Checkliste zur Prüfung/Kontrolle der Einhaltung

der Regelungen der BAIT

Inhaltsverzeichnis

1.0 IT Management 1.0

Die vorliegenden Dokumente soll im Rahmen der Governance dazu beitragen, dass die interne Revision durch ihre Prüfungshandlungen sicherstellen kann, dass die BAIT im Unternehmen formal beachtet werden. Die einzelnen Checklisten geben einen Überblich über die aufsichtsrechtlichen Anforderungen der BAIT und des AT 7.2 der MaRisk. Die einzelne Unterlage können auch von den Fachverantwortlichen zur eigenen Kontrolle herangezogen werden. Im Rahmen der SREP- Mechanismen ist für das Institut weiterhin die Vorgehensweise der Aufsichtsbehörden (NCA) von entscheidender Bedeutung.

Die Kenntnis und Beachtung der Leitlinien für die IKT-Risikobewertung im Rahmen des aufsichtlichen Überprüfungs- und Bewertungsprozesses (SREP) ist von wesentlicher Bedeutung für das Institut, auch wenn die Bank nicht Adressat der Leitlinie ist.

Die Leitlinie legen fest, was nach Ansicht der EBA angemessene Aufsichtspraktiken innerhalb des Europäischen Finanzaufsichtssystems sind oder wie das Unionsrecht in einem bestimmten Bereich anzuwenden ist. Dazu sollten die zuständigen Behörden gemäß Artikel 2 Absatz 4 der Verordnung (EU) Nr. 1093/2010 die an sie gerichteten Leitlinien in geeigneter Weise in ihre Aufsichtspraktiken (z. B. durch Änderung ihres Rechtsrahmens oder ihrer Aufsichtsverfahren) integrieren, einschließlich der Leitlinien in diesem Dokument, die in erster Linie an Institute gerichtet sind.

2.0 Dokumente der Unterlage zum IT- Management

Nachstehende Dokumente enthält das Paket zum IT Management:

1. IT-Strategie - 6 Seiten
2. IT Governance – 4 Seiten
3. Informationsrisikomanagement- 3 Seiten
4. Informationssicherheitsmanagement- 5 -Seiten
5. Benutzerberechtigungen – 6 Seiten
6. IT-Projekte, Anwendungsentwicklung

a. IDV Anwendungsmanagement – 10 Seiten
b. Patchversorgung 3 Seiten
c. Test und Freigabeverfahren einer erworbenen Software 7Seiten
d. Reporting oder IDA Abfrage - 6 Seiten

BEISPIELSEITEN

7. IT Betrieb – 6 Seiten
8. Auslagerungen und sonstiger Fremdbezug – 3 Seiten
9. MaRisk Anforderungen – 5 Seiten
10. IKT Risikopositionen 15 Seiten

11. Prüfungsbericht IT Management 23 Seiten

Die Unterlagen stellen keine Gewähr für eine korrekte Prüfung dar.

BEISPIELSEITEN

3.0 Beispielseiten Informationsrisikomanagement

Nr.	Mindestanforderungen[1]	Erläuterungen *(Nennung der Quelle)*	Anforderung ist erfüllt:
9	Die Bestandteile eines Systems zum Management der Informationsrisiken sind unter Mitwirkung aller maßgeblichen Stellen und Funktionen kompetenzgerecht und frei von Interessenkonflikten umgesetzt Eingebunden wurden insbesondere nebenstehende Bereiche:	Eingebundene Bereiche:	☐ Ja
10	Besteht ein Überblick über die Bestandteile des festgelegten Informationsverbundes (geschäftsrelevante Informationen, Geschäftsprozesse, IT-Systeme sowie Netz- und Gebäude-infrastrukturen)	Hierzu bestehen in der Bank Nachweise über (z.B. eine Softwareanwendung)	☐ Ja
10	Abhängigkeiten sind definiert		☐ Ja
10	Schnittstellen sind bekannt und wurden berücksichtigt		☐ Ja
11	Methodik zur Ermittlung des Schutzbedarfs	Nennung des Standards (z.B. die SOIT)	☐ Ja
12	Die Anforderungen des Instituts zur Umsetzung der Schutzziele in den		☐ Ja

[1] Häufig werden softwarebasierte Software unter Beteiligung von Beratungsgesellschaften eingesetzt. Auf diese Systeme ist dann zu reflektieren.

