



BERICHT DER FMA

**BLACKOUT MATURITY
LEVEL ASSESSMENT 2022**

INHALTSVERZEICHNIS

1	Einleitung	3
1.1	Relevanz eines Blackout für die Aufsicht	3
1.2	Massnahmen der FMA.....	4
1.3	Hinweise	4
2	Executive Summary.....	5
3	Blackout Assessment der FMA.....	6
3.1	Massnahmen im Pensionskassensektor	6
3.1.1	Vorbereitung.....	7
3.1.2	Bewältigung & Reaktion.....	8
3.1.3	Wiederanlaufen & Wiederherstellung.....	9
3.2	Legistische Anregungen der FMA	10
3.2.1	Möglichkeit der Fristerstreckung bzw. Fristunterbrechung.....	10
3.2.2	Informationspflichten und Wohlverhaltensregeln	10
4	Abkürzungsverzeichnis	12
5	Abbildungsverzeichnis	12

1 EINLEITUNG

1.1 RELEVANZ EINES BLACKOUT FÜR DIE AUFSICHT

Unsere Gesellschaft ist an die laufende und uneingeschränkte Stromversorgung und die damit verbundenen Bequemlichkeiten, die im Alltag meist als selbstverständlich wahrgenommen werden, gewöhnt. Ein Blackout – ein im Gegensatz zu lokalen Störungen länger andauernder und weite Teile Europas betreffender Strom-, Infrastruktur- sowie Versorgungsausfall – brächte jedoch neben nicht mehr funktionierender Beleuchtung und Heizung beispielsweise auch Wasser- und Treibstoffversorgungsprobleme durch dann ausgefallene Pumpen oder Auswirkungen auf den Verkehr und die Lebensmittelversorgung und damit auch gesellschaftliche Herausforderungen mit sich.

Das österreichische Bundesministerium für Landesverteidigung schätzte 2022 schon vor dem Ausbruch des Russland-Ukraine-Kriegs die Eintrittswahrscheinlichkeit eines Blackout in den kommenden fünf Jahren als hoch ein.¹ Seit Februar 2022 hat die Komplexität der Rahmenbedingungen für die europäische Stromnetzinfrastuktur noch weiter zugenommen. Im derzeitigen Umfeld stehen einem durch die Digitalisierung steigenden Stromverbrauch vor allem die folgenden Herausforderungen gegenüber:²

- die Abwehr potenzieller Cyberattacken auf das zusammenhängende europäische Stromnetz
- die vermehrte Umstellung auf erneuerbare Energien und damit teilweise auf eine stark wetterabhängige und dadurch volatile Produktivität dezentraler Windkraft-, Photovoltaik- oder Wasserkraftanlagen
- Auswirkungen des Klimawandels, z. B. mangelndes Kühlwasser zur Stromerzeugung bei Hitzewellen
- der Umgang mit veralteten Anlagen
- die verminderten bzw. eingestellten Gasflüsse aus Russland und auch
- Auswirkungen der geopolitisch veränderten Lage, die z. B. das Risikomanagement von Stromlieferanten mit bislang unbekanntem Situationen konfrontiert.

Insgesamt muss durch die Nichtspeicherbarkeit elektrischer Energie im Netz der erzeugte Strom immer im Einklang mit dem Verbrauch stehen. Der österreichische Übertragungsnetzbetreiber Austrian Power Grid muss hier fast täglich ausgleichend ein sogenanntes Redispatching (RD) – das sind Anweisungen zur Verschiebung der Stromproduktion – betreiben, um Engpässe im Stromnetz zu vermeiden. 2021 waren derartige Eingriffe an 241 Tagen notwendig. Heuer waren es bis Ende Juli schon 144 Tage. Das zeigt, dass im Stromnetz die Wahrung des erforderlichen Gleichgewichts zwischen Stromerzeugung und -verbrauch schon vor dem mit Spannung erwarteten Winter einen anspruchsvollen Prozess darstellt.

