Held/Kühn (Hrsg.)

Praktikerhandbuch IT- und Informationssicherheitsbeauftragter

Vorgaben – Anforderungen – Aufgaben – Verantwortlichkeiten – Handlungsempfehlungen

Finanz Colloquium Heidelberg, 2018

Zitiervorschlag:

Autor in Held/Kühn (Hrsg.), Praktikerhandbuch IT- und Informationssicherheitsbeauftragter, RdNr. XX.

ISBN: 978-3-95725-114-5

Finanz Colloquium Heidelberg GmbH
Im Bosseldorn 30, 69126 Heidelberg
www.FC-Heidelberg.de
info@FC-Heidelberg.de
Titelfoto: Silberberg GmbH Montafon
Satz: Finanz Colloquium Heidelberg GmbH
Druck: STRAUSS GmbH, Mörlenbach

Held/Kühn (Hrsg.)

Praktikerhandbuch IT- und Informationssicherheitsbeauftragter

Vorgaben – Anforderungen – Aufgaben – Verantwortlichkeiten – Handlungsempfehlungen

Dr. Jochen Dinger
Leiter Sicherheitsmanagement
Fiducia & GAD IT AG

Maximilian Ehrlich
Informationssicherheitsbeauftragter
LBS Norddeutsche Landesbausparkasse Berlin – Hannover

Dr. Wolfgang Finkler
Referent Referat CK 34
KRITIS-Sektoren Finanz- und Versicherungswesen, Gesundheit, IT und TK Bundesamt für Sicherheit in der Informationstechnik (BSI)

Dr. Jens Gampe
Referat BA 51 – Kompetenzcenter IT-Sicherheit
Bundesanstalt für Finanzdienstleistungsaufsicht

Alexander Graf
Geschäftsführender Gesellschafter
Finance Consult Unternehmensberatung GmbH & Co. KG

Dr. Markus Held (Hrsg.)
Referatsleiter Mindeststandards und Produktsicherheit
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Reiner Hoffmann
Leiter IT- und Gebäudemanagement
Volksbank Kaiserslautern eG

Murat Kizilelma
Leiter Datenschutz und Informationssicherheit
Berliner Sparkasse

Steffen Korn
Prüfungsgruppenleiter IT
Baden-Württembergischer Genossenschaftsverband e.V.

Prof. Dr. Ralf Kühn (Hrsg.)
Geschäftsführer
Audit GmbH Karlsruhe Stuttgart Wirtschaftsprüfungsgesellschaft

Peter Kullmann
Ressortvorstand Produktion
Volksbank Kaiserslautern eG

Jonas Müller
IT-Administrator
Volksbank Kaiserslautern eG

Ulrike Seip
Senior Referentin Datenschutz
DZ BANK AG

Oliver Wagner
Leiter Interne Revison
Sparda-Datenverarbeitung eG

Finanz Colloquium Heidelberg, 2018

Inhaltsübersicht

Inhaltsverzeichnis

Vorwort

Vom elektronischen Zahlungsverkehr über den Algorithmushandel bis hin zu Robo Avisory ist festzustellen: Der Bankbetrieb hat sich in den vergangenen Jahrzehnten stärker verändert als in den Jahrhunderten zuvor. Klar scheint nur, dass die Umbrüche weitergehen und sich sogar noch stärker als je zuvor im Alltag auswirken werden.

Die Kredit- und Zahlungsinstitute können sich insbesondere den disruptiven Effekten der Informationstechnik nicht entziehen. Zwar wurde die IT bisher häufig als reiner Kostenfaktor behandelt, jedoch stellt eine stabile, sichere und flexible IT in der heutigen Zeit einen wesentlichen Wettbewerbsfaktor dar.

Denn immer mehr Kunden erwarten ein komfortables Angebot zur Nutzung der Bankleistungen über digitale Kanäle. FinTechs greifen an, mit Bank-ähnlichen, technologiegetriebenen Geschäftsmodellen. Der Gesetzgeber unterstützt diese Entwicklung sogar ausdrücklich mit der PSD 2. Auch können viele Geschäftsprozesse vom Risikomanagement über den Wertpapierhandel bis hin zum Meldewesen nur noch IT-gestützt vernünftig betrieben werden.

