parcIT

ZAM eG

Vom IKT-Risikomanagement zum operationellen Risiko

So gelingt der Übergang

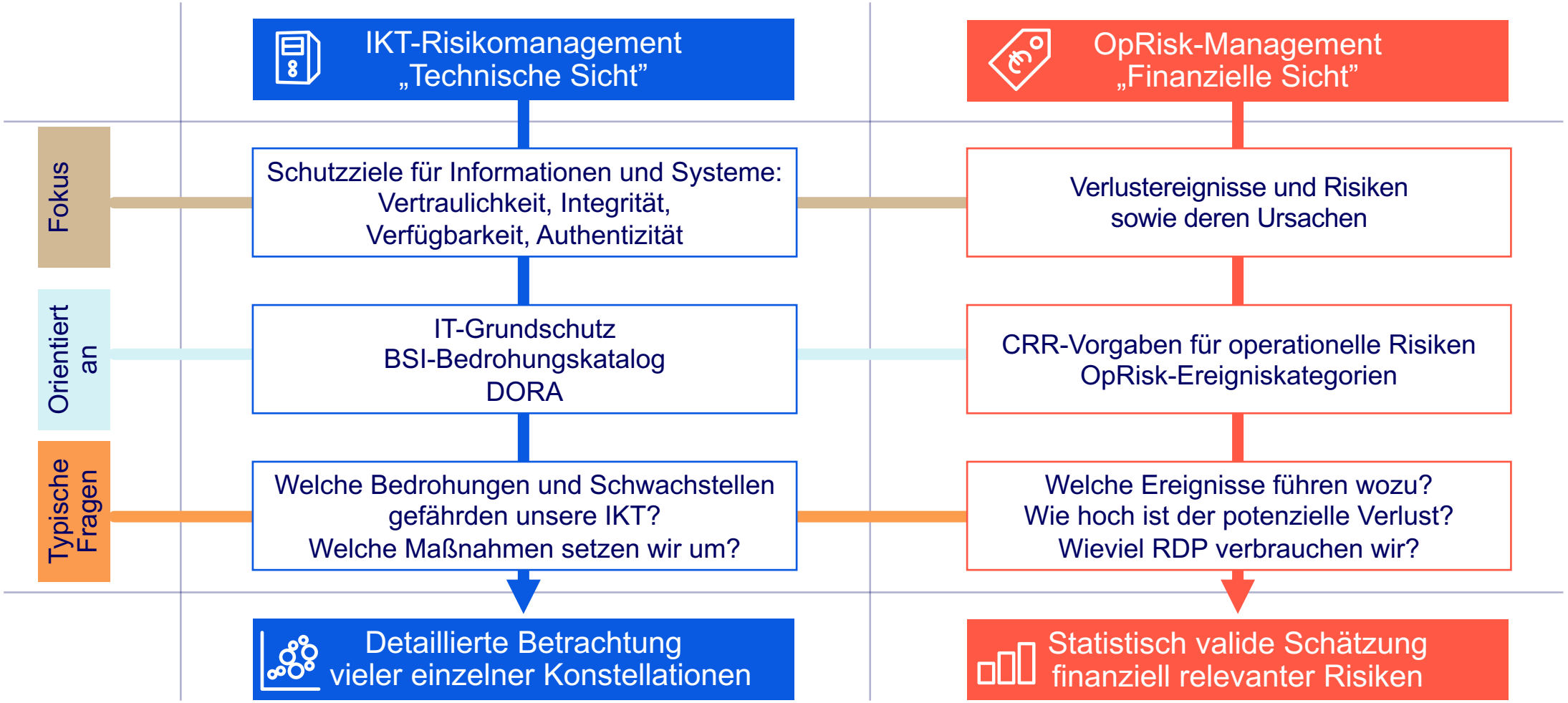
upDATE 26, 7. Mai 2026

Petra Ludwig, parcIT GmbH, Sönke Nißen, ZAM eG

Mitglied der
ATRUVIA GRUPPE

Herausforderung IKT-Risiken im Risikomanagement

Unterschiedliche Betrachtungsweisen



Bisherige Praxis in der Informationssicherheit

Unterschiedliche Herangehensweise bei der Ermittlung von Risiken

Vorgehensweise ISB / IKT-Risikokontrollfunktion bisher

- **Verschiedenste Varianten der Risikoermittlung:**
  - Risiken aus Risikoberichterstattung der Dienstleister, insb. Atruvia
  - Assetspezifische Risiken wie „Ausfall“, „Fehlbedienung durch MA“, „kriminelle Handlungen“
- Viel Bauchgefühl / Expertenschätzung
- Kein wiederholbares System

