§ 8 Ordnungsgemäße Geschäftsorganisation bei ZAG-Instituten

I. Begriff der ordnungsgemäßen Geschäftsorganisation

Eine ordnungsgemäße Geschäftsorganisation ist für jedes Zahlungs- und E-Geld-Institut Pflicht. Nach § 27 ZAG sind die Geschäftsleiter[1] für diese verantwortlich. § 27 ZAG konkretisiert, was eine ordnungsgemäße Geschäftsorganisation zu umfassen hat; durch die Verwendung des Begriffs „insbesondere" macht der Gesetzgeber jedoch klar, dass es sich bei der Aufzählung in § 27 Abs. 1 S. 2 ZAG um keine abschließende handelt. Genannt werden folgende Verpflichtungen in Bezug auf die Gewährleistung einer ordnungsgemäßen Organisation des Geschäfts: **1**

1. *angemessene* Maßnahmen der Unternehmenssteuerung, Kontrollmechanismen und Verfahren, die gewährleisten, dass das Institut seine Verpflichtungen erfüllt;
2. das Führen und Pflegen einer Verlustdatenbank sowie eine vollständige Dokumentation der Geschäftstätigkeit, die eine lückenlose Überwachung durch die Bundesanstalt für ihren Zuständigkeitsbereich gewährleistet;
3. ein *angemessenes* Notfallkonzept für IT-Systeme;
4. interne Verfahren und Kontrollsysteme, die die Einhaltung der Verordnung (EG) Nr. 924/2009[2], der Verordnung (EU) Nr. 260/2012 und der Verordnung (EU) 2015/751 des Europäischen Parlaments und des Rates vom 29. April 2015 über Interbankenentgelte für kartengebundene Zahlungsvorgänge gewährleisten;
5. unbeschadet der Pflichten der §§ 4 bis 7 des Geldwäschegesetzes *angemessene* Maßnahmen, einschließlich Datenverarbeitungssysteme, die die Einhaltung der Anforderungen des Geldwäschegesetzes und der Verordnung (EU) 2015/847 gewährleisten; soweit dies zur Erfüllung dieser Pflicht erforderlich ist, darf das Institut personenbezogene Daten verarbeiten.

§ 27 Abs. 2 ZAG verweist im Übrigen auf die §§ 6a, 24c, 25i, 25m und 60b KWG sowie § 93 Abs. 7, 8 iVm § 93b AO, die ebenfalls für Zahlungs- und E-Geld-Institute Geltung finden. Auch sind die Vorgaben des § 24c KWG mit der Maßgabe anzuwenden, dass die BaFin einzelne Daten aus dem Dateisystem nach § 24c Abs. 1 S. 1 KWG abrufen darf, soweit dies zur Erfüllung ihrer aufsichtsrechtlichen Aufgaben iSd ZAG und GwG, „insbesondere im Hinblick auf unerlaubte Zahlungsdienste und unerlaubte E-Geld-Geschäfte erforderlich ist und besondere Eilbedürftigkeit im Einzelfall vorliegt". **2**

[1] Aus Gründen der Lesbarkeit wird nur die männliche Form „Geschäftsleiter" benutzt. Erfasst sind jedoch alle Geschlechter. Diese verkürzte Sprachform beinhaltet keine Wertung.
[2] VO (EG) Nr. 924/2009, über grenzüberschreitende Zahlungen in der Gemeinschaft; nicht mehr in Kraft, aufgehoben durch VO (EU) 2021/1230.

Neben dem Vorstehenden mangelt es in § 27 Abs. 1 ZAG an konkreten Vorgaben, wie eine solche „ordnungsgemäße Geschäftsorganisation" auszuführen und auszugestalten ist. Die Ausgestaltung ist vielmehr einzelfallabhängig, daher auch die stetige Verwendung des Adjektivs *„angemessen"*. Die Regelung erinnert damit an § 25a KWG – die Parallelnorm aus dem Kreditwesengesetz. Mit dieser verbleibenden Freiheit soll der geschäftsinterne Entscheidungs- und Ermessensspielraum gewährleistet werden.

