NEWSletter

Ausgabe 4/2015

CASIS

WIRTSCHAFTSPRÜFUNG

„Ein neues Buch, ein neues Jahr.

Was werden die Tage bringen?

Wird‘s werden, wie‘s immer war?

Halb scheitern, halb gelingen?“

(Theodor Fontane)

Inhalt

I. Schwerpunktthema

Hinweise zur Prüfungsplanung 2016 — 2018 4

Risikomanagement 6

Kreditgeschäft 8

Meldewesen 10

IT-Verfahren und IT-Systeme 12

II. Kurz notiert

Arbeitsgesetze im Aushang 14

III. CASIS intern

Beratungsangebote und weitere Dienstleistungen 15

Seminar– und Workshop-Angebote 15

IV. Impressum 16

I. Schwerpunktthema

Hinweise zur Prüfungsplanung 2016—2018

Empfängerkreis

- Leiter(in) Interne Revision, Vorstände und Aufsichtsräte von Kreditinstituten

1. Hintergrund

Die jährliche Prüfungsplanung und die Aktualisierung der mehrjährigen Prüfungsplanung der Internen Revision stehen regelmäßig zum Jahresende an. Vor dem Hintergrund der weiterhin herausfordernden aufsichtsrechtlichen Entwicklungen und des aktuellen Marktumfelds sollten dabei für die kommenden Jahre alle wichtigen Themen im Blick sein und ausreichende Kapazitäten für projektbegleitende Prüfungen eingeplant werden. Insbesondere die zu erwartenden Anforderungen aus den MaRisk 6.0 und den BAIT, aber auch Indikationen aus der neuen PrüfbV und den SREP-Anforderungen rücken die Themen Non-Financial Risks, Datenqualitätsmanagement, IT-Sicherheit und die Überwachung ausgelagerter Aktivitäten und Prozesse weiter in den Fokus der Überwachungstätigkeiten der Geschäftsführungs– und Aufsichtsorgane und damit auch in den Prüfungsfokus der Internen Revision. Auf den nachfolgenden Workshop-Folien haben wir zentrale Hinweise zur aktuellen Prüfungsplanung für Sie zusammengefasst und zeigen für ausgewählte Prüffelder aktuelle Themenschwerpunkte auf (Auszug).

2. Prüfungsplanung und Validierung des Risikomodells

Grundlage der Prüfungstätigkeit der Internen Revision ist die risikoorientierte Prüfungsplanung, die zunächst die Erstellung eines Rahmenplans (Audit Universe) und einer Mehrjahres– und Jahresplanung inklusive Kapazitätsplanung beinhaltet und letztlich in einer operativen Prüfungsplanung je Prüffeld mündet. Von entscheidender Bedeutung ist, dass die Vollständigkeit des Audit Universe, das grundsätzlich alle Betriebs– und Geschäftsabläufe im Institut inklusive der ausgelagerten Aktivitäten und Prozesse zu berücksichtigen hat, sichergestellt ist. Im Optimalfall kann eine Orientierung an der Prozesslandkarte der Bank erfolgen. Einen Überblick über Maßnahmen zur Identifikation und Bewertung von Risikoobjekten bietet die erste Folie auf Seite 5. Zu beachten sind hier insbesondere die Indikationen aus den SREP-Guidelines, die aufgrund der direkten und indirekten EZB-Aufsicht seit November 2014 auch Auswirkungen auf nicht systemrelevante Institute haben.

Die Risikobewertung der Prüfungsobjekte und die daraus erfolgende Ableitung der Prüfungsturnusse sollte auf einem Risikomodell basieren, das auf der Grundlage quantitativer und qualitativer Kriterien die wirtschaftliche Bedeutung, die inhärenten Risiken und die Kontrollrisiken der Prüffelder berücksichtigt. Es ist darauf zu achten, dass die Risikobewertungssystematik der Internen Revision im Einklang mit den Risikomodellen anderer zentraler Funktionen der Bank (insbesondere Risikocontrolling und Compliance) steht. Zwischen diesen Bereichen sollte eine laufende Abstimmung stattfinden. Zudem ist das Risikomodell regelmäßig einer Validierung zu unterziehen (Anhaltspunkte hierzu gibt die zweite Folie auf Seite 5).

In der Mehrjahres– und Jahresprüfungsplanung sind thematische Neuerungen sowie der erhöhte Kapazitätsbedarf, der sich aus den neuen oder intensiver zu beleuchtenden Prüfungsthemen (gegebenenfalls einhergehend mit einer Verkürzung von Prüfungsturnussen ergibt, zu berücksichtigen. Nicht vernachlässigt werden darf auch der Kapazitätsbedarf, der mit der erforderlichen projektbegleitenden Beratung der Internen Revision einhergeht. Zudem gilt: Beratungs– und Umsetzungsprojekte von heute sind Prüfungsthemen von morgen.

Handlungsbedarf

- Überprüfung der Grundlagen der Prüfungsplanung (MaRisk 6.0, GAP-Analyse der SREP-Guidelines, PrüfbV) und des Audit Universe, um eine Vollständigkeit sicher zu stellen,
- Überprüfung, ob eine Harmonisierung der Prüfungsansätze auf Gruppenebene erforderlich ist,
- Verschaffung eines Überblicks über aktuelle und vorbereitende Projekte , insbesondere Anpassungsprozesse gemäß AT 8 MaRisk und Einplanung von Kapazitäten für projektbegleitende Tätigkeiten,
- Prüfung einer institutseinheitlichen Risikobewertung und Validierung des Risikomodells.