Neuerungen durch den Digital Operations Resilience Act / DORA

Umdenken in den Banken erforderlich

Gefordert ist ein IKT-Risikomanagementrahmen	▪ Beteiligung von Beauftragtenfunktionen wie IKT-Risikokontrollfunktion, Auslagerungs- und Notfallmanagement ▪ Aber auch Risikosteuerung / Controlling
Managementrahmen soll es ermöglichen, alle IKT-Risiken schnellstmöglich zu …	… identifizieren, … bewerten und … in die Risikosteuerung zu übernehmen
Herausforderung und Chance: Vermeidung von Doppelanrechnungen	Häufig gelebte Praxis ▪ Risiko wie „Fehlbedienung“ wird am Asset berücksichtigt ▪ Zusätzlich jedoch auch im Self-Assessment als Prozessrisiko

Schaffung eines neuen Verbundstandards

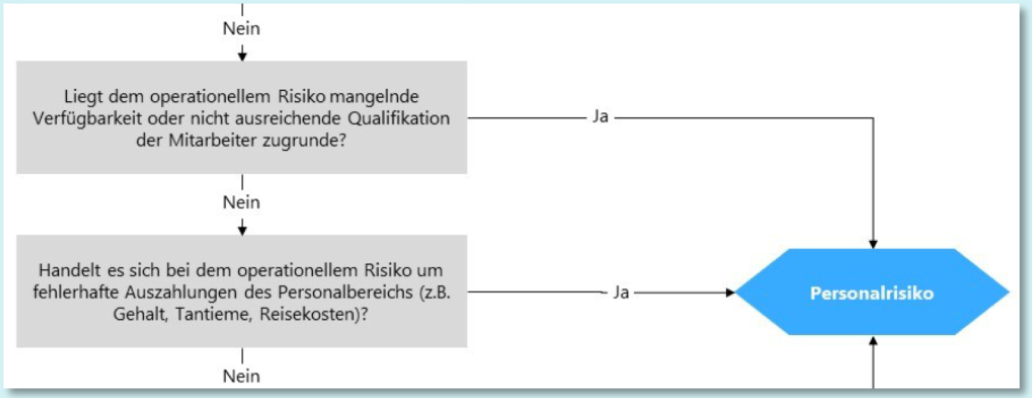
für das IKT-Risikomanagement durch die ZAM eG - DORA-konforme Vorgehensweise

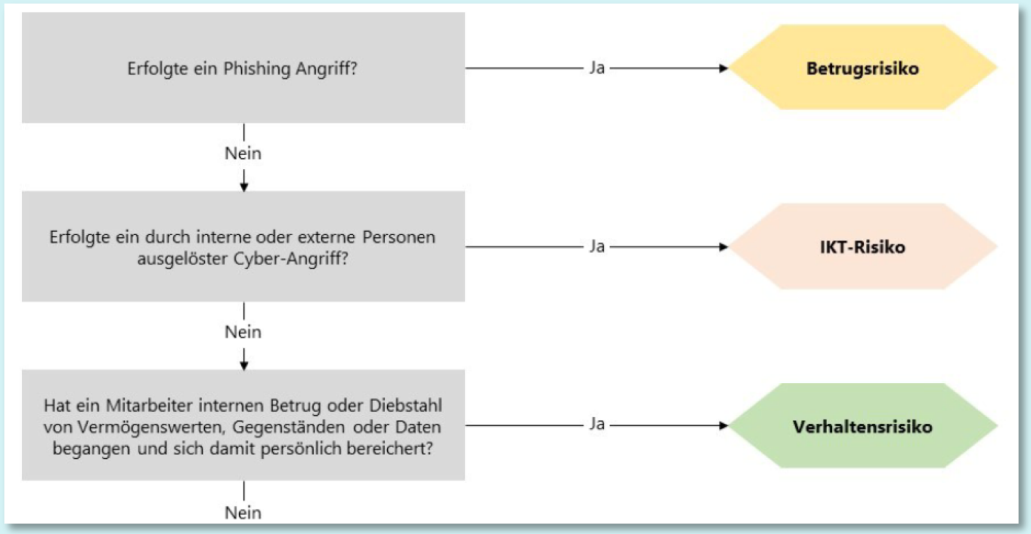
ZAM eG hat im Rahmen des Verbundstandards (Verfahrenslieferant) eine Logik entwickelt, die zum OpRisk-Entscheidungsbaum der parcIT passt

Zukünftig nur noch IKT-Risiken, die auch gemäß Entscheidungsbaum als „echte“ IKT-Risiken zu verstehen sind.

