Andreas Abel

Die Rolle der **Rechenzentren** in der Banken-Compliance

Zur ordnungsgemäßen Geschäftsorganisation gehört gemäß § 25 a KWG unter anderem auch eine angemessene technisch-organisatorische Ausstattung des Instituts. Zu dieser technisch-organisatorischen Ausstattung zählt ebenso die eingesetzte Informationstechnologie (IT) und die zugehörige IT-Aufbau- und IT-Ablauforganisation in der Bank, die somit selbst ihren Beitrag zur Ordnungsmäßigkeit der Geschäftsorganisation und somit zur Banken-Compliance im Sinne des § 25 a Abs. 1 KWG[1] leisten muss.

Relevanz der IT

Der Relevanz der IT zur Banken-Compliance ergibt sich dabei insbesondere aus zwei Aspekten:

1. Erst durch den Einsatz von Informations-Technologie kann die Bank Gesetzes- und Regelkonformität erreichen und somit compliant sein. Beispiele hierfür sind die gesetzlichen Vorgaben aus dem Steuerrecht, die sich zum Beispiel in § 24 c KWG zum automatisierten Abruf von Kontoinformationen niedergeschlagen haben, oder auch die Vorgaben aus dem Sepa-Begleitgesetz oder dem CRD-IV-Umsetzungsgesetz, die erst mit dem Einsatz geeigneter IT-Anwendungen umsetzbar sind.

2. Der IT-Einsatz erfordert selbst wiederum die Einhaltung von spezifischen gesetzlichen, behördlichen oder privatrechtlichen Vorgaben und beinhaltet somit für die Bank als verantwortliches Unternehmen per se Compliance- und gegebenenfalls Reputationsrisiken. Beispiele hierfür sind der Datenschutz, die Regelungen im Rechtsgebiet Informationstechnologierecht, die MaRisk-Anforderungen mit IT-Bezug sowie privatrechtliche Vereinbarungen mit Software-Lieferanten zur Software-Überlassung und -Nutzung.

Ein Bankbetrieb heutiger Ausprägung ist ohne den zumindest unterstützenden Einsatz von Informationstechnologie nicht mehr darstellbar[2] und unter Compliance-Aspekten auch nicht mehr möglich, da die vom Gesetzgeber ermächtigte Exekutive selbst Spezifikationen für IT-Systeme in technischen Durchführungsstandards festschreibt.[3] Der für den Bankbetrieb erforderliche IT-Betrieb wird bei deutschen Kreditinstituten insbesondere in den großen Finanzverbünden arbeitsteilig im Eigenbetrieb und unter Nutzung von Rechenzentrumsleistungen der gruppenspezifischen IT-Dienstleister erbracht, sodass auch diese Dienstleister eine bedeutende Rolle für die Ordnungsmäßigkeit der Geschäftsorganisation der Bank und somit in der Banken-Compliance wahrnehmen.

Eine Frage der Arbeitsteilung

Die Abbildung verdeutlicht die Zusammenhänge der Arbeitsteilung zwischen einer Bank und einer Rechenzentrale:

Dr. Andreas Abel, Leiter Risiko- und Compliance Management, GAD eG, Münster

Ohne die Technik wäre ein modernes Bankgeschäft gar nicht mehr denkbar. Dementsprechend, so erläutert der Autor, ließe sich auch die Gesetzes- und Regelkonformität wie sie die Banken-Compliance mit ihren immer umfangreicheren Regelungen und ihrer beachtlichen Veränderungsgeschwindigkeit erfordert ohne die Arbeit der beteiligten Rechenzentren kaum darstellen. Dementsprechend will er die Geschäftsorganisation der Rechenzentren so aufgestellt wissen, dass sie den Banken eine angemessene Steuerung und Überwachung der ausgelagerten IT-Aktivitäten und -Prozesse ermöglicht. Zum erforderlichen Leistungsspektrum rechnet er die Sichtung und Umsetzung aller relevanten Standards. (Red.)

– Die Geschäftsprozesse der Bank basieren auf Bank-Anwendungen, die von der Bank selbst oder von einer oder mehreren Rechenzentralen als IT-Dienstleister technisch betrieben werden.

– Die Geschäftsprozesse der Bank müssen eingebettet in das Risikomanagement und abgesichert durch das Notfallkonzept durchgeführt werden.

– Das Risikomanagement und die Ordnungsmäßigkeit der Bank erfordert als Teil der Banken-Compliance unter anderen erstens eine strategische Ebene, in der auch grundlegende IT-Fragestellungen beantwortet werden, zweitens ein Risikotragfähigkeitskonzept unter Berücksichtigung von IT-Risiken als Teil der operationellen Risiken[4] sowie drittens die Einbindung der IT in die internen Kontrollverfahren der Bank, insbesondere IT-Aufbau- und Ablauforganisation, IT-Risikocontrolling, IT-Compliance, IT-Revision, IT-Organisationsrichtlinien und die Dokumentation von IT-Kontrollen und IT-Überwachungen.

– Sofern Teile der notwendigen IT-Prozesse durch die Bank selbst erbracht werden, erfordert diese IT-Eigenerstellung die Dokumentation von IT-Kontrollen und IT-Überwachungen auf der Grundlage der schriftlich fixierten IT-Aufbau- und Ablauforganisation.