Identifikation und Bewertung von Risikoobjekten

Identifikation

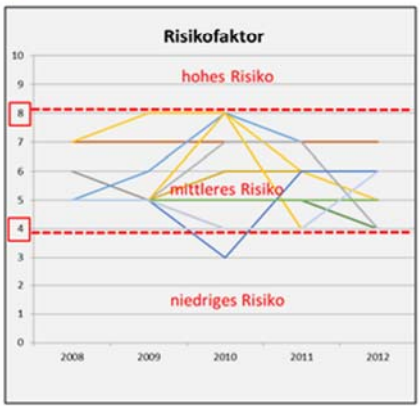
Interne Quellen	Externe Quellen
▪ Geschäfts- und Risikostrategie ▪ Gremienprotokolle ▪ Informationen zu Anpassungs-prozessen (AT 8 der MaRisk) ▪ Projekt-/Produkt-/ Prozessmanagement ▪ Schadensfalldatenbank, etc.	▪ Verlautbarungen der BaFin, Informationen der EZB, Dt. Bundesbank, des BMF, der DPR, EBA Dashboard ▪ Informationen des DIIR und des IDW ▪ Rechtsnormenmonitoring (z.B. über RADAR) ▪ Beiträge in Fachzeitschriften und Fachbüchern für Kreditinstitute und Interne Revision ▪ Fortbildungsveranstaltungen, Workshops, etc.

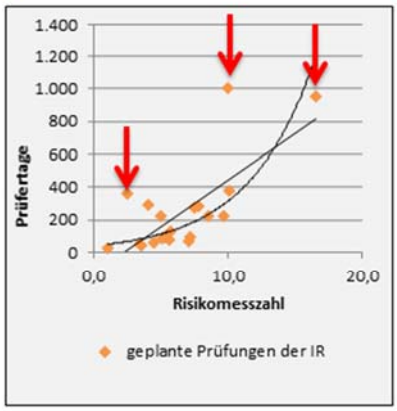
Bewertung (Festlegung von Risikomesszahlen)

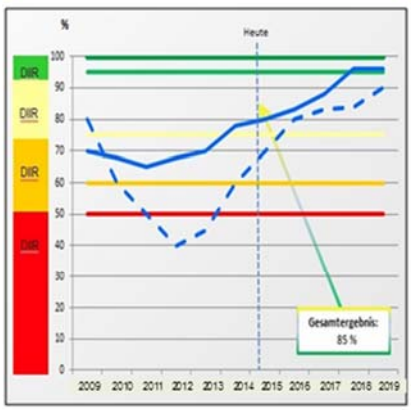
- Festlegung von quantitativen und qualitativen Beurteilungskriterien bzw. Risikokategorien (unter Einbezug der wirtschaftlichen Bedeutung, der inhärenten Risiken und der Kontrollrisiken) und Ermittlung der Risikomesszahlen pro Prüffeld durch Gewichtung der Kriterien/Kategorien
- Jährliche Revalidierung der Kriterien/Kategorien und Gewichtungsfaktoren mittels Expertenworkshops und Abweichungsanalysen

Quality Assessment Interne Revision

Trennschärfe Risikomodell (Plausibilität verwendeter Risikokategorien und Entwicklung der Risikomesszahlen)	Zusammenhang Risikomesszahl und geplante Prüfertage & Analyse von Abweichungen	Durchführung/Auswertung von Kundenbefragungen & Berechnung des QA-Zielerreichungsgrades gemäß DIIR Revisionsstandard Nr. 3







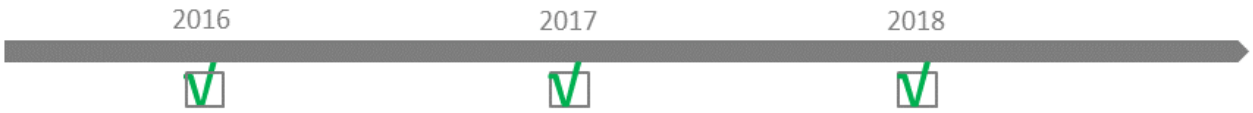
Risikomanagement

PRÜFUNGEN UND INHALT

Nr.	Unterprozesse	Teilprozesse in den Unterprozessen (Prüfungsfelder)
1. Risikomanagement/ Risikocontrolling (Auszug)		
	Produkte: alle Bankprodukte **Risikoarten:** Alle Risikoarten gem. Risikolandkarte (Adressausfall-, Marktpreis-, Liquiditätsrisiken, Operationelle Risiken inkl. Non-Financial Risks) **Prüfungsmaßstab:** § 25a, c, d KWG, BTR MaRisk, MaRisk 6.0: AT 4.3.1 i.V.m §25a KWG, BCBS 239	
1.1	**Grundlagen Risiko-management**	Allgemeine Anforderungen, Organisation des Risikomanagements, Querschnittsprüfung auf Einhaltung § 25a KWG relevanter Themen, Risikoinventur, Risikosteuerungs- und –controllingprozesse, Risikotragfähigkeit/Risikotragfähigkeitsrechnung (ICAAP), Stresstests (Methodik/Modelle/Durchführung/ Berichtswesen), Modellrisiken, Reporting, Identifizierung/Aggregation/Auswertung und Management von Risikodaten inkl. Überwachung der Datenqualität und zeitlichen Datenverfügbarkeit
1.2	**Kapitalplanung**	Kapitalplanungsprozess
1.3	**Adressausfall-risiko**	Adressenausfallrisiko-Management, Überwachung von Großkreditgrenzen, ARÜ, Ausfallerkennung/ Verlustdatenbank, Ratinganwendung und -validierung, Einbindung in die Risikostrategie, Risikoerfassung, Einbindung Risikosteuerung/Risikoüberwachung/Risikoberichterstattung (Schnittstellen zur Prüfung 1.1)
1.4	**Liquiditätsrisiko**	Liquiditätsrisiko-Management, ILAAP, Einbindung in die Risikostrategie, Risikoerfassung, Einbindung Risikosteuerung/Risikoüberwachung/Risikoberichterstattung (Schnittstellen zur Prüfung 1.1)
1.5	**Marktpreisrisiko**	Marktpreisrisiko-Management, Einbindung in die Risikostrategie, Risikoerfassung, Einbindung Risikosteuerung/Risikoüberwachung/Risikoberichterstattung (Schnittstellen zur Prüfung 1.1), Betrachtung von Zinsänderungsrisiken
1.6	**Operationelles Risiko**	Management von operationellen Risiken, Einbindung in die Risikostrategie, Risikoerfassung, Einbindung Risikosteuerung/Risikoüberwachung/Risikoberichterstattung (Schnittstellen zur Prüfung 1.1), Pflege Schadenfalldatenbank, Governance von Non-Financial Risks und Maßnahmen zur Risikominderung