3 Weitere Konkretisierungen dieser unbestimmten Rechtsbegriffe des § 27 ZAG fanden sich vormals in den allgemeinen Mindestanforderungen an das Risikomanagement („MaRisk")[3], die nach der herrschenden Meinung entgegen ihres Wortlautes „Dieses Rundschreiben gibt auf der Grundlage des § 25a Abs. 1 KWG einen flexiblen und praxisnahen Rahmen für die Ausgestaltung des Risikomanagements der Institute vor"[4] analog auch für ZAG-Institute heranzuziehen waren, allerdings nur an passenden Stellen.[5] Denn die aufsichtlichen Anforderungen an Kreditinstitute sind deutlich höher als die an Zahlungs- und E-Geld-Institute, so dass – dem Grundsatz der Angemessenheit und Proportionalität folgend – die Heranziehung entsprechend zu erfolgen hatte.

Die BaFin hat im Ende Mai 2024 die speziellen Mindestanforderungen an das Risikomanagement von ZAG-Instituten[6] („ZAG-MaRisk") veröffentlicht, die als speziellere Vorgabe die MaRisk ablöst. Diese spezielle Regelung für ZAG Institute ist zu begrüßen – da norminterpretierende Verwaltungsanweisungen zu einer deutlich gesteigerten Rechts- und Planungssicherheit beitragen. Dies gilt umso mehr, als dass die Einhaltung der Vorgaben des § 27 ZAG der Prüfung durch Dritte – wie etwa der Abschlussprüfung oder bei anlassbezogenen Sonderprüfungen – unterliegt.

4 Die Pflicht einer ordnungsgemäßen Geschäftsorganisation gilt für alle Zahlungsinstitute und E-Geld-Institute. Dies schließt auch Zweigniederlassungen deutscher Institute im Ausland ein, da sie rechtlich unselbstständige Teile des jeweiligen Instituts sind. Ebenso unterliegen inländische Zweigstellen von Unternehmen mit Sitz außerhalb des Europäischen Wirtschaftsraums („EWR") dem Anwendungsbereich. Denn diese gelten nach der Fiktion des § 42 Abs. 1 ZAG als Institute im Sinne des ZAG, wenn sie Zahlungsdienste oder E-Geld-Geschäfte erbringen. Wenn solche Institute ihren Sitz innerhalb des EWR haben, unterliegen sie nach § 39 Abs. 1 ZAG primär der Aufsicht des Herkunftsstaates. Nach § 39 Abs. 3 S. 2 ZAG sind aber die in § 27 Abs. 1 S. 2 Nr. 5 ZAG niedergelegten Maßnahmen zur Verhinderung der Geldwäsche und die Maßgaben der Geldtransfer-VO[7] von inländischen Zweigniederlassungen und Agenten zu erfüllen.

---

[3] BaFin, Rundschreiben 05/2023 (BA) – Mindestanforderungen an das Risikomanagement – MaRisk, 18.10.2023.
[4] MaRisk AT 1.
[5] AA Ellenberger/Findeisen/Nobbe/Böger/Findeisen ZAG § 27 Rn. 23, der die analoge Anwendbarkeit der MaRisk auf ZAG-Institute pauschal verneint.
[6] Bafin, Rundschreiben 07/2024 (BA) Mindestanforderungen an das Risikomanagement von ZAG-Instituten – ZAG-MaRisk, 7.6.2024.
[7] VO (EU) 2015/751.

II. Verantwortung für eine ordnungsgemäße Geschäftsorganisation

Die Geschäftsleiter des Institutes[8] iSd § 1 Abs. 8 ZAG sind für die ordnungsgemäße Geschäftsorganisation verantwortlich. **5**

Dies umfasst zugleich die Verpflichtung, den Betrieb der Geschäftsorganisation aufrechtzuerhalten. Dabei ist die Geschäftsorganisation an die jeweiligen Bedürfnisse des Institutes und die sich ändernden Rahmenbedingungen fortlaufend anzupassen. Indem § 27 Abs. 1 S. 1 Hs. 2 ZAG ausdrücklich auf die Geschäftsleiter verweist, ist klar, dass die Verantwortung nicht nur auf den Geschäftsleiter beschränkt ist, der nach dem Geschäftsverteilungsplan für die innerbetriebliche Organisation zuständig sind. Alle Geschäftsleiter sind nach S. 1 Hs. 2 vielmehr gehalten, die zuständigen Kollegen zu überwachen und im Bedarfsfall korrigierend einzugreifen.[9]

