Protokoll

zur Sitzung des Fachgremiums IT am Freitag, 20.05.2016, 10:30 Uhr bis 16:00 Uhr im Hause der Deutschen Bundesbank, Frankfurt am Main

TOP 1: Begrüßung und Vorstellung

Der Co-Vorsitzende begrüßte die Teilnehmer. Er wies darauf hin, dass TOP 2 einen wichtigen TOP dieser Sitzung darstelle. Dann erfolgte eine Vorstellungsrunde.

TOP 2: BAIT - Ausgangslage, Zielsetzung und weiteres Vorgehen

Ein Vertreter der Aufsicht führte aus, dass im Rahmen der heutigen Sitzung eine Diskussion der Themenbereiche IT-Strategie und Informationsmanagement geplant sei (vgl. Anlage 2).

Ein Vertreter der Kreditwirtschaft fragte mit Bezug auf Folie 5 der Präsentation, ob geplant sei, auch andere Themenbereiche der BAIT im Rahmen dieses Forums zu diskutieren. Seitens der Aufsicht wurde das bejaht und erläutert, dass die einzelnen Themen nicht in Unterarbeitsgruppen sondern fair und transparent im Rahmen des Fachgremiums IT besprochen und beschlossen werden sollen, insbesondere auch im Hinblick auf die bezüglich der kommenden Sitzung vorgesehene Einladung von Vertretern kleinerer Banken. Seitens der Aufsicht wird ferner ausgeführt, die BAIT sei ursprünglich als eigenständiges Werk – unabhängig von den MaRisk und zu diesen parallel als Konkretisierung des § 25a Abs. 1 KWG in Bezug auf die Anforderungen der IT der Institute - gedacht gewesen. Nunmehr sei das Verständnis jedoch dasjenige einer Konkretisierung der MaRisk in Bezug auf die dort nicht oder nicht abschließend geregelten Sachverhalte mit IT-Bezug.

Auf eine Anmerkung aus der Kreditwirtschaft, zu ebendieser Frage der hierarchischen Einordnung der BAIT, führte ein Vertreter der Aufsicht ergänzend aus, dass die BAIT nach wie vor als auf derselben Stufe wie die MaRisk angesiedelt angesehen würden. Es gehe in der Sache insbesondere darum, Anforderungen zu formulieren, welche an das Management der Banken, insbesondere die Geschäftsleitung, gerichtet und für dieses verständlich seien, unabhängig davon, ob das Management über IT-Fachkenntnisse verfüge oder nicht. Gegenüber einem Vertreter der Kreditwirtschaft, der die Bedeutung des Proportionalitätsansatzes unterstreicht, erläutert ein Vertreter der Aufsicht, dass grundlegende Anforderungen notwendiges Element der Proportionalität sind und das Proportionalitätsprinzip analog der MaRisk Anwendung findet.

Der Vertreter der Kreditwirtschaft erklärte, soweit von „Beschließen" der in dieser Sitzung zu besprechenden Themenbereiche der BAIT die Rede sei, gelte der Gremienvorbehalt für die einzelnen kreditwirtschaftlichen Verbände. Aussagen im Rahmen der heutigen Sitzung können daher nur beratenden Charakter haben.

Der Co-Vorsitzende führte aus, dass selbstverständlich das formale Konsultationsverfahren am Ende des Prozesses gesetzt sei und den Verbänden und Banken ausreichende Frist zur Kommentierung eingeräumt werden würde. Mit „Beschließen" im Rahmen der heutigen Sitzung sei nicht gemeint gewesen, dass heute abschließend und letztverbindlich über die

zur Diskussion gestellten Themenbereiche befunden werden solle. Vielmehr sei Zweck der heutigen Sitzung, zum frühestmöglichen Zeitpunkt Feedback von Seiten der Industrie und Wissenschaft zu bekommen. Ein Vertreter der Aufsicht ergänzte, dass man sich bewusst sei, dass die beiden heute zu diskutierenden Themen – wie alle Einzelthemen - auch noch einmal im Gesamtzusammenhang der BAIT betrachtet werden müssten.

