Digitale Workshop-Reihe
IT-Anforderungen für EbAV: Handlungsbedarfe und Schritte zur Umsetzung der DORA-Verordnung

Termine

- Termin 1: 14. März (Do), 10-13 Uhr
- Termin 2: 9. April (Di), 10-13 Uhr
- Termin 3: 7. Mai (Di), 10-13 Uhr
- **Termin 4: 4. Juni (Di), 14-17 Uhr**

Dauer

- Pro Workshop: 3 Stunden (165 Min. zzgl. einer Pause von 15 Min.)
- Insgesamt: 660 Minuten (ohne Pausen)

Zielsetzung

- Diese Workshop-Reihe – zusammen mit PwC und unterstützt v.a. durch die AG VAIT/DORA des aba-Fachausschusses Digitalisierung – will die EbAV bei der Vorbereitung auf die ab 17. Januar 2025 einzuhaltende DORA-Verordnung unterstützen und ihren Austausch dazu erleichtern.
- In den vier Terminen werden jeweils einzelne Themenschwerpunkt zur Umsetzung der DORA-Verordnung behandelt. Im Sinne einer Gap-Analyse sollen insbesondere Veränderungen im Vergleich zum VAIT-Rundschreiben herausgearbeitet werden. Die Einzelworkshops hängen zusammen, bauen aber inhaltlich nicht aufeinander auf. Eine Anmeldung nur zu einzelnen der vier Termine ist daher möglich.

Zielgruppe

Der digitale aba-Workshop richtet sich an Verantwortliche und Umsetzer der DORA-Verordnung in Pensionskassen und Pensionsfonds, die Mitglied der aba sind.

Referenten

- Rüdiger Giebichenstein (PwC Wirtschaftsprüfungsgesellschaft, Financial Services, Team Technology, Processes & Risk)
- Dirk Klevenhaus (PwC Wirtschaftsprüfungsgesellschaft, Financial Services, Team Technology, Processes & Risk)
- Verschiedene EbAV-Vertreter, v.a. aus der AG VAIT / DORA (siehe einzelne Workshop-Termine)

Digitale Workshop-Reihe
IT-Anforderungen für EbAV: Handlungsbedarfe und Schritte zur Umsetzung der DORA-Verordnung

INHALT UND THEMENSTELLUNG (Aktualisiert am 11.April 2024)

Die am 17. Januar 2023 in Kraft getretene und ab 17. Januar 2025 anzuwendende DORA-Verordnung wirft ihre Schatten voraus (Verordnung (EU) 2022/2554 vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011).

Bereits der Verordnungstext – als Level-I-Rechtsquelle künftig unmittelbar geltendes Recht – formuliert teils neue, teils detailliertere und darüber hinaus im Vergleich zum aktuellen VAIT-Rundschreiben der BaFin auch anders strukturierte aufsichtliche Anforderungen an die IT-Sicherheit.

Viele Details der Anforderungen wird die Kommission – basierend auf den Entwürfen der EU-Aufsichtsbehörden (ESA) – in Form technischer Regulierungs- und Durchführungsstandards (Level II-Regulierung) sowie von Leitlinien der ESA konkretisieren.

