jusline®
»» Recht. Schnell

Sie können die QR Codes nützen um später wieder auf die neuste Version eines Gesetzestexts zu gelangen.

TE Bvwg Erkenntnis 2018/10/24 W107 2196670-1

JUSLINE Entscheidung

Veröffentlicht am 24.10.2018

Entscheidungsdatum

24.10.2018

Norm

AVG §17
AVG §39
AVG §45 Abs2
B-VG Art.133 Abs4
BWG §1 Abs1
BWG §39
BWG §98 Abs5
FMABG §22 Abs2a
FMABG §22 Abs8
VStG 1950 §1 Abs2
VStG 1950 §19
VStG 1950 §45 Abs1
VStG 1950 §5 Abs1
VStG 1950 §5 Abs2
VStG 1950 §64
VStG 1950 §9 Abs1
VStG 1950 §9 Abs2
VStG 1950 §9 Abs7
VwGVG §24 Abs1
VwGVG §31 Abs1
VwGVG §50
VwGVG §52 Abs8
WAG 2007 §17 Abs3
WAG 2007 §95 Abs2 Z2
WAG 2018 §29
WAG 2018 §95 Abs1 Z14

Spruch

W107 2196670-1/9E

IM NAMEN DER REPUBLIK!

Das Bundesverwaltungsgericht erkennt durch die Richterin Dr. Sibyll BÖCK als Vorsitzende sowie die Richterin Dr. Anke SEMBACHER und den Richter Dr. Michael ETLINGER als Beisitzer über die Beschwerde des XXXX , vertreten durch HAUSMANINGER KLETTER Rechtsanwälte - GmbH, Franz Josefs-Kai 3, 1010 Wien, gegen das Straferkenntnis der Finanzmarktaufsichtsbehörde vom 24.04.2018, GZ: XXXX , nach Durchführung einer mündlichen Verhandlung am 02.10.2018 zu Recht:

A)

I. Gemäß § 50 VwGVG wird der Beschwerde in der Schuldfrage keine Folge gegeben.

II. Gemäß § 50 VwGVG wird der Beschwerde in der Straffrage insoweit Folge gegeben, als die Strafe auf insgesamt EUR 5.000,- (22 Stunden Ersatzfreiheitsstrafe) herabgesetzt wird.

III. Der Beitrag zu den Kosten des Verfahrens vor der belangten Behörde wird mit EUR 500,- bestimmt, das sind 10 % der nunmehr verhängten Geldstrafe.

B)

Die Revision ist gemäß Art. 133 Abs. 4 B-VG nicht zulässig.

Text

ENTSCHEIDUNGSGRÜNDE:

I. Verfahrensgang:

1. Das Straferkenntnis der Finanzmarktaufsichtsbehörde (im Folgenden: "FMA" oder "belangte Behörde") vom 24.04.2018, GZ: XXXX , richtet sich gegen XXXX (im Folgenden: "Beschwerdeführer", auch "BF2") als Beschuldigten und enthält folgenden Spruch:

"Sehr geehrter Herr XXXX !

Sie waren von 28.12.2007 bis 25.10.2015 Vorstand der XXXX , in der Folge XXXX oder Kreditinstitut), ein konzessioniertes Kreditinstitut gemäß § 1 Abs. 1 Bankwesengesetz (BWG) mit der Geschäftsanschrift

XXXX .

I. Sie haben in dieser Funktion als nach außen vertretungsbefugtes Organ gemäß § 9 Abs 1 Verwaltungsstrafgesetz (VStG) BGBl 52/1991 idF BGBl I 3/2008 im Zeitraum von 01.01.2014 - 25.10.2015 zu verantworten, dass es die XXXX im Zeitraum von 19.04.2013 - 13.12.2016 unterlassen hat, einen gesetzeskonformen Betriebskontinuitätsplan (Business Continuity Management - BCM) einschließlich einer gesetzeskonformen IT-Notfall-Planung betreffend bankgeschäftliche und bankbetriebliche Risiken in schriftlicher und nachvollziehbarer Weise zu dokumentieren, die bei einer schwerwiegenden Betriebsunterbrechung die Fortführung der Geschäftstätigkeit und die Begrenzung von Verlusten sicherstellen, sodass in diesem Zeitraum die Verwaltungs¬, Rechnungs- und Kontrollverfahren der XXXX betreffend das operationelle Risiko nicht angemessen in Bezug auf Art, Umfang und Komplexität der betriebenen Bankgeschäfte waren. Die Tat wurde von Ihnen vorsätzlich nicht verhindert.

a) Eine Frist für die Wiederaufnahme kritischer Prozesse in den Szenarien "Totalausfall XXXX " (Szenario 1, Option 2) sowie "Totalausfall IT" (Szenario 2, Option 2) war von 19.04.2013 bis 27.01.2014 nicht gesetzeskonform schriftlich festgelegt. Ab dem 27.01.2014 war im BCM-Konzept (Version 1.0., genehmigt 27.01.2014) die Frist mit 10 bis 14 Tagen unangemessen lange schriftlich festgelegt. Die Frist von 10-14 Tagen, um wesentliche Daten und Funktionen zurückzugewinnen, ist in Bezug auf die bankgeschäftlichen und bankbetrieblichen Risiken unangemessen lange und gewährleistet keine schnellstmögliche Behebung von Fehlern.

Erst mit 13.12.2016 (BCM-Konzept Version 1.2, Seite 10) wurde eine Wiederaufnahmefrist von maximal vier Stunden für die als kritischen Prozesse definierten Kerngeschäftsprozesse Zahlungsverkehr, Kundenhandel, Private Banking/Vermögensverwaltung, Anti Money Laundering, Treasury und Settlement schriftlich festgelegt und in nachvollziehbarer Weise dokumentiert.

b) Ein gesetzeskonformer schriftlicher Plan für die Szenarien "Totalausfall XXXX " (Szenario 1, Option 2) oder "Totalausfall IT" (Szenario 2, Option 2) war ab 19.04.2013 bis 13.12.2016 insofern nicht vorhanden, als nicht in gesetzeskonformer Weise schriftlich festgelegt und in nachvollziehbarer Weise dokumentiert war,

• wie, von wem und in welchem Zeitraum Ersatzräumlichkeiten für Bankgeschäfte der XXXX innerhalb angemessener Frist zur Verfügung gestellt werden;

• wie, von wem und in welchem Zeitraum die erforderliche Hardware für Bankgeschäfte innerhalb angemessener Frist zur Verfügung gestellt wird;

