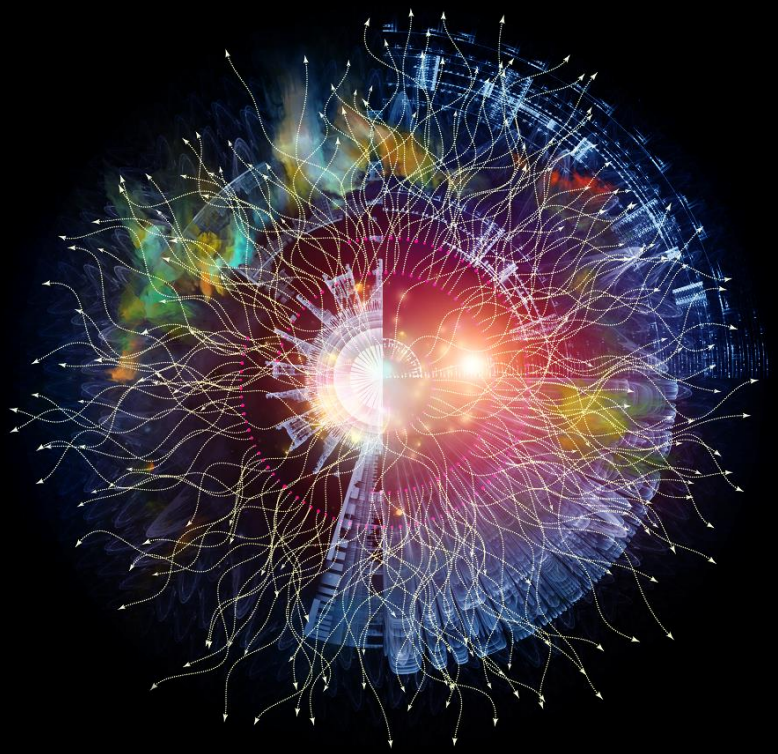
Deloitte.



TechCompliance Break
Anforderungen an und Potenziale für die IKT-/IT-Sicherheit

Wien, 18. Juni 2020

Agenda

1. Herausforderungen in Bezug auf COVID-19 und neue Technologien
2. Überblick zu den Umsetzungserfordernissen der EBA/GL/2019/04
3. Darstellung von Änderungen im Vergleich zu früheren Standards
4. Anwendungsfälle der IKT-Sicherheits- und Risikomanagementrichtlinie
5. Potenziale und Nutzen durch Umsetzung der Richtlinie

Herausforderungen in Bezug auf COVID-19 und neue Technologien

IKT-Sicherheit und -Risiken

Allgemeines zur aktuellen Lage

Ausgangslage

Die Vorteile der Digitalisierung erhöhen auch neue Risiken und Gefahren für Unternehmen. Cyber- Angriffe machen deutlich, wie verwundbar IT-Systeme sind. Die Leitlinien zum IKT- und Sicherheitsrisikomanagement (EBA/GL/ 2019/04) der Europäischen Bankenaufsichtsbehörde (EBA) konkretisiert deshalb grundlegende Anforderungen an IKT-/IT-Systeme.

In vergangenen Jahren und insbesondere durch die COVID-19 Pandemie werden durch Finanzdienstleister verstärkt Online-Services angeboten, wodurch auch Maßnahmen zur Sicherung der Verfügbarkeit dieser Services und dem Schutz deren Nutzer vor Betrugsfällen erforderlich werden. In einem Statement der EBA vom 22. April 2020 wird deshalb auf die Wichtigkeit der Anforderungen und einen Aufsichtsschwerpunkt auf die Sicherung der Betriebsstabilität gelegt.

Hinzu kommt, dass in Zeiten der allgemeinen Unsicherheit durch Regulatoren auch ein einheitliches und länderübergreifendes Rahmenwerk geschaffen werden soll. Um dies zu erreichen, wird die vorliegende Leitlinie mit ihrem Inkrafttreten am 30. Juni 2020 auch den für FMA-beaufsichtigte Kreditinstitute geltenden Leitfaden zur „IKT-Sicherheit in Kreditinstituten vom 28. Mai 2018 ablösen und ersetzen.