¹ Siehe z. B. *österreichisches Bundesministerium für Landesverteidigung, Sicher. Und Morgen? – Risikolandschaft Österreich 2022*, S. 54.

² Vgl. z. B. <https://www.saurugg.net/blackout/risiko-eines-strom-blackouts> vom 20. 9. 2022.

Zur aktuellen Lage der Gasversorgung Österreichs siehe <https://www.aggm.at/netzinformationen/versorgungssicherheit/lagebericht>.

1.2 MASSNAHMEN DER FMA

In diesem Umfeld kann jeder einen Beitrag leisten und Vorsorgemaßnahmen treffen.³ Die FMA hat in einem ersten Schritt zunächst die beaufsichtigten Unternehmen hinsichtlich der Problematik eines Blackout sensibilisiert und etwa Herbert Saurugg, MSc, Präsident der Österreichischen Gesellschaft für Krisenvorsorge, eingeladen, einen fachspezifischen Vortrag im Rahmen der FMA-Veranstaltung **Cyber-Resilienz für Leitungs- und Aufsichtsorgane** für Versicherungsunternehmen und Pensionskassen am 1. 6. 2022 zu halten.

In weiterer Folge hat die FMA ein eigenes Tool für ein **Blackout Maturity Level Assessment** entwickelt. Die grundsätzliche Struktur des Assessments ist an die von der FMA kreierten Cyber & Cloud Maturity Level Assessments angelehnt. Für Zwecke dieses Assessments wird ein „Blackout“ als ein plötzlicher überregionaler, weite Teile Europas betreffender und länger andauernder Strom-, Infrastruktur- sowie Versorgungsausfall verstanden. Konsequenzen eines solchen Ausfalls sind u. a. der Verlust des Telekommunikationsnetzwerks und der Stromversorgung für die IT-Infrastruktur, die weitgehende Störung der Verkehrsinfrastruktur sowie Einschränkungen grundlegender Versorgungsnetze (Treibstoff, Lebensmittel). Das Assessment ist in die drei Themenbereiche Vorbereitung, Bewältigung & Reaktion sowie Wiederanlaufen & Wiederherstellung unterteilt.

Im Sommer 2022 wurde das Blackout Maturity Level Assessment im Pensionskassensektor ausgerollt. Für 2023 ist geplant, diese Evaluierung auch im Versicherungsbereich durchzuführen. Die aus dem Assessment gewonnenen Erkenntnisse können auch bei potenziellen künftigen rollierenden Abschaltungen herangezogen werden.

Auf Basis der Auseinandersetzung mit der Problematik des Blackout hat die FMA schließlich legislatischen Handlungsbedarf identifiziert und **legistische Anregungen** formuliert.

1.3 HINWEISE

Dieser Bericht soll zur Sensibilisierung betreffend Blackout dienen und beleuchtet Maßnahmen, die die FMA sowie die österreichischen Pensionskassen bereits getroffen haben, um sich auf einen weite Teile Europas betreffenden und länger andauernden Strom-, Infrastruktur- sowie Versorgungsausfall vorzubereiten.

Aufgrund der leichteren Lesbarkeit wird in diesem Bericht durchgängig die männliche Form verwendet. Diese Bezeichnungen sind als geschlechtsneutral zu betrachten. Es wird ausdrücklich darauf hingewiesen, dass sich alle personenbezogenen Formulierungen grundsätzlich gleichermaßen auf Frauen und Männer beziehen.

Der Inhalt des Berichts basiert auf den Wahrnehmungen aus der Aufsichtstätigkeit sowie auf Informationen aus externen Quellen. Die rechtlichen Grundlagen bleiben durch diesen Bericht unberührt. Über die gesetzlichen Bestimmungen hinausgehende Rechte und Pflichten können aus diesem Dokument nicht abgeleitet werden.

Trotz sorgfältiger Aufbereitung und Recherche übernimmt die FMA keine Haftung für die Richtigkeit und Vollständigkeit der Daten und Inhalte in diesem Bericht.