– Sofern Teile der wesentlichen IT-Prozesse durch eine oder mehrere Rechenzentren beziehungsweise IT-Dienstleister im Sinne einer IT-Fremderstellung erbracht werden, ist ein geordnetes IT-Auslagerungsmanagement in der Bank erforderlich, das auf der Grundlage von geeigneten Verträgen die Überwachung, Beurteilung und Steuerung des IT-Dienstleisters beziehungsweise des Rechenzentrums als IT-Auslagerungsunternehmen übernimmt.[5]

Vor der Diskussion der besonderen Rolle der Rechenzentren in der Banken-Compliance, bedarf es in einem ersten Schritt zunächst der Klärung des Begriffes Rechenzentrum.

Interne Organisationseinheit oder rechtlich selbstständig

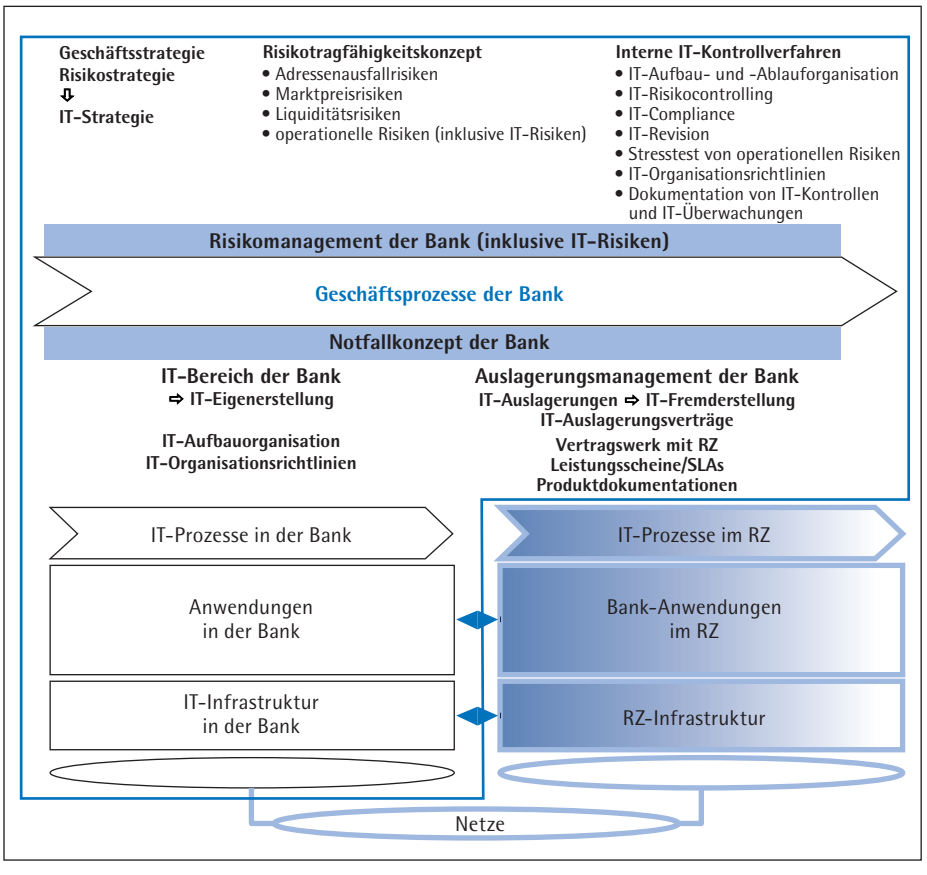
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt im Baustein B 2.9 ein Rechenzentrum wie folgt:

„Als Rechenzentrum werden die für den Betrieb von komplexen IT-Infrastrukturen (Server- und Speichersysteme, Systeme zur Datensicherung, aktive Netzkomponenten und TK-Systeme, zentrale Drucksysteme) erforderlichen Einrichtungen (Klimatechnik, Elektroversorgung, überwachende und alarmierende Technik) und Räumlichkeiten (zum Beispiel Rechnersaal, Räume für die aktiven Netzkomponenten, Technikräume, Archiv, Lager, Aufenthaltsraum) bezeichnet."[6]

Diese enge Beschreibung mit Schwerpunkt auf den Infrastrukturcharakter eines Rechenzentrums wird für diesen Beitrag weiter gefasst und umfasst neben den vom BSI beschriebenen infrastrukturellen Komponenten die für eine Bank-Anwendung erforderlichen IT-Systeme und IT-Prozesse, die von einem RZ-Betreiber in der Regel als Paket angeboten werden. Der RZ-Betrieb kann dabei in zwei grundlegend unterschiedlichen organisatorischen Strukturen eingebettet sein. Zum einen in einer internen Organisationseinheit in der Bank oder zum anderen in einer rechtlich selbstständigen Firma, die im Auftrag der Bank RZ-Leistungen erbringt.