IT-Risiken können sich hingegen immer stärker auf das Bankgeschäft auswirken. Ausfälle von IT-Systemen wirken sich unmittelbar auf den Geschäftsbetrieb aus und können somit besonders schnell öffentlichkeitswirksam werden. Schlimmer noch, Mängel in IT-Systemen können zu falschen Kennzahlen führen, die nicht sofort als solche erkannt werden. Cyber-Kriminelle attackieren in zunehmendem Maße nicht nur die Bankkunden, sondern auch Backend-Systeme, insbesondere im Zahlungsverkehr.

Damit gewinnt auch die Arbeit von Informationssicherheitsbeauftragten immer stärker an Bedeutung. Der vorliegende Band thematisiert zahlreiche aktuelle drängende Praxisfragen im Informationssicherheitsmanagement in der Kreditwirtschaft. Als Beispiele seien genannt:

- Welche unmittelbaren Konsequenzen ergeben sich aus neuer Regulierung, etwa den BAIT oder dem IT-SiG?
- Wie sieht das Informationssicherheitsmanagement in Banken aus?
- Worauf ist bei IT-Auslagerungen, auch auf Mehrmandantendienstleister, zu achten?
- Wie können Banken Cloud Computing nutzen?
- Wie kann man die Benutzerberechtigungsvergabe effektiv managen?
- Wie ist mit IDV umzugehen?

Die verschiedenen Beiträge geben damit einen Überblick über die Besonderheiten, die das Informationssicherheitsmanagement in Banken in der heutigen Zeit auszeichnen. Zugleich zeigen sie anhand vieler Beispiele konstruktive Wege auf, wie anspruchsvolle Probleme gelöst werden können. Wir wünschen allen Leserinnen und Lesern viel Spaß bei der Lektüre und gutes Gelingen bei der Arbeit!

Dr. Markus Held Prof. Dr. Ralf Kühn

A.

Regulatorische Rahmenbedingungen und Tendenzen

A. Regulatorische Rahmenbedingungen und Tendenzen

I. Aus MaRisk und BAIT – aufsichtsrechtliche Erwartungshaltung an den Informationssicherheitsbeauftragten und Prüfungspraxis[1]

1. Einleitung – oder: Einige Worte zum Umfeld dieses Beitrags

Die deutsche Kreditwirtschaft hat in den vergangenen zehn Jahren im Zusammenhang mit IT-Themen einen signifikanten Wandel erfahren. Was vor zehn Jahren noch als »nicht vorstandsrelevantes«, nicht bankspezifisches und auch nicht besonders erfolgskritisches Thema galt, das man den »Freaks« und »Nerds« der IT überlassen hat, ist sukzessive in den Fokus gerückt. Banken begannen einerseits zu verstehen, dass sie an einer Zeitenwende ihres Geschäftsmodells stehen – und dass die IT eine prominente Rolle bei der Frage spielt, ob es in der Zukunft nicht nur weiterhin Bankdienstleistungen, sondern eben auch Banken als Leistungserbringer gibt und geben kann. Die Diskussion und der Findungsprozess darum sind im vollen Gang. Wenn man dabei die Geschäfts- und/oder IT-Strategie vieler Institute betrachtet, fällt auf: Zahlreiche Institute reden dort zwar viel über Digitalisierung, Cloud Computing, Agilität und viele andere Stichworte. Was das aber konsequenterweise für die Unternehmens- und Risikokultur eines Instituts, die Steuerung der IT, für deren Verzahnung mit der alten bankfachlichen Welt bedeutet oder wie sich folglich das Interne Kontrollsystem entwickeln muss, bleibt oft mehr als vage. Daran wird erkennbar, dass der Umbruch zwar begonnen hat und beschleunigt wird durch Niedrigzinsphase, regulatorischen Druck u.v.m, dass die Branche aber doch erst am Anfang des Umbruchs steht. 1

Dieser Beitrag führt vor diesem Verständnishintergrund einleitend ein in die Rolle des Informationssicherheitsbeauftragten in der Risikokultur eines Instituts und in der IT-Steuerung. Darauf aufbauend thematisiert er wesentliche Aspekte der aufsichtsrechtlichen Erwartungshaltung an den Informationssicherheitsbeauftragten auf Basis der Prüfungspraxis der Bankenaufsicht der letzten Jahre – die sich zugleich spiegelt in den aktuellen Formulierungen der BAIT. 2

1 *Prof. Dr. Ralf Kühn*, WP/CPA/StB, CISA/CIA, Geschäftsführer Audit GmbH Karlsruhe Stuttgart Wirtschaftsprüfungsgesellschaft, seit vielen Jahren spezialisiert u. a. auf die Themen dieses Buches.