³ Vgl. z. B. <https://gfkv.at/vorsorge/> vom 26. 9. 2022.

2 EXECUTIVE SUMMARY

Zur Evaluierung der Verwundbarkeit der Pensionskassen gegenüber dem Risiko eines Blackout hat die FMA im Jahr 2022 ein Blackout Maturity Level Assessment im Pensionskassensektor durchgeführt.

Das Ergebnis zeigt, dass Pensionskassen auch im Hinblick auf die vorherige Sensibilisierung durch die FMA bereits Maßnahmen einen möglichen Blackout betreffend gesetzt haben. Der Pensionskassensektor hat sich insbesondere mit den Möglichkeiten der Vorbereitung auf einen weite Teile Europas betreffenden und länger andauernden Strom-, Infrastruktur- sowie Versorgungsausfall auseinandergesetzt und auch konkrete Maßnahmen zur Bewältigung eines solchen Blackout vorgesehen. Schritte zum Wiederanlaufen bzw. zur Wiederherstellung weisen aktuell das größte Verbesserungspotenzial auf.

3 BLACKOUT ASSESSMENT DER FMA

Zur Evaluierung der Verwundbarkeit gegenüber dem Risiko eines Blackout hat die FMA im 2. Quartal 2022 die PK für das Risiko sensibilisiert und im 3. Quartal 2022 ein Blackout Maturity Level Assessment im Pensionskassen-sektor durchgeführt. Das Ergebnis: PK haben sich schon mit Maßnahmen, die infolge eines Blackout zu setzen wären, auseinandergesetzt – insbesondere mit Möglichkeiten zur Vorbereitung auf ein solches Ereignis, aber auch mit konkreten Maßnahmen zu seiner Bewältigung. Aktuell weisen das größte Verbesserungspotenzial Schritte zum Wiederanlaufen bzw. zur Wiederherstellung des Betriebs auf.

3.1 MASSNAHMEN IM PENSIONSKASSESEKTOR

Das FMA Blackout Maturity Level Assessment hat gezeigt: Bei einer Betrachtung nach Themenbereichen wird der höchste durchschnittliche Gesamtreifegrad bezüglich der Vorbereitung auf einen möglichen Blackout ausgewiesen. Knapp danach folgt der Themenbereich Bewältigung & Reaktion, während Wiederanlaufen & Wiederherstellung das größte Verbesserungspotenzial aufweist. Die Berechnungen basieren dabei auf einer dreistufigen Reifegradskala, bei der ein höherer Wert mit spezifischeren und detaillierteren Maßnahmensetzungen einhergeht.

Durchschnittsreifegrade pro Themenbereich

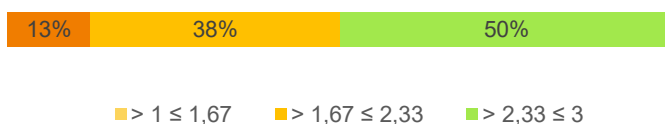
Vorbereitung	2,4
Bewältigung und Reaktion	2,4
Wiederanlaufen und Wiederherstellung	2,3

Am stärksten ist die Auseinandersetzung mit einem möglichen Blackout bislang im Hinblick auf vorbereitende Schritte erfolgt. Während die Kategorie Bewältigung & Reaktion knapp dahinterliegt, ergeben sich im Hinblick auf das Wiederanlaufen bzw. die Wiederherstellung nach einem Blackout die größten Verbesserungsmöglichkeiten.

Abbildung 1: Durchschnittsreifegrad pro Themenbereich

Die Hälfte der Pensionskassen erzielt einen jeweiligen Gesamtreifegraddurchschnitt, der im obersten Drittel der Reifegradbandbreite liegt.

Reifegradverteilung der Pensionskassen



Die Hälfte der PK konnte einen jeweiligen Gesamtreifegraddurchschnitt im obersten Drittel der erzielbaren Reifegradbandbreite erzielen, 13 % der PK befinden sich dagegen am anderen Ende des Spektrums.