Unter dem Compliance-Aspekt bedeutet dies für eine Bank grundlegende Unterschiede in der Einbindung des RZ-Betriebs in die eigene ordnungsgemäße Geschäftsorganisation. Im ersten Fall muss die für den RZ-Betrieb zuständige interne Organisationseinheit wie alle anderen Organisationseinheiten auch in die ordnungsgemäße Geschäftsorganisation eingebunden werden. Im zweiten Fall – bei einem rechtlich selbstständigen Unternehmen – sollte das Rechenzentrum als Nebendienstleister im Sinne § 1 Abs. 3 c KWG[7] über eine geeignete Ausgestaltung des Vertragswerkes im Sinne des § 25 a Abs. 2 KWG in Verbindung mit AT 9 Tz. 6 MaRisk auf eine eigene ordnungsgemäße Geschäftsorganisation für die ausgelagerten IT-Services verpflichtet werden.

Abbildung: Grundlegender Zusammenhang zwischen der Geschäftsorganisation einer Bank, der IT und der Zusammenarbeit mit einer Rechenzentrale



Angemessenes und wirksames Risikomanagement

Folgt man der Meinung von Kokert/Held, dass „[es keinen Bankprozess gibt], der heute nicht durch IT unterstützt wird"[8], kann man den § 25 a Abs. 2 KWG zur Verdeutlichung wie folgt umformulieren:

– „Ein Institut muss abhängig von Art, Umfang, Komplexität und Risikogehalt einer Auslagerung von (IT-Leistungen [inklusive RZ-Leistungen]) auf ein anderes Unternehmen, die für die Durchführung von Bankgeschäften, Finanzdienstleistungen oder sonstigen institutstypischen Dienstleistungen wesentlich sind, angemessene Vorkehrungen treffen, um übermäßige zusätzliche Risiken zu vermeiden.

– Eine [IT-]Auslagerung darf weder die Ordnungsmäßigkeit dieser Geschäfte und Dienstleistungen noch die Geschäftsorganisation [...] beeinträchtigen.

– Insbesondere muss ein angemessenes und wirksames Risikomanagement durch das Institut gewährleistet bleiben, welches die ausgelagerten [IT-]Aktivitäten und [IT-]Prozesse einbezieht.

– Die [IT-]Auslagerung darf nicht zu einer [Übertragung] der Verantwortung der [Geschäftsleiter] an das [IT-]Auslagerungsunternehmen führen.

– Das Institut bleibt bei einer [IT-]Auslagerung für die Einhaltung der vom Institut zu beachtenden gesetzlichen Bestimmungen verantwortlich.

– Durch die [IT-]Auslagerung darf die Bundesanstalt an der Wahrnehmung ihrer Aufgaben nicht gehindert werden; ihre Auskunfts- und Prüfungsrechte sowie Kontrollmöglichkeiten müssen in Bezug auf die ausgelagerten Aktivitäten und Prozesse auch bei einer [IT-]Auslagerung auf ein Unternehmen mit Sitz in einem Staat des europäischen Wirtschaftsraums oder einem Drittstaat durch geeignete Vorkehrungen gewährleistet werden.

– Entsprechendes gilt für die Wahrnehmung der Aufgaben der Prüfer des Instituts.

– Eine [IT-]Auslagerung bedarf einer schriftlichen Vereinbarung, welche die zur Einhaltung der vorstehenden Voraussetzungen erforderlichen Rechte des Instituts, einschließlich Weisungs- und Kündigungsrechten sowie die korrespondierenden Pflichten des [IT-]Auslagerungsunternehmens festschreibt."

Grundsätze zur Sicherstellung eines regelkonformen Verhaltens

„Unter einem Compliance-Management-System sind die auf der Grundlage der von den [Geschäftsleitern] festgelegten Ziele eingeführten Grundsätze und Maßnahmen [des Instituts] zu verstehen, die auf die Sicherstellung eines regelkonformen Verhaltens der gesetzlichen Vertreter und der Mitarbeiter des Unternehmens sowie gegebenenfalls [von Kunden, Vermittlern, Lieferanten und Dienstleistern] abzielen, das heißt auf die Einhaltung bestimmter Regeln beziehungsweise die Verhinderung von wesentlichen Verstößen".[9]

Das Compliance-Management-System unterstützt das Institut also bei der Ordnungsmäßigkeit der Geschäfte und Dienstleistungen sowie der eigenen Geschäftsorganisation.

Auf andere Rechtsräume lässt sich die Argumentation in diesem Aufsatz ebenfalls übertragen, indem die Bezüge zu deutschen Regelungen und Vorgaben gegen die entsprechenden Regelungen und Vorgaben aus dem zu betrachtenden Rechtsraum ersetzt werden.

Nach diesen Vorüberlegungen nun zu den verschiedenen Aspekten der Rolle von externen Rechenzentren als IT-Dienstleister in der Banken-Compliance: Handelt es sich bei dem zu betrachtenden Rechenzentrum um ein inländisches Unternehmen, das über eine ordnungsgemäße Geschäftsorganisation verfügt, so sollte der vorab dargestellte Zusammenhang der Geschäftsleitung bekannt sein und bereits in die Ausgestaltung der IT-Auslagerungsverträge eingeflossen sein.

Geschäftszweck eines Rechenzentrums als IT-Dienstleister für Banken muss es sein, der Bank als Kunde selbst wiederum die Ordnungsmäßigkeit der mit der IT unterstützten Geschäfte und Dienstleistungen und somit die Ordnungsmäßigkeit der Geschäftsorganisation der Bank zu ermöglichen.