Bedeutet Risiken mit einem Ursprung …

- … aus Schwachstellen beim IKT-Asset
- … beim Dienstleister
- … aus unzureichender Notfallvorsorge





Logiken für IT-, Drittpartei- und Notfallrisiken

Von der Erkennung bis zur Überführung ins Risikocontrolling

Verfahrenslieferant liefert Methodik für IKT-Risiken unter Berücksichtigung der aktuellen Anforderungen aus der DORA

Beinhaltet IT-Risiken, Drittparteirisiken und Risiken aus Notfallmanagement (Letzteres noch in Entwicklung)

Institut überprüft intern wie extern, ob Schwachstellen zu erkennen sind

- Bedrohungslage der Bank wird individuell berücksichtigt
- Externe Schwachstellen (d.h. bei IKT-Dienstleistern) werden für ZAM-gesteuerte Dienstleister durch die ZAM ermittelt und in ForumISM zur Verfügung gestellt
- Ergebnisse werden in einen Export überführt, der in agree21ORM genutzt werden kann

Risikomethodik für IT-Risiken

Analyse, ob intern wie extern ein sicherer IT-Betrieb gewährleistet ist

Schwachstelle entsteht dann, wenn intern ein sicherer IT-Betrieb nicht gewährleistet ist

Schwachstelle entsteht auch, wenn Anforderungen zum sicheren IT-Betrieb nicht in Arbeitsanweisungen verankert sind

- Definiert sich als bankinterne Soll-Soll- oder Soll-Ist-Abweichung zum Bankensollmaßnahmenkatalog

Schwachstelle entsteht dann, wenn extern ein sicherer IT-Betrieb nicht gewährleistet ist

- ZAM-gesteuerte Dienstleister (Atruvia, DZ Bank, usw.) werden von der ZAM laufend überwacht und die Ergebnisse den Banken bereitgestellt
- Eigene Dienstleister muss die Bank individuell betrachten

Individuelle Risikoermittlung

Berücksichtigung bankindividueller Bedrohungslage

Sobald eine Schwachstelle identifiziert wurde, entsteht für die Bank ein Risiko

- Darstellung der Risiken analog der Grundeinstellungen aus agree21ORM möglich
- Empfehlung, dass die Grundeinstellungen in ForumISM zwischen Risikocontrolling und IKT-Risikokontrollfunktion abgestimmt werden soll

Für das Risiko wird der Bedrohungskatalog der Bank herangezogen

- Institutseigene Einschätzung notwendig, wie relevant die Bedrohungen sind (47 Stück nach BSI)
- Einschätzung hat direkte Auswirkung auf die Eintrittswahrscheinlichkeit des Risikos
- Mapping OpRisk-Kategorie bereits gepflegt