Aktuelle Herausforderungen im Risikomanagement

Indikationen für die Prüfung des Risikomanagements



- Halten die aufbau- und ablauforganisatorischen Regelungen auch einer Beurteilung im Sinne des **SREP** stand (**Nachhaltigkeit** der Strategien, Ermittlung der Risikotragfähigkeit, **IKS** und insbesondere wirksame Risikocontrolling- und Compliance-Funktion, Angemessenheit der personellen und technisch-organisatorischen Ausstattung)?
- Werden durch das **Niedrigzinsniveau** bedingte Risiken angemessen berücksichtigt?
- Bestehen in der Bank angemessene Prozesse, um die Inventur und Bewertung von **Non-Financial Risks** durchzuführen (Früherkennungsindikatoren, Bewertung von RTB- und CTB-Aktivitäten) und adäquate Risikominderungstechniken einzusetzen?
- Ist die Bank in der Lage, die Anforderungen aus **BCBS 239** umzusetzen? Bestehen angemessene **Datenqualitätssicherungsmaßnahmen** in allen risikorelevanten Prozessen?
- Werden die erwarteten Anforderungen der **MaRisk 6.0** in den Risikomanagement- und -controllingprozessen und dem Anweisungswesen abgebildet (z.B. **Liquiditätsverrechnungssystem**)?

Handlungsbedarf

Hinsichtlich der Erfüllung der Anforderungen an die Kreditinstitute bedarf es nicht nur einer Berücksichtigung der Themenbereiche in der Prüfungsplanung der Internen Revision. Zunächst sollten auch Geschäftsführung und Aufsichtsorgan über die zuständigen Fachbereiche sicherstellen, dass der Anpassungsbedarf rechtzeitig erhoben wird und Umsetzungsprojekte mit angemessenen zeitlichen und personellen Kapazitäten geplant und durchgeführt werden.

Wichtige Fragestellungen sind hier:

- Implementierung/Anpassung der Prozesse zur Identifizierung, Bewertung und Minimierung von Non-Financial Risks.
- Überprüfung der Risikoeinschätzung aufgrund des anhaltenden Niedrigzinsniveaus.
- Überprüfung der Prozesse und Systeme zur Datenqualität und Datensicherung.
- Überprüfung der bestehenden Notfallkonzepte, insbesondere unter Berücksichtigung von ausgelagerten Bereichen.

Kreditgeschäft

PRÜFUNGEN UND INHALT

Nr.	Unterprozesse	Teilprozesse in den Unterprozessen (Prüfungsfelder)
2. Kreditgeschäft (Auszug)		
	Produkte: Kontokorrent, Darlehen, Ratenkredite, Mitarbeiterkredite, Organkredite, Avale, Konsortialkredite, Großkredite **Kunden/Ratingverfahren:** Mengengeschäft, bilanzierende Unternehmen **Prüfungsmaßstab:** § 25a, c, d KWG, BTO 1 MaRisk	
2.1	**Kreditgewährung**	Informationsauswertung/Bedarfsanalyse, Produktauswahl, Zusammenführung zu Kreditnehmereinheiten oder Gruppe verbundener Kunden, Offenlegung der wirtschaftlichen Verhältnisse, Bonitätsbeurteilung, Sicherheitenbewertung, Risikoklassifizierung/Rating, Konditionierung, kompetenzgerechte Genehmigung, Erstellung der Verträge, Überwachung ausstehender Unterlagen, Überwachung Auflagen, Valutierung (Auszahlungsvoraussetzungen/-kontrolle), Erfassung im System, Erfassung abgelehnter Kreditanträge
2.2	**Kreditweiter-bearbeitung**	Laufende Offenlegung der wirtschaftlichen Verhältnisse, Aktualisierung Risikoklassifizierungsverfahren, Kreditverwendungskontrolle, Überziehungsbearbeitung, Rückstandsbearbeitung, Änderung bestehender Kreditverträge (z.B. Tilgungsaussetzung, Sondertilgungen, Schuldnerwechsel, außerplanmäßige Tilgung), laufende Überprüfung der Sicherheiten, Verwahrung und Verwaltung der Sicherheiten, Zinsprolongationen, Vertragsbeendigung, Archivierung (Kreditakten und -unterlagen), Limitlisten, Rückzahlung
2.3	**Intensivbetreuung**	Definition der Kriterien, Erfassung und Überprüfung der Kriterien, Funktionstrennung bei Beschlussfassung, Durchführung der Bestandsaufnahme, Festlegung und Durchführung/Einhaltung der Maßnahmen, Beurteilung der weiteren Zuordnung (Normal-, Intensiv-, Problemkreditbearbeitung), Erstellung eines Maßnahmenplans in Abhängigkeit von Komplexität und Risikogehalt sowie Überwachung und turnusmäßige Überprüfung
2.4	**Problemkredit-bearbeitung und Risikovorsorge**	Definition der Kriterien, Erfassung und Überprüfung der Kriterien, Durchführung der Bestandsaufnahme, Festlegung und Durchführung/Einhaltung der Maßnahmen, Beurteilung der weiteren Behandlung (Sanierung, Abwicklung) und laufende Überprüfung der Vorgehensweise, Erfassung/Bewertung/ Kommunikation von Risikovorsorge