Abhängig von der Ausgestaltung der konkreten IT-Auslagerung lassen sich folgende grundlegende RZ-Leistungen mit zunehmendem Leistungsumfang und zunehmender Bedeutung für die Banken-Compliance skizzieren:

Infrastructure as a Service (IaaS): Bereitstellung, Betrieb und Wartung der Gebäudeinfrastruktur (Energie, Klima, Datenleitungen) als Basis für IT-Systeme, die von der Bank bereitgestellt, betrieben und verantwortet werden.

Platform as a Service (PaaS): Bereitstellung, Betrieb und Wartung von IT-Systemen im Rechenzentrum als Plattform für Bank-Anwendungen, die von der Bank bereitgestellt, betrieben und verantwortet werden.

Software as a Service (SaaS): Bereitstellung, Betrieb und Wartung von Bank-Anwendungen als Standardsoftware im Rechenzentrum, die von der Bank genutzt werden, zugekaufte Software, die einer oder mehreren Banken bereitgestellt wird und selbst entwickelte Software, die einer oder mehreren Banken bereitgestellt wird.

Beitrag zur Banken-Compliance

Der Beitrag des Rechenzentrums zur Bank-Compliance ist abhängig vom vereinbarten Leistungsumfang und von der Beurteilung der Wesentlichkeit der vereinbarten Leistung aus Sicht der Bank. Der Zusammenhang zwischen zunehmendem Leistungsumfang und der zunehmenden Bedeutung des Rechenzentrums für die Bank-Compliance lässt sich anhand der Anforderungen aus MaRisk AT 7 „Ressourcen" gut verdeutlichen:

Leistungen im IaaS-Modell: Einhaltung „MaRisk AT 7.1 Personal" für das Personal im Rechenzentrum, Einhaltung „MaRisk AT 7.2 Technisch-organisatorische Ausstattung" (insbesondere Tz. 1, 2 und 3) für die bereitgestellte RZ-Infrastruktur und Einhaltung „MaRisk AT 7.3 Notfallkonzept" für die RZ-Infrastruktur.

Leistungen im PaaS-Modell: Einhaltung „MaRisk AT 7.1 Personal" für das Personal im Rechenzentrum, Einhaltung „MaRisk AT 7.2 Technisch-organisatorische Ausstattung" (insbesondere Tz. 1, 2 und 3) für die bereitgestellten IT-Systeme und die zugrunde liegende RZ-Infrastruktur und Einhaltung „MaRisk AT 7.3 Notfallkonzept" für die IT-Systeme und die RZ-Infrastruktur.

Leistungen im SaaS-Modell: Einhaltung „MaRisk AT 7.1 Personal" für das Personal im Rechenzentrum, Einhaltung „MaRisk AT 7.2 Technisch-organisatorische Ausstattung" (Tz. 1-4) für die bereitgestellten Bank-Anwendungen und die dafür erforderlichen IT-Systeme sowie die zugrunde liegende RZ-Infrastruktur, Einhaltung „MaRisk AT 7.3 Notfallkonzept" für die Bank-Anwendungen, IT-Systeme und die RZ-Infrastruktur, Einhaltung „MaRisk AT 8.2 Änderungen betrieblicher Prozesse oder Strukturen". Hier insbesondere: „Vor wesentlichen Veränderungen [...] in den IT-Systemen hat das Institut die Auswirkungen der geplanten Veränderungen auf die Kontrollverfahren und die Kontrollintensität zu analysieren. [...]"

MaRisk-Anforderungen mit Relevanz für die Geschäftsorganisation

Abhängig von der Beurteilung der Wesentlichkeit der IT-Auslagerung durch die beauftragende Bank und der konkreten Vertragsgestaltung können zum Beispiel noch folgende MaRisk-Anforderungen Relevanz für die Geschäftsorganisation des Rechenzentrums erhalten: AT 4.3 Internes Kontrollsystem (AT 4.3.1 Aufbau- und Ablauforganisation, AT 4.3.2 Risikosteuerungs- und –controllingprozesse); AT 4.4 besondere Funktionen (AT 4.4.1 Risikocontrolling-Funktion, AT 4.4.2 Compliance-Funktion, AT 4.4.3 Interne Revision); AT 5 Organisationsrichtlinien; AT 6 Dokumentation; AT 9 Outsourcing; BT 1 besondere Anforderungen an das interne Kontrollsystem; BTR 4 Operationelle Risiken; BT 2 besondere Anforderungen an die Ausgestaltung der Internen Revision.

Das Rechenzentrum sollte die eigene Geschäftsorganisation derart ausgestalten, dass die genannten Anforderungen erfüllt werden, um der Bank als Kunden eine angemessene Steuerung und Überwachung der an das Rechenzentrum ausgelagerten IT-Aktivitäten und IT-Prozesse zu ermöglichen. Hierzu gehört unter anderem die Bereitstellung von geeigneten Informationen an das Auslagerungsmanagement der Bank

– zur Leistungserfüllung auf Grundlage von festgelegten Leistungsscheinen beziehungsweise Service-Level-Agreements (SLA),

– vierteljährliche IT-Risikoberichte für die ausgelagerten Leistungen,

– die Notfalltestplanung und die Berichte über durchgeführte Notfalltests,

– Prüfungsberichte der internen Revision und

– Prüfungsberichte von Wirtschaftsprüfern zur Ordnungsmäßigkeit der ausgelagerten Leistungen (zum Beispiel auf Grundlage des IDW PS 951).

