Community DRAFT

- Template -

Strategie für das IKT- Drittparteienrisiko und Multi-Vendor Strategie

Zuletzt aktualisiert am: 03.06.2024

Disclamer

Die in diesem Dokument formulierten Texte verstehen sich als exemplarische Formulierungsvorschläge, um die Anforderungen der DORA-Verordnung Art. 28 Abs. 2 sowie Art. 6 Abs. 9 DORA der DORA-VO zum IKT-Drittparteirisikomanagement zu adressieren.

Art. 28 Abs. 2 DORA: „Finanzinstitute, […], beschließen im Rahmen ihres IKT-Risikomanagementrahmens eine **Strategie für das IKT- Drittparteienrisik**o und überprüfen diese regelmäßig, wobei gegebenenfalls die […] Strategie zur Nutzung mehrerer Anbieter Berücksichtigung findet. Die Strategie zum IKT-Drittparteienrisiko umfasst eine **Leitlinie für die Nutzung von IKT-Dienstleistungen** zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden, und gilt auf individueller und gegebenenfalls teilkonsolidierter und konsolidierter Basis. Das Leitungsorgan überprüft auf der Grundlage einer Bewertung des Gesamtrisikoprofils des Finanzunternehmens und des Umfangs und der Komplexität der Unternehmensdienstleistungen regelmäßig Risiken, die im Zusammenhang mit den vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen ermittelt werden."

Art. 6 Abs. 9 DORA: „Finanzunternehmen können im Zusammenhang mit der Strategie für die digitale operationale Resilienz nach Absatz 8 eine ganzheitliche **Strategie zur Nutzung mehrerer IKT-Anbieter auf Gruppen- oder Unternehmensebene** festlegen, in der wesentliche Abhängigkeiten von IKT-Drittdienstleistern aufgezeigt und die Gründe für die Nutzung verschiedener IKT-Drittdienstleister erläutert werden."

Es handelt sich um freibleibende Formulierungsvorschläge, welche mit größter Sorgfalt erstellt wurden. Die Autorin übernimmt keinerlei Gewähr für die Aktualität, Richtigkeit und Vollständigkeit der bereitgestellten Informationen.

Alle Angebote sind freibleibend und unverbindlich. Die Autorin behält sich ausdrücklich vor, die bereitgestellten Informationen ohne gesonderte Ankündigung zu verändern, zu ergänzen, zu löschen oder die Veröffentlichung zeitweise oder endgültig einzustellen.

Quellen

DORA-Verordnung: VERORDNUNG (EU) 2022/2554 DES EUROPÄISCHEN PARLAMENTS UND DES RATES 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

Special Publication (NIST SP) - 800-161r1: Boyens, J. , Smith, A. , Bartol, N. , Winkler, K. , Holbrook, A. and Fallon, M. (2022), Cybersecurity Supply Chain Risk Management for Systems and Organizations, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, https://doi.org/10.6028/NIST.SP.800-161r1, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934690 (Accessed June 2, 2024)

FITKO: Föderale IT-Kooperation (2021), Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung, Strategische Ziele, Lösungsansätze und Maßnahmen zur Umsetzung, – Version 1.0 Januar 2021 – [online], CIO Bund - Digitale Souveränität, Downloadlink: hier

1 INHALT

1 ÄNDERUNGSHISTORIE

Versions-nummer	Datum	Beschreibung der Änderungen	Betroffene Sektionen	Änderung durch
0.9	03.06.24	Neuerstellung des Community-Templates, Download unter www.marlen-hofmann.de	Alle	Dr. Marlen Hofmann

2 MANAGEMENT SUMMARY

Um mit der Geschwindigkeit der fortschreitenden Digitalisierung mithalten und gleichzeitig sichere und wirtschaftlich tragfähige Produkte und Dienstleistungen anbieten zu können, ist die Einbindung von IKT-Dienstleistern in die eigene Wertschöpfungskette des Hauses unerlässlich.