Ein Vertreter der Kreditwirtschaft merkte an, das beschlossene Mandat des Fachgremiums stehe der Veröffentlichung von Sitzungsprotokollen entgegen. Der Co-Vorsitzende erläuterte, dass die Aufsicht in der Einladung zur Fachgremiumssitzung den Arbeitsmodus für die Erarbeitung und Diskussion der BAIT beschrieben und darauf hingewiesen hat, dass Beratungen des Fachgremiums zur BAIT nach außen transparent gemacht werden.

Ein Vertreter der Kreditwirtschaft äußerte, vor dem Hintergrund, dass hier unter Änderung der bisher beabsichtigten Vorgehensweise in die fachliche Diskussion eingestiegen werden solle, benötige man die entsprechenden Unterlagen mit mehr Vorlauf (mindestens 14 Tage vor der Sitzung). Ein Vertreter der Aufsicht erklärte, die nunmehrige Vorgehensweise habe den Vorteil, dass zunächst einmal die einzelnen Themen so, wie die Aufsicht sich diese vorstellten, präsentiert werden und mit den jeweiligen Fachleuten aus den Instituten und den Verbandsvertretern ausführlich diskutiert – auch im Sinne von Praxistauglichkeit - werden könnten. Ein anderer Vertreter der Aufsicht führte ergänzend aus, dass die Diskussion der Themen im Fachgremium IT den Vorteil habe, dass man bereits an dem Werk, welches anschließend in die Konsultation geht, mitgearbeitet habe.

Auf die Frage eines Vertreters der Kreditwirtschaft, inwieweit die EZB bereits involviert sei, erklärte ein Vertreter der Aufsicht, dass seitens der Aufsicht beabsichtigt sei, sich zeitnah an DG IV der EZB zu wenden. Auf die Frage eines Vertreters der Kreditwirtschaft, ob die Notwendigkeit der Kompatibilität der BAIT mit den SSM-Vorgaben berücksichtigt werde, erklärte ein Vertreter der Aufsicht, es werde ein Abgleich der Anforderungen mit den entsprechenden Anforderungen des SSM Supervisory Manuals erfolgen.

Auf die Frage eines Vertreters der Kreditwirtschaft, wie sich die Verzahnung mit den MaRisk im Hinblick auf deren mögliche zukünftige Änderungen gestalten werde, führte ein Vertreter der Aufsicht aus, dass dem mittels jeweiliger dynamischer Verweisungen auf die MaRisk in den Obersätzen zu den einzelnen Themen Rechnung getragen werde; es sei ein Gleichlauf von etwaigen Änderungen der MaRisk und der BAIT vorgesehen. Ein anderer Vertreter der Aufsicht erklärte, für sein Haus gelte, dass die Befassung mit beiden Regelwerken aufbauorganisatorisch sichergestellt sei.

Auf die Frage von eines Vertreters der Kreditwirtschaft, ob die als „Konkretisierung" der MaRisk bezeichnete Funktion der BAIT dahin zu verstehen sei, dass durch die BAIT keine neuen Anforderungen eingeführt werden würden, erläuterte ein Vertreter der Aufsicht, dass dem so sei, es sei denn, die Vertreter der Kreditwirtschaft würden Regelungsbedarf äußern, dessen Umsetzung die Schaffung neuer Anforderungen erforderlich mache. Ein anderer Vertreter der Kreditwirtschaft ergänzte, man müsse zwischen der logischen Dimension (BAIT als Rundschreiben auf Ebene der MaRisk) und der inhaltlichen Dimension (BAIT als Konkretisierung der MaRisk) unterscheiden.

TOP 3: IT-Strategie

Ein Vertreter der Aufsicht trug zum Thema IT-Strategie vor.