Das Auslagerungsmanagement der Bank sollte diese Informationen zum einen zur Überwachung, Beurteilung und Steuerung des Auslagerungsunternehmens gemäß MaRisk AT 9 Tz. 7 nutzen und zum anderen an die eigene Organisationsabteilung, die eigene Risikocontrolling- und die Compliance-Funktion sowie an die eigene interne Revision weiterleiten, damit diese Informationen in die Steuerungs-, Kontroll- und Überwachungsprozesse der Bank in geeigneter Form einfließen können.

Informationstechnologierecht

Eine besondere Rolle haben Rechenzentren für das Rechtsgebiet „Informationstechnologierecht", das insbesondere die Kernkompetenz als IT-Dienstleister berührt. Hier kommt neben der Leistungserbringung auch die Beratungsleistung gegenüber Banken hinzu, damit aus diesem Rechtsgebiet resultierende Compliance- und gegebenenfalls Reputationsrisiken für die Banken vermieden werden können. Hierzu gehören insbesondere

– das „Recht des Datenschutzes und der Sicherheit der Informationstechnologien […],

– das Recht der Kommunikationsnetze und -dienste, insbesondere das Recht der Telekommunikation und deren Dienste"[10] sowie

– Lizenzvereinbarungen.

Neben dieser Informations- und Beratungsrolle hat ein Rechenzentrum, das gleichzeitig auch Software-Haus ist, noch zusätzlich die Aufgabe, bei der eigenen Softwareentwicklung und -weiterentwicklung die fachlichen Vorgaben des Gesetzgebers und von Behörden sowie die technischen Vorgaben von Behörden als Anforderungen zu berücksichtigen und in den eigenen Produkten zu realisieren.

Systematische Bearbeitung im Software-Entwicklungsprozess

Insbesondere gesetzliche Anpassungen im Steuer- (zum Beispiel Abgeltungssteuer) sowie im Banken- und Kapitalmarktrecht (zum Beispiel Sepa-Begleitgesetz, CRD-IV-Umsetzungsgesetz) führen häufig zu Anpassungsbedarf bei Banken-Anwendungen mit zum Teil erheblichen Auswirkungen auf bestehende IT-Lösungen. Hier besteht für die Rechenzentralen aufgrund der vom Gesetzgeber zum Teil knapp bemessenen Umsetzungszeiträume eine große Herausforderung, die insbesondere nach MaRisk AT 7.2 Tz. 3 und 4 gestellten Anforderungen einzuhalten. Dies wird darüber hinaus erschwert, dass die näheren Ausführungsbestimmungen seitens der Behörden zum Beispiel über „Art und Umfang und über die zulässigen Datenträger, Übertragungswege und Datenformate"[11] ebenfalls ihre Zeit benötigen bis eine hinreichende technische Spezifikation verbindlich veröffentlicht worden ist.

Derartige Anforderungen werden im Requirements Engineering in verschiedene Kategorien eingeordnet, um eine systematische Bearbeitung im Software-Entwicklungsprozess und im anschließenden Produktionsbetrieb erreichen zu können[12]:

Kundenanforderungen: Von den Banken festgelegte Anforderungen (Anforderungen in Bezug auf das Produkt[13]; Anforderungen hinsichtlich Lieferung[14], zum Beispiel Implementierung in der Produktionsumgebung erst nach erfolgreichen Test-, Abnahme- und Freigabeprozessen; Anforderungen hinsichtlich Tätigkeiten nach der Lieferung[15], zum Beispiel Bereitstellung von Daten in einem bestimmten Format, zu bestimmten Zeitpunkten und an bestimmte Systeme von Dritten, etwa Systeme der Deutschen Bundesbank wie Target-2-Bundesbank, Bundesbank Extra-Net).

Eigene Anforderungen des Rechenzentrums: Alle vom Hersteller des Software-Produktes zum Beispiel aufgrund von Sicherheitsstandards selbst festgelegter Anforderungen.[16]

Compliance-Anforderungen: Erstens vertragliche Anforderungen;[17] zweitens zwingend erforderliche vom (potenziellen) Anwender nicht angegebene Anforderungen, die jedoch für den festgelegten oder den beabsichtigten Gebrauch, soweit bekannt, notwendig sind.[18]

Hierzu zählen etwa nationale und internationale Normen sowie Branchen- (zum Beispiel Standards der deutschen Kreditwirtschaft) und Prüfungsstandards (wie IdW-Standards); drittens gesetzliche Anforderungen in Bezug auf das Produkt.[19] Unter diesen Punkt fallen allgemeine gesetzliche Regelungen (zum Beispiel Handelsgesetzbuch), rechtsformspezifische Gesetze (etwa Aktiengesetzbuch) und branchen- beziehungsweise einsatzspezifische Gesetze (wie Kreditwesengesetz); viertens behördliche Anforderungen in Bezug auf das Produkt.[20] Dies sind unter anderem Vorgaben (beispielsweise Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme, Mindestanforderungen an das Risikomanagement, Solvabilitätsverordnung) seitens der Finanz- und Aufsichtsbehörden (wie Bundesministerium der Finanzen, Bundesanstalt für Finanzdienstleistungsaufsicht).