Abbildung 2: Reifegradverteilung der PK

3.1.1 VORBEREITUNG

Drei Viertel der Pensionskassen befassen sich in ihrer IKT-Business Continuity Policy ausdrücklich mit Blackouts. Entsprechende Notfallpläne wurden von den meisten Unternehmen vorbereitet, wobei ein Notfallstab in allen Unternehmen entweder vorab vorgesehen ist oder auf Basis anderer Notfallplanvorgaben abgeleitet werden kann. Auch die der Erstellung eines Notfallplans vorangehenden Business-Impact-Analysen und Risikoanalysen wurden in knapp zwei Drittel der Unternehmen umfassend durchgeführt. Verbesserungsmöglichkeiten ergeben sich in diesem Themenbereich vor allem hinsichtlich der Durchführung von Notfallplantests.

Zu den Details:

- **IKT-Business Continuity Policy (IKT-BCP):** Drei Viertel der Unternehmen nennen Blackouts in deren IKT-BCP explizit.
- **Notfallpläne:** Diese wurden von den meisten Unternehmen vorbereitet. Die Hälfte der Pensionskassen behandelt ein Blackout-Szenario explizit und umfassend in Notfallplänen, wobei auch Schnittstellen zu IKT-Drittanbietern klar geregelt sind. Die meisten anderen Pensionskassen berücksichtigen kurzfristige bzw. lokal beschränkte Stromausfälle.

Notfallpläne: Diese behandeln das Szenario eines Blackouts. Auch Schnittstellen zu IKT-Drittanbietern sind in den Plänen umfasst.

