Abhängig, aber nicht machtlos – Third Party Risk Management

Know-how to go

HiSolutions Berlin, 25.09.2024

Unternehmen sind keine isolierten Inseln

© HiSolutions 2024

TPRM wird zunehmend an Relevanz gewinnen, nicht nur aufgrund von neuen und aktualisierten regulatorischen Anforderungen…

Beispiel: Cloud Computing

In 5 Jahren wollen 56 % der Unternehmen den Großteil der IT-Anwendungen aus der Cloud beziehen

Derzeit nutzen

89 %

der Unternehmen Cloud Computing.

Quelle: Bitkom 2023 *Cloud-Nutzung wird rasant zunehmen*
https://www.bitkom.org/Presse/Presseinformation/Cloud-Report-2023-Nutzung-rasant-zunehmen#_

Status Quo

- Diverse Unternehmen mit „Cloud only"- oder „Cloud first"-Strategie
- ITSCM in Verantwortung der Cloud-Dienstleister
- Aufsichtsrechtliche Verantwortung und BCM liegen beim Auftraggeber

Risiken

Dienstleistersteuerung	→ Verträge
Vendor-Lock-In	→ Exit-Strategie
Verfügbarkeit	→ BCM/Multi-Cloud
IT-Sicherheit und Datenschutz	→ Private Cloud

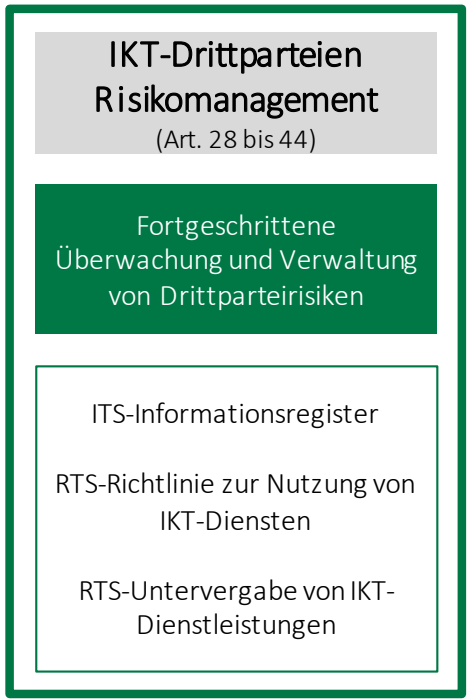
© HiSolutions 2024

Kenne deine Dienstleister-Risiken!

Risikobasierter und verhältnismäßiger Ansatz

© HiSolutions 2024

DORA und TPRM



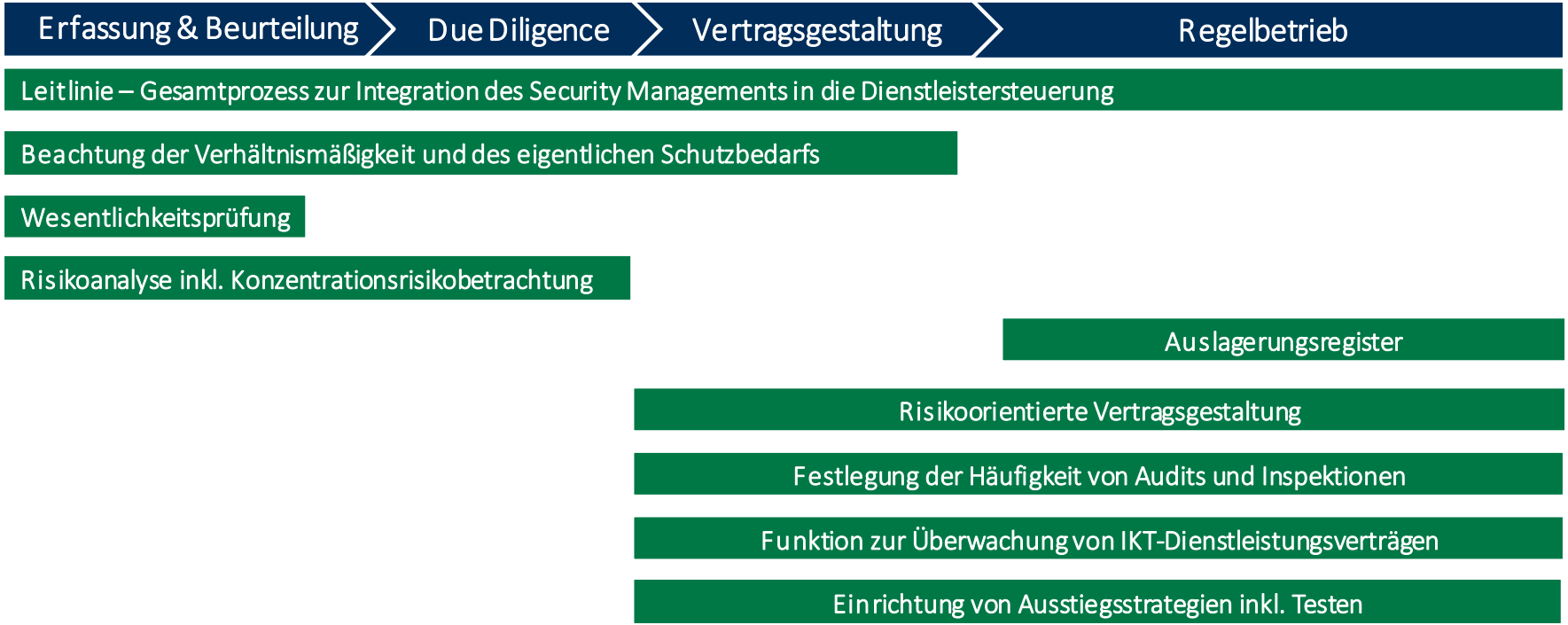
Anforderungen an Drittanbieter und Outsourcing

