnungsmäßigkeitskriterien, die Verarbeitungsregeln im Sinne einer wirkungsvollen Workflowunterstützung sowie deren Dokumentation und die Softwareentwicklungsumgebung.

Die gesetzlichen Vertreter der bit Informatik GmbH sind für die Software und die Planung, Durchführung und Überwachung der Softwareentwicklung verantwortlich. Diese Verantwortung wird durch unsere Prüfung nicht berührt oder eingeschränkt. Unsere Aufgabe ist es, auf Grundlage der von uns durchgeführten Prüfung eine Beurteilung über die Software abzugeben.

Wir haben unsere Prüfung unter Beachtung des IDW Prüfungsstandards: Die Prüfung von Softwareprodukten (IDW PS 880) durchgeführt. Die Prüfung wurde so geplant und durchgeführt, dass aufgrund der bei der Prüfung gewonnenen Erkenntnisse mit hinreichender Sicherheit beurteilt werden kann, ob die Software bit-MaRisk, Version 23.3 bei sachgerechter Anwendung eine wirkungsvolle Unterstützung einer ordnungsgemäßen Geschäftsorganisation ermöglicht und den im Prüfungsauftrag vereinbarten Kriterien, die die fachlichen Anforderungen an eine Software darstellen, entspricht.

Grundlage der Prüfung sind die Ordnungsmäßigkeitskriterien Vollständigkeit, Richtigkeit, Zeitgerechtheit, Nachvollziehbarkeit und Unveränderlichkeit, deren Einhaltung unter Voraussetzung der Sicherheit, insbesondere der Integrität der verarbeiteten Daten, beurteilt wurden.

Das Kriterium der Unveränderlichkeit sowie die Sicherheitsanforderungen sind durch weiterführende Maßnahmen der Kunden der bit Informatik GmbH zu gewährleisten. Insbesondere sind durch die Kunden geeignete Berechtigungen für das Programm zu vergeben. Dieses Kriterium bzw. die Sicherheitsanforderungen waren daher nicht Gegenstand der Prüfung.

Für den genannten Auftragsumfang und die Auftragsdurchführung haben wir zudem Kriterien auf Basis der folgenden gesetzlichen und regulatorischen Anforderungen zugrunde gelegt, die Maßstab zur Beurteilung der Ordnungsmäßigkeit der Software waren:

- Anforderungen an das Risikomanagement nach § 25a KWG
- Mindestanforderungen an das Risikomanagement (MaRisk), Rundschreiben 05/2023 (BA) der BaFin vom 18. Oktober 2023
- Bankaufsichtliche Anforderungen an die IT (BAIT), Rundschreiben 10/2017 (BA) der BaFin in der Fassung vom 16. August 2021
- Grundsätze ordnungsmäßiger Buchführung gemäß §§ 238 und 239 HGB bzw. die hieraus abgeleiteten regulatorischen Vorschriften zur Rechnungslegung und dem Internen Kontrollsystem.

Es wurden seitens der bit Informatik GmbH keine zusätzlichen Kriterien i.S.d. IDW PS 880 zur Beurteilung der Software herangezogen. Unsere Prüfung basiert somit ausschließlich auf den oben beschriebenen gesetzlichen und regulatorischen Anforderungen.

Unsere Prüfung umfasst die Beurteilung, ob die Kriterien durch die Verarbeitungsfunktionen und durch das programminterne Kontrollsystem angemessen umgesetzt sind und ob eine aussagefähige Verfahrensdokumentation vorliegt. Die Wirksamkeit bzw. Funktionsfähigkeit der Programmfunktionen wurde anhand von Testfällen beurteilt.

Aufgrund der Anpassungen von Softwareprodukten an die Anforderungen des Einsatzgebietes, kann sich unser Urteil ausschließlich darauf beziehen, dass das Softwareprodukt bei sachgerechter Anwendung ermöglicht, den Kriterien zu entsprechen.

Wir sind der Auffassung, dass unsere Prüfung eine hinreichend sichere Grundlage für unsere Beurteilung bildet.