● 1 ● 2 ● 3

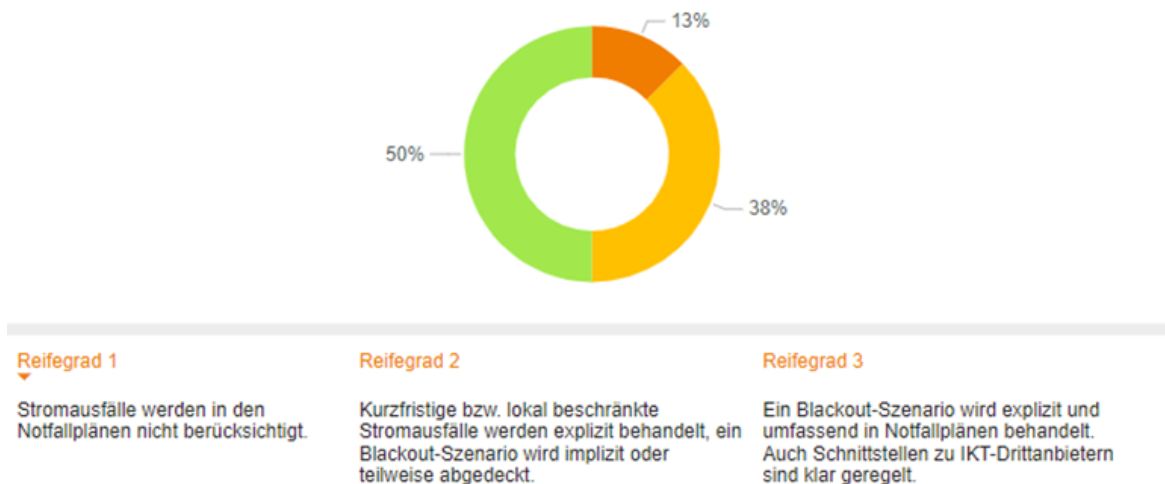


Abbildung 3: Notfallpläne

- **Notfallstab:** Pensionskassen sehen einen Blackout-Notfallstab entweder explizit vor oder können diesen aus anderen Notfallplanvorgaben ableiten. Die Frage nach dem Notfallstab erzielt in diesem Themenbereich den höchsten durchschnittlichen Gesamtreifegrad.
- **Business-Impact-Analyse und Risikoanalyse:** Knapp zwei Drittel der Pensionskassen geben an, für diese dem Notfallplan vorgelagerten Analysen ein volles Blackout-Szenario explizit und umfassend abgedeckt zu haben.
- **Abstimmung mit Fachexperten:** Blackout-Erfordernisse wurden von rund 40 % der Pensionskassen mit externen Fachexperten strukturiert abgestimmt.
- **Tests von Notfallplänen:** Rund 40 % der Pensionskassen haben solche Tests schon regelmäßig durchgeführt und dabei auch einen weiten Mitarbeiterkreis und externe Dienstleister in diese Übungen einbezogen. Über alle

Pensionskassen ergibt sich bezüglich der Notfallplantests in der Kategorie Vorbereitung insgesamt der niedrigste durchschnittliche Gesamtreifegrad.

Tests von Notfallplänen: Tests und komplexere Übungen von Notfallplänen sind ausgewählt und umgesetzt. Solche Tests beziehen (in deren Endausbaustufe) auch die wichtigsten Vertragspartner umfassend ein.

● 1 ● 2 ● 3



Abbildung 4: Test von Notfallplänen

3.1.2 BEWÄLTIGUNG & REAKTION

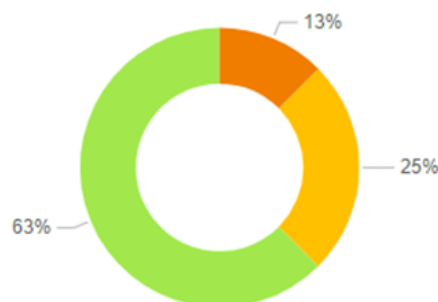
Die konkrete Auslösung eines Notfallplans ist in den meisten Pensionskassen entweder explizit klar vorgegeben oder die Auslöskriterien enthalten auch Einschätzungselemente. Die nach der Blackout-Identifikation erforderlichen Notfallpläne sind in knapp zwei Drittel der Pensionskassen in Papierform vor Ort verfügbar. Sodann nimmt das Ziel des Schutzes der IKT-Infrastruktur und der Informationssicherheit einen hohen Stellenwert ein. Pensionskassen definieren meist auch detaillierte Maßnahmen zur Absicherung der Betriebsgebäude. Konkrete Dienstanweisungen für Mitarbeiter, die den zu erwartenden Ausfall der üblichen Kommunikationskanäle berücksichtigen und Vorgaben zu Verhaltensweisen umfassen, sind demgegenüber meist ausbaufähig. Einen Notbetrieb erachten mehr als die Hälfte der Pensionskassen im Blackout-Fall für nicht erforderlich.

Zu den Details:

- **Auslösung Notfallpläne:** Das Eintreten eines Blackout ist in einem frühen Stadium von einem „gewöhnlichen“ Stromausfall nur schwer zu unterscheiden. Knapp zwei Drittel der Pensionskassen geben an, die Kriterien zur Auslösung eines Blackout-Notfallplans klar definiert zu haben, sodass für die jeweils zuständigen Personen das Erfordernis der Notfallplanauslösung eindeutig vorgegeben ist.

Auslösung Notfallpläne: Die Auslösung der Blackout-Notfallpläne ist klar definiert.

● 1 ● 2 ● 3



Reifegrad 1

Bislang wurden keine solchen Notfallpläne erstellt.

Reifegrad 2

Kriterien sind vorgegeben - die Auslösung des jeweiligen Notfallplans enthält auch Einschätzungselemente.

Reifegrad 3

Kriterien sind klar vorgegeben, sodass für die jeweils zuständigen Personen das Erfordernis einer Auslösung des jeweiligen Blackout-Notfallplans eindeutig definiert ist.