*Das IKT-Drittparteirisikomanagement (IKT-DPRM) adressiert die Risiken in der Lieferkette, die sich durch den Einsatz der IKT-Dienstleister, der Unterauftragnehmer und der Hersteller von IKT-Produkten ergeben. In diesem Kontext legt das vorliegende Dokument die **Strategie für das IKT-Drittparteienrisiko** (IKT-Drittparteirisikostrategie) nach Art. 28 Abs. 2 für das IKT-DPRM fest. Ferner umfasst das Dokument die **Multi-Vendor Strategie** nach Art. 6 Abs. 9 DORA zur Reduktion von Abhängigkeiten und Konzentrationsrisiken im Bereich der IKT-Dienstleister.*

Die Strategien beinhalten strategische Ziele und strategische Maßnahmen, die im Einklang mit der Geschäfts- und Risikostrategie, der DOR-Strategie, der Auslagerungsstrategie und der IT-Strategie des Hauses festgelegt wurden. Eine Übersicht der strategischen Ziele und Zuordnungen zu den übergeordneten Zielen der jeweiligen (Teil-) Strategien findet sich nachstehend.

Strategie	*Ziele*	*Zuordnung zu den Zielen der Geschäfts-, Risiko-, Auslagerungs-. DOR- und/oder IT-Strategie*
IKT-Drittparteirisiko-strategie	*Effektives Management von IKT-Risiken beim Bezug von IKT-Dienstleistungen*	*…*
	Bereitstellung von sicheren Produkten und Dienstleistungen	*…*
	Positionierung in der Branche	*…*
IKT Multi-Vendor Strategie	*Wechselmöglichkeit*	*…*
	Gestaltungsfähigkeit	*…*
	Einfluss auf IKT-Dienstleister	*…*

3 Zweck und Zielsetzung des Dokumentes

Das vorliegende Strategiedokument beschreibt den Ansatz zur Implementierung und Sicherstellung eines effektiven IKT-Drittparteirisikomanagements gemäß DORA-Verordnung. Es setzt die Leitplanken für die Governance zum IKT-Drittparteirisikomanagement (IKT-DPRM) und geht auf die Rollen und Verantwortlichkeiten ein. Das Strategiedokumentiert enthält zudem die strategischen Ziele des IKT-DPRMS und beschreibt die strategischen Maßnahmen sowie Verantwortlichkeiten und Rahmenbedingungen zur Erreichung dieser Ziele.

Die IKT-Drittparteirisikostrategie wird durch die im Kapitel „Mitgeltende Dokumente" dargestellten Richtlinien, Verfahrensanweisungen und Prozesse konkretisiert.

4 Gesetzliche Rahmenbedingungen

Das Strategiedokument setzt Anforderungen der DORA-Verordnung Art. 28 Abs. 2 sowie Art. 6 Abs. 9 DORA der DORA-VO zum IKT-Drittparteirisikomanagement um und überführt diese in die schriftlich fixierte Ordnung des Hauses.

Zur inhaltlichen Ausgestaltung des Dokumentes orientiert sich das Haus an den Ausführungen des National Institute of Standards and Technology (NIST) gemäß NIST SP 800-161r1 (Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations).

5 Geltungsbereich

Die in diesem Dokument beschriebenen strategischen Vorgaben, Ziele und Maßnahmen gelten für alle Bereiche und Beschäftigten des Hauses (ggf. mit Ausnahme von …).

6 Inkraftsetzung, Veröffentlichung & Aktualisierung

Die Inkraftsetzung der IKT-Drittparteirisikostrategie erfolgt durch Beschlussfassung durch den Vorstand. Das Datum der Inkraftsetzung bzw. der letzten Aktualisierung sowie ggf. bestehende Übergangsfristen werden transparent im Dokument dargestellt.

Nach Inkraftsetzung wird die Strategie im Organisationshandbuch des Hauses veröffentlicht und damit allen betroffenen Bereichen und Beschäftigten des Hauses zur Kenntnis gegeben.