Herausforderungen

- Durch eine Online-Bereitstellung der Mehrheit von Services bestehen neue Herausforderungen, um deren Betrieb und Verfügbarkeit sicherzustellen und gleichzeitig auch ein angemessenes Maß an Informationssicherheit zu gewährleisten.
- Speziell durch die Einschränkung des persönlichen Kontakts mit Kunden ergeben sich neue Bedrohungsszenarien durch gesteigerte Cyber-Sicherheitsrisiken. Dies zeigt sich auch durch Meldungen eines Anstiegs von Cyberkriminalität bspw. durch vermehrte Phishing-Nachrichten mit Bezug zur COVID-19 Pandemie der Präsidentin der Europäischen Kommission und der World Health Organization (WHO).
- Diese gesteigerten Sicherheitsbedürfnisse konkurrieren mit der Forderung von Kunden nach einer durchgehenden Verfügbarkeit und Beschleunigung der Abläufe durch Kunden, wodurch sich ebenso Anforderungen an die Betriebssteuerung und -sicherung ergeben.

IKT-Sicherheit und -Risiken

Definition und Anforderungen an das IKT-/IT-/IS-Risikomanagement

Anforderungen

Festgestellte Mängel in der IKT-Sicherheit können sich bei Kreditinstituten auf den SREP-Score auswirken. Um dem vorzubeugen und in Hinblick auf die EBA/GL/2019/04 ergeben sich folgende Anforderungen:

IKT-Strategie, Governance & Risikomanagement

- Einrichtung detaillierter Prozess- und Managementstrukturen der IKT-Landschaft
- Festlegung der strategischen Entwicklung, des IKT-Aufbaus und der IKT-Ablauforganisation inkl. der IKT-Zielarchitektur
- Durchführung von Risikoanalysen und -bewertungen (nach jeder Änderung der Rahmenbedingungen)

Access, Vulnerability & Change Management

- Erstellung einer zentralen Informations sicherheitsrichtlinie sowie genauer themenspezifischer Richtlinien
- Implementierung eines zyklischen Prozesses zur Identifikation und Beseitigung von Schwachstellen
- Festlegung und Dokumentation von regelmäßigen Penetrationstests & Virenscans

Datenintegrität

- Entwurf eines schriftlichen Rahmenwerkes für die Minderung des Datenintegritätsrisikos gemäß BCBS 239 und vergleichbaren Standards und Rahmenwerken

BCM und DRM

- Erstellung eines Rahmenwerkes zur Identifikation, Messung und Begrenzung des Verfügbarkeits und Kontinuitätsrisikos
- Implementierung von Strategien und Maßnahmen zur Notfallvorsorge, -bewältigung und -nachsorge

Auslagerungsvereinbarungen

- Festlegung von Kriterien, was eine wesentliche IKT-Auslagerung iSd § 25 Abs 2 BWG darstellt
- Berücksichtigung der Anforderungen an Auslagerungsvereinbarungen (EBA/GL/2019/02)

Überblick zu den Umsetzungs-erfordernissen der EBA/GL/2019/04

IKT-Sicherheit und -Risiken

Kernelemente der EBA-Richtlinie „EBA/GL/2019/04“ (1/6)

Governance und Strategie

Governance

Strategie

Auslagerungen

Zusammenfassung

Ziele

- Die IKT-Strategie steht im Einklang mit der allgemeinen Geschäftsstrategie und unterstützt das Geschäftsmodell. Dabei beinhaltet die IKT-Strategie die strategischen Leitlinien zur IKT. Ziel der IKT-Strategie ist, einen proaktiven Austausch zwischen der IKT-Organisation und den Entscheidungsträgern zu schaffen, eine klare Kompetenzordnung zu erstellen und gegebenenfalls Ausschüsse für IKT- und Fachbereiche einzurichten.
- Besonderes Augenmerk ist dabei aus Sicht der EBA auch auf den Umgang mit Auslagerungsvereinbarungen und die Abstimmung der IKT-Strategie mit der Outsourcing-Strategie des Instituts zu legen. „Auslagerung“ (Outsourcing) eine Vereinbarung jeglicher Form, die zwischen dem Institut und einem Dritten (Dienstleister) getroffen wird, auf Grund derer der Dritte direkt oder durch weiteres Auslagern einen Prozess, eine Dienstleistung oder eine Tätigkeit erbringt, die ansonsten vom Institut selbst erbracht werden würde.