- DORA gilt auch für kritische (IT-)Dienstleister
- Kritische IT-Dienstleister werden durch Aufsichtsbehörden selbst überwacht
- Erweiterung der Verträge um spezifische Sicherheits- und Resilienzanforderungen
- Umfassende und regelmäßige Due-Diligence-Prüfungen sind durchführen um sicherzustellen, dass diese den gleichen hohen Standards entsprechen wie das Finanzinstitut selbst.
- Vereinbarung von Notfallplänen und Exit-Strategien für den Fall von schwerwiegenden Störungen oder Beendigung der Dienstleistungsverträge

RTS/ITS = Technische Regulierungs-/Implementierungsstandards der ESAs

© HiSolutions 2024

HiSolutions Best Practice Model meets DORA



© HiSolutions 2024

Feststellung der Relevanz für das Security Management

Notfallrelevanz
Wurden die betroffenen Prozesse mittels einer aktuellen Business Impact Analyse als zeitkritisch identifiziert?

Relevanz für die Informationssicherheit
Wurde für die betroffenen Information Assets ein Schutzbedarf mittels einer aktuellen Schutzbedarfsfeststellung erhoben?

Datenschutzrelevanz
Werden personenbezogene Daten vom Dienstleister verarbeitet?

Security Management

© HiSolutions 2024

Ergebnis der Risikoanalyse

Input

- personenbezogene Daten
- Zeitkritikalität
- Schutzbedarf

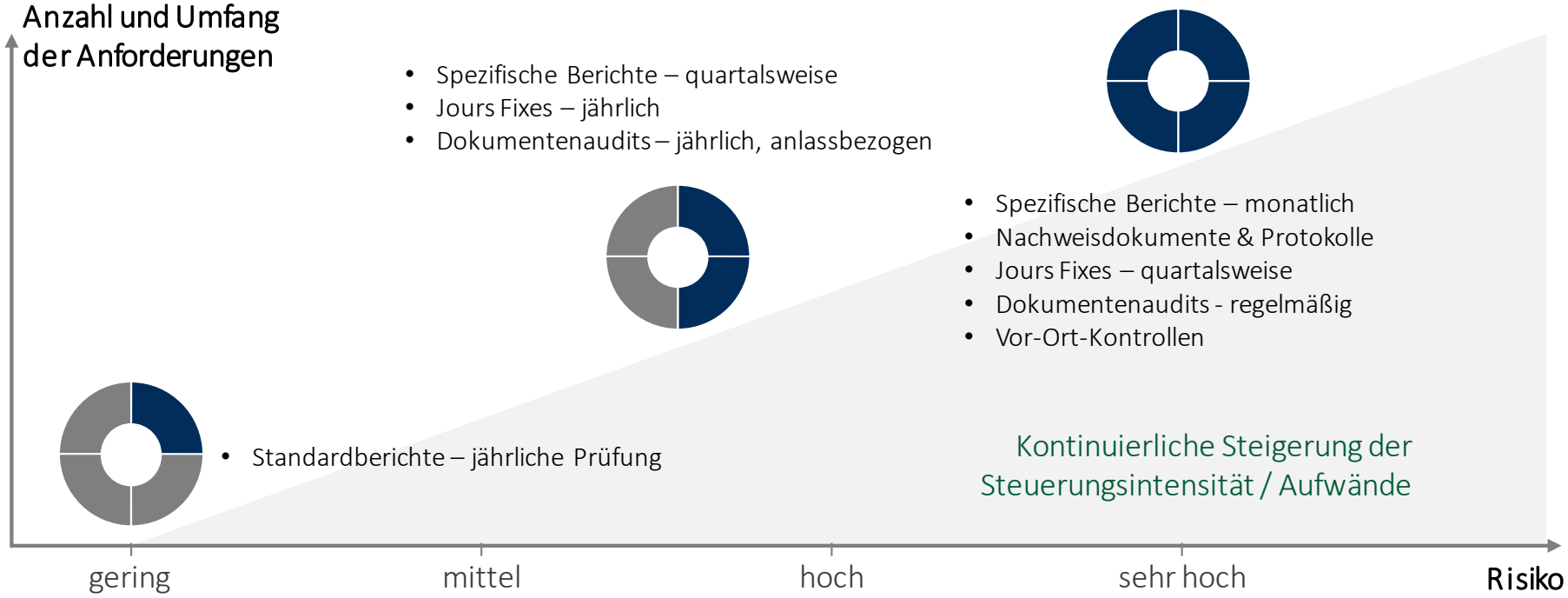
Risikoanalyse

Output

- Risikowert
- Steuerungs-maßnahmen
- Vertrags-anforderungen

© HiSolutions 2024

Festlegung von zielgerichteten Steuerungsmaßnahmen



© HiSolutions 2024

Risikomanagement für I(K)T-Dienstleister (DORA Kapitel V)

Fokus:
Vertragliche Mindestanforderungen mit allen Dienstleistern, die dauerhaft IKT-Dienstleistungen für Finanzunternehmen erbringen

Geltungsbereich:
Neben klassischen IKT-Services wie Cloud-Services, Hosting oder Netzwerkdiensten auch Anbieter von Softwarelizenzen, Datenservices oder Telekommunikationsdiensten*

Allgemeine Anforderungen an IKT-Drittdienstleister*

- Einhaltung angemessener Standards für Informationssicherheit
- Verpflichtung zur Zusammenarbeit mit den zuständigen Aufsichtsbehörden
- vertraglich vereinbarte Kündigungsrechte, etwa bei nachweislichen Schwächen des Dienstleisters in Bezug auf sein IKT-Risikomanagement
- …

Spezifische Anforderungen bei Unterstützung kritischer oder wichtiger Funktionen

- vollständige Beschreibung und Messung der Dienstleistungsgüte
- Implementierung und Test von Notfallplänen
- Recht auf fortlaufende Überwachung, beispielsweise im Rahmen von Vor-Ort-Inspektionen