Bei der Implementierung der angepassten Bank-Anwendungen in der Produktionsumgebung in einem Rechenzentrum ist dann neben den vorher erforderlichen Test-, Abnahme- und Freigabeprozessen gegebenenfalls noch die Anbindung des Produktionssystems an die Schnittstellen und Systeme von staatlichen Stellen (wie dem Extranet der Deutschen Bundesbank) erforderlich.

Unterstützung des Compliance-Managements in Banken

Die Rechenzentralen der genossenschaftlichen Finanzgruppe unterstützen ihre Kunden in der Ordnungsmäßigkeit ihrer eigenen Geschäftsorganisation durch ein umfassende Leistungs-, Beratungs- und Informationsangebot:

1) Bereitstellung eines „Ordnungsmäßigkeitshandbuches" für das jeweils eingesetzte Bankverfahren, in dem die MaRisk-Anforderungen mit IT-Bezug vor dem

Hintergrund der konkreten Vertragsbeziehung und daraus resultierenden Arbeitsteilung zwischen der Bank als Kunden und der Rechenzentrale als IT-Dienstleister erläutert wird.

2) Laufende Sichtung des Gesetzgebungsverfahrens und von Behördenverlautbarungen beziehungsweise -erlassen und Berücksichtigung dieser Veränderungen bei der Entwicklung beziehungsweise Weiterentwicklung von eigenen Bank-Anwendungen als Standardsoftware und bei der eigenen Organisationsgestaltung.

3) Laufende Mitarbeit und Sichtung von Branchenstandards der Deutschen Kreditwirtschaft und Berücksichtigung dieser Veränderungen bei der Entwicklung beziehungsweise Weiterentwicklung von eigenen Bank-Anwendungen als Standardsoftware.

4) Laufende Sichtung von Standards (zum Beispiel IDW-Standards) und Normen (DIN- und ISO-Normen) und gegebenenfalls Berücksichtigung dieser Veränderungen bei der Entwicklung beziehungsweise Weiterentwicklung von eigenen Bank-Anwendungen als Standardsoftware und bei der eigenen Organisationsgestaltung.

5) Identifikation von gängigen Standards für die verschiedenen technischen Aspekte und die verschiedenen IT-Prozesse, die gegebenenfalls über die in den MaRisk genannten gängigen Standards hinausgehen.[21)]

6) Durchführung und Unterstützung bei Test, Abnahme, Freigabe und Implementierung in die Produktionsprozesse und -umgebung.

7) Laufende Überwachung des IT-Betriebs (Monitoring).

8) Eingerichtetes Incident-, Problem- und Changemanagement.

9) Durchführung von Notfalltests zur Überprüfung der Wirksamkeit und Angemessenheit des Notfallkonzeptes.

10) Nachweis der Ordnungsmäßigkeit durch interne Prüfungen der internen Revision und externe Prüfungen durch Wirtschaftsprüfer sowie durch externe Audits; Beispiele: a) Interne Prüfungen auf Grundlage der schriftlich fixierten Ordnung der Rechenzentrale und den gängigen Standards für das Prüfungsgebiet; b) Zertifizierung des Managementsystems der Rechenzentrale zum Beispiel nach ISO 27001 und ISO 9001; c) Zertifizierung des IT-Servicemanagements zum Beispiel nach ISO 20000; d) Ordnungsmäßigkeitsprüfung der ausgelagerten Aktivitäten und Prozesse nach IDW PS 951; e) Prüfung von Softwareprodukten nach IDW PS 880 (SW-Bescheinigung).

11) Regelmäßige beziehungsweise laufende Berichterstattung, gegebenenfalls Störungsmeldungen; monatliche Service-Level-Berichte zu den vereinbarten Leistungsscheinen beziehungsweise Service-Level-Agreements, vierteljährlicher Risikobericht zu den mit der vereinbarten Auslagerung verbundenen IT-Risiken; Bericht über die Ergebnisse der durchgeführten Notfalltests, Berichte (inklusive Mängelverfolgung) mit Bezug zur vereinbarten Auslagerung der Internen Revision, externer Prüfungsgesellschaften und Aufsichtsbehörden.

12) Regelmäßiger Dialog mit den Banken und den gesetzlichen Prüfungsverbänden.

13) Regelmäßiger und anlassbezogener Dialog mit den Aufsichtsbehörden.

14) Schulungen und Beratungen zu Datenschutz, IT-Sicherheit und Ordnungsmäßigkeit des IT-Einsatzes.

15) Gegebenenfalls Unterstützung der Kunden bei IT-bezogenen Prüfungen.