Nach unserer Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse ermöglicht das von uns geprüfte Softwareprodukt bit MaRisk, Version 23.3 bei sachgerechter Anwendung eine wirkungsvolle Unterstützung einer ordnungsgemäßen Geschäftsorganisation und entspricht den im Prüfungsauftrag vereinbarten Kriterien, die die fachlichen Anforderungen an eine Software darstellen.

Wir erteilen diese Bescheinigung auf Grundlage des mit der bit Informatik GmbH geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten die beiliegenden Allgemeine Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 1. Januar 2017 zugrunde liegen.

Eine Verwendung unserer Bescheinigung ist nur im Zusammenhang mit der vollständigen Wiedergabe der Zusammenfassung unseres Prüfungsergebnisses zulässig.“

Flensburg, den 28. März 2024

SIGNOS
Singhofen & Gergen Partnerschaftsgesellschaft
Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft

Dr. Sebastian Brauer
Wirtschaftsprüfer
Steuerberater
CISA

Tim Meyer
Wirtschaftsprüfer
Steuerberater

Allgemeine Auftragsbedingungen
für
Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften
vom 1. Januar 2017

DokID:

1. Geltungsbereich

(1) Die Auftragsbedingungen gelten für Verträge zwischen Wirtschaftsprüfern oder Wirtschaftsprüfungsgesellschaften (im Nachstehenden zusammenfassend „Wirtschaftsprüfer“ genannt) und ihren Auftraggebern über Prüfungen, Steuerberatung, Beratungen in wirtschaftlichen Angelegenheiten und sonstige Aufträge, soweit nicht etwas anderes ausdrücklich schriftlich vereinbart oder gesetzlich zwingend vorgeschrieben ist.

(2) Dritte können nur dann Ansprüche aus dem Vertrag zwischen Wirtschaftsprüfer und Auftraggeber herleiten, wenn dies ausdrücklich vereinbart ist oder sich aus zwingenden gesetzlichen Regelungen ergibt. Im Hinblick auf solche Ansprüche gelten diese Auftragsbedingungen auch diesen Dritten gegenüber.

2. Umfang und Ausführung des Auftrags

(1) Gegenstand des Auftrags ist die vereinbarte Leistung, nicht ein bestimmter wirtschaftlicher Erfolg. Der Auftrag wird nach den Grundsätzen ordnungsmäßiger Berufsausübung ausgeführt. Der Wirtschaftsprüfer übernimmt im Zusammenhang mit seinen Leistungen keine Aufgaben der Geschäftsführung. Der Wirtschaftsprüfer ist für die Nutzung oder Umsetzung der Ergebnisse seiner Leistungen nicht verantwortlich. Der Wirtschaftsprüfer ist berechtigt, sich zur Durchführung des Auftrags sachverständiger Personen zu bedienen.

(2) Die Berücksichtigung ausländischen Rechts bedarf – außer bei betriebswirtschaftlichen Prüfungen – der ausdrücklichen schriftlichen Vereinbarung.

(3) Ändert sich die Sach- oder Rechtslage nach Abgabe der abschließenden beruflichen Äußerung, so ist der Wirtschaftsprüfer nicht verpflichtet, den Auftraggeber auf Änderungen oder sich daraus ergebende Folgerungen hinzuweisen.

3. Mitwirkungspflichten des Auftraggebers

(1) Der Auftraggeber hat dafür zu sorgen, dass dem Wirtschaftsprüfer alle für die Ausführung des Auftrags notwendigen Unterlagen und weiteren Informationen rechtzeitig übermittelt werden und ihm von allen Vorgängen und Umständen Kenntnis gegeben wird, die für die Ausführung des Auftrags von Bedeutung sein können. Dies gilt auch für die Unterlagen und weiteren Informationen, Vorgänge und Umstände, die erst während der Tätigkeit des Wirtschaftsprüfers bekannt werden. Der Auftraggeber wird dem Wirtschaftsprüfer geeignete Auskunftspersonen benennen.