- Ausstiegsstrategien einschließlich angemessener Übergangszeiträume…

*komplette Liste vgl. Anhang III des Konsultationsentwurfs zum ITS-Informationsregister

© HiSolutions 2024

NIS-2/KRITIS und TPRM

Wer?

- relevant für Unternehmen mit mind. 50 Mitarbeitern, mit über 10 Mio. € Jahresumsatz und mehr als 10 Mio. € Jahresbilanzsumme, sowie einer Wirtschaftstätigkeit in einem regulierten Sektor (bspw. IT-Sektor)

Was?

- Sicherung der Lieferkette durch geeignete Maßnahmen, d. h. Schutz der eigenen Systeme, aber auch Schutz der Lieferantensysteme
- Risikomanagement muss auch die eigenen Lieferketten und direkte Lieferanten berücksichtigen

Wie?

- Es kommt auf die nationale Umsetzung und die individuelle Vertragsgestaltung mit Third Parties an (NIS2UmsuCG)

© HiSolutions 2024

TPRM Essentials

Schritt 1

Identifizierung zeitkritischer Leistungsbezüge

- Outgesourcter Geschäfts-prozess zeitkritisch?
- Zeitkritische DL oder Güter im Notbetrieb nötig?

Schritt 2

Definition der BCM-Grundanforderungen

- Welche Grundanforderungen werden an zeitkritische Leistungsbezüge und Lieferketten gestellt?

Schritt 3

Eignungsprüfung des Dienstleisters

- Prüfung, ob der DL die Grundanforderungen erfüllt
- Ergänzende Risikoanalyse, wenn Grundanforderungen nicht vollständig erfüllt sind

Schritt 4

Entwicklung der Exit-Strategie

- Für geplante und ungeplante Unterbrechung/Beendigung des zeitkritischen Leistungsbezugs oder der Lieferkette

Schritt 5

Definition der Vertragsanforderungen

- Spezifische BCM-Anforderungen anhand RTO und Notbetriebsniveau entwickeln und vertraglich fixieren

Schritt 6

Überführung der Leistungserbringung

- Definieren von Rückfallvorkehrungen
- Überführen der Leistungserbringung auf den DL

Schritt 7

Dienstleistersteuerung während der Leistungserbringung

- Laufende Überwachung der zeitkritischen Leistungsbezüge und der Lieferketten
- Bedarfsweise Anpassung der BCM-Anforderungen

© HiSolutions 2024

TPRM - Aussicht

© HiSolutions 2024

Praxistipp

Gehen Sie Essen mit Ihren wichtigen Dienstleistern und Lieferanten

…und tauschen Sie sich dabei über ihre Notfallplanung aus

Achtung im regulierten Umfeld: Dies darf nur der erste Schritt sein, denn es sind schriftlich fixierte und abgestimmte Maßnahmen vertraglich zu fixieren und nachweislich zu steuern.

© HiSolutions 2024

Eine Abstimmung der Schnittstellen ist essenziell

© HiSolutions 2024

Inwiefern binden Sie Ihre Dienstleister in Ihre Notfallplanung ein?

© HiSolutions 2024