Erst mit 13.12.2016 (BCM-Konzept, Version 1.2., Seite 15f) wurden neun Notfallarbeitsplätze binnen vier Stunden für alle kritischen Kernprozesse (Zahlungsverkehr, Kundenhandel, Private Banking/Vermögensverwaltung, Anti Money Laundering, Treasury und Settlement) bzw. weitere sieben Notfallarbeitsplätze innerhalb 24 Stunden für die restlichen Fachabteilungen - alle am Hauptstandort XXXX im XXXX - schriftlich festgelegt und in nachvollziehbarer Weise dokumentiert. Darin finden sich auch konkrete Regelungen und Prozedere für den Zutritt zu den Räumlichkeiten sowie bezüglich deren Ausstattung.

c) Ein gesetzeskonformer schriftlicher Plan für die Szenarien "Totalausfall XXXX " (Szenario 1, Option 2) oder "Totalausfall IT" (Szenario 2, Option 2) war ab 19.04.2013 bis 13.12.2016 auch insofern nicht vorhanden, als nicht in gesetzeskonformer Weise schriftlich festgelegt und in nachvollziehbarer Weise dokumentiert war,

• wo, wie, von wem und in welchem Zeitraum die gesicherten Datenbanken und Daten (inkl. Betriebssysteme) für Bankgeschäfte innerhalb angemessener Frist zur Verfügung gestellt werden sowie

• wie und in welchem Zeitraum bankgeschäftliche und bankbetriebliche Dienste mit externer Anbietung von den jeweiligen Dienstleistern innerhalb angemessener Frist wiederhergestellt werden können.

Erst mit 13.12.2016 wurde durch den IT-Disaster-Recovery-Plan (Version 1.0, Seite 4) und den IT-Notfall-Plan (Version 2.0, Seite 16) schriftlich festgelegt und in nachvollziehbarer Weise dokumentiert, dass bei der XXXX auch ein Ausfallrechenzentrum inkl. Ausfallserver installiert ist, auf den alle bankgeschäftliche und bankbetriebliche Systeme der XXXX im vier Stunden Takt repliziert werden.

II. Sie haben in dieser Funktion als nach außen vertretungsbefugtes Organ gemäß § 9 Abs 1 Verwaltungsstrafgesetz (VStG) BGBl 52/1991 idF BGBl I 3/2008 im Zeitraum von 19.04.2013 - 25.10.2015 zu verantworten, dass in der XXXX keine angemessenen Systeme, Ressourcen und Verfahren eingerichtet wurden, die bei einer Unterbrechung ihrer Systeme und Verfahren gewährleisten, dass wesentliche Daten und Funktionen erhalten bleiben und Wertpapierdienstleistungen und Anlagetätigkeiten fortgeführt werden können. Es wurde in diesem Zeitraum auch nicht durch angemessene Vorkehrungen sichergestellt, dass Daten rechtzeitig zurückgewonnen werden können, damit die Wertpapierdienstleistungen und Anlagetätigkeiten rechtzeitig wiederaufgenommen werden können. Die Tat wurde von Ihnen vorsätzlich nicht verhindert.

a) Eine angemessene Frist für die Wiederaufnahme kritischer Prozesse in den Szenarien "Totalausfall XXXX " (Szenario 1, Option 2) sowie "Totalausfall IT" (Szenario 2, Option 2) war ab 19.04.2013 bis 27.01.2014 nicht schriftlich festgelegt. Es war ab dem 27.01.2014 bis 13.12.2016 die Frist im BCM-Konzept (Version 1.1., genehmigt 27.01.2014) mit 10 bis 14 Tagen unangemessen lange festgelegt und nicht in nachvollziehbarer Weise dokumentiert. Die Frist von 10-14 Tagen, um wesentlichen Daten und Funktionen zurückzugewinnen ist in Bezug auf die Erbringung von Wertpapierdienstleistungen und Anlagetätigkeiten unangemessen lange und gewährleistet keine schnellstmögliche Behebung von Fehlern. Damit ist keine Kontinuität der Erbringung von Wertpapierdienstleistungen und Anlagetätigkeiten sichergestellt.

Erst mit 13.12.2016 (BCM-Konzept Version 1.2, Seite 10) wurde eine Wiederaufnahmefrist von maximal vier Stunden für die als kritischen Prozesse definierten Kerngeschäftsprozesse Zahlungsverkehr, Kundenhandel, Private Banking/Vermögensverwaltung, Anti Money Laundering, Treasury und Settlement schriftlich festgelegt und in nachvollziehbarer Weise dokumentiert.

b) Ein gesetzeskonformer schriftlicher Plan für die Szenarien "Totalausfall XXXX " (Szenario 1, Option 2) oder "Totalausfall IT" (Szenario 2, Option 2) war ab 19.04.2013 bis 13.12.2016 insofern nicht vorhanden, als nicht in gesetzeskonformer Weise schriftlich festgelegt und in nachvollziehbarer Weise dokumentiert war,

• wie, von wem und in welchem Zeitraum Ersatzräumlichkeiten in Bezug auf die Erbringung von Wertpapierdienstleistungen und Anlagetätigkeiten innerhalb angemessener Frist zur Verfügung gestellt werden;

• wie, von wem und in welchem Zeitraum die erforderliche Hardware in Bezug auf die Erbringung von Wertpapierdienstleistungen und Anlagetätigkeiten innerhalb angemessener Frist zur Verfügung gestellt wird;

Erst mit 13.12.2016 (BCM-Konzept, Version 1.2., Seite 15f) wurden neun Notfallarbeitsplätze binnen vier Stunden für alle kritischen Kernprozesse (Zahlungsverkehr, Kundenhandel, Private Banking/Vermögensverwaltung, Anti Money Laundering, Treasury und Settlement) bzw. weitere sieben Notfallarbeitsplätze innerhalb 24 Stunden für die restlichen Fachabteilungen - alle am Hauptstandort XXXX - schriftlich festgelegt und in nachvollziehbarer Weise dokumentiert. Darin finden sich auch konkrete Regelungen und Prozedere für den Zutritt zu den Räumlichkeiten sowie bezüglich deren Ausstattung.

c) Ein gesetzeskonformer schriftlicher Plan für die Szenarien "Totalausfall XXXX " (Szenario 1, Option 2) oder "Totalausfall IT" (Szenario 2, Option 2) war von 19.04.2013 bis 13.12.2016 auch insofern nicht vorhanden, als nicht in gesetzeskonformer Weise schriftlich festgelegt und in nachvollziehbarer Weise dokumentiert war,

• wo, wie, von wem und in welchem Zeitraum die gesicherten Datenbanken und Daten (inkl. Betriebssysteme) für Wertpapierdienstleistungen und Anlagetätigkeiten innerhalb angemessener Frist zur Verfügung gestellt werden sowie

• wie und in welchem Zeitraum Wertpapierdienstleistungen und Anlagetätigkeiten mit externer Anbietung von den jeweiligen Dienstleistern innerhalb angemessener Frist wieder hergestellt werden können.