Anwendungsschwerpunkt des einzelnen Standards festlegen

Exkurs: Bei der Festlegung von gängigen Standards für das eigene Institut sollte der Anwendungsschwerpunkt des einzelnen Standards berücksichtigt werden. Beispiele für Standards, die von Rechenzentren als IT-Dienstleister für Banken genutzt und angewandt werden, sind nachfolgend mit ihrem Anwendungsbereich aufgeführt:

Managementsysteme: ISO/IEC 2700x Informationssicherheitsmanagement und IT-Sicherheit; ISO 9001 Qualitätsmanagement; ISO 31000 Risikomanagement – Grundsätze und Implementierung;

IT-Servicemanagement inklusive IT-Betrieb: ISO 20000 Service Delivery und Service Support; BSI IT-Grundschutz-Kataloge;

Software-Entwicklung: CMMI-DEV Softwareerstellung; ISO 90003 – Übertragung der ISO 9001 auf Softwareprodukte; DIN EN ISO 9241-210/01.2011 Software Lifecycle Process; ISO 9126-1 Software-Engineering – Qualität von Softwareprodukten;

Anwendungen: DIN EN ISO 9241-11 Anforderung an die Gebrauchstauglichkeit; DIN EN ISO 9241-110 Grundsätze der Dialoggestaltung;

Systeme: BSI IT-Grundschutz-Standards;

Einsatzspezifische Standards: PCI DSS – Sicherheitsanforderungen für die Verarbeitung von Kreditkarteninformationen; FinTS – Standard für sicheres Online-Banking; EBICS – Electronic Banking Internet Communication Standard;

RZ-Infrastruktur: Trusted Site Infrastructure (TSI).

Technischer Fortschritt und Banken-Compliance

Im Zuge des technischen Fortschritts beziehungsweise durch den technologischen Wandel verändern sich laufend die Basisprodukte für die Informationsverarbeitung. Hierzu zählen beispielsweise, Netzwerkprotokolle, Computerhardware, Betriebssysteme, Speichersysteme, Datenbanksysteme, Applikation-Server, Programmiersprachen, Bedienoberflächen beziehungsweise Nutzerschnittstellen und Endgeräte.

Diese Veränderungen laufend zu beobachten und in ihrer Bedeutung für die eigenen Leistungen und Service auch unter Berücksichtigung der Bank-Compliance zu beurteilen, ist eine unternehmerische Notwendigkeit für eine Rechenzentrale. Dieses Know-how der Rechenzentrale als IT-Spezialist kann seitens der Banken bei der eigenen Beurteilung von Anpassungsprozessen im Sinne des MaRisk AT 8 genutzt werden.

Daneben steht die permanente Aufgabe der Rechenzentrale aufgrund des technischen Fortschritts und technologischen Wandels auch zur Erfüllung der Banken-Compliance, die technisch-organisatorische Ausstattung der Rechenzentrale auf einem wartbaren und beherrschbaren

Stand der Technik zu halten. Dies erfordert aufgrund der Produktveränderungen im IT-Markt eine laufende Wartung und Instandhaltung der RZ-Infrastruktur und der IT-Systeme verbunden mit einer hinreichenden Ausbildung des zuständigen Personals bei gleichzeitiger Einhaltung der vorher skizzierten Compliance-Anforderungen an den IT-Einsatz.

Banken-Applikationen auf einem beherrschbaren Stand halten

Im SaaS-Modell muss das Rechenzentrum bei der Bereitstellung von Banken-Applikationen als Standardsoftware ebenso verfahren und die Banken-Applikationen laufend auf einem wartbaren und beherrschbaren Stand der Technik halten, ebenfalls verbunden mit einer hinreichenden Ausbildung des zuständigen Personals bei gleichzeitiger Einhaltung der Compliance-Anforderungen an den IT-Einsatz. Werden die Banken-Applikation von der Bank als Kunde bereitgestellt (PaaS-Modell), muss die Bank diese Aufgabe selbst übernehmen.

Die Rechenzentrale kann im PaaS-Modell bei zunehmender Standardisierung von Bank-Anwendungen die Bank um diese Aufgabe unter der Voraussetzung einer vertraglichen Vereinbarung entlasten. Hierdurch wird der technologische Wandel durch das Rechenzentrum als IT-Spezialist für die Bank abgefedert – auch in Bezug auf Compliance-Anforderungen. Ansonsten müsste das erforderliche Know-how gemäß MaRisk AT 7.1 in der Bank selbst vorgehalten beziehungsweise von der Bank extern beschafft werden.

Darüber hinaus ermöglicht die Ablösung von Individuallösungen in der Bank durch Standardlösungen seitens der Rechenzentrale eine mehrfache Entlastung für die Bank:

– Investitionen in Entwicklung, Weiterentwicklung und Wartung der Standardlösung verteilen sich auf alle Anwender der Standardlösung.

– Die erforderliche Trennung von Entwicklungs-, Test-, Schulungs- und Produktionsumgebungen kann zentralisiert für alle Anwender erfolgen.

– Die Prozesse für Test, Abnahme und technische Inbetriebnahme müssen nicht komplett individuell durchgeführt werden.

– Für die Schulung der Bankmitarbeiter als IT-Anwender auch aufgrund MaRisk AT 7.1 Tz. 2 können die Schulungsangebote der Rechenzentrale genutzt werden.