(2) Auf Verlangen des Wirtschaftsprüfers hat der Auftraggeber die Vollständigkeit der vorgelegten Unterlagen und der weiteren Informationen sowie der gegebenen Auskünfte und Erklärungen in einer vom Wirtschaftsprüfer formulierten schriftlichen Erklärung zu bestätigen.

4. Sicherung der Unabhängigkeit

(1) Der Auftraggeber hat alles zu unterlassen, was die Unabhängigkeit der Mitarbeiter des Wirtschaftsprüfers gefährdet. Dies gilt für die Dauer des Auftragsverhältnisses insbesondere für Angebote auf Anstellung oder Übernahme von Organfunktionen und für Angebote, Aufträge auf eigene Rechnung zu übernehmen.

(2) Sollte die Durchführung des Auftrags die Unabhängigkeit des Wirtschaftsprüfers, die der mit ihm verbundenen Unternehmen, seiner Netzwerkunternehmen oder solcher mit ihm assoziierten Unternehmen, auf die die Unabhängigkeitsvorschriften in gleicher Weise Anwendung finden wie auf den Wirtschaftsprüfer, in anderen Auftragsverhältnissen beeinträchtigen, ist der Wirtschaftsprüfer zur außerordentlichen Kündigung des Auftrags berechtigt.

5. Berichterstattung und mündliche Auskünfte

Soweit der Wirtschaftsprüfer Ergebnisse im Rahmen der Bearbeitung des Auftrags schriftlich darzustellen hat, ist alleine diese schriftliche Darstellung maßgebend. Entwürfe schriftlicher Darstellungen sind unverbindlich. Sofern nicht anders vereinbart, sind mündliche Erklärungen und Auskünfte des Wirtschaftsprüfers nur dann verbindlich, wenn sie schriftlich bestätigt werden. Erklärungen und Auskünfte des Wirtschaftsprüfers außerhalb des erteilten Auftrags sind stets unverbindlich.

6. Weitergabe einer beruflichen Äußerung des Wirtschaftsprüfers

(1) Die Weitergabe beruflicher Äußerungen des Wirtschaftsprüfers (Arbeitsergebnisse oder Auszüge von Arbeitsergebnissen – sei es im Entwurf oder in der Endfassung) oder die Information über das Tätigwerden des Wirtschaftsprüfers für den Auftraggeber an einen Dritten bedarf der schriftlichen Zustimmung des Wirtschaftsprüfers, es sei denn, der Auftraggeber ist zur Weitergabe oder Information aufgrund eines Gesetzes oder einer behördlichen Anordnung verpflichtet.

(2) Die Verwendung beruflicher Äußerungen des Wirtschaftsprüfers und die Information über das Tätigwerden des Wirtschaftsprüfers für den Auftraggeber zu Werbezwecken durch den Auftraggeber sind unzulässig.

7. Mängelbeseitigung

(1) Bei etwaigen Mängeln hat der Auftraggeber Anspruch auf Nacherfüllung durch den Wirtschaftsprüfer. Nur bei Fehlschlagen, Unterlassen bzw. unberechtigter Verweigerung, Unzumutbarkeit oder Unmöglichkeit der Nacherfüllung kann er die Vergütung mindern oder vom Vertrag zurücktreten; ist der Auftrag nicht von einem Verbraucher erteilt worden, so kann der Auftraggeber wegen eines Mangels nur dann vom Vertrag zurücktreten, wenn die erbrachte Leistung wegen Fehlschlagens, Unterlassung, Unzumutbarkeit oder Unmöglichkeit der Nacherfüllung für ihn ohne Interesse ist. Soweit darüber hinaus Schadensersatzansprüche bestehen, gilt Nr. 9.

(2) Der Anspruch auf Beseitigung von Mängeln muss vom Auftraggeber unverzüglich in Textform geltend gemacht werden. Ansprüche nach Abs. 1, die nicht auf einer vorsätzlichen Handlung beruhen, verjähren nach Ablauf eines Jahres ab dem gesetzlichen Verjährungsbeginn.