Die ZAG-MaRisk ist ebenfalls deutlich, wenn es um die Verantwortung geht: **6**
Alle Geschäftsleiter (§ 1 Abs. 8 ZAG) 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, einschließlich ESG-Risiken, beurteilen und die erforderlichen Maßnahmen zu ihrer Begrenzung treffen. Hierzu zählen auch die Entwicklung, Förderung, Integration und Überwachung einer angemessenen Risikokultur auf allen Ebenen innerhalb des Instituts.[10]

III. ZAG-MaRisk

Die ZAG-MaRisk soll als Rundschreiben auf der Grundlage des § 27 Abs. 1 ZAG einen flexiblen und praxisnahen Rahmen für die Ausgestaltung einer ordnungsgemäßen Geschäftsorganisation der Institute vorgeben. Eine ordnungsgemäße Geschäftsorganisation umfasst demzufolge insbesondere angemessene Maßnahmen der Unternehmenssteuerung sowie Kontrollmechanismen und Verfahren, die gewährleisten, dass das Institut seine Verpflichtungen erfüllt. Es enthält spezielle Regelungen für Zahlungsinstitute; bislang fehlte es an solchen, so dass nach der hM in Teilen die allgemeine, auf KWG-Institute ausgerichtete MaRisk hinzuzuziehen war. Mit Inkrafttreten der ZAG-MaRisk wird diese analoge Anwendung obsolet und die ZAG-MaRisk ist als geschäftsmodell-spezifisches Rundschreiben unmittelbar anzuwenden. **7**

Die ZAG-MaRisk enthält auch Vorgaben zur Art und Weise der Geschäftsorganisation, die im Wesentlichen den Anforderungen der MaRisk entsprechen. So sollen die internen Kontrollmechanismen aus dem internen Kontrollsystem und der Internen Revision bestehen und umfassen insbesondere Regelungen zur Aufbau- und Ablauforganisation und Prozesse zur Identifizierung, Beurteilung, Steuerung, Überwachung sowie Kommunikation der Risiken (Risikosteuerungs- und -controllingprozesse). Das interne Kontrollsystem impliziert ebenfalls die

[8] Vgl. auch ZAG-MaRisk AT 3 „Gesamtverantwortung der Geschäftsleitung".
[9] Reischauer/Kleinhans/Bitterwolf KWG § 25a Rn. 6, deutlich hierzu auch ZAG-MaRisk AT 3.
[10] ZAG-MaRisk AT 1.

Einrichtung einer Risikocontrolling-Funktion und einer Compliance-Funktion. Ein wirksames Risikomanagement ist ein Verfahren, das sicherstellt, dass ein Institut seine Verpflichtungen gemäß § 27 Abs. 1 ZAG erfüllen kann. Soweit ein Aufsichtsorgan besteht, schafft das Risikomanagement auch eine Grundlage für die sachgerechte Wahrnehmung der Überwachungsfunktionen des Aufsichtsorgans und beinhaltet deshalb auch dessen angemessene Einbindung.[11]

8 Wie erwähnt, ähnelt die ZAG-MaRisk insgesamt im Aufbau und Inhalt stark der MaRisk. Allerdings werden in ihr lediglich operationelle Risiken als per se „wesentlich" eingestuft, während in den MaRisk für Banken darüber hinaus auch Adressenausfallrisiken einschließlich Länderrisiken, Marktpreis- und Liquiditätsrisiken als „wesentlich" einzuordnen und behandeln sind.

Wie unter die MaRisk fallende Institute müssen nach der ZAG-MaRisk auch Zahlungsdienstleister ihre Risikotragfähigkeit sicherstellen, indem jederzeit ausreichend Risikodeckungspotenzial vorhanden sein muss. Die ZAG-MaRisk macht iÜ geschäftsmodell-spezifische Vorgaben zu Sicherheitsvorfällen, Betrugsprävention, Haftungsrisiken, Kundenbeschwerden und Agenten. Zudem sind ESG-Risiken und auch ein angemessenes Auslagerungsmanagement genauso zu beachten, wie bei der MaRisk für Banken. Nicht zuletzt weist die ZAG-MaRisk die Verpflichtung aus, dass eine angemessene Compliance-Funktion sowie Interne Revision vorzuhalten ist.