Erst mit 13.12.2016 wurde durch den IT-Disaster-Recovery-Plan (Version 1.0, Seite 4) und den IT-Notfall-Plan (Version 2.0, Seite 16) schriftlich festgelegt und in nachvollziehbarer Weise dokumentiert, dass bei der XXXX auch ein Ausfallserver installiert ist, auf den alle Systeme der Bank mit Bezug zu Wertpapierdienstleistungen und Anlagetätigkeiten im vier Stunden Takt repliziert werden. Zusätzlich wurde ab 13.12.2016 schriftlich festgelegt und in nachvollziehbarer Weise dokumentiert, dass alle Daten mit Bezug zu Wertpapierdienstleistungen und Anlagetätigkeiten an den Tagen Montag - Donnerstag auf externes Band gespeichert und einmal wöchentlich aus der Bank zu dem externen Verwahrer " XXXX " verbracht wird (IT-Disaster-Recovery-Plan Version 1.0 Seiten 4 und 7, IT-Notfall-Plan Version 2.0 Seite 12).

III. Die XXXX haftet gemäß § 9 Abs 7 VStG für die über den Beschuldigten verhängte Geldstrafe und die Verfahrenskosten zur ungeteilten Hand.

Sie haben dadurch folgende Rechtsvorschriften verletzt:

Ad. I. § 39 Abs 2 iVm Abs 2b Z 5 BWG,BGBl Nr. 532/1993 idF BGBl. I Nr. 184/2013 iVm § 11 Abs 2 KI-RMV BGBl II Nr 487/2013 iVm § 98 Abs 5 Z 4 BWG, BGBl Nr 532/1993 idF BGBl I Nr 117/2015;

Ad. II. § 17 Abs 3 WAG 2007, BGBl I Nr 60/2007 idF BGBl I Nr 69/2015 iVm § 95 Abs 2 Z 2 WAG 2007, BGBl I Nr 60/2007 idF BGBl I Nr 184/2013

Wegen dieser Verwaltungsübertretungen wird über Sie folgende Strafe verhängt:

Tabelle kann nicht abgebildet werden

Weitere Verfügungen (z.B. Verfallsausspruch, Anrechnung von Vorhaft):

--

Ferner haben Sie gemäß § 64 des Verwaltungsstrafgesetzes (VStG) zu zahlen:

• 1.000 Euro als Beitrag zu den Kosten des Strafverfahrens, das sind 10% der Strafe, mindestens jedoch 10 Euro (ein Tag Freiheitsstrafe gleich 100 Euro);

• 0 Euro als Ersatz der Barauslagen für .

Der zu zahlende Gesamtbetrag (Strafe/Kosten/Barauslagen) beträgt daher

11.000 Euro."

2. Mit Prüfbericht der XXXX vom 30.01.2013 wurden bei der haftungspflichtigen Gesellschaft Mängel im Business Continuity Management und im Bereich Notfallplanung aufgezeigt (FMA-Akt, Beilagenakt, Beilage ./1).

3. Mit Schreiben vom 19.04.2013 erfolgte eine Stellungnahme der haftungspflichtigen Gesellschaft (FMA-Akt, Beilagenakt, Beilage ./2).

4. Mit Aufforderung zur Rechtfertigung vom 21.04.2017, dem BF2 zugestellt am 25.04.2017, leitete die FMA das gegenständliche Verwaltungsstrafverfahren ein (FMA-Akt, ON 06).

5. Am 08.05.2017 nahm der ausgewiesene Rechtsvertreter des BF2 Akteneinsicht bei der belangten Behörde (FMA-Akt, ON 09).

6. Mit Schreiben vom 30.05.2017 übermittelte der BF2 durch seinen Rechtsvertreter eine schriftliche Stellungnahme (FMA-Akt, ON 11).

7. Am 24.04.2018 erließ die FMA das gegenständlich angefochtene Straferkenntnis, welches dem BF2 nachweislich am 27.04.2018 zugestellt wurde (FMA-Akt, ON 14).

8. Mit Schreiben vom 24.05.2018, am selben Tag eingelangt bei der FMA, erhob der BF2 Beschwerde gegen das oben angeführte Straferkenntnis dem Grunde und der Höhe nach.

9. Mit Schriftsatz vom 28.05.2018 legte die FMA die Beschwerde und die Akten des Verwaltungsstrafverfahrens dem Bundesverwaltungsgericht (im Folgenden: BVwG) zur Entscheidung vor (BVWG-Akt, OZ 1).

10. Am 02.10.2018 fand eine öffentliche mündliche Verhandlung vor dem BVwG statt. Das gegenständliche Verfahren wurde mit expliziter Zustimmung des ausgewiesenen Rechtsvertreters aller BF und der haftungspflichtigen Gesellschaft mit den Verfahren zu W107 2196664-1 (MMag. Peter WEINZIERL; "BF1") und zu W107 2196658-1 (Meinl Bank AG, haftungspflichtige Gesellschaft) zur gemeinsamen Verhandlung verbunden; der BF1, der BF2 und der ausgewiesene Rechtsvertreter aller BF sowie der haftungspflichtigen Gesellschaft und die belangte Behörde wurden gehört.

II. Das Bundesverwaltungsgericht hat erwogen:

Beweis wurde erhoben durch Einsicht in die diesen Verfahren zugrundeliegenden Verwaltungsakten aller Beschwerdeführer in den verbundenen Verfahren sowie die korrespondierenden Gerichtsakten und durch Abhaltung einer mündlichen Verhandlung am 02.10.2018 vor dem BVwG.

1. Festgestellter Sachverhalt: 1. Sachverhalt:

Der BF2 war von 28.12.2007 bis 25.10.2015 (Ende des Tatzeitraums zu allen Spruchpunkten) Mitglied des Vorstandes der haftungspflichtigen Gesellschaft. Der BF2 war als Vorstand für die Bereiche BackOffice und Marktfolge zuständig. Mit 25.10.2015 ist der BF2 aus dem Vorstand der haftungspflichtigen Gesellschaft ausgeschieden und aktuell als Bankangestellter bei der haftungspflichtigen Gesellschaft beschäftigt.

Die haftungspflichtige Gesellschaft ist ein im Firmenbuch unter FN XXXX eingetragenes Kreditinstitut mit Sitz und Geschäftsanschrift im Tatzeitraum in XXXX und einer Bankkonzession gemäß § 1 Abs. 1 BWG; sie ist gemäß Art. 1 Abs. 1 Nummer 1 der Verordnung Nr. 575/2013 ("Capital Requirements Directive" - "CRR") ein CRR-Kreditinstitut gemäß § 1a Abs. 1 BWG.