Den Vertretern der Kreditwirtschaft wurde erläutert, dass

- die IT-Strategie Teil der Geschäftsstrategie sei;
- die IT-Strategie nicht notwendig im selben Dokument wie die Geschäftsstrategie enthalten sein müsse. Vielmehr sei entscheidend, dass auch bezüglich der Weiterentwicklung/Fortschreibung der IT-Strategie ein adäquater Strategieprozess in den Häusern durchlaufen wird.
- die IT-Strategie die strategischen Leitlinien zur IT beinhalten solle, wohingegen Ausführungen zur operativen Umsetzung in nachgeordneten Regelwerken enthalten sein sollten;
- die auf der Erläuterungsseite des Modulentwurfs aufgeführten wesentlichen Bestandteile als Mindestanforderungen zu verstehen seien. Vor diesem Hintergrund kam man überein, das Wort „exemplarisch" zu streichen.
- das Proportionalitätsprinzip im Rahmen der IT-Strategie insbesondere bedeute, dass dies für kleinere Häuser Anwendung findet und sich für größere Häuser die Notwendigkeit weiterer Bestandteile oder einer ausführlicherer Darstellung der im Entwurf als „wesentlich" ausgewiesenen Bestandteile ergeben könne.

Sodann wurde der Text des Entwurfs zur „IT-Strategie" im Einzelnen diskutiert. Es wurden diverse Änderungen (z.B. geänderte Aufteilung zwischen Anforderung und Erläuterungen sowie Ergänzung von Beispielen) als sinnvoll bzw. wünschenswert angesehen.

TOP 4: Informationsrisikomanagement

Es fand eine Diskussion des Entwurfs zum Themenbereich „Informationsrisikomanagement" statt.

Grundlegend wurde seitens der Teilnehmer der Aspekt artikuliert, dass eine Behandlung des „Informationsrisikomanagements" insofern über den Umfang der BAIT hinausgehe, als damit begrifflich auch das Risikomanagement bezüglich nur in physischer Form vorliegender Informationen (Papierdokumente) bzw. physischer Einrichtungen (Rechenzentren) erfasst sei. Es wurden mögliche gangbare Wege zur Behandlung dieses Aspekts diskutiert. Ein Vertreter der Aufsicht wies darauf hin, dass international und zunehmend auch national (BSI) der Begriff „Informations…-" statt „IT…" im Kontext genutzt werde.
Man kam überein, dass sich die Aufsicht mit dieser Thematik im Hinblick auf den Umfang der BAIT und die Konsistenz der Begrifflichkeit innerhalb derselben grundlegend befassen und einen diesbezüglichen Vorschlag erarbeiten werde.

Sodann wurde der Text des Entwurfs zur „Informationsrisikomanagement" im Einzelnen diskutiert. Seitens der Teilnehmer wurde angemerkt, dass der Grundsatz der Methodenfreiheit gewährleistet bleiben muss. Es wurden diverse Änderungen (z.B. geänderte Aufteilung zwischen Anforderung und Erläuterungen sowie diverse Anpassungen bei der Formulierung) als sinnvoll bzw. wünschenswert angesehen.