Wesentliche Bestandteile

- Vorliegen einer von der Geschäftsstrategie abgeleiteten und durch die Verwaltungsorgane freigegebene IKT-/IT-Strategie
- Notwendigkeit zur Abbildung von
  - Strategischer Ausrichtung
  - IKT-/IT-Ablauf- und Aufbauorganisation
  - Berücksichtigte Rahmenwerke
  - IT-Zielarchitektur
  - BCM und Disaster Recovery
  - Auslagerungen und IDV
  - Einbindung der Innenrevision
- Vorliegen einer Policy zur Auslagerung von Systemen und Services
- Definition der Wesentlichkeit von Auslagerungen für den Geschäftsbetrieb
- Einhaltung der Anzeigepflichten für Auslagerungen

IKT-Sicherheit und -Risiken

Kernelemente der EBA-Richtlinie „EBA/GL/2019/04“ (2/6)

IKT- und Sicherheitsrisikomanagementframework

- Organisation und Ziele
- Identifikation von Funktionen, Prozessen und Assets
- Risikoklassifizierung und -evaluierung
- Risikomitigation
- Berichterstattung
- Überprüfung

Zusammenfassung

Ziele

- Die IKT-Governance baut auf der IKT-Strategie des Instituts auf und ist ein wesentlicher Bestandteil der Unternehmensführung. Sie liegt in der Verantwortung der Geschäftsleitung und stellt sicher, dass die IKT die Unternehmensziele und -strategie optimal unterstützt. Die IKT-Governance setzt sich u.a. aus folgenden wesentlichen Elementen zusammen: Prozessstrukturen, Organisationsvorgaben und Führungsstrukturen für die komplette IKT-Infrastruktur im Institut. Zweck der IKT-Governance ist somit die Steuerung und Überwachung des Betriebs und der Weiterentwicklung der im Institut verwendeten IKT-Systeme samt der dazugehörigen IKT-Prozesse.
- Das Informationsrisikomanagement gewährleistet, dass die Informationsverarbeitung und -weitergabe im Institut durch adäquate IKT-Systeme (Hard- und Softwarekomponenten) und Prozesse unterstützt wird. Bei der Ausgestaltung derselben wird beachtet, dass die Integrität, die Verfügbarkeit, die Authentizität und die Vertraulichkeit der Daten gewährleistet ist. Bezüglich deren Umfang und Qualität erfolgt eine Orientierung an den betriebsinternen Erfordernissen, den Geschäftsaktivitäten und der Risikosituation.

Wesentliche Bestandteile

- Regelungen zur Umsetzung der IKT-/IT-Strategie und Berücksichtigung kritischer IKT-/IT-Systeme und –Services
- Organisationsstrukturen zur Informationssicherheit
- Rollendefinition und Stellenbeschreibungen eingebundener Mitarbeiter und personelle Ressourcenausstattung
- Errichtung eines internen Kontrollsystems in der IT
- Prozesse zur Prozesse zur Identifikation, Bewertung, Steuerung und Überwachung der wesentlichen IKT-Risiken
- Risikoanalysen und Schadensfalldatenbank sowie Risikoüberwachung und OpRisk-Integration
- Maßnahmenkatalog zu Cyber-Sicherheitsthemen
- Verwundbarkeitsanalysen und Maßnahmen zur Schadensbeurteilung
- Kommunikation von Anforderungen an externe Dienstleister
- Berücksichtigung der obigen Punkte durch die Innenrevision

IKT-Sicherheit und -Risiken

Kernelemente der EBA-Richtlinie „EBA/GL/2019/04“ (3/6)

Information Security

- Sicherheitsrichtlinie
- Logische Sicherheit
- Physische Sicherheit
- IKT-Betriebssicherheit
- Überwachung
- Reviews & Assessments
- Trainings & Awareness