Abbildung 5: Auslösung Notfallpläne

- **Zugänglichkeit Notfallpläne:** In knapp zwei Drittel der Pensionskassen sind Blackout-Notfallpläne in Papierform verfügbar.
- **Schutz der IKT-Infrastruktur und der Informationssicherheit:** Maßnahmen zum Schutz der IKT-Infrastruktur und der Informationssicherheit sind für Pensionskassen von hoher Bedeutung. In drei Viertel der Unternehmen können kritische IKT-Systeme im Fall eines Blackout so heruntergefahren bzw. im Notbetrieb aufrechterhalten werden, dass keine physischen Schäden oder Verletzungen der IKT- bzw. der Informationssicherheit auftreten. Darüber hinaus sind Back-ups und Speicherprozesse von vornherein darauf ausgelegt, die Resynchronisierung von Daten und Systemen nach der Wiederherstellung einer stabilen Stromversorgung zu gewährleisten.
- **Absicherung von Betriebsgebäuden:** Ein Konzept für die längerfristige Sicherung des Betriebsgeländes bei einem Blackout liegt in jeder zweiten Pensionskasse vor.
- **Dienstanweisungen für Mitarbeiter:** Ein Viertel der Unternehmen hat Dienstanweisungen, die den zu erwartenden Ausfall der üblichen Kommunikationskanäle berücksichtigen und Vorgaben zu Verhaltensweisen im Blackout-Fall enthalten, umfassend und strukturiert ausgearbeitet. In rund 40 % der Pensionskassen liegen Dienstanweisungen und Kommunikationspläne zu einzelnen Teilaspekten vor. Bezüglich konkreter Dienstanweisungen sind somit im Pensionskassensektor insgesamt noch weitere Konkretisierungen möglich.
- **Notstromversorgung:** Mehr als die Hälfte der Pensionskassen geben an, keinen Notbetrieb während des Blackout zu benötigen. Nur in einem Ausnahmefall kann eine Notstromversorgung für mehr als 36 Stunden aufrechterhalten werden.

3.1.3 WIEDERANLAUFEN & WIEDERHERSTELLUNG

Während ein Notbetrieb bis zur Rückkehr zu einer stabilen Funktionsweise in allen Pensionskassen adressiert wird, haben nicht alle Unternehmen ein Vorgehen für die (vollständige) Wiederaufnahme des Geschäftsbetriebs definiert.

- **Notbetrieb bis zur Rückkehr zu einer stabilen Funktionsweise:** Knapp 40 % der Pensionskassen definieren in ihren Notfallplänen für diese Phase – bis hin zur Stabilisierung der Stromversorgung – Maßnahmen und

Prozesse detailliert und strukturiert. Auch in den anderen Unternehmen sind für einzelne Teilbereiche Maßnahmen und Prozesse vorgesehen.

- **Wiederanlaufen:** In knapp 40 % der Pensionskassen liegt ein Plan für die Einleitung und Umsetzung der Wiederaufnahme des Geschäftsbetriebs nach einem Blackout vor, und Prioritäten hinsichtlich des Wiederanlaufens (der kritischen Prozesse) sind in den Notfallplänen klar festgelegt. Zudem werden auch grundlegende Folgeproblematiken (z. B. der Ausfall von Mitarbeitern, Lieferketten, Geschäftspartnern etc.) berücksichtigt. Keine Kriterien und kein Vorgehen für die (vollständige) Wiederaufnahme des Geschäftsbetriebs haben ein Viertel der Pensionskassen definiert.

Im Ergebnis hat die FMA Pensionskassen zum Thema Blackout sensibilisiert und diesen ein eigens entwickeltes FMA Blackout Maturity Level Assessment zur Verfügung gestellt, das zeigt, dass die Pensionskassen bereits Maßnahmen im Hinblick auf einen potenziellen künftigen Blackout gesetzt haben. Die Unternehmen können aus dem Assessment ableiten, welche individuellen Verbesserungen noch möglich sind.