TOP 5: Sonstiges

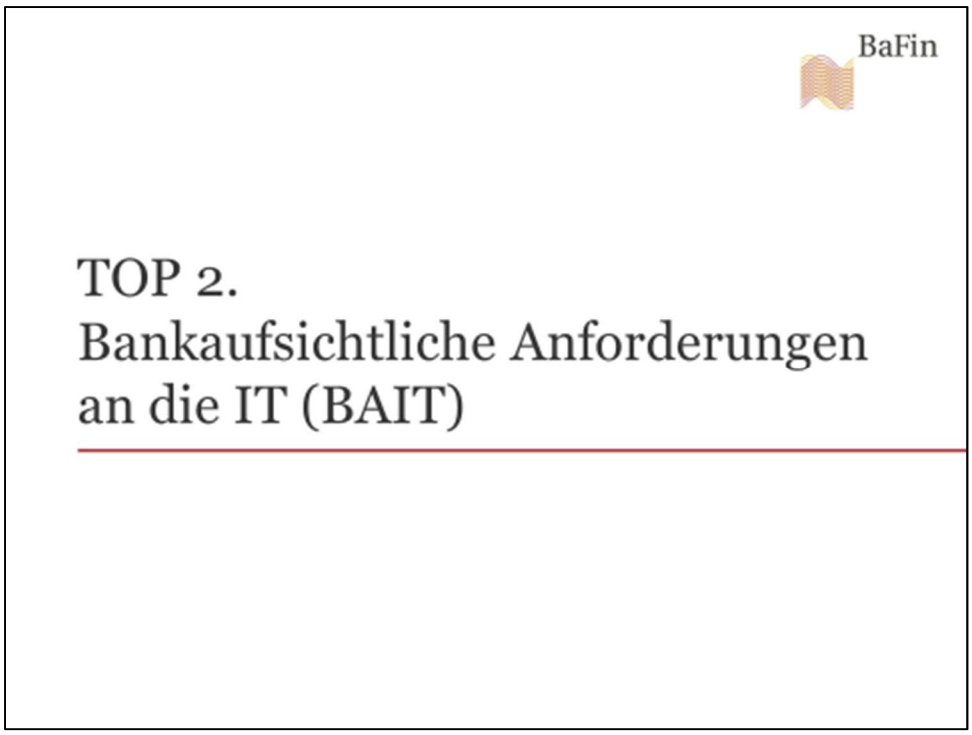
Der Co-Vorsitzende führte aus, dass die diskutierten und im Änderungsmodus festgehaltenen Modifizierungen der Entwürfe zu „IT-Strategie" und „Informationsrisikomanagement"

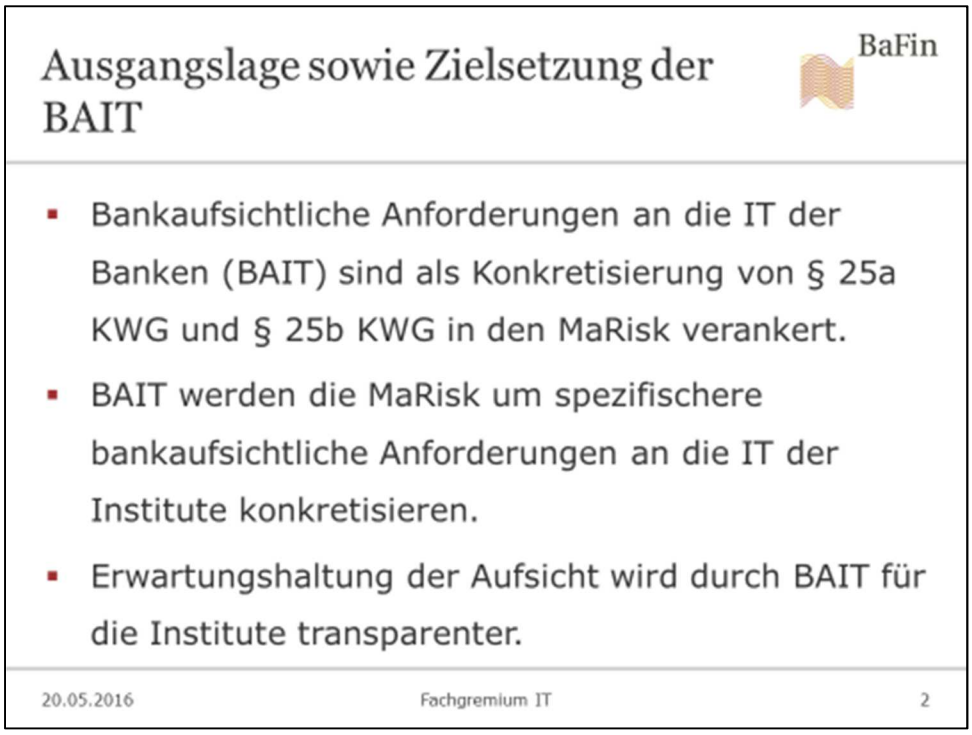
unter den Teilnehmern zur Information zirkuliert werden. Der Termin für die nächste Sitzung sei zunächst noch aufsichtsintern abzustimmen. Tendenziell könne sich im Hinblick auf den Zeitplan für den Eintritt in die Konsultation die Notwendigkeit ergeben, im Rahmen einer Sitzung ggf. mehr als zwei Themenbereiche zu diskutieren. Die Teilnehmer aus der Kreditwirtschaft zeigten sich offen für die Möglichkeit, im Sinne eines effektiven Ressourceneinsatzes ggf. zwei- oder mehrtägige Sitzungen durchzuführen.