Aktuelle Herausforderungen im Kreditgeschäft

Wohnimmobilienkreditrichtlinie:
- Ziel: Transparenter, effizienter und wettbewerbsfähiger Kreditmarkt in der EU

Gruppe verbundener Kunden:
- Wegfall von Ausnahmeregelungen
- Modifizierte Regelungen zur Durchschau von Konstrukten

PrüfbV:
- Vollprüfung von Organkrediten

Online-Kreditvergabe:
- Geringere regulatorische Kosten und höhere Effizienz bei gleichzeitig steigende Betrugsrisiken
- Steigende Attraktivität von Online-Kreditmarktplätzen für Kunden

AnaCredit:
- Neue Komplexität und Granularität
- Meldung von ca. 100 Datenattributen zu Kreditnehmern

Niedrigzinsumfeld:
- „Schrottimmobilien"
- Klumpenrisiken

BCBS 239:
Anforderungen an Aggregation von Risikodaten und Risikoberichterstattung

Indikationen für die Prüfung des Kreditgeschäfts

- Erfolgt die richtige Abbildung von **Gruppen verbundener Kunden** (Wegfall der Ausnahmeregelungen u.a. für Bund/Länder/Gemeinden, Kommunalkonzernsplitting und modifizierte Regelungen zur Durchschau von Konstrukten)?
  Wichtig: Prüfung des **Durchschauprozesses** inkl. Schnittstellen zum Meldewesen!
- Berücksichtigen sämtliche Konto- und Kreditprozesse die Anforderungen an die **Datenqualität gemäß AnaCredit und BCBS 239** (Stammdatenpflege, Verschlüsselung, Verkürzung der Bearbeitungsfristen, etc.)?
- Werden die Auswirkungen der **Niedrigzinsphase** in der Prüfung berücksichtigt – Stichworte „Schrottimmobilien" und „Klumpenrisiken"?
- Berücksichtigt der Prüfungsplan eine Vollprüfung der **Organkredite** (analog der Anforderungen der PrüfbV)?
- Werden die Prozesse der **Online-Kreditvergabe** sowie die damit im Zusammenhang stehenden Betrugs- und IT-Risiken in der Prüfung berücksichtigt? Werden auch ggf. erforderliche Auslagerungsmaßnahmen (Stichwort „Legitimationsprüfung") und die Anpassung der Geschäfts-, Risiko- und IT-Strategie beleuchtet?

Handlungsbedarf

Für die Fachabteilungen besteht hinsichtlich der aktuellen konjunkturellen und aufsichtsrechtlichen Entwicklungen folgender Überprüfungs– und Umsetzungsbedarf:

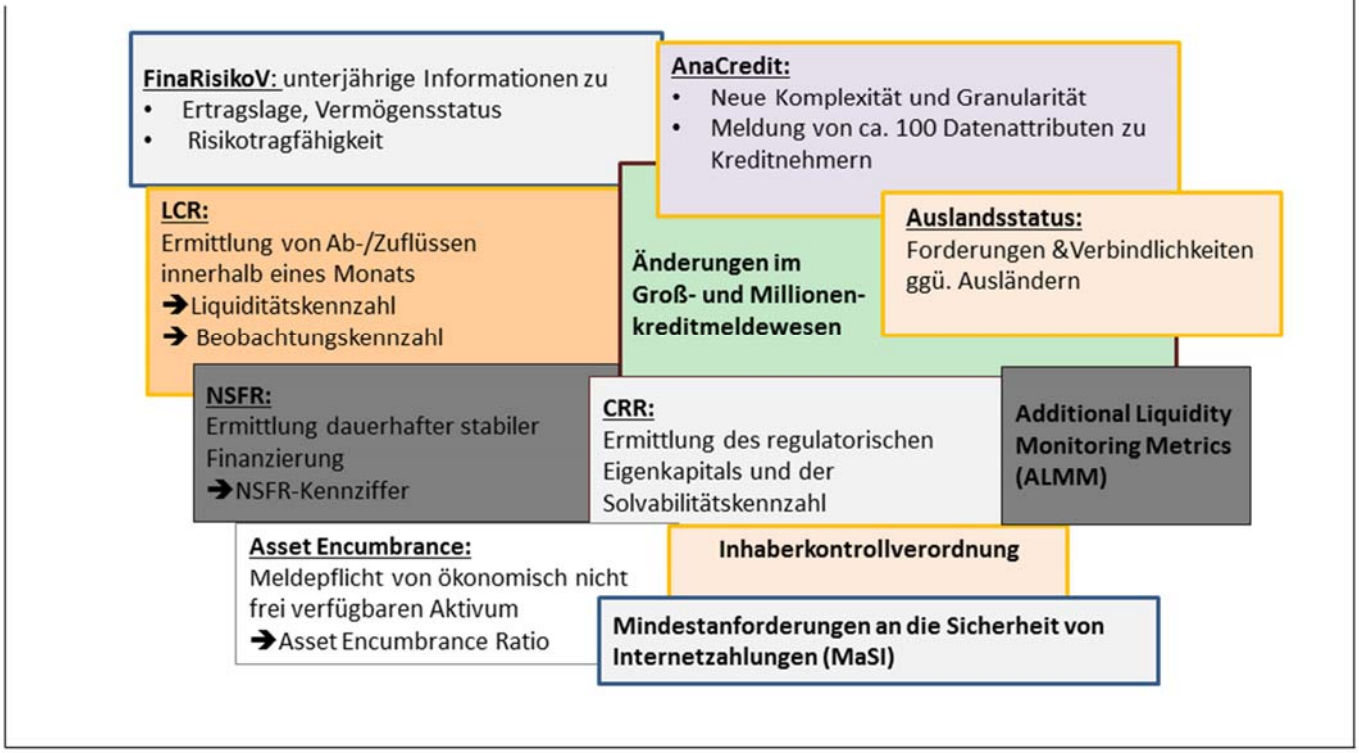
- Prüfung der vorhandenen Prozesse und Systeme inklusive des Anweisungswesens auf die neuen Anforderungen nach AnaCredit und BCBS 239. Bestehen angemessene Vertretungsregelungen, so dass die rechtzeitige Erstellung der Risikoberichterstattung auch im Vertretungsfall sichergestellt ist? Bestehen angemessene Datenqualitätssicherungsprozesse und eine klare Definition der Datenanforderungen?
- Prüfung des Portfolios auf erhöhte Risiken aus „Schrottimmobilien", Beachtung der weiterhin herrschenden Niedrigzinsphase: Sind die Mitarbeiter in den Kreditabteilungen sensibilisiert auf die typischen Anzeichen eines Betrugsfalls im Vermittlungsgeschäft (Kopien und vorformulierte Bonitätsunterlagen, notarielle Urkunden mit hoher Rollennummer, Einkommensnachweise erstellt mit Standardsoftware, etc.)?
- Mitteilung an Organmitglieder über die neuen Prüfungspflichten nach PrüfbV sowie Überprüfung der Marktgerechtigkeit der Konditionen.
- Sensibilisierung der Mitarbeiter hinsichtlich der aktuell geltenden Regelungen zur Bildung von Gruppen verbundener Kunden in Abgrenzung zur Bildung von Kreditnehmereinheiten sowie klare Vorgaben in der schriftlich fixierten Ordnung.

Meldewesen

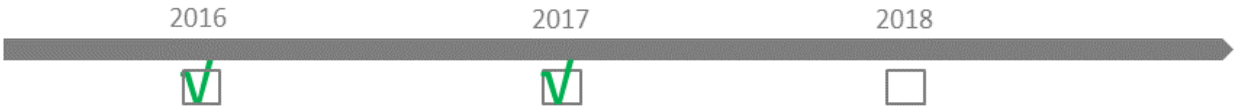
PRÜFUNGEN UND INHALT

Nr.	Unterprozesse	Teilprozesse in den Unterprozessen (Prüfungsfelder)
3. Meldewesen (Auszug)		
	Produkte: alle Bankprodukte **Risikoarten:** Alle Risikoarten gem. Risikolandkarte (Adressausfall-, Marktpreis-, Liquiditätsrisiken, Operationelle Risiken, Sonstige Risiken) **Prüfungsmaßstab:** KWG, CRR 92/95/97/98, InhKontrollV, AnzV, WpHG, GwG	
3.1	**Grundlagen Meldewesen**	Allgemeine Anforderungen an das Meldewesen, Organisation des Meldewesens; Übersicht, Zuständigkeiten, "Meldewesenevidenz", Querschnittsprüfung von Themen, die in den einzelnen Meldungen nicht berücksichtigt sind
3.2	**Meldung Eigenmittel/Kapitalkennziffern/Asset Encumbrance**	Meldung Eigenmittel, Kapitalquoten und -puffer, Leverage Ratio, Erstellung Vorstandsreporting Basel III, belastete Vermögenswerte
3.3	**Kreditmeldewesen**	Groß- und Millionenkredite, Stammdaten, Auslandskreditvolumen etc. (gem. Übersicht Meldungen), Verlustdatenmeldung, Schnittstellen zu Durchschauprozess für Konstrukte, Bildung Gruppe verbundener Kunden/Kreditnehmereinheiten
3.4	**Meldung Liquidität und FinaRisikoV**	Ermittlung und Meldung Liquiditätskennzahlen, LCR, NSFR,ALMM, Erstellung Vorstandsreporting Basel III, Meldung Finanzinformationen und Risikotragfähigkeitsinformationen
3.5	**Offenlegung**	Offenlegung nach CRR
3.6	**Beteiligungsanzeigen und sonstiges Anzeige- und Meldewesen**	Beteiligungsanzeigen, Meldung personeller, finanzieller oder organisatorischer Gegebenheiten/ Veränderungen (§§ 2c, 24 KWG, InhKontrollV, GwG, MaRisk), Meldung von Informationen bzgl. Sicherungseinrichtung, EMIR, Angaben zu den Handelsbuchpositionen, Meldepflicht nach § 9 WpHG (Geschäfte Finanzinstrumente), Verbandsmeldewesen, Meldung nach Außenwirtschaftsverordnung, Statistische Meldungen