Zusammenfassung

Ziele

- Ein wesentliches Instrument zum Schutz von Informationen sind Sicherheitsrichtlinien. Diese beziehen sich nicht nur auf die Sicherheit der IKT-Systeme und der darin gespeicherten Daten, sondern umfassen auch generell das Thema Informationssicherheit (und somit auch die Sicherheit von nicht elektronisch verarbeiteten Informationen). Der Schutz der IKT-Systeme ist nur als Teilaspekt der Informationssicherheit zu sehen.
- Das Benutzerberechtigungsmanagement umfasst alle Prozesse, die der Autorisierung eines Anwenders (inklusive privilegierter Benutzer) hinsichtlich Berechtigungen auf IKT-Ressourcen (Einrichtung, Zugriff und Nutzung, Bearbeitung, Deaktivierung, Löschung) dienen. Ziel des Benutzerberechtigungsmanagements ist es, dass nur autorisierte Benutzer im Institut auf IKT-Services und -Anwendungen zugreifen können. Zudem soll vor allem missbräuchliche Verwendung und unautorisierte Manipulation von Daten und IKT-Systemen verhindert werden.
- Schwachstellenmanagement als integraler Bestandteil der IKT-Sicherheit ist ein zyklischer Prozess zur Identifikation, Klassifizierung und Beseitigung von Schwachstellen insbesondere in Software und Firmware.

Wesentliche Bestandteile

- Einrichtung von Sicherheitsrichtlinien zu folgenden Bereichen
  - Netzwerksicherheit, Kryptographie, Authentifizierung, Protokollierung, Physische Sicherheit, etc.
- Einrichtung eines dokumentierten Berechtigungskonzepts und Benutzer- und Berechtigungsverwaltungsprozesse
- Kennwort- und Sperrrichtlinien, Vermeidung von Sammelbenutzerkonten
- Definition und Berücksichtigung von Dateneignern und unabhängige Prüfung von Berechtigungen
- Verfahren zur Vermeidung von Schadensfällen und Maßnahmen zur Schwachstellenbeseitigung
- Auswirkungs- und Risikoanalyse von Schwachstellen und Bildung einer Restrisikoliste
- Meldeverpflichtungen im Schadensfall
- Regelmäßige Reviews und Aktualisierungen
- Kommunikation und Awareness-Bildung

IKT-Sicherheit und -Risiken

Kernelemente der EBA-Richtlinie „EBA/GL/2019/04“ (4/6)

IKT-Betriebssteuerung

- Betriebsplanung
- Betriebssteuerung
- Betriebsüberwachung
- Datenintegrität
- IKT-Incident und -Problem Management

Zusammenfassung

Ziele

- Als IKT-Betrieb ist in diesem Zusammenhang die Organisationseinheit eines Unternehmens gemeint, welche die Aufgabe hat, die erforderliche IKT-Infrastruktur (Hard- und Software) in angemessenem Umfang zur Verfügung zu stellen und störungsfrei zu betreiben. Die Anforderungen an den IKT-Betrieb eines Instituts ergeben sich aus der Geschäftsstrategie und lassen sich aus den IKT unterstützten Geschäftsprozessen ableiten. Die Funktionsweise des IKT-Betriebs wird im Rahmen eines Betriebskonzeptes festgehalten.
- Grundlage ist die Einrichtung von Prozessen und Abläufen zur Behandlung von IKT-Incidents und –Problemen sowie deren Beurteilung und Ursachenforschung.
- Zu berücksichtigen sind unter Anderem auch Maßnahmen zur Gewährleistung einer angemessenen Datenintegrität. Hierbei ist zu empfehlen, sich an internationalen Standards, wie beispielsweise BCBS 239, zu orientieren.