IV. Grundsatz der Proportionalität

9 Eine ordnungsgemäße Geschäftsorganisation ist abhängig von der Art, dem Umfang, der Komplexität und dem Risikogehalt der Geschäftstätigkeit des Zahlungsinstitutes bzw. E-Geld-Institutes.[12] Es kommt also immer auf den konkreten Einzelfall an – starre Regelungen, wann, was in welchem Rahmen erforderlich ist, bestehen nicht. Diese Flexibilität bezeichnet man als *doppeltes Proportionalitätsprinzip*.

Auch wenn dieses doppelte Proportionalitätsprinzip nicht ausdrücklich im ZAG bzw. in § 27 ZAG aufgeführt ist (anders etwa in § 25a Abs. 1 S. 4 KWG bzgl. Risikomanagement), findet es als aufsichtliches Grundprinzip insb. auf die Vorgaben des § 27 ZAG Anwendung,[13] – zumal an die Regulierung von ZAG Instituten weniger hohe Anforderungen bestehen als an die Regulierung nach dem KWG beaufsichtigter Institute.

Nach dem Prinzip bzw. Grundsatz der sog. doppelten Proportionalität ist bei der Regulierung und bei der Auslegung von Normen und Verwaltungsanweisungen in der aufsichtlichen Praxis das Risikoprofil des jeweiligen Unternehmens zu berücksichtigen.[14] Entscheidend sind hierbei nicht nur Größe, Art und Umfang der Geschäfte, sondern auch das Geschäftsmodell und die Komplexität der Risiken.[15]

---

[11] ZAG-MaRisk AT 1.

[12] Ellenberger/Findeisen/Nobbe/Böger/Findeisen ZAG § 27 Rn. 32.

[13] Vgl. allgemein zum Proportionalitätsprinzip: Krimphove, Was ist Proportionalität?, BKR 2017, 353; vgl. auch EBA/GL/2019/02, Leitlinie 1; EBA/GL/2017/11, Title I Tz. 17 ff.

[14] Vgl. BaFin Happel, Wer angemessene Regulierung fordert, darf damit nicht Deregulierung als sein eigentliches Ziel maskieren, 18.2.2019.

[15] BaFin, Happel, Wer angemessene Regulierung fordert, darf damit nicht Deregulierung als sein eigentliches Ziel maskieren, 18.2.2019.

Die ZAG-MaRisk geht ebenfalls in AT 1 auf diesen Grundsatz ein, indem sie ausdrücklich erwähnt, dass das Rundschreiben einen Regelungsrahmen für die qualitative Aufsicht von Instituten unter Berücksichtigung des Prinzips der doppelten Proportionalität bildet. Der sachgerechte Umgang mit dem Proportionalitätsprinzip seitens der Institute beinhaltet in dem prinzipienorientierten Aufbau der ZAG-MaRisk auch, dass Institute im Einzelfall über bestimmte, in den ZAG-MaRisk explizit formulierte Anforderungen hinaus weitergehende Vorkehrungen treffen, soweit dies zur Sicherstellung der Angemessenheit und Wirksamkeit des Risikomanagements erforderlich sein sollte.[16] **10**

Nach Maßgabe des Proportionalitätsgrundsatzes müssen Institute Maßnahmen treffen, die der Art und den Umständen ihrer jeweiligen Tätigkeiten gerecht werden.[17] Erbringen Institute besonders zahlreiche oder risikobehaftete, erlaubnispflichtige Tätigkeiten, ist entsprechend ein deutlich höherer Grad an Anforderungen an die Geschäftsorganisation gestellt als bei kleinen Instituten, die sich auf weniger und mit niedrigerem Risiko verbundene Geschäfte des ZAG beschränken. Die in § 27 Abs. 1 S. 3 Nr. 1 – 4 ZAG niedergelegten Mindestanforderungen sind jedoch von allen Instituten zu erfüllen, wobei die konkrete Ausgestaltung jeweils wieder von der Einzelsituation des jeweiligen Institutes abhängig ist. Es empfiehlt sich, entsprechende Abwägungen in Bezug auf den Grundsatz sowie im Allgemeinen sorgfältig zu dokumentieren.