Aktuelle Herausforderungen im Meldewesen



Indikationen für die Prüfung des Meldewesens



- Welche Auswirkungen haben die Veränderung der Bemessungsgrundlage „Anrechenbares Eigenkapital“, die Meldepflicht für Kredite von Finanzinstituten/ -unternehmen und die Senkung der Meldegrenzen für Millionenkredite auf **Verschlüsselungs-, Stammdatenpflege-, Beschlussfassungs- und Meldeprozesse**?
- Wurden die neuen Meldepflichten hinsichtlich **FinaRisikoV** (Risikotragfähigkeits-informationen), **Asset Encumbrance**, **LCR** und **NSFR**, **ALMM**, **Einlagensicherungsgesetz** und **MaSI** vollständig, richtig und termingerecht umgesetzt und sowohl in den dokumentierten **Prozessen** als auch im **Anweisungswesen** adäquat berücksichtigt? Werden die **Schnittstellen** zwischen den Fachbereichen (zuliefernde Abteilungen) und dem Meldewesen sowie die **Datenqualitätsanforderungen** ausreichend beschrieben?
- Verfügt die Bank über angemessene Prozesse zur Überwachung von Entwicklungen, aus denen sich anzeigepflichtige Tatbestände ergeben können (Stichwort „**InhKontrollV**“)?
- Ist das Meldewesen auf die Anforderungen aus **AnaCredit** vollumfänglich vorbereitet?
- Ist die **personelle Ausstattung** in den zuständigen (Melde-)Fachbereichen im Hinblick auf den deutlichen Mehraufwand im Meldewesen noch angemessen?

Handlungsbedarf

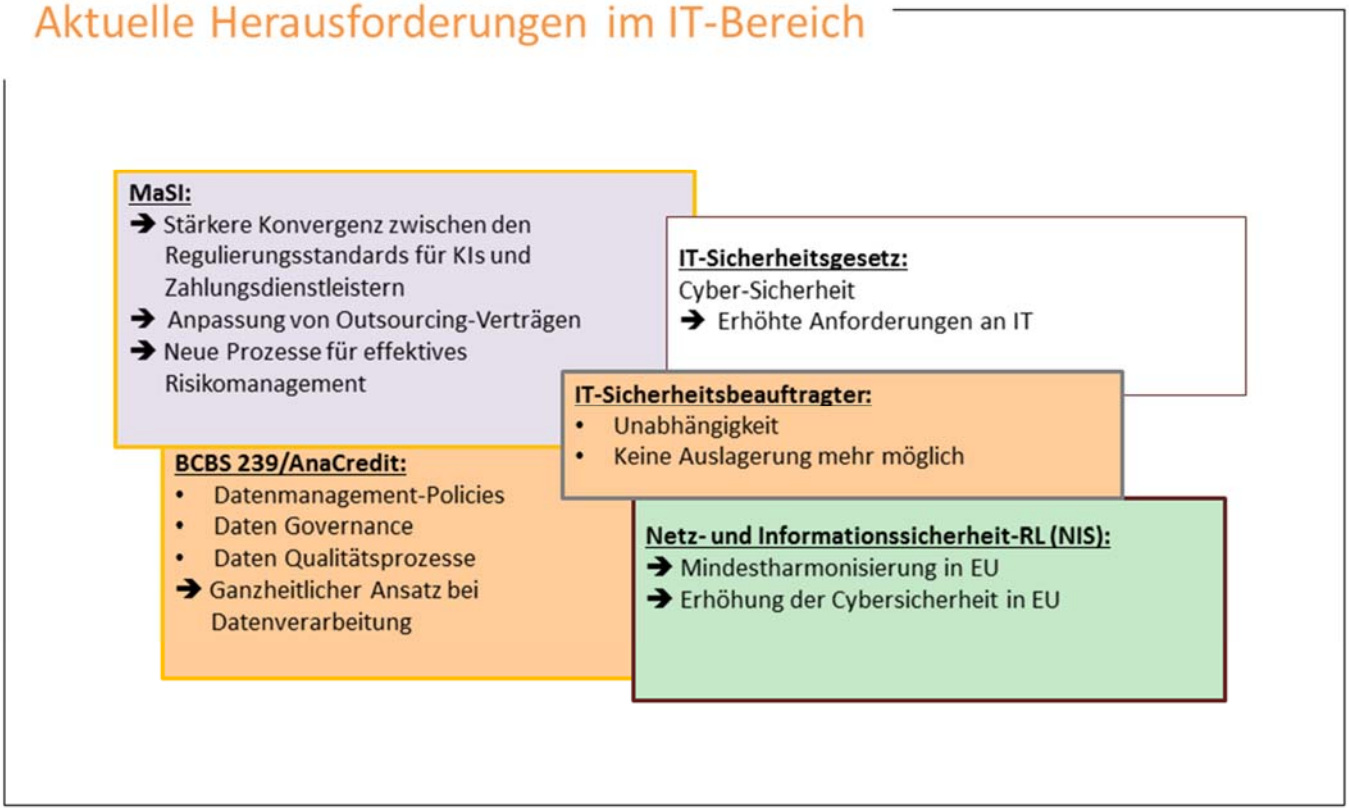
Für die Fachabteilungen, insbesondere das Meldewesen und Rechnungswesen, besteht hinsichtlich der aktuellen aufsichtsrechtlichen Entwicklungen folgender Überprüfungs– und Umsetzungsbedarf:

- Erarbeitung einer institutsspezifischen Meldeübersicht, auf der sämtliche abzugebende Meldungen und Anzeigen an Aufsichtsbehörden, Verbände, etc., die Meldetermine und die Meldefristen verzeichnet sind. Es bietet sich an, eine laufende Aktualisierung der Übersicht auf der Grundlage des Rechtsnormenmonitorings der MaRisk Compliance-Funktion vorzunehmen.
- Prüfung vor dem Hintergrund von AnaCredit und BCBS 239, ob die bestehenden Datenqualitätssicherungsmaßnahmen auch die Harmonisierung der Daten und Abstimmungen zwischen Rechnungswesen, Meldewesen und Risikocontrolling berücksichtigen.
- Überprüfung der Stammdatenpflege und Verschlüsselungsprozesse.
- gegebenenfalls Fassung oder Nachholung von Großkreditbeschlüssen bei Feststellung neuer Großkredite aufgrund geänderter Eigenkapitalbestimmungen und Aufhebung von Ausnahmeregelungen bei der Bildung von Gruppen verbundener Kunden.