Am 13. März 2024 hat die Kommission gebilligte Fassungen von drei technischen Regulierungsstandards veröffentlicht, die ihr am 17. Januar 2024 als finale Entwürfe von den ESA zugeschickt wurden. Sie betreffen die weitere Harmonisierung von Tools, Methoden, Prozessen und Richtlinien für das IKT-Risikomanagement (Art. 15 Abs. 6 DORA-VO), die Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen (Art. 18 Abs. 3 DORA-VO) sowie die Prinzipien für das Management des IKT-Drittparteienrisikos (Art. 28 Abs. 10 DORA-VO). Die Billigung des ebenfalls im Januar 2024 von den ESA fertiggestellten Entwurfs eines technischen Durchführungsstandards über das Informationsregister(Art. 28 Abs. 9 DORA-VO) steht noch aus. Vor der endgültigen Verabschiedung der Regulierungsakte sind außerdem noch Rat und Europäisches Parlament zu beteiligen, die das Recht haben, Einwände zu erheben. Wegen der Europawahlen könnte sich die Veröffentlichung der finalen Texte bis Herbst verzögern. Weitere Teile des Level-II-Regulierungspakets wurden von den ESA am 8. Dezember 2023 bis zum 4. März 2024 zur Konsultation gestellt. Auch zu diesen Regulierungsakten müssen die ESA noch finale Entwürfe erstellen, die dann bis Anfang 2025 von der Kommission (unter Beteiligung von Rat und Europäischem Parlament) gebilligt werden müssen.

Änderungen in Details der Level-II-Regulierungstexte sind zwar noch möglich. Insgesamt liegt aber bereits jetzt eine verlässliche Informationsbasis für die verbleibende Vorbereitungszeit vor.

Angesichts des Umfangs der sich abzeichnenden Änderungen an die Anforderungen an die IT-Sicherheit durch die DORA-VO, ist die Frage, ob und wie die BaFin-Rundschreiben (VAIT, BAIT, ZAIT, KAIT) über Mitte Januar 2025 fortbestehen werden, derzeit noch offen. Es ist aber davon auszugehen, dass die BaFin auch nach dem Wirksamwerden der DORA-Verordnung in bestimmten Bereichen noch Raum für aufsichtliche Orientierung sieht. So wurde etwa am 1. Februar 2024 – unter expliziter Bezugnahme auf die DORA-Verordnung – das erstmals im Jahr 2018 von BaFin und Bundesbank veröffentlichte Merkblatt „Orientierungshilfe zu Auslagerungen an Cloud-Anbieter“ in überarbeiteter und erweiterter Form veröffentlicht, als „Aufsichtsmitteilung zu Auslagerungen an Cloud-Anbieter“.

Digitale Workshop-Reihe
IT-Anforderungen für EbAV: Handlungsbedarfe und Schritte zur Umsetzung der DORA-Verordnung

Konferenztechnik

Für die Veranstaltungen verwenden wir Microsoft Teams in der Webinar-Funktionalität. Nach Ihrer Anmeldung erhalten Sie einen Registrierungs-Link, über den Sie Zugang zu den Veranstaltungen erhalten.

Ihre Einbindung als Teilnehmer in den Workshop

Während der Vorträge besteht die Möglichkeit, Fragen über eine Chatfunktion zu stellen, danach jeweils auch mündlich.

Sie können auch gerne schon im Vorfeld des Workshops Fragen an die aba richten, möglichst zwei Werktage vor dem jeweiligen Workshop-Termin an veranstaltungen@aba-online.de. Ihre Fragen werden dann im Rahmen der Vorträge oder im jeweils anschließenden Fragenteil aufgegriffen.

Teilnahmegebühr

Die Teilnahmegebühr (da Verzicht auf externen Dienstleister für die Technik) für die nunmehr zwei Veranstaltungen beträgt 300 € und ist gem. § 4 Nr. 22a UStG von der Umsatzsteuer befreit. Die Gebühr für die Teilnahme an einer einzelnen Veranstaltung beträgt 150 €.

Die Anmeldung zu den verbleibenden zwei Workshops (III und IV) ist bis **6. Mail 2024** möglich. Anmeldungen zu einzelnen Workshops sind bis jeweils einen Tag vor Veranstaltungsbeginn möglich. Bitte verwenden Sie auch in diesem Fall das aktuelle Anmeldeformular zur gesamten restlichen Workshop-Reihe und nutzen Sie die Ankreuzoptionen für Angaben zu Ihrer Auswahl.