Die haftungspflichtige Gesellschaft ist eine international tätige Privatbank mit besonderem Fokus auf zentral - und osteuropäische Märkte. Die primären strategischen Geschäftsfelder sind Corporate & Investment Banking, Corporate & Bank Clients Relations, Customer Relations & Asset Management sowie Salestrading. Der Eigenhandel sowie das Kreditgeschäft spielen eine untergeordnete Rolle. Die Geschäftsbereiche Corporate & Banking Clients Relations sowie Corporate & Investment Banking sind im Tatzeitraum die primären Ertragsbringer, die beiden Geschäftsbereich sind für 60% der gesamten Betriebserträge verantwortlich, wobei rund 50% der gesamten Betriebserträge aus dem Treuhandgeschäft stammen (FMA-Akt, Beilagenakt, Beilage ./1).

Die Bilanzsummer der haftungspflichtigen Gesellschaft betrug per 30.09.2012 rund XXXX Mio., das EGT EUR - XXXX . Die Eigenmittel beliefen sich per 30.09.2012 auf rund EUR XXXX ., was zu einer Eigenmittelquote von 28,8% führte. Gemäß Mitarbeiterliste waren 60 Personen zum 30.09.2012 in der haftungspflichtigen Gesellschaft beschäftigt (FMA-Akt, Beilagenakt, Beilage ./1) und 67 Mitarbeiter im Jahr 2016 (FMA-Akt, ON 14).

Die haftungspflichtige Gesellschaft erbringt Wertpapierdienstleistungen und Anlagetätigkeiten und verfügt über eine direkte Anbindung zur Wiener Börse (ON 14).

Im Jahr 2016 verzeichnete die haftungspflichtige Gesellschaft EUR XXXX ,- an Betriebserträgen und erwirtschaftete EUR XXXX ,- an Provisionserträgen aus Wertpapiergeschäften. Die Provisionserträge aus Wertpapiergeschäften betrugen im Jahr 2016 sohin rund 19 % der Betriebserträge (ON 14).

Der BF2 hat keine Sorgepflichten. Er machte im gesamten Verfahren keine Angaben zu seinen Einkommens- und Vermögensverhältnissen (VP, S. 15). Der BF2 ist strafgerichtlich unbescholten.

Vom 16.11.2012 bis 14.01.2013 führte die XXXX am Hauptstandort der haftungspflichtigen Gesellschaft, XXXX , eine Vorortprüfung durch, im Zuge derer folgende - für das gegenständliche Verfahren relevante - Mängel im Bereich "Operationelles Risiko" der haftungspflichtigen Gesellschaft festgestellt und im Prüfbericht vom 30.01.2013 wie folgt dokumentiert wurden (FMA-Akt, Beilagenakt, Beilage ./1; wörtlich, auszugsweise):

-

"Nr. 88. - Strategische Vorgaben zum Management der Risiken aus Infrastruktur und externen Ereignissen sind nicht vorhanden".

-

"Nr. 89. - Die Notfallplanung ist unzureichend und enthält keine ausreichenden Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebes".

-

"Nr. 94. - Eine tourliche Überprüfung der IT-Notfallplanung findet nicht statt bzw. sind Teilbereiche bisher noch nicht evaluiert."

Zur Feststellung Nr. 88 wurde erläuternd ausgeführt (FMA-Akt, Beilagenakt, Beilage ./1, Rz 308, wörtlich):

"Zu den weiteren Infrastrukturrisiken bzw. Risiken aus externen Ereignissen wurden diverse Unterlagen übergeben. Diese umfassen vorwiegend den Leitfaden zum Brandschutz, den Leitfaden zum Stromausfall, die Brandschutzordnung sowie eine Übersicht über Kontaktdaten diverser Dienstleister. Festzustellen ist jedoch, dass strategische Vorgaben zum Management der Risiken aus Infrastruktur und externen Ereignissen nicht vorliegen. Adäquate strategische Vorgaben sind zu erstellen und deren Einhaltung zu überwachen.".

Zur Feststellung Nr. 89 wurde erläuternd ausgeführt (FMA-Akt, Beilagenakt, Beilage ./1, Rz 309, wörtlich):

"Darüber hinaus ist festzustellen, dass die erwähnten Unterlagen keine ausreichende Notfallplanung darstellen, da es sich - insbesondere bei den beiden Leitfäden - um eine kurze Auflistung von Fakten handelt und nicht um einen umfassenden Plan einschließlich relevanter Notfallmaßnahmen sowie Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebs. Ein adäquater Notfallplan ist zu erstellen und um Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebs zu erweitern.".

Zur Feststellung Nr. 94 wurde erläuternd ausgeführt (FMA-Akt, Beilagenakt, Beilage ./1, Rz 321, wörtlich):

"Eine IT-Notfallplanung wurde vorgelegt. Festzustellen ist, dass eine tourliche Überprüfung der Notfallplanung nicht stattfindet sowie das wesentliche Szenario "Totalausfall XXXX " bisher keiner Evaluierung unterzogen wurde. Die IT-Notfallplanung ist regelmäßig und umfassend auf Aktualität und Umsetzbarkeit zu prüfen.".

Der Prüfbericht der XXXX vom 30.01.2013 enthält die Feststellung, dass die IT-Notfallplanung selbständig von der EDV erstellt wird, allerdings ohne Schnittstellen zum OpRisk - Verantwortlichen, und die Empfehlung, dass die IT-Notfallplanung nicht ausreichend in das OpRisk - Management integriert ist, und deshalb eine entsprechende Kommunikation zu implementieren und zu dokumentieren ist (FMA-Akt, Beilagenakt, Beilage ./1, Rz 322).

Der Prüfbericht der XXXX vom 30.01.2013 wurde der haftungspflichtigen Gesellschaft mit Schreiben vom 14.03.2013, adressiert "zu Handen des Vorstandes", zugestellt.

Vorstandsmitglieder zum damaligen Zeitpunkt waren der BF1 und der BF2.