IT-Verfahren und –Systeme

PRÜFUNGEN UND INHALT

Nr.	Unterprozesse	Teilprozesse in den Unterprozessen (Prüfungsfelder)
4. IT-Verfahren und -Systeme (Auszug)		
	Produkte: alle Bankprodukte **IT-Systeme und Verfahren:** Alle Systeme und Verfahren inkl. IDV **Prüfungsmaßstab:** § 25a, c, d KWG, DIN ISO 27000 ff., AT 7 MaRisk, MaRisk 6.0: AT 7.2 Tz. 4 i.V.m. § 25a KWG, IDW RS FAIT 1 in Verbindung mit Revisionsstandard 1 des DIIR, BCBS 239	
4.1	IT-Betrieb	Berechtigungsmanagement inkl. IDV/Berechtigungskonzepte, Changemanagement (Testmanagement, Management von Hardware, Dokumentation der Änderungen, Konzepte, Programmauftrag-Anforderungsmanagement, IDV, Einführung Anwendungssoftware, Pflege Kernbanksystem, Organisationsmodell), Releasemanagement (Testmanagement, Releaseplanung, Dokumentation der Änderungen, Konzepte, Patch- und Änderungsmanagement), Incidentmanagement (inkl. IDV, Sicherung IT-Bereitschaft), Datensicherung (Prüfung, Wiederherstellung, Anpassung Umfang), Archivierung, Löschen und Vernichten von Daten (inkl. IDV)
4.2	IT-Infrastruktur	Rechenzentrum und Standorte Serverräume, techn. und bauliche Risiken, techn. Infrastruktur
4.3	IT-Netze	Netzwerke und Strukturen, Netz- und Systemmanagement, VPN, WLAN, VoIP, ISDN, Firewall
4.4	Anwendungen (Einzelprüfungen)	Prüfung risikoorientiert ausgewählter IT-Anwendungen
4.5	Systeme (Einzelprüfungen)	Prüfung risikoorientiert ausgewählter IT-Systeme



Indikationen für die Prüfung der IT-Verfahren und -Systeme

- Werden im Rahmen der Prüfung **Cyber-Risks** berücksichtigt, die z.B. aufgrund des Einsatzes digitaler Geschäftsmodelle bestehen?
- Entspricht die organisatorische Stellung und der Aufgabenbereich des **IT-Sicherheitsbeauftragten** (Stichwort „Nichtauslagerung“) den Anforderungen der Aufsicht? Erfolgt eine klare Abgrenzung des Verantwortungsbereichs zu anderen Beauftragten und Kontrollinstanzen?
- Werden die erwarteten Anforderungen aus den **MaRisk 6.0** sowie den **BAIT** und den **MaSI** im Rahmen der projektbegleitenden Prüfung und Prozessprüfungen berücksichtigt?
- Bestehen angemessene **quantitative und qualitative personelle Ressourcen** im IT-Bereich und den unterstützenden Stellen, um die Anforderungen, die sich aus der Vielzahl von Projekten (u.a. BCBS 239, AnaCredit, PRIIP, MaSI, MiFID II) ergeben, termin- und sachgerecht erfüllen zu können?

Handlungsbedarf

Für die Fachabteilungen, insbesondere den IT-Bereich, besteht hinsichtlich der aktuellen gesetzlichen und aufsichtsrechtlichen Entwicklungen folgender Überprüfungs– und Umsetzungsbedarf:

- Besteht ein Programm-Management, um durch Koordination und Kombination der IT-Projekte Kosteneffizienzen durch Synergieeffekte zu heben (Standardisierung, größere Volumina, Clusterung)?
- Prüfung der vorhandenen Systeme auf die neuen Anforderungen (BAIT, MaSI, BCBS 239, AnaCredit, PRIIP, MiFID II),
- Beobachtung der Entwicklungen auf dem FinTech Sektor.
- Prüfung/Erarbeitung einer Strategie zum Digital-Banking.
- Einrichtung von reproduzierbaren Systematiken und Prozessabläufen sowie Schaffung von klaren Rollen- und Verantwortungsbeschreibungen mit immer wiederkehrenden Aufgaben.
- Schaffung von Akzeptanz bei den Beteiligten durch Erwartungs- und Veränderungsmanagement sowie klare und effektive Kommunikation.
- Einrichtung eines Kontinuierlichen Verbesserungsprozesses (KVP), um Gefahren und Risiken aus der Einzelprojektbetrachtung auf ihre Wiedereintrittswahrscheinlichkeit in anderen Projekten zu bewerten und gegebenenfalls systematisch zu beheben.

Arbeitsgesetze im Aushang

Empfängerkreis

- Leiter Personal bzw. personalverantwortliche Bereiche von Kreditinstituten

Hintergrund

Für Betriebe bestehen arbeitsrechtliche Pflichten zum „Aushang am Schwarzen Brett".

Aushangpflichtige Gesetze bzw. Normen sind das AGG, § 61b ArbGG, ArbZG, §§ 611 ff. BGB, MuSchG, JArbSchG, UVV sowie die Verordnung über den Verkauf bestimmter Waren an Sonn- und Feiertagen.