Anlage 1: Teilnehmer

Prof. Dr. Gabi Dreo Rodosek	BW-Uni München
Hans Köster	FinanzInformatik
Dr. Andreas Abel	Fiducia & GAD IT AG
André Nash	BdB
Markus Tacke	DSGV
Dr. Carsten Eckhardt	Deutsche Bank
Dr. Brigitte Penther	HSH Nordbank
Dr. Heino Gärtner	Nord-LB
Andreas Fichelscher	KfW
Stefan Finkenzeller	Bayern LB
Stefan Böse	DZ Bank
Sven Freisendorf	UniCredit
Thomas Kohaut	Helaba
Christopher Nolte	CoBa
Oliver Oreskowitz	LBBW
Michael Rabe	VÖB
Berit Schimm	BVR
Dr. Jens Gampe	BaFin
Renate Essler	BaFin
Dr. Sebastian Silberg	BaFin
Dr. Michael Paust (Co-Vorsitz)	Deutsche Bundesbank
Clemens Dargel	Deutsche Bundesbank
Dr. Rainer Janlewing	Deutsche Bundesbank
Anke Habicht	Deutsche Bundesbank

Anlage 2: Bankaufsichtliche Anforderungen an die IT (BAIT)





Ausgangslage sowie Zielsetzung der BAIT

BaFin

- BAIT sind in Gesamtschau mit den MaRisk risikoorientiert umzusetzen.
- Mit BAIT wird ein flexibler und praxisnaher Rahmen insbesondere für das Management der IT-Ressourcen und das IT-Risikomanagement geschaffen.
- BAIT tragen dazu bei, das unternehmensweite IT-Risikobewusstsein im Institut und gegenüber den Auslagerungsunternehmen zu erhöhen.

Aufbau der BAIT

BaFin

- Prinzipienorientiertheit und Proportionalitätsprinzip bleiben wie in der MaRisk erhalten
- Anlehnung an den Aufbau der MaRisk
- Verweise auf die MaRisk in Obersätzen

Aufbau der BAIT - Themenbereiche

BaFin

- Grundsätzlich geplante Themenbereiche:
  - IT-Governance
  - Informationssicherheits- und Informationsrisikomanagement
  - IT-Betrieb
  - IT-Auslagerung
  - IT-Revision

Weiteres Vorgehen

BaFin

- Grundsätzliche Abstimmung zum Vorgehen zwischen BaFin und der Bundesbank ist bereits erfolgt ✓
- Erste Diskussion der Themenbereiche IT-Strategie und Informationsrisikomanagement im Fachgremium IT im Mai 2016

Weiteres Vorgehen

- Inhaltliche Erarbeitung und Abstimmung weiterer Themen ab Juni 2016
- Übersendung des Konsultationsentwurfes Ende 2016
- Frühzeitige Information der EZB geplant
- Veröffentlichung des Rundschreibens zu BAIT in 2017