Automatische Risikoermittlung

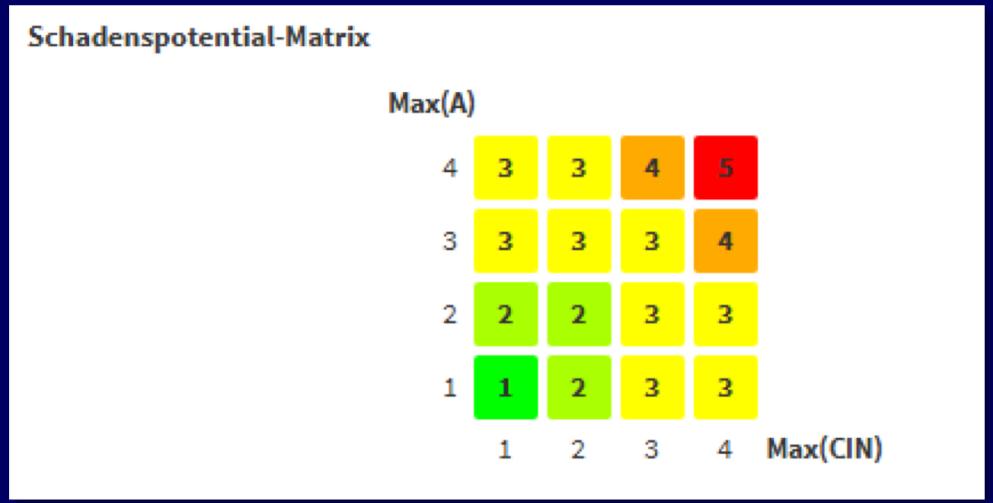
Keine Expertenschätzung notwendig

Bewertung der Eintrittswahrscheinlichkeit

Aus der Kombination von Schwachstelle und Bedrohung wird eine Eintrittswahrscheinlichkeit errechnet (JRE-Wert)

Bewertung Schadenspotential

- Anhand Schutzbedarf der Prozesse, die von der Schwachstelle betroffen wären, wird ein Schadenspotential ermittelt
- Logik: Je schützenswerter ein Prozess ist, umso höher fällt tendenziell ein Schaden aus
  - Vergleich der Prozesse …
  - … „Fuhrpark managen“ (A1CIN2) zu
  - … „Wertpapiergeschäft“ (A4CIN3)



Ermittlung von Restrisiken

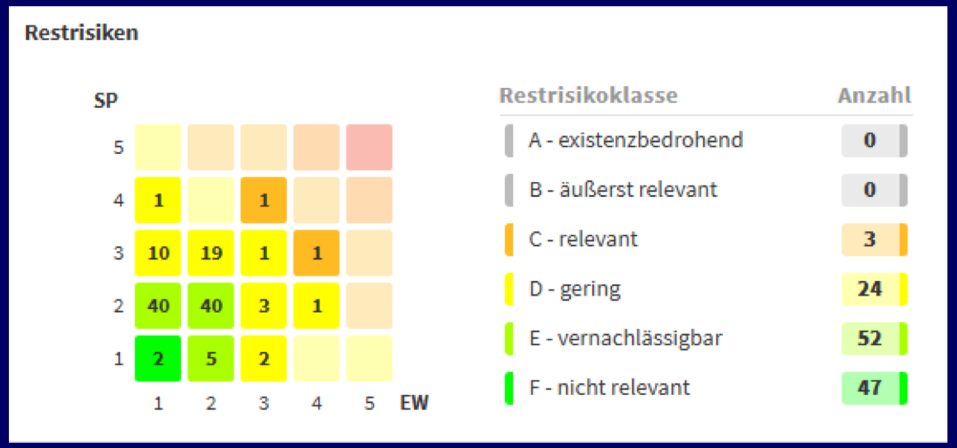
Individuelle Festlegung der Maßnahmen

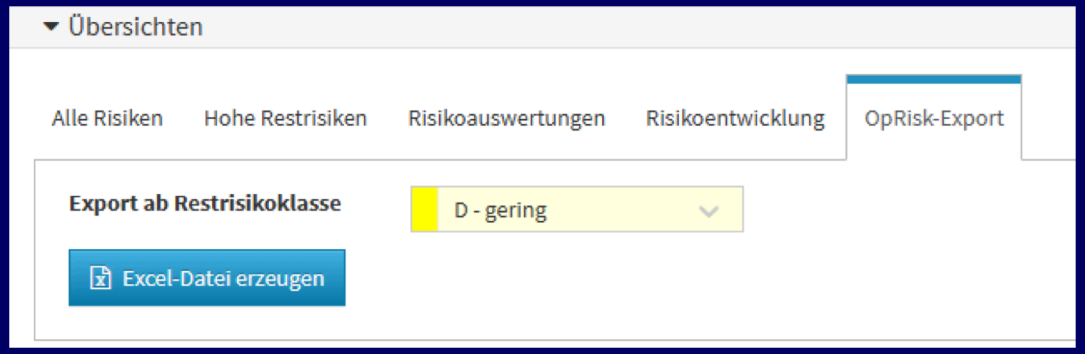
Das ermittelte Risiko muss von der Bank geprüft und ein Umgang festgelegt werden