	Schutzbedarfskategorien sind festgelegt und dokumentiert (Sollmaßnahmenkatalog).		
13	Die Risikoanalyse auf Basis der festgelegten Risikokriterien ist auf Grundlage eines Vergleichs der Sollmaßnahmen mit den jeweils wirksam umgesetzten Maßnahmen erfolgt.		☐ Ja
13	Sonstige risikoreduzierende Maßnahmen aufgrund unvollständig umgesetzter Sollmaßnahmen werden wirksam koordiniert, dokumentiert, überwacht und gesteuert.		☐ Ja
13	Die Ergebnisse der Risikoanalyse wurden genehmigt und in den Prozess des Managements der operationellen Risiken überführt.		☐ Ja
13	Die Risikokriterien beinhalten	☐ Bedrohungen ☐ Schadenpotential ☐ Schadenshäufigkeit ☐ Riikoappetit	
14	Die Geschäftsleitung wird regelmäßig, mindestens jedoch vierteljährlich, insbesondere über die Ergebnisse der Risikoanalyse sowie Veränderungen an der Risikosituation unterrichtet	Datum der letzten Berichterstattungen:	☐ Ja

BEISPIELSEITEN

4.0 Beispielseiten Test und Freigabeverfahren

Inhalte des zentralen Registers gemäß Tz 44 der BAIT	
Name und Zweck der Anwendung	
Versionierung, Datumsangabe	
Fremd- oder Eigenentwicklung	
Fachverantwortlicher MA	
Technisch verantwortlicher MA	
Technologie	z.B. Office mit VBA Programmierung

Testinhalte Tz 41 der BAIT	
Funktionalität der Anwendung	☐ Ja
Sicherheitskontrollen	☐ Ja
Systemleistung unter verschiedenen Bedingungen (Stresssbelastungsszenarien)	☐ Ja

Testdokumentation Tz 41 der BAIT	
Testfallbeschreibung	
Parameter des Testfalls wurden festgehalten	
Testdaten wurden gesichert	
Ergebnis des Tests	
Maßnahmen aufgrund des Tests	

BEISPIELSEITEN

5.0 Beispielseiten IT Betrieb

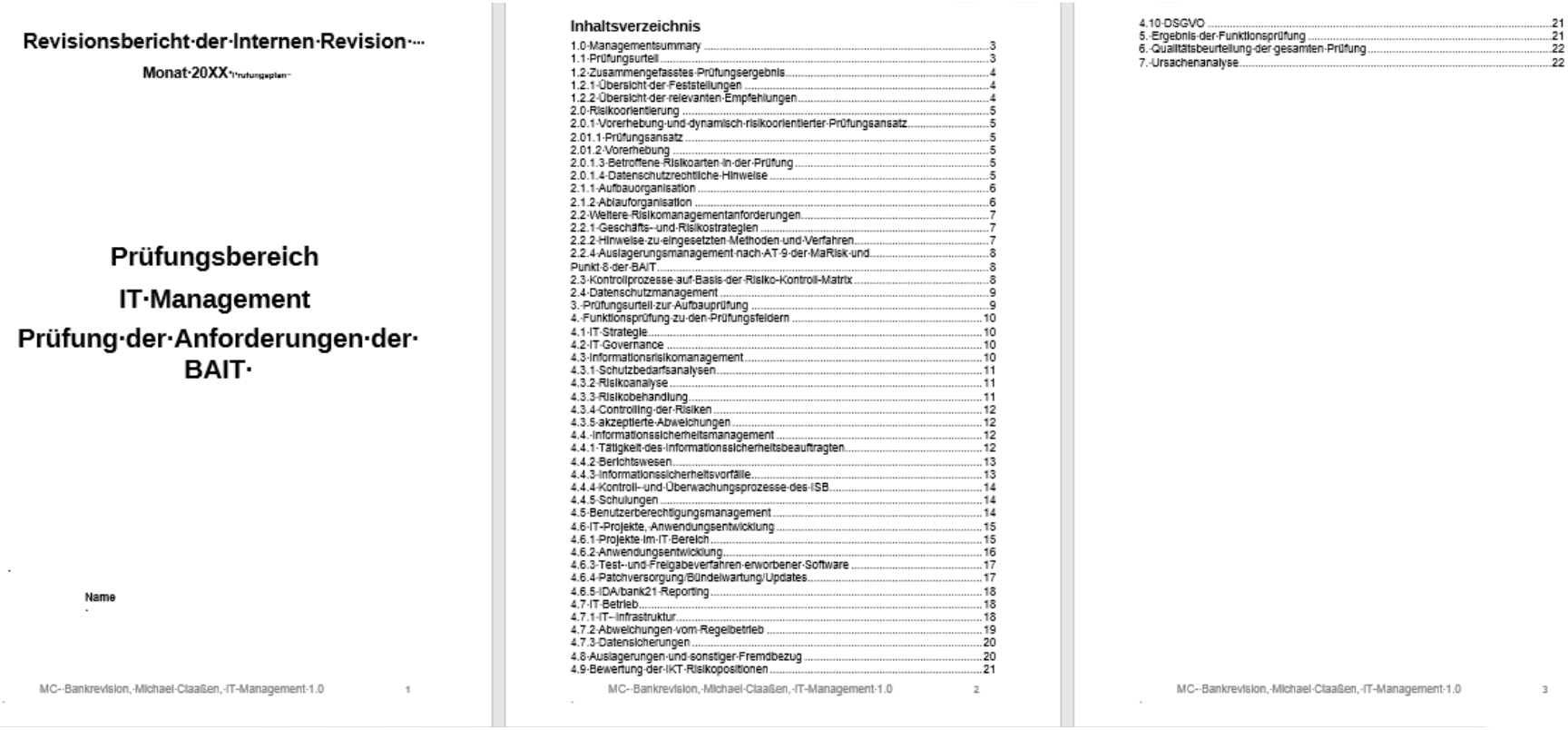
Nr.	Mindestanforderungen[2]	Erläuterungen	Anforderung ist erfüllt
46	Die Komponenten der IT-Systeme sowie deren Beziehungen zueinander werden in geeigneter Weise verwaltet, und die hierzu erfassten Bestandsangaben regelmäßig sowie anlassbezogen aktualisiert.	Letzte Aktualisierungen des IT-Dienstleisters *Nachweise und Kontrollhandlungen betrachten*	☐ Ja
46	Zu den Bestandsangaben zählen insbesondere		
	Bestand und Verwendungszweck der Komponenten der IT-Systeme mit den relevanten Konfigurationsangaben		☐ Ja
	Standort der Komponenten der IT-Systeme	*z.B. Hardwareaustausch, Wechsel Betriebsssystem, usw.*	☐ Ja