(3) Offenbare Unrichtigkeiten, wie z.B. Schreibfehler, Rechenfehler und formelle Mängel, die in einer beruflichen Äußerung (Bericht, Gutachten und dgl.) des Wirtschaftsprüfers enthalten sind, können jederzeit vom Wirtschaftsprüfer auch Dritten gegenüber berichtigt werden. Unrichtigkeiten, die geeignet sind, in der beruflichen Äußerung des Wirtschaftsprüfers enthaltene Ergebnisse infrage zu stellen, berechtigen diesen, die Äußerung auch Dritten gegenüber zurückzunehmen. In den vorgenannten Fällen ist der Auftraggeber vom Wirtschaftsprüfer tunlichst vorher zu hören.

8. Schweigepflicht gegenüber Dritten, Datenschutz

(1) Der Wirtschaftsprüfer ist nach Maßgabe der Gesetze (§ 323 Abs. 1 HGB, § 43 WPO, § 203 StGB) verpflichtet, über Tatsachen und Umstände, die ihm bei seiner Berufstätigkeit anvertraut oder bekannt werden, Stillschweigen zu bewahren, es sei denn, dass der Auftraggeber ihn von dieser Schweigepflicht entbindet.

(2) Der Wirtschaftsprüfer wird bei der Verarbeitung von personenbezogenen Daten die nationalen und europarechtlichen Regelungen zum Datenschutz beachten.

9. Haftung

(1) Für gesetzlich vorgeschriebene Leistungen des Wirtschaftsprüfers, insbesondere Prüfungen, gelten die jeweils anzuwendenden gesetzlichen Haftungsbeschränkungen, insbesondere die Haftungsbeschränkung des § 323 Abs. 2 HGB.

(2) Sofern weder eine gesetzliche Haftungsbeschränkung Anwendung findet noch eine einzelvertragliche Haftungsbeschränkung besteht, ist die Haftung des Wirtschaftsprüfers für Schadensersatzansprüche jeder Art, mit Ausnahme von Schäden aus der Verletzung von Leben, Körper und Gesundheit, sowie von Schäden, die eine Ersatzpflicht des Herstellers nach § 1 ProdHaftG begründen, bei einem fahrlässig verursachten einzelnen Schadensfall gemäß § 54a Abs. 1 Nr. 2 WPO auf 4 Mio. € beschränkt.

(3) Einreden und Einwendungen aus dem Vertragsverhältnis mit dem Auftraggeber stehen dem Wirtschaftsprüfer auch gegenüber Dritten zu.

(4) Leiten mehrere Anspruchsteller aus dem mit dem Wirtschaftsprüfer bestehenden Vertragsverhältnis Ansprüche aus einer fahrlässigen Pflichtverletzung des Wirtschaftsprüfers her, gilt der in Abs. 2 genannte Höchstbetrag für die betreffenden Ansprüche aller Anspruchsteller insgesamt.

(5) Ein einzelner Schadensfall im Sinne von Abs. 2 ist auch bezüglich eines aus mehreren Pflichtverletzungen stammenden einheitlichen Schadens gegeben. Der einzelne Schadensfall umfasst sämtliche Folgen einer Pflichtverletzung ohne Rücksicht darauf, ob Schäden in einem oder in mehreren aufeinanderfolgenden Jahren entstanden sind. Dabei gilt mehrfaches auf gleicher oder gleichartiger Fehlerquelle beruhendes Tun oder Unterlassen als einheitliche Pflichtverletzung, wenn die betreffenden Angelegenheiten miteinander in rechtlichem oder wirtschaftlichem Zusammenhang stehen. In diesem Fall kann der Wirtschaftsprüfer nur bis zur Höhe von 5 Mio. € in Anspruch genommen werden. Die Begrenzung auf das Fünffache der Mindestversicherungssumme gilt nicht bei gesetzlich vorgeschriebenen Pflichtprüfungen.