Veranstaltungsunterlagen

Der Bereich „Veranstaltungsunterlagen“ auf der Veranstaltungsseite jedes einzelnen Workshops auf der aba-Homepage wird vsl. ein bis zwei Tage vor dem Termin freigeschaltet. Voraussichtlich zwei Tage vor den Workshop-Terminen werden wir den aktuellen Stand der Vortragsfolien von Herrn Giebichenstein und Herrn Klevenhaus (PwC) sowie die Teilnehmerliste einstellen. Die Veröffentlichung der Folien der EbAV-Vertreter erfolgt nach der Veranstaltung.

Ansprechpartner

Interessenten wenden sich bitte wegen weiterer Informationen an:
Frau Ulrike Schulz
E-Mail: ulrike.schulz@aba-online.de

Digitale Workshop-Reihe
IT-Anforderungen für EbAV: Handlungsbedarfe und Schritte zur Umsetzung der DORA-Verordnung

Workshop I (14.03.2024, bereits durchgeführt):
VAIT-Rundschreiben und DORA: Gap-Analyse und Handlungsbedarfe
Grundlagen des IKT-Risikomanagements

- **Zielsetzung dieses Workshops**
  - Überblick über Struktur und Inhalte der VO
  - Priorisierungsmöglichkeiten bei der Umsetzung der Anforderung?
  - Zentrale Ergebnisse eines Mappings der Anforderungen im VAIT-Rundschreiben und der DORA-VO einschließlich der zugehörigen Regulierung auf Level II und III: Welche Herausforderungen kommen auf EbAV (neu) zu?
  - Proportionalität im VAIT-Rundschreiben und in der DORA-Verordnung: welche Gestaltungsräume verbleiben ab Januar 2025?

- **Schwerpunkte**
  - Anforderungen an Governance und die IT-Strategie und die von EbAV zu entwickelnden Strategien und Leitlinien
  - Ausgestaltung des IKT-Risikomanagementrahmens

    Hierbei u.a. behandelte Inhalte der DORA-VO: Artikel 5 und 6 aus Kapitel II „IKT-Risikomanagement“

- **Referenten**
  - Jörg Paßmann (RWE AG): Einführung und anschließende Moderation
  - Dirk Klevenhaus / Rüdiger Giebichenstein (PwC): Impulsvorträge
  - Gerald Kupatt (BASF SE, BASF Pensionskasse), Dr. Andreas Jurk (Barmer Pensionskasse), Dr. Thomas Müller (SOKA BAU), Christian Wolf (BVV): Praxisberichte und Fragen aus EbAV-Sicht

Digitale Workshop-Reihe
IT-Anforderungen für EbAV: Handlungsbedarfe und Schritte zur Umsetzung der DORA-Verordnung

Workshop II (09.04.2024, bereits durchgeführt):
Praktische Fragen des IKT-Risikomanagements

- **Zielsetzung dieses Workshops**
  - Die praktische Ausgestaltung des IKT-Risikomanagements, das sowohl in der DORA-Verordnung als auch über umfangreiche Level-II-Regulierungsakte detailliert geregelt ist, soll im Rahmen dieses Workshops näher untersucht werden.
  - Worauf sollten EbAV bei der Umsetzung achten?

- **Schwerpunkte**
  - Von EbAV zu entwickelnden Tools, Methoden, Prozesse und Richtlinien zum Umgang mit IKT-Risiken
  - Identifikation von Risiken, Schutz und Prävention, Erkennung, Reaktion und Wiederherstellung von Daten und Prozessen

    Hierbei u.a. behandelte DORA-Anforderungen:
    Artikel 7 bis 12 aus Kapitel II „IKT-Risikomanagement“