Mit Schreiben vom 19.04.2013 (Beginn des Tatzeitraums zu Spruchpunkt II.) übermittelte die haftungspflichtige Gesellschaft eine Stellungnahme (Beilage ./2 im Beilagenakt der FMA), welche vom BF2 gemeinsam mit einer weiteren Person (" XXXX ") unterschrieben ist. In dieser Stellungnahme führte die haftungspflichtige Gesellschaft zu den Feststellungen Nr. 88, 89 und 94 zusammengefasst aus, dass in der haftungspflichtigen Gesellschaft

-

im 3. Quartal 2013 ein Handbuch zum "Business Continuity Management" erstellt wird (zu Nr. 88), wobei die beabsichtigte Vorgangsweise, die Ausgangsbasis und das beabsichtigte Ergebnis explizit angeführt wi (FMA-Akt, Beilagenakt, Beilage./2, S. 9);

-

ein Notfallkonzept inkl. Notfallplänen für ausgewählte Szenarien - auf Basis der Business Impact Analyse - definiert und dokumentiert wird (zu Nr. 89), wobei die beabsichtigte Vorgangsweise, die Ausgangsbasis und das beabsichtigte Ergebnis explizit angeführt wird (FMA-Akt, Beilagenakt, Beilage./2, S.9);

-

eine Überprüfung der IT-Notfallplanung im 3. Quartal 2013 geplant ist (Zu Nr. 94), wobei die beabsichtigte Vorgangsweise - Fokus auf Evaluierung bzw. Testen des Szenarios "Totalausfall XXXX " - und das beabsichtigte Ergebnis explizit angeführt wird (FMA-Akt, Beilagenakt, Beilage./2, S.9).

Die haftungspflichtige Gesellschaft verfügte in den Tatzeiträumen (zu Spruchpunkt I.: 01.01.2014 - 25.10.2015; Spruchpunkt II.:

19.04.2013 - 25.10.2015) über folgendes, gegenständlich relevante, Regelwerk:

* Regelwerk "Notfallplan für IT", Stand: Oktober 2013 (im Folgenden:

Regelwerk "Notfallplan für IT"; Beilage ./1 zum VP), aktualisiert am 09.12.2013;

* Regelwerk "Business Continuity Management Konzept" Version 1.0, vom 20.01.2014, genehmigt vom Gesamtvorstand am 27.01.2014 (im Folgenden: Regelwerk "BCM-Konzept"; Beilage ./1 zur Rechtfertigung).

Das Regelwerk "Notfallplan für IT" vom Oktober 2013 wurde am 09.12.2013 aktualisiert und war im hier gegenständlichen Tatzeitraum die einzig maßgebliche Version; es gab darüber hinaus im hier maßgeblichen Tatzeitraum keine weiteren Versionen dieses Regelwerks. Erst im März 2016 (Genehmigung durch den Gesamtvorstand 15.03.2016) wurde das Regelwerk "Notfallplan für IT" überarbeitet und durch das Dokument "IT-Notfallplan", Version 1.0, ersetzt.

Vor dem 27.01.2014 verfügte die haftungspflichtige Gesellschaft über kein schriftliches Regelwerk betreffend "BCM-Konzept." Die Erstversion des Regelwerks "BMC-Konzept", Version 1.0, stammt aus dem Jahr 2014, konkret vom 20.01.2014 (Genehmigung Gesamtvorstand 27.01.2014) und wurde im März 2016 (Genehmigung Gesamtvorstand 11.03.2016) durch das Regelwerk "Business Continuity Management Konzept", Version 1.1., ersetzt (FMA-Akt, Beilagenakt, Beilage ./2, S. 9; BVwG-Akt, VP S. 10).

Zu den Räumlichkeiten der haftungspflichtigen Gesellschaft ist festzustellen, dass sich der Kassensaal in den Tatzeiträumen im 1. Stock des Hauptgebäudes der haftungspflichtigen Gesellschaft an der Adresse XXXX , befand. Das Hauptgebäude an der gennannten Adresse ist das Zentrum der Geschäftstätigkeit der haftungspflichtigen Gesellschaft. Das primäre Rechenzentrum (zur technischen Abwicklung der Geschäftstätigkeiten) der haftungspflichtigen Gesellschaft befand sich in den Tatzeiträumen im 5. Stock des Hauptgebäudes und war branchenüblich ausgestattet (BVwG-Akt, VP S.7, 8, Beilage./2). Für den Fall eines Ausfalls des Rechenzentrums im 5. Stock war laut Regelwerk "BCM-Konzept", Version 1.0, als auch laut Regelwerk "Notfallplan für IT" aus dem Jahr 2013, ein unabhängiger Ersatz-Serverraum im 1. Stock des Hauptgebäudes eingerichtet. Die Datensicherung zwischen dem Rechenzentrum im 5. Stock und dem Ersatz-Serverraum im 1. Stock des Hauptsandorts erfolgte im Tatzeitraum laufend und in Echtzeit. Die externe Datensicherung der haftungspflichtigen Gesellschaft fand im Tatzeitraum über Bänder bei den externen Dienstleistern XXXX und einem Schließfachverwaltungsdienst statt (BVwG-Akt, VP S.11, 12).

Die Regelungen über die verwendete Hard- und Software für das Backup- und Restoresystem der haftungspflichtigen Gesellschaft waren im Regelwerk "Backup/Restore Konzept", Stand Mai 2014 (FMA-Akt, ON11, Beilage ./3) festgelegt. Danach erfolgt das "Backup" der Daten der haftungspflichtigen Gesellschaft auf Bandlaufwerken als auch auf virtuellen Libraries (Punkt 2. Hardware und Software) und werden für alle Backups Kopien erzeugt (Punkt 4. Copy jobs). Unter Punkt 5. (Restore) ist die Wiederherstellung von Daten festgelegt.

Über weitere Regelwerke verfügte die haftungspflichtige Gesellschaft in den angeführten Tatzeiträumen nicht.

Mit Schreiben der haftungspflichtigen Gesellschaft vom 13.12.2016 wurden der belangten Behörde die Umsetzungsmaßnahmen zu den Beanstandungen, wie im Straferkenntnis ausgeführt, mitgeteilt und damit den Beanstandungen entsprochen (Ende Tatzeitraum haftungspflichtige Gesellschaft).

1.2. Zum Regelwerk "Notfallplan für IT", Stand Oktober 2013:

Dieses Regelwerk definiert die Szenarien betreffend den Hauptstandort der haftungspflichtigen Gesellschaft XXXX "Stromausfall", "Serverraum 1. Stock fällt aus", "Serverraum 5. Stock fällt aus" und "Standort XXXX fällt aus" (Beilage ./1 zum VP).

Der interne Serverbetrieb der haftungspflichtigen Gesellschaft ist sowohl bei Ausfall eines Serverraums als auch bei einem Ausfall von bis zu drei Switches gewährleistet (Beilage ./1 zum VP, S. 4).

Für das Szenario "Standort XXXX fällt aus" ist Folgendes ausgeführt (wörtlich, auszugsweise):

"Dieses Szenario müsste ob seiner Durchführbarkeit evaluiert werden. Der angenommene Zeitraumen setzt eine rasche Verfügung sämtlicher im Folgenden beschriebener Ressourcen voraus.

Bei Ausfall des Hauptstandortes ist als Ersatzstandort das Büro XXXX denkbar.