(6) Ein Schadensersatzanspruch erlischt, wenn nicht innerhalb von sechs Monaten nach der schriftlichen Ablehnung der Ersatzleistung Klage erhoben wird und der Auftraggeber auf diese Folge hingewiesen wurde. Dies gilt nicht für Schadensersatzansprüche, die auf vorsätzliches Verhalten zurückzuführen sind, sowie bei einer schuldhaften Verletzung von Leben, Körper oder Gesundheit sowie bei Schäden, die eine Ersatzpflicht des Herstellers nach § 1 ProdHaftG begründen. Das Recht, die Einrede der Verjährung geltend zu machen, bleibt unberührt.

10. Ergänzende Bestimmungen für Prüfungsaufträge

(1) Ändert der Auftraggeber nachträglich den durch den Wirtschaftsprüfer geprüften und mit einem Bestätigungsvermerk versehenen Abschluss oder Lagebericht, darf er diesen Bestätigungsvermerk nicht weiterverwenden.

Hat der Wirtschaftsprüfer einen Bestätigungsvermerk nicht erteilt, so ist ein Hinweis auf die durch den Wirtschaftsprüfer durchgeführte Prüfung im Lagebericht oder an anderer für die Öffentlichkeit bestimmter Stelle nur mit schriftlicher Einwilligung des Wirtschaftsprüfers und mit dem von ihm genehmigten Wortlaut zulässig.

(2) Widerruft der Wirtschaftsprüfer den Bestätigungsvermerk, so darf der Bestätigungsvermerk nicht weiterverwendet werden. Hat der Auftraggeber den Bestätigungsvermerk bereits verwendet, so hat er auf Verlangen des Wirtschaftsprüfers den Widerruf bekanntzugeben.

(3) Der Auftraggeber hat Anspruch auf fünf Berichtsausfertigungen. Weitere Ausfertigungen werden besonders in Rechnung gestellt.

11. Ergänzende Bestimmungen für Hilfeleistung in Steuersachen

(1) Der Wirtschaftsprüfer ist berechtigt, sowohl bei der Beratung in steuerlichen Einzelfragen als auch im Falle der Dauerberatung die vom Auftraggeber genannten Tatsachen, insbesondere Zahlenangaben, als richtig und vollständig zugrunde zu legen; dies gilt auch für Buchführungsaufträge. Er hat jedoch den Auftraggeber auf von ihm festgestellte Unrichtigkeiten hinzuweisen.

(2) Der Steuerberatungsauftrag umfasst nicht die zur Wahrung von Fristen erforderlichen Handlungen, es sei denn, dass der Wirtschaftsprüfer hierzu ausdrücklich den Auftrag übernommen hat. In diesem Fall hat der Auftraggeber dem Wirtschaftsprüfer alle für die Wahrung von Fristen wesentlichen Unterlagen, insbesondere Steuerbescheide, so rechtzeitig vorzulegen, dass dem Wirtschaftsprüfer eine angemessene Bearbeitungszeit zur Verfügung steht.

(3) Mangels einer anderweitigen schriftlichen Vereinbarung umfasst die laufende Steuerberatung folgende, in die Vertragsdauer fallenden Tätigkeiten:

a) Ausarbeitung der Jahressteuererklärungen für die Einkommensteuer, Körperschaftsteuer und Gewerbesteuer sowie der Vermögensteuererklärungen, und zwar auf Grund der vom Auftraggeber vorzulegenden Jahresabschlüsse und sonstiger für die Besteuerung erforderlicher Aufstellungen und Nachweise

b) Nachprüfung von Steuerbescheiden zu den unter a) genannten Steuern

c) Verhandlungen mit den Finanzbehörden im Zusammenhang mit den unter a) und b) genannten Erklärungen und Bescheiden

d) Mitwirkung bei Betriebsprüfungen und Auswertung der Ergebnisse von Betriebsprüfungen hinsichtlich der unter a) genannten Steuern

e) Mitwirkung in Einspruchs- und Beschwerdeverfahren hinsichtlich der unter a) genannten Steuern.