[2] Auf die Unterlagen des IT Dienstleisters wird verwiesen.

	Aufstellung der relevanten Angaben zu Gewährleistungen und sonstigen Supportverträgen (ggf. Verlinkung)	*Vertragsspiegel mit Servicevereinbarungen*	☐ Ja
	Angaben zum Ablaufdatum des Supportzeitraums der Komponenten der IT-Systeme	*Insbesondere Freigaben des IT Dienstleisters bzw. Support für erworbene Software*	☐ Ja
	Akzeptierter Zeitraum der Nichtverfügbarkeit der IT-Systeme sowie der maximal tolerierbare Datenverlust.	*Siehe Ergebnisse BCM*	☐ Ja
47	Das Portfolio aus IT-Systemen wird angemessen gesteuert: Hierbei werden auch die Risiken aus veralteten IT-Systemen berücksichtigt (Lebens-Zyklus Management).	Anzahl der AP/Systeme *Abkündigung von Systemen, usw.*	☐ Ja
48	Die Prozesse zur Änderung von IT-Systemen sind abhängig von Art, Umfang, Komplexität und Risikogehalt ausgestaltet und umgesetzt. *Dies gilt ebenso für Neu- bzw. Ersatzbeschaffungen von IT-Systemen sowie für sicherheitsrelevante Nachbesserungen (Sicherheitspatches).*		
48	Ergaben sich nachs[illegible]nde Prozesse		
	Funktionserweiterungen oder Fehlerbeheb[illegible]n Software-Komponenten	*Siehe z.B. Updates, Releaseänderungen Werden diese zeitnah eingespielt?*	☐ Ja
	Datenmigrationen		☐ Ja
	Änderungen an Konfigurationseinstellungen von IT-Systemen	*s.o.*	☐ Ja
	Austausch von Hardware-Komponenten (Server, Router etc.)		☐ Ja
	Einsatz neuer Hardware-Komponenten Umzug der IT-Systeme zu einem anderen Standort.	*s. auch obige Fragen*	☐ Ja

BEISPIELSEITEN

6.0 Inhaltsverzeichnis Prüfungsbericht



Revisionsbericht·der·Internen·Revision·…

Monat·20XX·Prüfungsplan·

Prüfungsbereich

IT·Management

Prüfung·der·Anforderungen·der·BAIT·

Name

MC-·Bankrevision,·Michael·Claaßen,·IT-Management·1.0 1

Inhaltsverzeichnis

MC-·Bankrevision,·Michael·Claaßen,·IT-Management·1.0 2

MC-·Bankrevision,·Michael·Claaßen,·IT-Management·1.0 3

7.0 Hinweise

Es handelt sich um Musterseiten aus den Dokumenten zum IT-Management 1.0 von MC-Banksoftware von Michael Claaßen, Herrenstein 52, 48317 Drensteinfurt

Tel.: 02387 941142
Fax.: 02387 919838
E-Mail: info@mc-bankrevision.deMichel Claaßen, www.mc-banksoftware.de

Michael Claaßen
Herrenstein 52
48317 Drensteinfurt

Tel.: 02387 941142
Fax.: 02387 919838
E-Mail: info@mc-bankrevision.de

BEISPIELSEITEN