Ein Wiederherstellen der derzeitigen Infrastruktur ist in einem annehmbaren Zeitraum nicht möglich.

Für einen Notbetrieb sind folgende Punkte abzuklären:

1. Räumlichkeiten [...]

2. Provideranbindung [...]

3. Hardware [...]

4. Daten

Sämtliche Daten und Datenbanken sind nicht ad hoc wieder herstellbar. Mangels Speicherkapazitäten kann auch nur ein Teil der Daten wiederhergestellt werden.

5. Dienste

Alle Dienste mit externer Anbindung können nicht kurzfristig wiederhergestellt werden. Darunter fallen unter anderem Datenträgeraustausch, XXXX . [...]." (Beilage ./1 zum VP, S. 18 f.)

Im Punkt "Zeitaufwand Wiederherstellung" ist für das Szenario "Standort XXXX fällt aus" festgelegt (wörtlich, auszugsweise):

"Die Zeiträume für die Wiederherstellung aller Systeme hängen von der Verfügbarkeit der Ressourcen ab. Ein eingeschränkter Betrieb soll in etwa ein bis zwei Wochen möglich sein." (Beilage ./1 zum VP, S. 21).

Im Regelwerk "Notfallplan für IT" ist nicht festgelegt, welche Daten der haftungspflichtigen Gesellschaft, wie die Kundendaten und Buchungszeilen der haftungspflichtigen Gesellschaft aus dem Prozess "Zahlungsverkehr" und wie die Rechnungslegung sowie die Belege aus dem Prozess "Kassageschäft" gespeichert werden.

1.3. Zum Regelwerk "BCM-Konzept", Version 1.0:

1.3.1. Allgemeines:

Im Regelwerk "BCM-Konzept" definiert die haftungspflichtige Gesellschaft folgende Prozesse ihres Kerngeschäfts als kritisch (FMA-Akt, ON 11, Beilage ./1, S. 9):

* Zahlungsverkehr

* Wertpapier Kundenhandel

* Kassa.

Im Regelwerk "BCM-Konzept" definiert die haftungspflichtige Gesellschaft folgende Sachverhalte als potentielle Krisenszenarien (FMA-Akt, ON 11, Beilage ./1, S. 9; wörtlich):

* "Szenario 1: (Teil-)Ausfall Gebäude - Kein bzw. limitierter Zugang zu den betreffenden Bereichen im Hauptgebäude (XXXX).

o Ursachen: ua. Brand, Bombendrohungen, Geiselnahme, Überfall, Terroranschlag, Naturkatastrophen, statische Probleme aufgrund von Erdbeben, Sturm, etc.;

o Auswirkungen/Konsequenzen: Gebäude ist nicht betretbar (ohne Vorankündigung); Es liegt ein behördliches Betretungsverbot vor;

* Szenario 2: (Teil-)Ausfall IT Infrastruktur d.h. Ausfall XXXX - Totaler bzw. teilweiser Ausfall der geschäftsrelevanten IT-Infrastruktur bzw. -Systeme

o Ursachen: ua. Leitungsbruch, Cyberangriff, Hackingangriff, Sabotage, Stromausfall, Naturkatastrophen, Elementarereignisse

o Auswirkungen/Konsequenzen: Kein Zugriff zu wesentlichen (geschäftsrelevanten) IT Systemen/Applikationen wie XXXX ; Keine Anmeldung (direkt oder via Webmail) möglich; kein Zugang zum Windows-Server."

Zudem ist Folgendes festgehalten (FMA-Akt, ON 11, Beilage ./1, S. 10; wörtlich, auszugsweise):

"Für die aktuell als ‚kritisch' definierten Kerngeschäftsprozesse gelten beispielsweise die folgenden strategischen Prämissen (‚BCP Strategie'):

• Zahlungsverkehr: Der ZV für die Kunden der XXXX ist unverändert aufrecht zu erhalten dh insb. die Ausführung bereits erhaltener Zahlungsaufträge (vor Eintritt der Krisensituation) sowie die Entgegennahme und Ausführung von neuen Zahlungsaufträgen (während der Krisensituation) muss gewährleistet werden.

• Wertpapier Kundenhandel: Es muss durch die Notfallplanung gewährleistet werden, dass der Verkauf und die damit verbundenen Arbeitsschritte zeitnah durchgeführt werden können, damit es zu keiner erheblichen Verzögerung und damit zu keinen (negativen) Auswirkungen auf die Verkaufskurse infolge der Verzögerung kommen kann.

• Kassageschäft: Die BCP Strategie für den Geschäftsprozess Kassa zielt darauf ab, den Kunden jederzeit die Durchführung von Bartransaktionen und Überweisungsauftragen ohne Verzögerung zu ermöglichen."

Für Details verweist das Regelwerk "BCM-Konzept" auf seinen Anhang II.

Der Anhang II besteht aus drei tabellarischen Listen, unterteilt in:

"a. Liste mit kritischen Geschäftsprozessen", "b. Kritische Geschäftsprozesse - Auswirkungen/Maßnahmen Szenario 1" und "c. Kritische Geschäftsprozesse - Auswirkungen/Maßnahmen Szenario 2" (FMA-Akt, ON 11, Beilage ./1, S. 15ff).

1.3.2. Zum Anhang II, Tabelle "a. Liste mit kritischen Geschäftsprozessen":

Diese Tabelle enthält eine Übersicht über die als kritisch definierten Prozesse ("Zahlungsverkehr", "Wertpapier Kundenhandel" und "Kassa") und die als kritisch (erforderlich) definierten Ressourcen (FMA-Akt, ON 11, Beilage ./1, S. 15).

Die Spalte "Kritische (erforderliche) Ressourcen" wird in die Rubriken "Personal", "Systeme", "Standort/Gebäude" und "Externe Zulieferer" untergliedert.

Die Rubrik "Personal" ist in "Abteilung" und "Mitarbeiter" untergliedert. In dieser Rubrik werden für die darin angeführten Abteilungen jeweils die erforderliche Anzahl an Mitarbeitern und ihren Positionen definiert.

Die Rubrik "Systeme" ist in "Hardware" und "Software" untergliedert. Unter "Hardware" werden angeführt: "2 PCs", "Telefon/alternativ Mobiltelefon (pro MA)", "Providerleitung", "Alarmanlage/Videoüberwachung" und "Zutrittskarten (-berechtigung)". Unter "Software" werden anfgeführt: " XXXX ", " XXXX ", "Zugang XXXX (für AVZ", " XXXX (für IZV)", " XXXX " und " XXXX ".

Die Rubrik "Standort/Gebäude" ist unterteilt in "erforderlich" und "s.o.".

Die Rubrik "Externe Zulieferer" ist unterteilt in: " XXXX " [Anm.:

gemeint wohl XXXX], " XXXX ", " XXXX (z.B. Broker, Banken)" und " XXXX (Sondertransport)".