V. Konkrete Erfordernisse

ZAG-Institute müssen über angemessene Maßnahmen zur Unternehmenssteuerung, Kontrollmechanismen und Verfahren, die die Erfüllung der Verpflichtungen gewährleisten, verfügen. Hierzu zählen insbesondere die Bereiche: Unternehmenssteuerung, Sicherstellung von Kontrollen, Erfüllung von Verpflichtungen und Einrichtung von Verfahren, die im Folgenden konkretisiert werden sollen. **11**

1. Unternehmenssteuerung

Eine angemessene Unternehmenssteuerung bedeutet, dass die Geschäftsleitung in der Lage ist, die in der jeweiligen Situation notwendigen Maßnahmen zu ergreifen, um die Einhaltung ihrer Verpflichtungen gewährleisten zu können; besondere Vorgaben bestehen gemäß § 52 ZAG für das Risikomanagement. **12**

Zur Unternehmenssteuerung hat die Geschäftsleitung eine Aufbau- und Ablauforganisation zu errichten und aufrechtzuerhalten (mithin jeweils auf dem aktuellen Stand zu halten). Die aufbau- und ablauforganisatorischen Regelungen haben dabei angemessen zur Erreichung der unternehmerischen Zielsetzung wie auch der aufsichtsrechtlichen Anforderungen zu sein. Diese internen Regelungen sind schriftlich zu dokumentieren, die betroffenen Mitarbeiter sind zu unterrichten und ihre Kenntnis der Regelungen ist sicher zu stellen, beispielsweise durch

[16] ZAG-MaRisk AT 1.
[17] Reischauer/Kleinhans/Bitterwolf KWG § 25a Rn. 5.

entsprechende Trainings/Schulungen, Erfahrungen. Dies ist laufend zu überwachen und entsprechend zu dokumentieren.

13 Die aufbau- und ablauforganisatorischen Regelungen sollten wenigstens Folgendes beinhalten:

- Organigramme,
- Kompetenzregelungen/Dokumentation aller Geschäftsvorgänge,
- Stellen-/Jobbeschreibungen inkl. Arbeitsplatzanweisungen,
- Arbeitsanweisungen und Arbeitsablaufbeschreibungen (Prozesse),
- Geschäftsstrategie(n),
- Notfallpläne,
- Regelungen zur Auslagerung sowie zum Risikomanagement.

14 Die aufbau- und ablauforganisatorischen Regelungen sind so zu verfassen, dass der Inhalt für die Mitarbeitenden des Instituts nachvollziehbar ist. Dies setzt voraus, dass diese über die Regelungen informiert und in Kenntnis gesetzt werden (etwa im Rahmen des Onboarding Prozesses bei Aufnahme der Tätigkeit sowie bei Änderungen laufend im Rahmen von sog. All-Hands oÄ).

Diese aufbau- und ablauforganisatorischen Regelungen müssen kontinuierlich aktualisiert werden; hierfür sind ebenfalls geeignete Prozesse zur Überwachung von Aktualisierungen zu etablieren und nachzuhalten.

Die Geschäftsleitung hat die Prozesse und die damit verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen sowie Kommunikationswege einschließlich der Schnittstellen im Fall von Auslagerungen klar zu definieren und aufeinander abzustimmen. Dabei ist ferner zu berücksichtigen, dass nicht nur eine einzige Person alle Phasen eines Geschäftsvorfalles durchführt (Grundsatz der Funktionstrennung). Das sog. Vier-Augen-Prinzip, welches der Kontrolle dient, ist zu gewährleisten. Laufende vor-, gleich- oder nachgeschaltete Kontrollen müssen die Überwachung sicherstellen; diese sind umso intensiver auszuführen, desto umfangreicher die Tätigkeiten der operativ tätigen Person sind.

15 Eine ordnungsgemäße Geschäftsorganisation umfasst ferner eine funktionale Trennung zwischen unvereinbaren Bereichen bzw. Positionen, idealerweise unter Berücksichtigung des Grundsatzes der Trennung von Markt und Marktfolge. Eine solche verhindert idR, dass eine Person miteinander unvereinbare Tätigkeiten durchführt.

Beispiel:

– Trennung von Markt, Handel und Marktfolge.

Entsprechend sind bestimmte Funktionen in unterschiedlichen, voneinander unabhängigen organisatorischen Einheiten anzusiedeln. Vertretungsregelungen sind dabei zu berücksichtigen.