Es besteht nur für solche Gesetze eine Aushangpflicht, die auf das Institut Anwendung finden. Erfolgt beispielsweise keine Beschäftigung von Jugendlichen, ist der Aushang des JArbSchG nicht erforderlich.

Die Aushänge müssen zumindest in jedem Gebäude des Instituts erfolgen. Alternativ kann der Aushang auch über das Intranet erfolgen, da auch dieses „innerhalb des Instituts" befindlich ist. Dort sollte ein „Schwarzes Brett" eingerichtet werden, auf dem die relevanten Gesetze und Normen gespeichert sind und auf das alle Mitarbeiter Zugriff haben. Von einer Verlinkung des betriebseigenen Servers auf eine Website mit Gesetzestexten im Internet ist aus sicherheitstechnischen und aus arbeitsrechtlichen Gründen abzuraten.

Im Falle einer wesentlichen Änderung eines Gesetzes hat der Arbeitgeber den Mitarbeitern ein vollständiges, aktuelles Gesetz zur Verfügung stellen. Der Verstoß gegen diese Aushangpflicht ist bußgeldbewährt.

Unterweisungen und Schulungen:

Über die Verpflichtung zum Aushang hinaus bestehen auf der Grundlage einzelner Gesetze Unterweisungspflichten des Arbeitgebers:

- Jugendarbeitsschutzgesetz (JArbSchG): Bei regelmäßig mindestens drei jugendlichen Arbeitnehmern muss der Arbeitgeber vor Beschäftigungsbeginn auf die Gefahren der Arbeit hinweisen und über Sicherheitsvorkehrungen und Maßnahmen bei Schäden informieren.
- Allgemeines Gleichbehandlungsgesetz (§ 12 (1) AGG): Der Arbeitgeber wird verpflichtet, die „erforderlichen Maßnahmen zum Schutz vor Benachteiligungen wegen eines in § 1 genannten Grundes (Rasse oder ethnischer Herkunft, des Geschlechts, der Religion oder Weltanschauung, einer Behinderung, des Alters oder der sexuellen Identität) zu treffen". Dieser Schutz umfasst auch vorbeugende Maßnahmen, wie z. B. Schulungen. Hierbei handelt es sich um eine „Soll-Vorschrift", Konsequenzen wie z. B. Bußgelder sind nicht normiert.

Handlungsbedarf

- Prüfung, ob alle vorgeschriebenen Aushänge an Schwarzen Brettern oder im Intranet vorhanden sind, gegebenenfalls Ergänzung oder Aktualisierung der Aushänge;
- Prüfung, ob Zuständigkeiten geklärt sind und ein Prozess zur regelmäßigen Aktualisierung vorgesehen ist, gegebenfalls Definition und Implementierung eines solchen Prozesses;
- Prüfung, ob Zuständigkeiten für Pflichtunterweisungen/Schulungen geklärt sind, gegebenenfalls. Festlegung der Zuständigkeiten und Einführung eines Überwachungsmechanismus;
- Prüfung, ob die vorgeschriebenen Unterweisungen/Schulungen erfolgt sind , gegebenenfalls Durchführung dieser Unterweisungen.

Beratungsangebote und weitere Dienstleistungen (Auszug)

- Umsetzung BCBS 239 Risikoreporting
- SREP Quick Scan
- Simulation und Change Management einer Sonderprüfung nach § 44 KWG
- Umsetzung Asset Encumbrance
- Optimierungsprozesse im Rahmen von aufsichtsrechtlichen Umsetzungsprojekten
- Rechtliche Gestaltungsberatung (CASIS Rechtsanwaltsgesellschaft)
- Marken– und Lizenzanmeldungen (CASIS Rechtsanwaltsgesellschaft)

Aus unserem Seminar- und Workshop-Angebot (Auszug)

- Aktuelle Hinweise für die Gesamtprüfungsplanung der Internen Revision 2016
- IT-Prüfung
- MaRisk 6.0
- Aufsichtsenglisch für nationale/lokale Banken
- § 44 KWG reloaded—SREP, AQR, Challenger Modell in der Bankpraxis
- Gestaltungsansätze und Fallstricke: Wertberichtigungen im Straf-, Handels-, Steuer– und Aufsichtsrecht
- Zielgruppenorientierte Seminare für Aufsichtsrecht, z. B. Aufsichtsrecht für
  - Mitarbeiter in der Organisation
  - Mitarbeiter der IT-Abteilung
  - Mitarbeiter des Personalbereichs
  - Mitarbeiter in Marktbereichen
  - Mitarbeiter in Marktfolgebereichen (Marktfolgen Passiv/Aktiv, Zahlungsverkehr)

V. Impressum

Herausgeber dieser Ausgabe sind:

CASIS Heimann Buchholz Espinoza
Partnerschaft
Wirtschaftsprüfungsgesellschaft

Esplanade 41
20354 Hamburg
T: +49 40 80 80 110 20
F: +49 40 80 80 110 29
E-Mail: info@casis-wp.de

CASIS
Rechtsanwaltsgesellschaft mbH

Esplanade 41
20354 Hamburg
T: +49 40 80 80 110 24
F: +49 40 80 80 110 29
E-Mail: s.beiersdorfer@casis-wp.de

Wenn Sie Fragen zu unseren Themen haben und weitergehende Hinweise wünschen, freuen wir uns auf Ihre Kontaktaufnahme.

Dr. Antje Buchholz
a.buchholz@casis-wp.de

Redaktionsschluss: 08.01.2015

CASIS Newsletter im Online-Abo unter **www.casis-wp.de/aktuelles**