1.3.3. Zum Anhang II, Tabelle "b. Kritische Geschäftsprozesse - Auswirkungen/Maßnahmen Szenario 1" - hier: " (Teil)Ausfall Gebäude":

In dieser Tabelle sind betreffend das Szenario 1 "(Teil)Ausfall Gebäude" die möglichen Auswirkungen für die als kritisch definierten Prozesse ("Zahlungsverkehr", "Wertpapier Kundenhandel" und "Kassa") definiert (FMA-Akt, ON 11, Beilage

./1, S. 16). Die Spalte "Auswirkungen" ist in die Rubriken "Max. Wiederanlaufzeit", "Auswirkungen im Detail" und "Maßnahmen im Detail" gegliedert.

In der Rubrik "Max. Wiederanlaufzeit" ist für den kritischen Prozess "Zahlungsverkehr" als Option 1 "ca. 1 Tag" und als Option 2 "10 bis 14 Tage" festgelegt.

In der Rubrik "Max. Wiederanlaufzeit" ist für den kritischen Prozess "Wertpapier Kundenhandel" als Option 1 "ca. 1 Tag" festgelegt. Eine Option 2 ist für diesen kritischen Prozess nicht definiert.

In der Rubrik "Max. Wiederanlaufzeit" ist für den kritischen Prozess "Kassa" als Option 1 "ca. 1 Tag", als Option 2 "10 bis 14 Tage" und als zusätzliche Option 2a "ca. 2 bis 3 Tage" festgelegt.

In der Rubrik "Auswirkungen im Detail" sind für die kritischen Prozesse "Zahlungsverkehr" und "Kassa" als Option 1 "Gebäude nicht betretbar (Strom vorhanden; Systeme laufen)" und als Option 2 "Gebäude nicht betretbar (Neuinstallation Software erforderlich)" definiert.

In der Rubrik "Auswirkungen im Detail" ist für den kritischen Prozess "Wertpapier Kundenhandel" als Option 1 "Gebäude nicht betretbar (Strom vorhanden; Systeme laufen)" definiert. Eine Option 2 ist für diesen kritischen Prozess nicht definiert; es ist angeführt: "keine Option 2!".

In der Rubrik "Maßnahmen im Detail" wird für die kritischen Prozesse "Zahlungsverkehr" und "Kassa" für die Option 2 (Wiederanlaufzeit ca. 10 bis 14 Tage) unterschieden in "1. Vor der Krisensituation" und

"2. Während der Krisensituation". Als Detailmaßnahme vor der Krisensituation ist angeführt: "Ersatzgebäude XXXX mit kritischen Ressourcen ausstatten (siehe kritische Hardware, Pkt. II.)."

Als Detailmaßnahmen für die Option 2 während der Krisensituation ist für die kritischen Prozesse "Zahlungsverkehr" und "Kassa" ausgeführt (wörtlich, auszugsweise):

-

"Entsendung der ausgewählten ZV & Treasury MA ins Ersatzgebäude (AL/AL Stv ZV & Treasury entscheiden über Versendung)

-

Server: Aufsetzen der Server im Ersatzgebäude durch IT -> siehe ,IT Notfallplan (Ausfall XXXX)'

-

Daten: "Abholung Daten-Back Up Bänder (Tresor XXXX) durch Leitung Verwaltung & Einspielung Daten durch Leitung IT

-

Kommunikation (extern): Aushang am Gebäude, Notfallhandy (mit Rufumleitung und Mailbox inkl. Verweis auf aktiven ZV sowie relevante Telefonnummern für Kontaktaufnahme

-

Rufumleitung auf Telefon XXXX

-

Verteilung bzw. Aktivierung Mobiltelefone für ausgewählte AMPB Kundenbetreuer".

Für den kritischen Prozess "Kassa" ist für die Option 2a "(zur Sicherstellung der raschen Auszahlung): Wiederanlaufzeit ca. 2 bis 3 Tage" als Detailmaßnahme ist darüber hinaus festgelegt: "Datenbank Auswertung über SQL und Aufsetzen von Grunddaten auf Excel Tabellen (statt Aussetzen Datenbank und Einspielung der Back Up Daten -> siehe Option 2)".

Für den kritischen Prozess "Wertpapier Kundenhandel" sind ausschließlich "Maßnahmen im Detail" für die Option 1 (Wiederanlaufzeit ca. 1 Tag) definiert. Für die Option 2 (Wiederanlaufzeit ca. 10 bis 14 Tage) wurden keine Detailmaßnahmen festgelegt.

1.3.4. Zum Anhang II, Tabelle "c. Kritische Geschäftsprozesse - Auswirkungen/Maßnahmen Szenario 2" - hier: " (Teil)Ausfall IT":

In dieser Tabelle sind für das Szenario 2 "(Teil)Ausfall IT" für die als kritisch definierten Prozesse ("Zahlungsverkehr", "Wertpapier Kundenhandel" und "Kassa") mögliche Auswirkungen festgelegt (FMA-Akt, ON 11, Beilage ./1, S. 17). Die Spalte "Auswirkungen" ist in die Rubriken "Max. Wiederanlaufzeit", "Auswirkungen im Detail" und "Maßnahmen im Detail" gegliedert.

In der Rubrik "Max. Wiederanlaufzeit" ist für alle kritischen Prozesse ("Zahlungsverkehr", "Wertpapier Kundenhandel" und "Kassa") als Option 2 jeweils "10 bis 14 Tage" festgelegt.

In der Rubrik "Auswirkungen im Detail" ist für alle kritischen Prozesse ("Zahlungsverkehr", "Wertpapier Kundenhandel" und "Kassa") als Option 1 "Teilausfall (Stromausfall, Ausfall Serverraum 1. Stock, Ausfall Serverraum 5. Stock)" und als Option 2 "Totalausfall IT Infrastruktur" definiert.

In der Rubrik "Maßnahmen im Detail" wird für die Option 1 auf den "IT Notfallplan für Wiederherstellungszeiten sowie konkrete Maßnahmen" verwiesen.

Für die kritischen Prozesse "Zahlungsverkehr" und "Kassa" wird in Option 2 "(Wiederanlaufzeit ca. 10 bis 14 Tage)" zwischen "1. Vor der Krisensituation" und "2. Während der Krisensituation" unterschieden.

Als Detailmaßnahme vor der Krisensituation sind hier für die kritischen Prozesse "Zahlungsverkehr" und "Kassa" angeführt:

"Ersatzgebäude XXXX mit kritischen Ressourcen ausstatten (siehe kritische Hardware, Pkt. II.)."