2. Kontrollmechanismen

16 Unter dem Begriff „Kontrollmechanismen" sind *interne Kontrollverfahren* zu verstehen. Diese internen Kontrollverfahren setzen sich aus dem internen Kontrollsystem und der Internen Revision zusammen und sind zwingend in Organisationsrichtlinien, Funktionstrennungen und Kompetenzzuweisungen niederzulegen.

Das *interne Kontrollsystem* (sog. *second line of defence / control*) bezweckt die Sicherung und den Schutz insb. des vorhandenen Vermögens sowie vor sonstigen Verlusten. Interne Kontrollen setzen dokumentierte Prozesse voraus, die überprüfbar sind.

Kontrollen sind risikobasiert durchzuführen; allgemein gilt der Grundsatz, dass je höher das Risiko, desto öfter und umfangreicher sind die Kontrollen durchzuführen und zu dokumentieren. Die interne Kontrolle erfolgt typischerweise durch das Compliance Team, welches zugleich für das Aufsetzen der Prozesse verantwortlich ist.

Von der internen Kontrolle ist die sog. *Interne Revision* zu trennen, die eine prozessunabhängige Überwachung darstellt (third line of control bzw. defence).[18] Prozessunabhängig meint damit, dass diese zwingend zu trennen ist von der internen Kontrolle respektive von anderen, operativen Teams (wie etwa auch das Compliance Team); sie darf nicht an den zu prüfenden Aktivitäten und Prozessen operativ mitarbeiten. Sie ist vielmehr im Auftrag der Geschäftsleitung eine vollkommen unabhängige Stelle, die die Aufgabe hat, die gesamte Geschäftsorganisation zu überprüfen.

Die in ihr beschäftigten Mitarbeitenden sind nicht befugt, ihre Arbeitsleistung **17**
auch an revisionsfremde Aufgaben zu widmen (Interessenkonflikt). Aufgrund des damit verbundenen hohen Kostenaufwands – schließlich sind Personen ausschließlich für die interne Revision einzustellen – hat es sich etabliert, dass kleine Institute diese Funktion auslagern, um insbesondere Kosten zu sparen. Der Aufwand ist in Bezug auf die Größe des Instituts zu klein, als dass es sich lohnen würde, hierfür eine Stelle einzufügen. Die Auslagerung der internen Revision qualifiziert idR als wesentliche. Darüber hinaus besteht bei kleinen Instituten wohl auch die Möglichkeit, dass die Aufgaben der internen Revision von einem Geschäftsleiter erfüllt werden können.[19] (Näheres zur Auslagerung in → § 9 Rn. 2 ff.)

Die interne Revision überprüft als sog. *third line of defence / control* ebenfalls die Ordnungsmäßigkeit aller Aktivitäten und Prozesse – insb. das Risikomanagement iSd § 53 ZAG – eines Instituts anhand eines zu erstellenden Prüfungsplans und hat dabei weisungsunabhängig zu agieren (dh keine Berichterstattung oder Weisungsgebundenheit an die Geschäftsleitung). Gleichwohl kann die Geschäftsleitung aber weitere Prüfungen durch die interne Revision anordnen. Nach erfolgter Prüfung ist von der Internen Revision jeweils ein Prüfungsbericht zu erstellen und der Geschäftsleitung vorzulegen. Der Bericht umfasst typischerweise (i) Verbesserungsvorschläge und einen (ii) sog. Remediation Plan[20], mithin konkrete Zeitangaben, bis wann die festgestellten Mängel (durch wen) zu beheben sind. Dies prüft die interne Revision sodann ebenfalls. Werden schwerwiegende Mängel im Rahmen der Prüfung festgestellt, hat die Interne Revision immer (auch) eine *ad hoc*-Information abzugeben, die Geschäftsleiter also unverzüglich zu informieren.

Neben dem reinen Prüfungsergebnis sollten auch Verbesserungsvorschläge und **18**
Lösungsmöglichkeiten in den Bericht aufgenommen werden. Die Geschäftslei-

[18] Ellenberger/Findeisen/Nobbe/Böger/Findeisen ZAG § 27 Rn. 74.

[19] Die ZAG-MaRisk sieht vor, dass „Jedes Institut […] über eine funktionsfähige Interne Revision verfügen [muss]. Bei Instituten, bei denen aus Gründen der Betriebsgröße die Einrichtung einer Revisionseinheit unverhältnismäßig ist, können die Aufgaben der Internen Revision von einem Geschäftsleiter erfüllt werden.“, vgl. AT ZAG-MaRisk.