Immer wieder gilt es daher auch Bezug zu nehmen auf die Frage, welche Rolle dem Informationssicherheitsbeauftragten im Internen Kontrollsystem eines Instituts zukommt. Schließlich dient ein Abschnitt der Herstellung des Bezugs zu einem weiteren aktuellen Thema, dem Datenqualitätsmanagement.

2. Aufsichtsrechtliche Erwartungshaltungen an die IT-Steuerung einer Bank – und was der Informationssicherheitsbeauftragte damit zu tun hat

3 Die IT-Steuerung – auch IT-Governance bezeichnet – findet sich als Stichwort zwar in der Diskussion von IT-bezogenen Veranstaltungen, Gremien und Publikationen seit langem – nicht aber in KWG oder MaRisk. Neben der Einhaltung der aufsichtsrechtlichen Anforderungen umfasst IT-Steuerung auch die Steuerung der Werthaltigkeit des IT-Engagements und die Erreichung des erhofften Wertbeitrags für die Unternehmenszielsetzungen insgesamt. Erwartet werden hierbei Qualität, Effizienz, Serviceorientierung, Unterstützung bei Wertsteigerung und die Begrenzung der Risiken. Letzteres – die Begrenzung der Risiken aus der Nutzung von Informationstechnologie in der bankfachlichen Leistungserbringung – ist Grund der Existenz des Informationssicherheitsbeauftragten. Wie zu zeigen sind wird: Es ist nicht die Aufgabe des Informationssicherheitsbeauftragten allein, für Informationssicherheit zu sorgen, die Risiken zu begrenzen. Daher wurde auch die Formulierung »Grund der Existenz« bewusst gewählt. Doch dazu später….

4 In der IT-Steuerung darf es keine Werte- oder Strukturbrüche geben. IT-Steuerung besteht aus Führung, Organisationsstrukturen, Werten und Prozessen, die sicherstellen, dass die IT die Unternehmensziele und-strategien unterstützt. Die IT muss in ein einheitliches Rahmenwerk eingebunden sein, das sich am Geschäftszweck des Unternehmens orientiert. Daher hat auch der Informationssicherheitsbeauftragte dafür zu sorgen, dass er keine Inselwelten schafft, sondern ins Interne Kontrollsystem des Unternehmens insgesamt integriert handelt. Allzu oft ist bereits das ein Hauptdefizit des Informationssicherheitsmanagements einer Bank. Die Welt des »BSI-Grundschutzes«, des »Sicheren IT-Betriebs«, der »SOIT« oder wie die Ansätze der verschiedenen Institutsgruppen auch heißen mögen, ist nicht mit dem Rest des Internen Steuerungs- und Kontrollsystems ausreichend verbunden, hängt quasi in der Luft.

IT-Steuerung aber erfordert einen gesamthaften Ansatz zur wirksamen Steuerung des IT-Einsatzes von der IT-Strategie und IT-Architektur über eine konsistente Daten-Steuerung und einem Daten-Qualitätsmanagement bis hin zum ordnungsgemäßen Betrieb und eben zum Informationssicherheitsmanagement und zur Notfallvorsorge. Diesem gesamthaften Ansatz aber muss neben klaren Vorgaben etwa der Geschäfts- und Risikostrategie, klaren Regelungen, einer Vielzahl von Methoden, Konzepten und Umsetzungshilfen auch ein gemeinsamer Geist mit Blick auf den Umfang mit Risiken zu Grunde liegen. 5

Gerade in Zeiten, in denen sich Banken einer stetig steigenden Dichte und Komplexität aufsichtsrechtlicher Anforderungen gegenübersehen, in denen sie über Digitalisierung, Agilität und Wandel der Prozessketten nachdenken, kommt der damit verbundenen Ergänzung der Regelungswelt durch eine Wertewelt und dem Umbau der Regelungswelt auf ein handhabbares Maß entscheidende Bedeutung zu. 6