- **Referenten**
  - Dr. Christoph Schulte (Hoechster Pensionskassen): Begrüßung und Moderation
  - Dirk Klevenhaus / Rüdiger Giebichenstein (PwC): Impulsvorträge
  - Marcus Ippisch (Verka VK Kirchliche Vorsorge), Gabriele Mazarin (Philips Pensionskasse), Dr. Christoph Schulte (Hoechster Pensionskassen): Praxis-Berichte und Fragen aus EbAV-Sicht
  - Marco Suty (AKA): Business Continuity Management unter Anwendung der DORA-VO

Digitale Workshop-Reihe
IT-Anforderungen für EbAV: Handlungsbedarfe und Schritte zur Umsetzung der DORA-Verordnung

Workshop III (07.05.2024, bereits durchgeführt)
Drittparteienmanagement

- **Inhalte dieses Workshops**
  - Das Management des IKT-Drittparteienrisikos bildet einen inhaltlichen Schwerpunkt der DORA-Verordnung und untergliedert sich in Anforderungen an ein solides Management des IKT-Drittparteienrisikos durch Finanzinstitute einerseits und in die Vorschriften über einen Überwachungsrahmen für kritische IKT-Drittdienstleister andererseits. Insbesondere der erstgenannte Aspekt steht an diesem Workshop-Tag im Vordergrund.
  - Ein besonderer Fokus liegt auf die bei EbAV übliche Zusammenarbeit mit Dienstleistern bzw. mit Trägerunternehmen im Falle von Unternehmenseinrichtungen.

- **Schwerpunkte**
  - Erstellung eines Informationsregisters über vertragliche Vereinbarungen zur IKT-Nutzung, Vorschriften zur Bewertung von Konzentrationsrisiken, Anforderungen an die Ausgestaltung von Ausgliederungsvereinbarungen

    Hierbei u.a. behandelte DORA-Anforderungen:
    Artikel 28 bis 30 aus Kapitel V „Management des IKT-Drittparteienrisikos“

- **Referenten**
  - Christian Wolf (BVV): Einführung und Moderation
  - Dirk Klevenhaus / Rüdiger Giebichenstein (PwC): Impulsvortrag
  - Christian Betmann (Bayer-Pensionskasse), Christian Hartmann und Holger Prinz (SOKA-BAU), Gabriele Mazarin (Philips Pensionskasse) und Marcus Trommler (Evonik Industries): Praxis-Berichte und Fragen aus EbAV-Sicht

Digitale Workshop-Reihe
IT-Anforderungen für EbAV: Handlungsbedarfe und Schritte zur Umsetzung der DORA-Verordnung

Workshop IV (04.06.2024):
Weitere Fragen der DORA-Umsetzung: IT-Vorfälle und Meldeverpflichtungen, Testen der digitalen operationellen Resilienz

- **Inhalte dieses Workshops**
  - Als Abschluss der Workshopreihe werden zwei weitere Anforderungsbereiche der DORA-VO behandelt, zu denen umfangreiche Regulierungen durch technische Regulierungs- und Durchführungsstandards vorgesehen sind: Der Umgang mit Vorfällen und Anforderungen an das Testen der digitalen Betriebssicherheit.

- **Schwerpunkte**
  - Prozesse für die Behandlung IKT-bezogener Vorfälle, Klassifizierung und Meldung von Vorfällen
  - Allgemeine Testanforderungen und Regelungen zur Durchführung von Penetrationstests

    Hierbei u.a. behandelte DORA-Anforderungen:
    Artikel 17 bis 22 aus Kapitel III „Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle“
    Artikel 24 bis 25 aus Kapitel IV „Testen der digitalen operationalen Resilienz“

- **Referenten**
  - Marco Suty (AKA): Einführung und Moderation
  - Dirk Klevenhaus / Rüdiger Giebichenstein (PwC): Impulsvortrag:
  - Thomas Aschenbrenner (Mercer Pensionsfonds), Yannick Helmke und Nizar Jeribi (IBM Pensionskasse VVaG) und Alexander Kaesler (Hamburger Pensionsverwaltung): Praxis-Berichte und Fragen aus EbAV-Sicht