Die Strategie ist Gegenstand eines kontinuierlichen Verbesserungsprozesses. Sie wird regelmäßig und bei Bedarf anlassbezogen gemäß den Vorgaben zur Dokumentenlenkung des Hauses überprüft und aktualisiert.

7 Definitionen

Nachfolgende Definitionen sind von besonderer Relevanz für das IKT-DPRM und wurden unverändert aus der DORA-Verordnung entnommen.

- *„**IKT-Risiko**" jeden vernünftigerweise identifizierbaren Umstand im Zusammenhang mit der Nutzung von Netzwerk- und Informationssystemen, der bei Eintritt durch die damit einhergehenden nachteiligen Auswirkungen im digitalen oder physischen Umfeld die Sicherheit der*

Netzwerk- und Informationssysteme, jeglicher technologieabhängiger Instrumente oder Prozesse, von Geschäften und Prozessen oder der Bereitstellung von Diensten beeinträchtigen kann.

- *„**IKT-Drittparteienrisiko**“ ein IKT-bezogenes Risiko, das für ein Finanzunternehmen im Zusammenhang mit dessen Nutzung von IKT-Dienstleistungen entstehen kann, die von IKT-Drittdienstleistern oder deren Unterauftragnehmern, einschließlich über Vereinbarungen zur Auslagerung, bereitgestellt werden;*
- *„**IKT-Drittdienstleister**“ ein Unternehmen, das IKT-Dienstleistungen bereitstellt;*
- *„**IKT-Dienstleistungen**“ digitale Dienste und Datendienste, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern dauerhaft bereitgestellt werden, einschließlich Hardware als Dienstleistung und Hardwaredienstleistungen, wozu auch technische Unterstützung durch den Hardwareanbieter mittels Software- oder Firmware- Aktualisierungen gehört, mit Ausnahme herkömmlicher analoger Telefondienste;*
- *„**IKT-Konzentrationsrisiko**“ die Exposition gegenüber einzelnen oder mehreren verbundenen kritischen IKT- Drittdienstleistern, die zu einer gewissen Abhängigkeit von diesen Dienstleistern führt, sodass die Nichtverfügbarkeit, der Ausfall oder sonstige Defizite dieser Dienstleister die Fähigkeit eines Finanzunternehmens gefährden könnten, kritische oder wichtige Funktionen zu erfüllen, oder bei dem Finanzunternehmen andere Formen nachteiliger Auswirkungen, einschließlich großer Verluste, herbeiführen oder die finanzielle Stabilität der Union insgesamt gefährden könnten;*
- *„**Schwachstelle**“ eine Schwachstelle, Empfindlichkeit oder Fehlfunktion eines Vermögenswerts, eines Systems, eines Prozesses oder einer Kontrolle, die ausgenutzt werden kann;*
- *„**Bedrohungsanalyse**“ Informationen, die aggregiert, umgewandelt, analysiert, ausgewertet oder erweitert wurden, um den notwendigen Kontext für die Entscheidungsfindung zu schaffen und ein relevantes und ausreichendes Verständnis für die Abmilderung der Auswirkungen eines IKT-bezogenen Vorfalls oder einer Cyberbedrohung zu ermöglichen, einschließlich der technischen Einzelheiten eines Cyberangriffs, der für den Angriff verantwortlichen Personen und ihres Modus Operandi und ihrer Beweggründe;*

8 STRATEGIE ZUM IKT-DRITTPARTEIRISIKOMAMAGENT

Das Haus verfolgt eine Strategie zum IKT-Drittparteirisikomanagement, um eine systematische Identifikation, Bewertung und Steuerung von IKT-Risiken in der Lieferkette sicherzustellen. Dazu werden folgende strategische Ziele formuliert:

8.1 STRATEGISCHE ZIELE[1]

8.1.1 Effektives Management von IKT-Risiken beim Bezug von IKT-Dienstleistungen

Das Haus stellt eine sachgerechte und effektive Identifikation, Bewertung und Steuerung von Bedrohungen, Schwachstellen und IKT-Risiken in der Lieferkette sicher. Ein besonderer Schwerpunkt liegt dabei auf den Teilen der Lieferketten, die direkt oder indirekt die wichtigen und kritischen Funktionen des Hauses unterstützten.