[20] Abarbeitungs- bzw. Mängelbehebungsplan.

tung entscheidet anhand der Informationen durch die Interne Revision über mögliche Maßnahmen sowie darüber, ob und in welcher Weise sie die Informationen an das zuständige Aufsichtsorgan weiterreicht. Die in MaRisk BT 2.4 vorgesehene Berichtspflicht der Internen Revision direkt gegenüber dem Aufsichtsorgan oder gegenüber der BaFin hat im ZAG keine gesetzliche Grundlage. Neben der reinen Feststellung von Mängeln und der Nennung von möglichen Lösungsvorschlägen ist die Interne Revision auch für die Überwachung der Mängelbeseitigung verantwortlich.

Zu kontrollieren ist auch, dass das Institut über Verfahren verfügt, die die Erfüllung seiner Verpflichtungen sicherstellen. Verpflichtungen umfassen dabei alle gesetzlichen Anforderungen aus dem ZAG und Begleitnormen wie die ZAG-Anzeigenverordnung („ZAGAnzV"), die ZAG-Monatsausweisverordnung („ZAGMonAwV") oder das Geldwäschegesetz („GwG"). Erfasst sind dabei auch allgemeine Anforderungen, mithin solche, die nicht speziell für Zahlungsdienstleistungsinstitute iSd ZAG gelten wie beispielsweise aus dem HGB und GmbHG.[21]

3. Führen einer Verlustdatenbank

19 § 27 Abs. 1 S. 2 Nr. 2 ZAG verpflichtet Institute, eine sog. Verlustdatenbank zu führen. Diese Verpflichtung dient dem Zweck der Steuerung der operationellen Risiken. Diese Pflicht umfasst Folgendes:

- Eine umfangreiche und vollständige Verlustdatenbank aufzubauen;
- Aufgetretene Schadensereignisse
  - präzise zu formulieren bzw. zu beschreiben
  - mit dem Zeitpunkt des Schadenseintrittes und
  - der Höhe des entstandenen Schadens aufzunehmen;
  - dabei ist eine Bagatellgrenze zu bestimmen (ab wann ein Schaden relevant und damit aufzunehmen ist) und
  - die Schäden sind zu kategorisieren

20 In der Verlustdatenbank sollte zudem eine Risikomatrix angelegt werden, die eine Risikoarten- bzw. Geschäftsfeldkategorisierung enthält.

Weiterhin muss das Institut eine vollständige Dokumentation seiner Geschäftstätigkeit erstellen, anhand derer eine lückenlose Überwachung durch die BaFin gewährleistet ist. Die Parallelnorm des § 25a Abs. 1 S. 6 KWG[22] ist viel konkreter

[21] Ellenberger/Findeisen/Nobbe/Findeisen ZAG § 27 Rn. 25; eine andere Ansicht geht hingegen davon aus, dass dies nicht der Fall sei, denn eine Anwendung auf alle gesetzlichen Regelungen auch ohne Bezug zu Zahlungsdiensten bzw. E-Geld-Geschäfte würde dazu führen, dass die BaFin bzw. der Abschlussprüfer des Institutes indirekt über Abs. 1 die Einhaltung von sämtlichen zivilrechtlichen, steuerrechtlichen, arbeitsrechtlichen und sozialrechtlichen Regelungen zu überprüfen und zu bewerten hätte. Dieses Argument ist jedoch dahingehend zu relativieren, als dass die Aufsicht dies nicht zwingend zu überprüfen hat – sondern nur dann, wenn Anlass dazu besteht, dass geltendes Recht nicht hinreichend berücksichtigt wird, siehe auch: Boos/Fischer/Schulte-Mattler/Braun KWG § 25a Rn. 36.

[22] Dort heißt es: „Eine ordnungsgemäße Geschäftsorganisation umfasst darüber hinaus angemessene Regelungen, anhand derer sich die finanzielle Lage des Instituts jederzeit mit hinreichender Genauigkeit bestimmen lässt; eine vollständige Dokumentation der Geschäftstätigkeit, die eine lückenlose Überwachung durch die Bundesanstalt für ihren Zuständigkeitsbereich