- Akzeptanz
- Behandlung
- Vermeidung
- Übertragung

Je nach Umgang mit dem Risiko ergibt sich ein Restrisiko

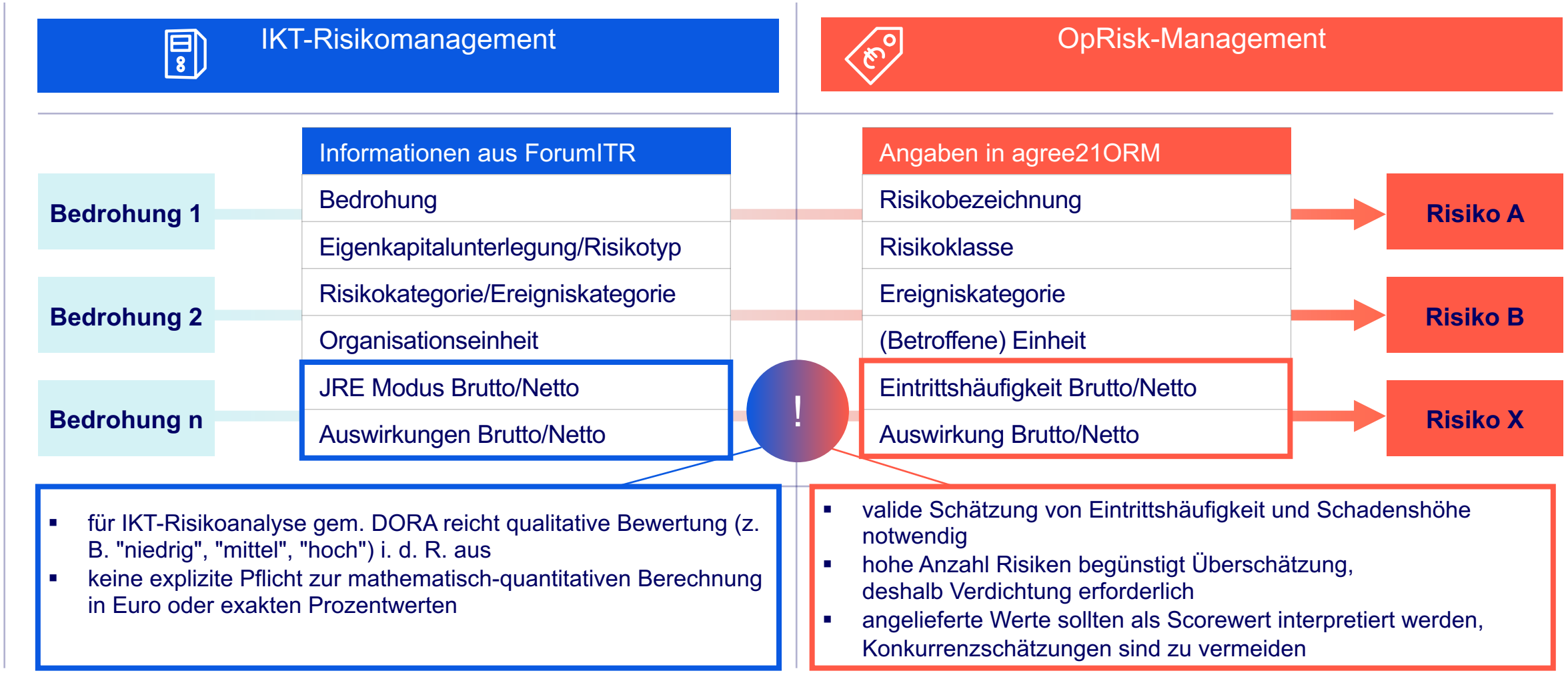
- Risiko muss dem Risikocontrolling in geeigneter Form mitgeteilt werden (vgl. IKT-Risikomanagementrahmen)
- Ergebnisse werden in einen Export überführt, der in agree21ORM genutzt werden kann





Überführungen der Bedrohungen als Risiken in das Self-Assessment

Übergabe der Bedrohungen mit den notwendigen Attributen für das OPR-Verfahren kein Automatismus



Was der OpRisk-Manager im Self-Assessment zusammenführen sollte:

Verschiedene Informationsquellen zu einer validen Einschätzung

Intensiver Austausch zwischen IKT- und OpRisk-Manager ist essentiell.