8.1.2 Bereitstellung von sicheren Produkten und Dienstleistungen

Das Haus bietet seinen Kundinnen und Kunden ausschließlich Produkte und Dienstleistungen an, die höchsten Sicherheitsanforderungen genügen. Dazu werden Bedrohungen und Schwachstellen in den Lieferketten mit größter Sorgfalt überwacht und gesteuert.

8.1.3 Positionierung in der Branche

Das Haus unterstützt aktiv alle Branchenakteure, die Sicherheit in den Lieferketten zu verbessern und potentielle IKT-Risiken zu mitigieren. Insbesondere wirkt das Haus darauf hin, die eigenen sowie die aufsichtlichen Anforderungen und Erwartungen zum IKT-Drittparteirisikomanagement transparent an seine IKT-Dienstleister zu vermitteln und deren Einhaltung sicherzustellen.

8.2 STRATEGISCHER MAßNAHMENPLAN

Die strategischen Ziele der IKT-Drittparteirisikostrategie werden durch nachfolgend dargestellte strategische Maßnahmen in einem Maßnahmenplan konkretisiert.

Ziel 1: Effektives Management von IKT-Risiken beim Bezug von IKT-Dienstleistungen

Strategische Maßnahme	*Maßnahmen-verantwortung*	*Zieldatum*	*Priorität*
Erstellung einer Richtlinie zum IKT-Drittparteirisikomanagement	*…*	*…*	*…*
Etablierung einer Überwachungsfunktion für das IKT-Drittparteirisikomanagement	*…*	*…*	*…*
Schaffung von Schnittstellen zum IKT-Risikomanagement	*…*	*…*	*…*
Schulung der Business Owner zum IKT-Drittparteirisikomanagement	*…*	*…*	*…*
…	*…*	*…*	*…*

[1] Die Ziele basieren auf den Ausführungen in Special Publication (NIST SP) - 800-161r1. Die Autorin hat eine inhaltliche Interpretation und Anpassung für den Kontext dieses Dokumentes vorgenommen.

Ziel 2: Bereitstellung von sicheren Produkten und Dienstleistungen

Strategische Maßnahme	Maßnahmen-verantwortung	Zieldatum	Priorität
Etablierung einer verantwortlichen Stelle für die Kundenkommunikation zu IKT-Risiken	…	…	…
Etablierung von Qualifizierungs- und Schulungsmaßnahmen im Bereich IKT-Drittparteirisikomanagement	…	…	…
Etablierung von Rollen und Verantwortlichkeiten zur Durchführung von Security Assessments in Produkten und Dienstleistungen	…	…	…
…	…	…	…

Ziel 3: Positionierung in der Branche

Strategische Maßnahme	Maßnahmen-verantwortung	Zieldatum	Priorität
Aufnahme der Verbändearbeit im Bereich IT-Regulatorik	…	…	…
Aufbau von Lieferantennetzwerken und Durchführung von Regulatorik-Schulungen	…	…	…
Netzwerkaufbau und Netzwerkpflege zum Thema IKT-Drittparteirisikomanagement	…	…	…
…	…	…	…

9 IKT Multi-Vendor Strategie (optional)

Das Haus verfolgt eine risikoorientiere Multi-Vendor-Strategie, um seine digitale Souveränität kontinuierlich zu verbessern und Abhängigkeiten von einzelnen IKT-Dienstleistern sowie damit verbundene Konzentrationsrisiken zu reduzieren. Dazu werden folgende strategische Ziele formuliert:

9.1 Strategische Ziele[2]

9.1.1 Wechselmöglichkeit

Das Haus strebt eine wandelbare IKT-Infrastruktur an, die es erlaubt, flexibel zwischen IKT-Lösungen, IKT-Komponenten und IKT-Dienstleistern zu wechseln. Hierfür werden unter Berücksichtigung von Wirtschaftlichkeit und Risikogehalt leistungsfähige und sichere Alternativen bereitgestellt, auf die kurzfristig zurückgegriffen werden kann.