Der Wirtschaftsprüfer berücksichtigt bei den vorgenannten Aufgaben die wesentliche veröffentlichte Rechtsprechung und Verwaltungsauffassung.

(4) Erhält der Wirtschaftsprüfer für die laufende Steuerberatung ein Pauschalhonorar, so sind mangels anderweitiger schriftlicher Vereinbarungen die unter Abs. 3 Buchst. d) und e) genannten Tätigkeiten gesondert zu honorieren.

(5) Sofern der Wirtschaftsprüfer auch Steuerberater ist und die Steuerberatervergütungsverordnung für die Bemessung der Vergütung anzuwenden ist, kann eine höhere oder niedrigere als die gesetzliche Vergütung in Textform vereinbart werden.

(6) Die Bearbeitung besonderer Einzelfragen der Einkommensteuer, Körperschaftsteuer, Gewerbesteuer, Einheitsbewertung und Vermögensteuer sowie aller Fragen der Umsatzsteuer, Lohnsteuer, sonstigen Steuern und Abgaben erfolgt auf Grund eines besonderen Auftrags. Dies gilt auch für

a) die Bearbeitung einmalig anfallender Steuerangelegenheiten, z.B. auf dem Gebiet der Erbschaftsteuer, Kapitalverkehrsteuer, Grunderwerbsteuer,

b) die Mitwirkung und Vertretung in Verfahren vor den Gerichten der Finanz- und der Verwaltungsgerichtsbarkeit sowie in Steuerstrafsachen,

c) die beratende und gutachtliche Tätigkeit im Zusammenhang mit Umwandlungen, Kapitalerhöhung und -herabsetzung, Sanierung, Eintritt und Ausscheiden eines Gesellschafters, Betriebsveräußerung, Liquidation und dergleichen und

d) die Unterstützung bei der Erfüllung von Anzeige- und Dokumentationspflichten.

(7) Soweit auch die Ausarbeitung der Umsatzsteuerjahreserklärung als zusätzliche Tätigkeit übernommen wird, gehört dazu nicht die Überprüfung etwaiger besonderer buchmäßiger Voraussetzungen sowie die Frage, ob alle in Betracht kommenden umsatzsteuerrechtlichen Vergünstigungen wahrgenommen worden sind. Eine Gewähr für die vollständige Erfassung der Unterlagen zur Geltendmachung des Vorsteuerabzugs wird nicht übernommen.

12. Elektronische Kommunikation

Die Kommunikation zwischen dem Wirtschaftsprüfer und dem Auftraggeber kann auch per E-Mail erfolgen. Soweit der Auftraggeber eine Kommunikation per E-Mail nicht wünscht oder besondere Sicherheitsanforderungen stellt, wie etwa die Verschlüsselung von E-Mails, wird der Auftraggeber den Wirtschaftsprüfer entsprechend in Textform informieren.

13. Vergütung

(1) Der Wirtschaftsprüfer hat neben seiner Gebühren- oder Honorarforderung Anspruch auf Erstattung seiner Auslagen; die Umsatzsteuer wird zusätzlich berechnet. Er kann angemessene Vorschüsse auf Vergütung und Auslagenersatz verlangen und die Auslieferung seiner Leistung von der vollen Befriedigung seiner Ansprüche abhängig machen. Mehrere Auftraggeber haften als Gesamtschuldner.

(2) Ist der Auftraggeber kein Verbraucher, so ist eine Aufrechnung gegen Forderungen des Wirtschaftsprüfers auf Vergütung und Auslagenersatz nur mit unbestrittenen oder rechtskräftig festgestellten Forderungen zulässig.

14. Streitschlichtungen

Der Wirtschaftsprüfer ist nicht bereit, an Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle im Sinne des § 2 des Verbraucherstreitbeilegungsgesetzes teilzunehmen.

15. Anzuwendendes Recht

Für den Auftrag, seine Durchführung und die sich hieraus ergebenden Ansprüche gilt nur deutsches Recht.