Als Detailmaßnahmen während der Krisensituation sind hier ausgeführt (wörtlich, auszugsweise):

-

"Entsendung der ausgewählten ZV & Treasury MA ins Ersatzgebäude (AL/AL Stv ZV & Treasury entscheiden über Versendung)

-

Server: Aufsetzen der Server im Ersatzgebäude durch IT -> siehe ‚IT Notfallplan (Ausfall XXXX)'

-

Daten: "Abholung Daten-Back Up Bänder (Tresor XXXX) durch Leitung Verwaltung & Einspielung Daten durch Leitung IT

-

Kommunikation (extern): Aushang am Gebäude, Notfallhandy (mit Rufumleitung und Mailbox inkl. Verweis auf aktiven ZV sowie relevante Telefonnummern für Kontaktaufnahme)

-

Rufumleitung auf Telefon XXXX bzw. Mobiltelefone für ausgewählte Kundenbetreuer".

Für den kritischen Prozess "Kassa" ist als Detailmaßnahmen für die Option 2 zudem definiert: "Koordination XXXX Sondertransport (‚Geldwagen') durch AL/AL Stv. Kassensaal - Leiter Kassensaal direkt Vorort. Info zu Kontostand über MA am XXXX ."

Für den kritischen Prozess "Kassa" ist als Detailmaßnahmen für die Option 2a "(zur Sicherstellung der raschen Auszahlung):

Wiederanlaufzeit ca. 2 bis 3 Tage" als Detailmaßnahme darüber hinaus festgelegt: Datenbank Auswertung über SQL und Aufsetzen von Grunddaten auf Excel Tabellen (statt Aussetzen Datenbank und Einspielung der Back Up Daten -> siehe Option 2)".

Für den kritischen Prozess "Wertpapier Kundenhandel" ist in der Rubrik "Maßnahmen im Detail" angeführt: "Option 1 & 2 siehe oben".

1.3.5. Zusammenfassung:

Die folgenden, von der haftungspflichtigen Gesellschaft definierten Szenarien waren zu prüfen:

* Szenario 1 "(Teil)-Ausfall Gebäude", Option 1, (in Folge: Szenario "Teilausfall Gebäude")

* Szenario 1 "(Teil)-Ausfall Gebäude", Option 2, (in Folge: Szenario "Totalausfall Gebäude")

* Szenario 2 "(Teil)-Ausfall IT Infrastruktur", Option 1, (in Folge: Szenario "Teilausfall IT")

* Szenario "(Teil)-Ausfall IT Infrastruktur", Option 2, (in Folge: Szenario "Totalausfall IT").

Für den Fall, dass es überhaupt keinen Zugang zum Hauptgebäude der haftungspflichtigen Gesellschaft gibt oder es zu einem Totalausfall der IT-Infrastruktur bzw. der IT-Systeme im Hauptgebäude kommt, war sowohl im Regelwerk "BCM-Konzept" als auch im Regelwerk "Notfallplan für IT" als externes Ausweichgebäude ein Haus am XXXX festgelegt.

Konkretisierungen hinsichtlich der Zurverfügungstellung der im Regelwerk "BCM-Konzept" als erforderlich definierten Ressourcen für die Erbringung der Bankgeschäfte der haftungspflichtigen Gesellschaft im Ersatzgebäude sowie für die Erbringung der Wertpapierdienstleistungen und Anlagetätigkeiten durch die haftungspflichtige Gesellschaft sind im Regelwerk "BCM-Konzept" weder für das Szenario "Totalausfall Gebäude" noch für das Szenario "Totalausfall IT" festgelegt.

Für alle als kritisch definierten Prozesse wird im Regelwerk "BCM-Konzept" sowohl für das Szenario "Totalausfall IT" als auch für das Szenario "Totalausfall Gebäude" eine maximale Wiederanlaufzeit von 10 bis 14 Tagen festgelegt.

Für den kritischen Prozess "Wertpapier Kundenhandel" ist im Regelwerk "BCM-Konzept" kein Szenario "Totalausfall Gebäude" festgelegt.

Für das Szenario "Teilausfall IT" werden für alle kritischen Prozesse als Detailmaßnahmen auf den IT-Notfallplan verwiesen.

Für den kritischen Prozess "Wertpapier Kundenhandel" werden im Regelwerk "BCM-Konzept" weder im Szenario "Teilausfall IT" noch im Szenario "Totalausfall IT" Detailmaßnahmen angeführt, sondern hierfür lediglich auf "oben" verwiesen.

Für die Szenarien "Totalausfall Gebäude" und "Totalausfall IT" ist eine Konkretisierung der Zurverfügungstellung der Datenbanken, Daten und Betriebssysteme der haftungspflichtigen Gesellschaft im Regelwerk "BCM-Konzept" weder für Wertpapierdienstleistungen und Anlagetätigkeiten der haftungspflichtigen Gesellschaft noch für die Erbringung der Bankgeschäfte der haftungspflichtigen Gesellschaft festgelegt.

Eine Konkretisierung betreffend die Wiederherstellung der bankbetrieblichen und bankgeschäftlichen Dienste der haftungspflichtigen Gesellschaft mit externer Anbietung durch die jeweiligen Dienstleister ist im Regelwerk "BCM-Konzept" weder für das Szenario "Totalausfall Gebäude" noch für das Szenario "Totalausfall IT" enthalten.

Eine Konkretisierung hinsichtlich der Wiederherstellung von Wertpapierdienstleistungen und Anlagetätigkeiten der haftungspflichtigen Gesellschaft mit externer Anbietung durch die jeweiligen Dienstleister ist im Regelwerk "BCM-Konzept" weder für das Szenario "Totalausfall Gebäude" noch für das Szenario "Totalausfall IT" festgelegt.

Die Szenarien "Totalausfall Gebäude" und "Totalausfall IT" sind mit dem Szenario "Standort XXXX fällt aus" im Regelwerk "Notfallplan für IT" gleichzusetzen.

Das Regelwerk "BCM-Konzept" verweist im Anhang I unter der Überschrift "Notfallpläne der XXXX " auf ein Dokument "IT-Notfallplan", Stand: 09.12.2013 (FMA-Akt, ON11, Beilage ./1, S. 14).

2. Beweiswürdigung:

Der festgestellte Sachverhalt ergibt sich aus den Verwaltungsakten der belangten Behörde zu den Verfahren und den Akten des Bundesverwaltungsgerichts sowie durch Durchführung einer mündlichen Verhandlung, insbesondere aus den Angab

Quelle: Bundesverwaltungsgericht BVwg, https://www.bvwg.gv.at

© 2025 JUSLINE

JUSLINE® ist eine Marke der ADVOKAT Unternehmensberatung Greiter & Greiter GmbH.

www.jusline.at