In den Regelungen der schriftlich fixierten Ordnung sind damit bewusst Handlungsspielräume vorzusehen, die jeder Einzelne mit seinem individuellen Können und Erfahrungshorizont einsetzen kann, aber eben auch muss. Damit aber sind Rollenklarheit, entsprechende Personalentwicklung und Wertschätzung für das »Mitdenken« der Mitarbeiter auch im Sinne des Risikomanagements bei gleichzeitigem Einziehen und Stärken der »Verteidigungslinien« nötig. Jeder Beschäftigte hat dann verankert in der Risikokultur nicht nur auf dem Papier, sondern real die Verantwortung, die Fähigkeiten, Erfahrungen und das eigene Verhalten zu reflektieren – und gleichzeitig das Recht dazu. Für diejenigen, die Bilder aus der Welt des Sports hilfreich finden: Nicht mehr wie früher das starre Festhalten eines Spielers an der hierarchischen Vorgabe, sondern die Nutzung von Spielintelligenz im Rahmen gegebener Leitplanken mit Doppelabsicherung im Fehlerfall ist die Taktik erfolgreicher Trainer heute – und der Informationssicherheitsbeauftragte ist eben genau das, eine Absicherung für die Spieler in der ersten Prozessverantwortung, sollten sie Fehler machen oder schlicht überrannt werden. 7

Damit aber ist Risikokultur nicht an einzelne Stellen, ans Risikocontrolling oder an die Beauftragten und die Revision delegierbar. Risikokultur fängt insbesondere in den Marktbereichen, in den bankfachlichen Prozessverantwortungen an und erfordert die intelligente und flexible Organisation des Zusammenspiels. 8

9 Jeder Mitarbeiter einer Bank sollte daher im Sinne einer risikobewussten Steuerung folgende Fragen beantworten können:

- Ist mir bewusst, welche Werte und Überzeugungen die Grundlage der Prozess- und Risikokultur meiner Bank sind?
- Kenne ich den Handlungsrahmen für meinen Umgang mit Risiken?
- Welche Risiken habe ich im Rahmen meines Arbeitsplatzes zu berücksichtigen?
- Welche Kommunikationswege für Risiken gibt es?
- Kenne ich meine Handlungsspielräume?
- Bin ich bereit, Handlungsweisen zu hinterfragen, von denen ich denke, dass diese falsch sind?
- Wie kann ich meine Erfahrungen und Fähigkeiten durch die Interaktion mit Kollegen/innen und Führungskräften erweitern?
- Bin ich mir über die Folgen meiner Entscheidungen oder meines Handelns im Klaren und bin ich bereit, für diese Folgen einzustehen?

10 Und im Sinne des Themas dieses Buches ist das für das Thema Informationssicherheit nicht minder nötig als etwa für klassische Bankthemen wie Adressrisiken. Es ist also Merkmal einer adäquaten Risikokultur eines Instituts, dass gerade nicht Informationssicherheit als Aufgabe der IT-Abteilung oder des Informationssicherheitsbeauftragten verstanden wird, sondern als Gegenstand des Internen Kontrollsystems einer Bank insgesamt, das durch verschiedene Aufgabenträger und verschiedene Mechanismen und Maßnahmen ausgestaltet wird.

11 In den MaRisk wird der dazu Grund legende Begriff Risikokultur nach dem bei Verfassung dieses Artikels aktuellen Stand des Zwischenentwurfs der MaRisk in der Fassung vom 23. Juni 2016 gültigen Stand innerhalb der AT 3 adressiert mit dem Text:

12 »Alle Geschäftsleiter (§ 1 Abs. 2 KWG) sind, unabhängig von der internen Zuständigkeitsregelung, für die ordnungsgemäße Geschäftsorganisation und deren Weiterentwicklung verantwortlich. Diese Verantwortung bezieht sich unter Berücksichtigung ausgelagerter Aktivitäten und Prozesse auf alle wesentlichen Elemente des Risikomanagements. Die Geschäftsleiter werden dieser Verantwortung nur gerecht, wenn sie die Risiken beurteilen können und die erforderlichen Maßnahmen zu ihrer Begrenzung treffen. **Hierzu zählt auch die Entwicklung, Förderung und Integration einer angemessenen Risikokultur innerhalb des Instituts und der Gruppe.«**