Wesentliche Bestandteile

- Prozessdefinition und Einrichtung eines Asset Registers
- Regelungen zur Neu- und Wiederbeschaffung von Hard- und Software
- Vorhandensein von Wartungsverträgen und Service Level Agreements
- Regelungen zur Betriebsüberwachung und zum Incident und Problem Management
- Maßnahmen zur Data Governance und zur Messung des Datenintegritätsrisikos

IKT-Sicherheit und -Risiken

Kernelemente der EBA-Richtlinie „EBA/GL/2019/04“ (5/6)

IKT-Projekt- und Change-Management

IKT-Projektmanagement

IKT-Systembeschaffung und -entwicklung

IKT-Change Management

Zusammenfassung

Ziele

- Institute erstellen im Falle von IKT-Projekten eine Analyse, die vorab die damit einhergehenden wesentlichen Veränderungen in den IKT-Systemen – in Hinblick auf deren Auswirkung auf die IKT-Aufbau- und IKT-Ablauforganisation sowie die dazugehörigen IKT-Prozesse – aufzeigt und eine Bewertung der damit verbundenen Risiken vornimmt. Um mögliche Beeinträchtigungen des Risikoprofils des Instituts identifizieren zu können, werden IKT-Projekte angemessen gesteuert, deren Risiken laufend berücksichtigt und dies vollständig dokumentiert.
- Im Zuge von Beschaffungs- und Entwicklungsprozessen sind unter Anderem auch Lebenszyklusmodelle für Systeme und Daten zu erheben und zu dokumentieren. Zu berücksichtigen sind dabei sowohl eigenbetreute als auch ausgelagerte Systeme und Dienstleistungen.

Wesentliche Bestandteile

- Prozessdefinitionen zum
  - IKT-/IT-Projektmanagement
  - IKT-/IT-Beschaffungsprozessen
  - Entwicklungstätigkeiten
  - Change Management
- Einrichtung von Teststrategien, -konzepten und –fällen
  - u.a. Definition von nichtfunktionalen und IT-sicherheitsbezogenen Testfällen
- Definition von Lebenszyklusmodellen für eigenbetriebene oder zum Betrieb ausgelagerte IKT-Systeme sowie darin verarbeitete Daten

IKT-Sicherheit und -Risiken

Kernelemente der EBA-Richtlinie „EBA/GL/2019/04“ (6/6)

Business Continuity Management

- Business Impact Analyse
- Business Continuity Planung
- BC- und DR-Pläne
- BC- und DR-Tests
- Krisenkommunikation

Zusammenfassung

Ziele

- Das Risiko aus Beeinträchtigungen der Leistung und Verfügbarkeit von IKT-Systemen wird angemessen geschätzt und abgedeckt. Insbesondere das Risiko aus der mangelnden Fähigkeit der zeitkritischen Wiederherstellung von Leistungen, die aufgrund von Hardware- oder Softwareversagen geschädigt wurden, sowie durch allgemeine Schwächen im Management von IKT-Systemen. Das Notfallmanagement fußt auf einer Analyse der Bedrohungsanfälligkeiten von Geschäftsprozessen und -ressourcen und umfasst präventive Notfallvorsorge und Notfallbewältigung. Im Fall einer Auslagerung verbleibt die Verantwortung für angemessene Notfallpläne in Bezug auf die ausgelagerten Tätigkeiten beim auslagernden Institut.

Wesentliche Bestandteile

- Definition von „Recovery Time Objectives“ (RTOs) und „Recovery Point Objectives“ (RPOs) für alle Systeme
- Vorgehensbeschreibung zur Identifikation von „Single Points of Failure“ (SPoF)
- Vorgehensweise bei Messung und Begrenzung des Verfügbarkeits- und Kontinuitätsrisikos
- Definition und Test von Notfallszenarien im BCM
- Abstimmung von Notfallplänen und –konzepten intern und mit Dienstleistern

Umgang mit Zahlungsdienstenutzern

Ziele

- Aufgrund der Erweiterung des Anwendungsbereichs auf Zahlungsdienstleister und für die Erbringung solcher Dienste konzessierten Bankinstituten ist ein weiterer Schwerpunkt der EBA-Richtlinie auf den Umgang mit Nutzern (Endverbraucher) dieser Dienstleistungen ausgerichtet. Hierbei ist sicherzustellen, dass entsprechende Informationspflichten sowie Sicherheitsmaßnahmen eingehalten werden. Mit Inkrafttreten der Richtlinie wird deshalb auch die EBA-Leitlinie „Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)” (EBA/GL/2017/17) abgelöst und deren Anforderungen wurden in die vorliegende Richtlinie integriert.