9.1.2 Gestaltungsfähigkeit

Das Haus verfügt über die erforderliche qualitative und quantitative Personalausstattung, um die IKT-Infrastruktur aktiv (mit-) gestalten zu können. Insbesondere verfügt es über die erforderlichen Fähigkeiten, um alternative IT-Lösungen verstehen und bewerten zu können sowie bei Bedarf deren Einführung, (Weiter-)Entwicklung und deren Betrieb sicherstellen zu können.

[2] Die Ziele basieren auf den Ausführungen in FITKO (Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung, Strategische Ziele, Lösungsansätze und Maßnahmen zur Umsetzung). Die Autorin hat eine inhaltliche Interpretation und Anpassung für den Kontext dieses Dokumentes vorgenommen.

9.1.3 Einfluss auf IKT-Dienstleister

Das Haus kann seine fachlichen sowie rechtlichen Anforderungen gegenüber den IKT-Dienstleistern formulieren und durchsetzen. Dies schließt insbesondere die Vorgaben zum IKT-Risikomanagement sowie zum Datenschutz ein. Ferner verfügt das Haus über die Position, individuelle fachliche, technische und sicherheitstechnische Entwicklungsbedarfe anzuzeigen und Einfluss auf eine priorisierte Bearbeitung dieser zu nehmen.

9.2 STRATEGISCHER MAßNAHMENPLAN

Die strategischen Ziele der Multi-Vendor-Strategie werden durch nachfolgend dargestellte strategische Maßnahmen in einem Maßnahmenplan konkretisiert.

Ziel 1: Wechselmöglichkeit

Strategische Maßnahme	*Maßnahmen-verantwortung*	*Zieldatum*	*Priorität*
Etablierung einer Analyse zur Identifikation und Bewertung von kritischen Abhängigkeiten und Lock-in-Effekten	…	…	…
Identifikation von potentiellen Maßnahmen zur Reduktion der Abhängigkeiten	…	…	…
Durchführung von Marktanalysen zur Identifikation von alternativen IKT-Lösungen und IKT-Anbietern	…	…	…
Durchführung von Proof of Concepts für alternative IKT-Lösungen	…	…	…
Diversifizierung von IT-Lösungen und Schaffung von Auswahl- und Wechselmöglichkeiten	…	…	…
Standardisierung der Prozesse, Produkte und Dienstleistungen	…	…	…
Modularisierung und konsequente Nutzung von (offenen) Standards und Schnittstellen	…	…	…
…	…	…	…

Ziel 2: Gestaltungsfähigkeit

Strategische Maßnahme	*Maßnahmen-verantwortung*	*Zieldatum*	*Priorität*
Erhebung von Skillbedarfen und Dokumentation von Skillmatrizen	…	…	…
Erhebung von quantitativen Personalbedarfen und Anpassung der Personalausstattung	…	…	…
Schulung von Mitarbeitern zum Aufbau von IT-Fachwissen und Kompetenzen	…	…	…
…	…	…	…

Ziel 3: Einfluss auf IKT-Dienstleister

Strategische Maßnahme	*Maßnahmen-verantwortung*	*Zieldatum*	*Priorität*
Identifikation der kritischen und wichtigen IKT-Dienstleister	…	…	…
Bildung von Interessensgemeinschaften in der Branche	…	…	…
Intensivierung der Zusammenarbeit mit IKT-Dienstleistern	…	…	…
Stärkung der eigenen Verhandlungspositionen	…	…	…
Aktive Kommunikation der Anforderungen und Einforderung der Umsetzung	…	…	…
Positionierung und Durchsetzung von rechtlichen und regulatorischen Anforderungen gegenüber IKT-Dienstleistern	…	…	…
…	…	…	…