– Hieraus verbessert sich für die Bank die Wirtschaftlichkeit des IT-Einsatzes und es erfolgt zusätzlich eine Entlastung des eigenen IT-Betriebs in der Bank. Verbunden ist der Entlastungseffekt mit der Erfordernis zum Ausbau eines hinreichend qualifizierten IT-Auslagerungsmanagements in der Bank, um bei wesentlichen IT-Auslagerungen die Anforderungen gemäß § 25a Abs. 2 in Verbindung mit MaRisk AT 9 einhalten zu können und somit compliant zu sein.[22)]

Eigene Leistungen und Produkte kontinuierlich anpassen

Die Banken-Compliance erfährt eine immer stärkere Komplexität durch immer detailliertere Regelungen. Sowohl die Menge als auch die Veränderungsgeschwindigkeit dieser Regelungen steigen laufend – zumindest in der subjektiven Wahrnehmung. Parallel erfordern die Compliance-Regeln in sich häufig selbst eine zusätzliche beziehungsweise veränderte IT-Unterstützung, um die von staatlichen Stellen geforderten Daten inhaltlich korrekt, im richtigen Datenformat, an der richtigen Schnittstelle und zeitgerecht zur Verfügung zu stellen.

Außerdem beinhaltet der technische Fortschritt in der Informationstechnologie ebenfalls eine laufende Anpassung der IT-Systeme, um die IT-spezifischen Compliance-Anforderungen einhalten zu können. Wegen beider Herausforderungen haben Rechenzentralen beziehungsweise IT-Dienstleister für Banken als ihre Kunden eine besondere Rolle in der Banken-Compliance, der sie sich täglich stellen und ihre eigene Leistungen und Produkte kontinuierlich diesen sich verändernden Rahmenbedingungen anpassen müssen, um selbst markt- und wettbewerbsfähig und ein strategischer Partner für die Banken als ihre Kunden zu bleiben.

Fußnoten

1) § 25a Abs. 1 KWG: „Ein Institut muss über eine ordnungsgemäße Geschäftsorganisation verfügen, die die Einhaltung der vom Institut zu beachtenden gesetzlichen Bestimmungen [...] gewährleistet."
2) Josef Kokert/Markus Held, „IT-Sicherheitsmanagement – die Sicht der BaFin" in Kreditwesen, Ausgabe Technik 2/2013, S. 6.
3) Vgl. Gesetzentwurf der Bundesregierung zum CRD IV-Umsetzungsgesetz, Bundesrat-Drucksache 510/12, S. 33, 44, 67 und 69.
4) Vgl. BCBS „Principles for the Sound Management of Operational Risk" 2011, S. 13.
5) Vgl. MaRisk AT 9 Tz. 7: „Das Institut hat [...] die Ausführung der ausgelagerten Aktivitäten und Prozesse ordnungsgemäß zu überwachen. Dies umfasst auch die regelmäßige Beurteilung der Leistung des Auslagerungsunternehmens [...]."
6) BSI – Baustein B 2.9 Rechenzentrum, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b02/b02009.html, abgerufen am 8. Juli 2013.
7) § 1 Abs. 3c KWG: „Anbieter von Nebendienstleistungen sind Unternehmen, die keine Institute oder Finanzunternehmen sind und deren Haupttätigkeit darin besteht, [...] Rechenzentren zu betreiben [...], die Nebentätigkeiten im Verhältnis zur Haupttätigkeit eines oder mehrerer Institute sind."
8) Josef Kokert/Markus Held, „IT-Sicherheitsmanagement – die Sicht der BaFin" in Kreditwesen, Ausgabe Technik 2/2013, S. 6.
9) Vgl. IDW PS 980 Tz. 6.
10) Vgl. Wikipedia „IT-Recht", http://de.wikipedia.org/wiki/Informationstechnologierecht, abgerufen am 8. Juli 2013.
11) Vgl. Gesetzentwurf der Bundesregierung zum CRD-IV-Umsetzungsgesetz, Bundesrat-Drucksache 510/12, S. 44.
12) Andreas Abel, „Compliance-Engineering", in Claus Rautenstrauch (Hrsg.) „Die Zukunft der Anwendungssoftware – die Anwendungssoftware der Zukunft" 2007, S. 53f.
13) Vgl. DIN EN ISO 9001:2008 7.2.1 a).
14) Vgl. DIN EN ISO 9001:2008 7.2.1 a).
15) Vgl. DIN EN ISO 9001:2008 7.2.1 a).
16) Vgl. DIN EN ISO 9001:2008 7.2.1 d).
17) Vgl. DIN EN ISO 9001:2008 7.2.2 und ISO 90003:2004 7.2.2.1 g).
18) Vgl. DIN EN ISO 9001:2008 7.2.1 b).
19) Vgl. DIN EN ISO 9001:2008 7.2.1 c).
20) Vgl. DIN EN ISO 9001:2008 7.2.1 c).
21) Josef Kokert/Markus Held, „IT-Sicherheitsmanagement – die Sicht der BaFin" in Kreditwesen, Ausgabe Technik 2/2013, S. 7.
22) Josef Kokert/Markus Held, „IT-Sicherheitsmanagement – die Sicht der BaFin" in Kreditwesen, Ausgabe Technik 2/2013, S. 8.