Darstellung von Änderungen im Vergleich zu früheren Standards

IKT-Sicherheit und -Risiken

Anpassungen in Folge geänderter Rahmenbedingungen

Neuerungen

- Der Anwendungsbereich der EBA-Richtlinie sieht neben der Abdeckung von in Kerngeschäftsprozessen eingesetzten Anwendungen und Systeme auch eine Abdeckung sämtlicher im externen Berichtswesen und der Finanzberichterstattung eingesetzter Anwendungen und Systeme vor.
- Für Anwendungen der individuellen Datenverarbeitung sind aus Sicht des Regulators Maßnahmen zur Erreichung eines angemessenen Zugriffsschutzes und Änderungswesen zu definieren, umzusetzen und zu dokumentieren.
- Mit Inkrafttreten der EBA-Richtlinie zu IKT- und Sicherheitsrisiko-management (EBA/GL/2019/04) treten in Bezug auf Outsourcing-Vereinbarungen für die durch die Richtlinie betroffenen Institute auch die Anforderungen der EBA-Richtlinie zu Auslagerungsver-einbarungen (EBA/GL/2019/02) in Kraft und sind anzuwenden.
- Für Auslagerungsvereinbarungen sind sicherheitsbezogene Standards zu definieren und an externe Dienstleister zu kommunizieren.
- Ergänzend zu vorhergehenden nationalen und internationalen Leitlinien zur IKT-Sicherheit wird durch die EBA-Richtlinie auch der notwendige Rahmen zur Erbringung von Zahlungsdienstleistungen im Sinne der PSD2 geregelt und umgesetzt.
- Maßnahmen zur Awarenessbildung und sicherheitsrelevante Trainings sind zukünftig allen Personen (intern oder extern) mit Zugriff auf Produktivsysteme zur Verfügung zu stellen.

Anpassungen

- Anforderungen an die Strukturierung und den Aufbau der internen Governance sind laut Definition der EBA nach den Anforderungen der EBA-Leitlinien zur internen Governance (EBA/GL/2017/11) aufzubauen.
- Grundlegend sind sämtliche Anforderungen an die IT-Sicherheit sowohl bei interner als auch externer Betreuung von Anwendungen und Systemen oder bei Erbringung von Dienstleistungen anzuwenden. Diese Standards sind als Grundlage und Mindestmaß für die Beurteilung von Dienstleistern zu sehen.
- Die Ermittlung von RTO- und RPO-Zeiten im Business Continuity Management wird auf Basis der Angaben in der EBA-Leitlinie zum ICT-Assessment im SREP (EBA/GL/2017/05) beibehalten. Empfehlungen tendieren jedoch dazu eine Orientierung an der ISO-Norm 22301:2019 anzustreben.

Anwendungsfälle der IKT-Sicherheits- und Risikomanagementrichtlinie

IKT-Sicherheit und -Risiken

Anwendungsbereiche der IKT-Sicherheitsrichtlinie EBA/GL/2019/04

Gültigkeitsbereich

- Zahlungsdiensteanbieter gemäß Artikel 4 (11) der PSD2
- Kreditinstitute und Investmentfirmen gemäß Punkt 3 des Artikel 4 (1) der EU-Verordnung 575/2013
- Aufsichtsbehörden gemäß Punkt 40 des Artikel 4 (1) der EU-Verordnung 575/2013
- die Europäische Zentralbank gemäß der EU-Verordnung 1024/2013
- Aufsichtsbehörden unter der PSD2 gemäß Punkt (i) des Artikel 4 (2) der EU-Verordnung 1093/2010

Während durch die europäische Richtlinie ergänzend zu früheren Rahmenwerken rund um die IKT-Sicherheit nunmehr auch Zahlungsinstitute, E-Geld-Institute und ausgewählte Sonderkreditinstitute umfasst sind, weitet die FMA den Anwendungsbereich generell auf alle durch sie beaufsichtigten Kreditinstitute aus:

- Kreditinstitute im Sinne des § 1 Abs. 1 BWG

Für Institute deren Konzession nicht unter einen der obigen Sachverhalte fällt und die sich unter Beaufsichtigung der FMA befinden, werden die nationalen Leitfäden zur IT-Sicherheit bis auf Weiteres beibehalten:

- FMA-Leitfäden zur IT-Sicherheit
  - IT-Sicherheit in Versicherungs- und Rückversicherungsunternehmen vom 3. Juli 2018
  - IT-Sicherheit in Verwaltungsgesellschaften (gilt auch für BVKs, AIFs und OGAWs) vom 29. August 2018
  - IT-Sicherheit in WPF und WPDLU vom 29. August 2018
  - IT-Sicherheit in Pensionskassen vom 21. Dezember 2018

Potenziale und Nutzen durch Umsetzung der Richtlinie

IKT-Sicherheit und -Risiken

Nutzen und Potenziale bei Umsetzung der Maßnahmen

Nutzen und Potenziale

- Ziel der Richtlinie ist es Instituten und Aufsichtsbehörden ein Rahmenwerk zur Verfügung zu stellen, dass auf europäischer Ebene einheitlich anzuwenden und damit auch innerhalb Europas vergleichbar sein soll. Dies soll insbesondere auch auf europäischer Ebene aktiven Instituten zu Gute kommen und die Kommunikation mit Aufsichtsbehörden erleichtern.
- Für Kunden der betroffenen Institute soll dadurch auch das Vertrauen in digitale Medien gestärkt und die Nutzung elektronisch verfügbarer Dienste forciert werden.
- Ferner bietet die Richtlinie für die Institute selbst insbesondere die folgenden Potenziale, welche zur verbesserten Überwachung und Steuerung bestehender Risiken dienen sollen:
    - Steigerung der Risikomanagementkapazitäten und Verbesserung der Prozesse zur Identifikation, Bewertung, Überwachung und Mitigation neuer Risiken
    - Verbesserte Prozesse zur Betriebsüberwachung und Erhöhung der Betriebssicherheit als Vorsorge für den Krisenfall
    - Verbesserte Kenntnis zu den eingesetzten Anwendungen und Daten, wodurch eine Optimierung von Geschäftsprozessen auf Basis moderner Technologien ermöglicht wird.
    - Zeitnahe Erkennung von Sicherheitsvorfällen und dadurch Ermöglichung der Einhaltung von Meldeverpflichtungen
- Für eine Umsetzung der aufsichtlichen Anforderungen empfiehlt sich typischerweise die Durchführung folgender Aktivitäten
    - Gap-Analysen und Reifegradbeurteilungen zur Erhebung des Status-Quo und Aufzeigen von Verbesserungspotenzialen
    - Erstellung, Überarbeitung und Qualitätssicherung von Richtlinien und Regelwerken
    - Unterstützung bei Definition, Aufbau und Implementierung von der Richtlinienumsetzung
    - Schulungen und Trainings zu ausgewählten Themenbereichen der Richtlinie
    - Unterstützung im Zusammenhang mit aufsichtlichen Prüfungen bei Prüfungsvorsorge, -begleitung oder -nachsorge

Q&A / Diskussion

Deloitte – Risk Advisory | TechCompliance

Bleiben wir in Kontakt

Alexander Ruzicka
Partner | Risk Advisory

Tel: +43 1 537 00 7950
Mobil: +43 664 80 537 7950
aruzicka@deloitte.at

Deloitte Audit Wirtschaftsprüfungs GmbH
Renngasse 1/Freyung
1010 Wien
www.deloitte.at

Thomas John
Senior Manager | Risk Advisory

Tel: +43 1 537 00 3723
Mobil: +43 664 80 537 3723
tjohn@deloitte.at

Deloitte Audit Wirtschaftsprüfungs GmbH
Renngasse 1/Freyung
1010 Wien
www.deloitte.at

Bei Fragen oder Anliegen zu den präsentierten Sachverhalten oder damit in Verbindung stehenden Themenbereichen kontaktieren Sie gerne auch unser TechCompliance Team unter

AT TechCompliance

(attechcompliance@deloitte.com)

Deloitte.

Für weitere Informationen kontaktieren Sie Deloitte Audit Wirtschaftsprüfungs GmbH.

Gesellschaftssitz Wien | Handelsgericht Wien | FN 36059 d