10 STRATEGIEUMSETZUNG

Die Umsetzung der strategischen Maßnahmenpläne wird durch verschiedene Mechanismen sichergesellt:

1) *Zu jeder Maßnahme werden im Maßnahmenplan Maßnahmenverantwortliche, Zieldaten und Prioritäten formuliert.*
2) *Die Maßnahmenverantwortlichen koordinieren die Umsetzung der Maßnahmen im Rahmen der Linie oder initiieren ggf. erforderliche Umsetzungsprojekte.*
3) *Die Maßnahmenverantwortlichen identifizieren ggf. weitere relevante Bereiche, Abteilungen oder Teams, die für die erfolgreiche Umsetzung der Maßnahme erforderlich sind.*
4) *Die Maßnahmenverantwortlichen sind für die fortlaufende Pflege der Maßnahmenpläne sowie für eine regelmäßige Berichterstattung zum Umsetzungsstatus verantwortlich.*
5) *Es erfolgt quartalsweise ein konsolidiertes Reporting zur Strategieumsetzung an den Vorstand*
6) *Eine Überprüfung und ggf. Re-Evaluierung der strategischen Ziele und der Maßnahmenpläne findet mindestens jährlich im Rahmen des Strategieprozesses, ggf. aber auch anlassbezogen sowie regelmäßig im Rahmen des quartalsweisen Strategie-Reportings statt.*
7) *Risiken und Hindernisse der Strategieumsetzung werden durch die Maßnahmenverantwortlichen proaktiv identifiziert und kommuniziert, sodass eine sachgerechte Steuerung der Strategieumsetzung ermöglicht wird.*

11 Rollen und Verantwortlichkeiten

- ***Geschäftsleitung/ Vorstand****: Der Vorstand ist verantwortlich für die Definition und Festlegung der Strategie zum IKT-Drittparteirisikomanagement sowie ggf. die Festlegung der Multi-Vendor Strategie. Ferner ist der Vorstand für die Überwachung und Sicherstellung der Strategieumsetzung verantwortlich.*
- ***Maßnahmenverantwortlicher*** *(Business Owner): Die erste Verteidigungslinie im IKT-Drittparteirisikomanagement bilden die Fachbereiche. Sie sind für die Identifikation, Bewertung und Steuerung der IKT-Drittparteirisiken verantwortlich und übernehmen die Verantwortung für die Umsetzung der strategischen Maßnahmen im Sinne der Maßnahmenverantwortlichen.*
- ***Kontrollfunkton für das IKT-Drittparteirisikomanagement****: Die Kontrollfunktion für das IKT-Drittparteirisikomanagement fungiert als zweite Verteidigungslinie und ist zuständig für die Überwachung der IKT-Drittparteirisiken, der IKT-Dienstleister sowie der IKT-Dienstleistungen, die durch IKT-Dienstleister bereitgestellt werden*
- ***Interne Revision****: Die Interne Revision bildet die dritte Verteidigungslinie und überwacht die Einhaltung der Vorgaben zum IKT-Drittparteirisikomanagement durch die erste und zweite Verteidigungslinie. Ferner führt die Interne Revision Überwachungshandlungen bei den IKT-Dienstleistern durch.*

12 Einordnung in den Risikomanagementrahmen

Das IKT-Drittparteirisikomanagement ist elementarer Bestandteil des internen Risikomanagement-rahmens des Hauses. IKT-Drittparteirisiken zählen zu den IKT-Risiken, die wiederum zur Risikoart der operationellen Risiken zählen.