Erläuternd wird ausgeführt: »**Risikokultur«:** 13

»Die Risikokultur beschreibt allgemein die Art und Weise, wie Mitarbeiter des Instituts im Rahmen ihrer Tätigkeit mit Risiken umgehen (sollen). Die Risikokultur soll die Identifizierung und den bewussten Umgang mit Risiken fördern und sicherstellen, dass Entscheidungsprozesse zu Ergebnissen führen, die auch unter Risikogesichtspunkten ausgewogen sind. Kennzeichnend für eine angemessene Risikokultur ist vor allem das klare Bekenntnis der Geschäftsleitung zu risikoangemessenem Verhalten, die strikte Beachtung des durch die Geschäftsleitung kommunizierten Risikoappetits durch alle Mitarbeiter und die Ermöglichung und Förderung eines transparenten und offenen Dialogs innerhalb des Instituts zu risikorelevanten Fragen.« 14

Folgende **Kernaussagen** sind es also zusammenfassend, die zu betonen sich zum jetzigen Zeitpunkt für das Thema Informationssicherheit lohnt. 15

- Risikokultur will die in den MaRisk stark betonte formale, dokumentierende Seite abrunden um die Erkenntnis und Erfordernis, dass erst die »**gelebte Haltung**« eigentliches Risikomanagement bedeutet. So ist es eben nicht damit getan, ein erkanntes IT-Risiko zu behandeln, indem »wir eben eine Risikoanalyse« machen, sondern indem überlegt wird, ob es sich um ein Risiko handelt, das tatsächlich getragen werden soll und kann, wie sich dieses zur Gesamtsituation der Bank verhält und wie es in der Gesamtbank wirkt.
- Risikokultur hat insoweit engen Bezug zur Gesamtsteuerungsphilosophie eines Hauses, aber auch eine starke Komponente von Führungsgrundsätzen, angefangen vom **»Tone from the top«.** Wer als Vorstand glaubt, sich mit Informationssicherheit nicht befassen zu müssen oder dies allenfalls noch als Thema des IT-Vorstands sieht, sollte aufhören, geschäftsstrategisch über Digitalisierung oder Agilität zu sprechen. Er kann und wird damit nämlich nicht in der Lage sein, diese Themen angemessen zu erfassen und zu entscheiden – oder wer wollte ernsthaft behaupten, man könnte Entscheidungen über die grundlegende Neufassung des Kreditgeschäfts treffen, ohne die Frage zu beantworten, wie man Kreditrisiken angemessen behandelt?
- Die betriebswirtschaftlich oder juristisch geprägte Ausbildung der meisten Entscheidungsträger in Banken führt dazu, dass das Risiko in IT-Systemen unbeschadet der stark sensibilisierenden Wirkungen sowohl von Aufsichtsprüfungen als auch von tatsächlichen Schäden und Sicherheitsvorfällen teilweise immer noch nicht als **»Chefsache«** angesehen, sondern an die operativ zuständigen Abteilungen oder an die Rechenzentren z. B. der Finanzverbünde delegiert wird. Bestehende Verantwortung wird demnach zwar formal akzeptiert, aber nach wie vor teilweise nicht

materiell angemessen wahrgenommen. Dies äußert sich in Prüfungen nach § 44 KWG dann z. B. in der Feststellung unzureichender Reportings, unzureichender Auswertung dieser Reportings bzw. unzureichender Rückkopplung in die Banksteuerung und das Risikomanagement.

- Zugleich fehlt – gerade vor diesem Hintergrund an sich verwunderlich – oft die in allen gängigen IT-Standards geforderte **Anbindung der IT an die Geschäftsprozesse** (»Business-Alignment«). Leider spielt der wichtigste Erfolgsfaktor, nämlich gesunder Menschenverstand, Sensibilisierung der Mitarbeiter, Schulung der Mitarbeiter und Schaffung eines stringenten und auf die Bank und ihre Prozesse passenden organisatorischen Rahmens, dabei viel zu oft eine zu geringe Rolle. Die wirksamsten und effizientesten Maßnahmen aber werden daher oft nicht ergriffen. Die fehlende ganzheitliche Systematik ist ebenfalls eines der häufig anzutreffenden wesentlichen Probleme.
- Sehr weit verbreitet ist, dass für unterschiedlichste Risikobehandlungskontexte einer Bank, etwa das Risikomanagement für operationelle Risiken, das Informationssicherheitsmanagement, die Dienstleistersteuerung, die Compliance-Funktionen etc. unterschiedliche Regelkreise, unterschiedliche Risikomessmethoden, unterschiedliche Schwellenwerte etc. existieren, ohne dass dies bankfachlich anders begründbar wäre als damit, dass es eben keine bekannte Risikoneigung des Vorstands, keine klaren Risikokommunikationswege und keine Kultur der kontinuierlichen Verbesserung gibt, die das Identifizieren und Melden von Fehlern und/oder Risiken und/oder Schäden belohnt. Das aber steht eindeutig im Widerspruch zum betriebswirtschaftlichen Eigeninteresse der Bank wie zu den MaRisk. Hier gilt es, eine bewusste Risikokultur durch **Methodenklärung, – bereinigung und – vereinfachung** zu unterstützen soweit eben methodisch und aufsichtsrechtlich möglich.