3.2 LEGISTISCHE ANREGUNGEN DER FMA

Die FMA hat im Zuge der Auseinandersetzung mit den verschiedenen Aspekten eines Blackout Bedarf für eine Evaluierung des rechtlichen Rahmens vor dem Hintergrund eines Blackout-Szenarios identifiziert:

3.2.1 MÖGLICHKEIT DER FRISTERSTRECKUNG BZW. FRISTUNTERBRECHUNG

So enthalten etwa die verschiedenen Aufsichtsgesetze Fristen, die sowohl für die beaufsichtigten Unternehmen als auch für die FMA relevant sind. Ein Blackout kann dazu führen, dass diese Fristen nicht eingehalten werden können. Die Nichteinhaltung von gesetzlichen Fristen kann verschiedene Konsequenzen nach sich ziehen. Es sollte deshalb definiert werden, dass im Fall eines Blackout oder eines anderen außergewöhnlichen Ereignisses diese Fristen entsprechend verlängert werden. Per Gesetz oder Verordnung festgesetzte Fristen können, wenn nicht ausdrücklich anderes bestimmt ist, nicht geändert werden. Das FMABG ermöglicht der FMA, die in den Materiengesetzen und Verordnungen genannten Fristen auf begründeten Antrag oder ohne Antrag durch Verordnung zu verlängern. Da im Fall eines Blackout sowohl eine Antragstellung als auch dessen Genehmigung bzw. die Erlassung einer Verordnung kaum möglich sein werden, sollte eine Fristerstreckung bzw. Fristunterbrechung bereits gesetzlich vorgesehen werden.

3.2.2 INFORMATIONSPFLICHTEN UND WOHLVERHALTENSREGELN

Durch einen Blackout wird aber etwa auch die Schadenabwicklung durch ein Versicherungsunternehmen verzögert bzw. können Schäden von betroffenen Versicherungsnehmern und Geschädigten nicht gemeldet werden. Ebenso würde im Pensionskassenbereich ein Blackout Leistungszahlungen der Pensionskassen beeinträchtigen, da sie nicht bzw. nur verspätet getätigt werden können.

Vor Abschluss eines Versicherungsvertrags ist der Versicherungsnehmer zu beraten, und diesem gegenüber bestehen Informationspflichten. Grundsätzlich hat die Informationserteilung auf Papier zu erfolgen, unter bestimmten Voraussetzungen kann diese auch auf elektronischem Weg erfolgen. Im Fall eines Blackout können diese Anforderungen möglicherweise nicht voll erfüllt werden.

Daher sollten entsprechende Anpassungen in Erwägung gezogen werden. Beispielsweise könnte die Beratungspflicht für die Dauer des Blackout ausgesetzt und – sobald dies wieder möglich ist – nachgeholt werden. Zu erwägen wäre aber auch, temporär die Möglichkeit von Execution-only-Geschäften zu schaffen. Die Informationspflichten könnten in eingeschränktem Umfang erfüllt und binnen einer gewissen Frist nach dem

Blackout nachgeholt werden. Ebenso könnte den laufenden Informationspflichten erst nach dem Ende des Blackout nachgekommen werden. Auch Pensionskassen haben Informationspflichten gegenüber Anwartschafts- und Leistungsberechtigten, die im Fall eines Blackout möglicherweise nicht oder nicht vollständig erfüllt und erst nach Beendigung des Blackout erbracht werden könnten.

4 ABKÜRZUNGSVERZEICHNIS

bzgl.	bezüglich
bzw.	beziehungsweise
d. h.	das heißt
etc.	et cetera
FMA	Finanzmarktaufsicht
vgl.	vergleiche
z. B.	zum Beispiel

5 ABBILDUNGSVERZEICHNIS

Abbildung 1: Durchschnittsreifegrad pro Themenbereich	6
Abbildung 2: Reifegradverteilung der PK	6
Abbildung 3: Notfallpläne	7
Abbildung 4: Test von Notfallplänen	8
Abbildung 5: Auslösung Notfallpläne	9