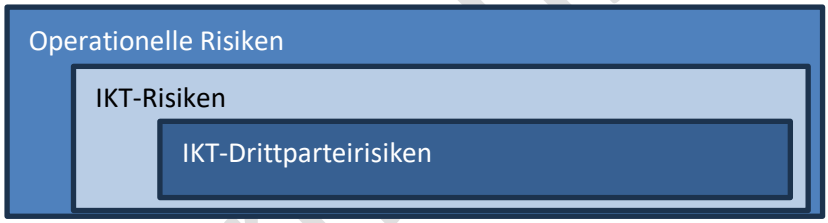
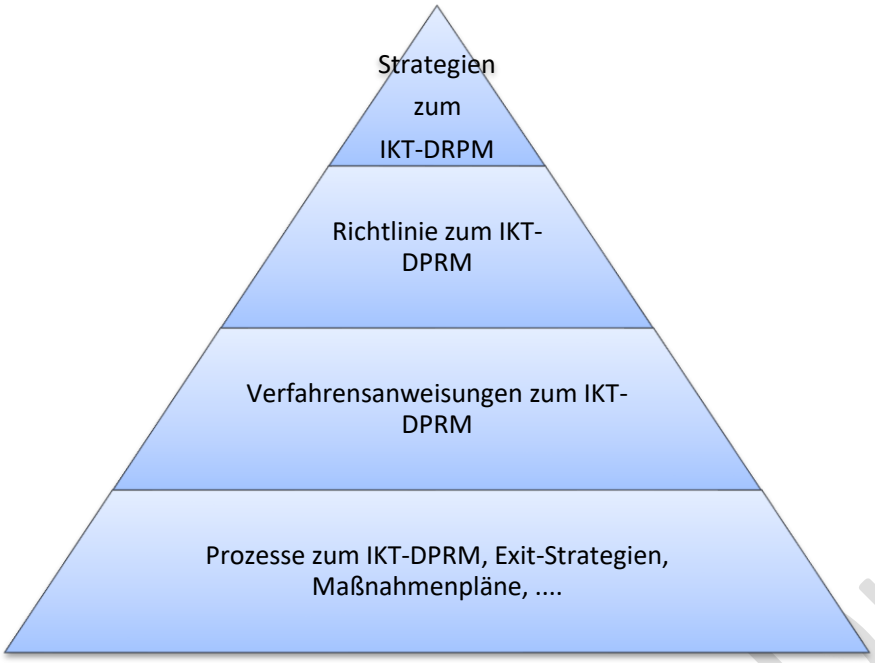


Abbildung 1 - eigene Darstellung zur Einordnung der IKT-Drittparteirisiken

Für IKT-Drittparteirisiken finden demnach grundsätzlich die Vorgaben zum Management von operationellen Risiken im Allgemeinen sowie die Vorgaben zum IKT-Risikomanagement im Speziellen Anwendung.

13 IKT-Drittpartei Governance Framework

Die Vorgaben der IKT-Drittparteirisikostrategie werden in der Richtlinie zum IKT-Drittparteirisikomanagement (Level-1 Dokument) konkretisiert. Ergänzende Verfahrensanweisungen (Level-2 Dokumente) beschreiben methodische und inhaltliche Detaillierungen. Sie werden ergänzt durch Prozessbeschreibungen und operative Aufzeichnungen (Level-3 Dokumente).



14 ABSTIMMBETEILIGTE

Das vorliegende Dokument wurde inhaltlich mit folgenden Funktionen abgestimmt.

Beispiele:

- *Zentraler Auslagerungsbeauftragter*
- *Informationssicherheitsbeauftragter*
- *Compliance-Funktion*
- *Risikomanagement-Funktion*
- *Kontrollfunktion für das IKT-Risikomanagement*
- *Kontrollfunktion für das IKT Drittparteirisikomanagement*
- *IT-Funktion*
- *…*

15 MITGELTENDE DOKUMENTE

Das vorliegende Dokument wird durch folgende mitgeltenden Dokumente der schriftlich fixierten Ordnung konkretisiert.

Beispiele:

- *Geschäftsstrategie*
- *Risikostrategie*
- *DOR-Strategie*
- *IT-Strategie*
- *Auslagerungsstrategie*
- *Richtlinie zum IKT-Drittparteirisikomanagement*
- *…*