3. Grundlagen des Informationsrisikomanagements

16 Die Mindestanforderungen an das Risikomanagement (MaRisk) definieren in AT 7.2 die Anforderungen an die IT-Systeme einer Bank und deren Management aus aufsichtsrechtlicher Sicht:

17 »Umfang und Qualität der technisch-organisatorischen Ausstattung haben sich insbesondere an betriebsinternen Erfordernissen, den Geschäftsaktivitäten sowie der Risikosituation zu orientieren. « (MaRisk AT 7.2, Tz. 1).

18 »Die IT-Systeme (Hardware- und Software-Komponenten) und die zugehörigen IT-Prozesse müssen die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherstellen. Für diese Zwecke ist bei der Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse grundsätzlich

auf gängige Standards abzustellen….. Die Eignung der IT-Systeme und der zugehörigen Prozesse ist regelmäßig von den fachlich und technisch zuständigen Mitarbeitern zu prüfen.« (MaRisk AT 7.2, Tz. 2).

Diese Textungen blieben auch in allen bisher vorliegenden Konsultations-(zwischen)entwürfen der MaRisk (neu) unverändert. 19

Ergänzt wurde in Tz. 4 der MaRisk AT 7.2: »Für IT-Risiken sind angemessene Überwachungs- und Steuerungsprozesse einzurichten, die insbesondere die Festlegung von IT-Risikokriterien, die Identifikation von IT-Risiken, die Festlegung des Schutzbedarfs, daraus abgeleitete Schutzmaßnahmen für den IT-Betrieb sowie die Festlegung entsprechender Maßnahmen zur Risikobehandlung und Risikominderung umfassen. Beim Bezug von Software sind die damit verbundenen Risiken angemessen zu bewerten.« 20

Als mit diesem Risikomanagement zu erreichenden Ziele definieren die MaRisk weiterhin die vier gleichermaßen relevanten und interdependenten Schutzziele, d. h. die Schutzziele Integrität, Verfügbarkeit, Authentizität und Vertraulichkeit. 21

a) Informationsrisikomanagement in den BAIT

Eine eindeutige und klarstellende Stellungnahme der Aufsicht, wie diese allgemeinen Anforderungen an das IT-Risikomanagement operativ zu interpretieren sind, wie sich die z. B. in den Finanzverbünden üblichen Aufgabenverteilungen aus zentralem Rechenzentrum und dezentraler Institutsstruktur hier einordnen lassen und welche Proportionalitäts- und Wesentlichkeitsüberlegungen bei der Umsetzung in einer Informationssicherheitsmanagementstruktur ggf. anzustellen sind, fehlte bisher. Stattdessen erfolgt die Kommunikation der Interpretation dieser Bestimmungen durch die Aufsicht in erster Linie über Prüfungsfeststellungen im Rahmen von IT-Prüfungen nach § 44 KWG. Diese »Lücke« zwischen der prinzipienorientierten knappen Formulierung der MaRisk und der zwischenzeitlich etablierten Prüfungspraxis zu reduzieren, sollte Aufgabe der BAIT sein. Dabei bewegen sich v.a. die Akteure der kreditwirtschaftlichen Verbände in einem erheblichen Spannungsfeld – im Wissen um die Prüfungspraxis sind an sich alle bekannten Formulierungen der BAIT nicht neu, sondern seit Jahren etablierte Prüfungspraxis. Zugleich aber sind diese sowohl von den Wirtschaftsprüfern als auch den kreditwirtschaftlichen Verbänden immer eher defensiv, mit sehr unterschiedlichen Messlatten zwischen »europäisch regulierten«, »bundesbankgeprüften«, »nicht bundesbankgeprüften« Häusern und oft erheblichen regionalen oder gar prüferpersönlichkeitsspezifischen Merkmalen 22