Pro Ereigniskategorie bzw. pro OpRisk-Risiko

Quelle	Bisherige Schätzung aus Vorjahres-Self-Assessment	Historische Schadensfälle (Institut)	Historische Schadensfälle (Pool)	IKT-Risikomanagement-Einschätzung	Weitere Quellen wie Mitarbeitende des Instituts, Revisionsberichte etc.
Leitfragen	▪ Aktualität gegeben? ▪ Veränderung am Institut (IT, Infrastruktur, Mitarbeitende..) ? ▪ Einfluss Bagatellgrenze?	▪ Übertragbarkeit auf Institut? ▪ Skalieren notwendig? ▪ Aktualität gegeben? ▪ Einfluss Bagatellgrenze?	▪ Übertragbarkeit qualitative Einschätzung? ▪ Granularität und Verdichtung? ▪ Kategorisierung?	▪ Welche Quellen? ▪ Aktualität? ▪ ….	

Schätzung von Eintrittshäufigkeit und Schadenshöhe (Modus/Max) durch den OpRisk-Manager

Self-Assessment: Vorbereitung und Durchführung

Beispiel Ereigniskategorie 6: Geschäftsunterbrechungen und Systemausfälle

Granularität der IKT-Risiken versus überschaubare historische Schadensfälle im OpRisk

Bezeichnung des Trägerobjektes	Risikobezeichnung: GAP-Risiko zu Sollmaßnahme ...	Bedrohung	Risikokategorie (bzw. Ereigniskategorie)	JRE	Eintrittswahrscheinlichk	Schadenspotenz
Banking	... „Anforderungen an die Anwendungssicherheit - Elektronische Bestell- und Zahlungsanwendungen“	G 0.18 Fehlplanung oder fehlende Anpassung	6.1.1 - Hardware/Software/Telekommunikation	0,194	2 - möglich	2 - mittel
Ermittlung und Bereitstellung von Risikokennza	... „Informationen zur Authentifizierung - sichere Anmeldeverfahren und Passwortschutz- Allgemeine Vorgaben“	G 0.18 Fehlplanung oder fehlende Anpassung	6.1.1 - Hardware/Software/Telekommunikation	0,223	2 - möglich	3 - hoch
NAVIGATO Vermögensplanung	... „Rückgabe von Werten - Außerbetriebnahme“	G 0.18 Fehlplanung oder fehlende Anpassung	6.1.1 - Hardware/Software/Telekommunikation	0,083	1 - unwahrscheinlich	1 - niedrig
Shop	... „Zugangssteuerung - Vergabe und Änderungsprozess“	G 0.18 Fehlplanung oder fehlende Anpassung	6.1.1 - Hardware/Software/Telekommunikation	0,250	2 - möglich	1 - niedrig
I-Rating	... „Zugangssteuerung - dokumentiertes Berechtigungskonzept“	G 0.18 Fehlplanung oder fehlende Anpassung	6.1.1 - Hardware/Software/Telekommunikation	0,250	2 - möglich	2 - mittel
Datentransfer	... „Zugangssteuerung - Regelungen und Konzepte“	G 0.18 Fehlplanung oder fehlende Anpassung	6.1.1 - Hardware/Software/Telekommunikation	0,194	3 - wahrscheinlich	2 - mittel
M365	... „Zugangssteuerung - Regelungen und Konzepte“	G 0.18 Fehlplanung oder fehlende Anpassung	6.1.1 - Hardware/Software/Telekommunikation	0,194	3 - wahrscheinlich	2 - mittel
Datentransfer	... „Zugangssteuerung - Regelungen und Konzepte“	G 0.24 Zerstörung von Geräten oder Datenträgern	6.1.1 - Hardware/Software/Telekommunikation	0,194	3 - wahrscheinlich	2 - mittel
M365	... „Zugangssteuerung - Regelungen und Konzepte“	G 0.24 Zerstörung von Geräten oder Datenträgern	6.1.1 - Hardware/Software/Telekommunikation	0,194	3 - wahrscheinlich	2 - mittel
Banking	... „Anforderungen an die Anwendungssicherheit - Elektronische Bestell- und Zahlungsanwendungen“	G 0.25 Ausfall von Geräten oder Systemen	6.1.1 - Hardware/Software/Telekommunikation	0,194	2 - möglich	2 - mittel
Ermittlung und Bereitstellung von Risikokennza	... „Informationen zur Authentifizierung - sichere Anmeldeverfahren und Passwortschutz- Allgemeine Vorgaben“	G 0.25 Ausfall von Geräten oder Systemen	6.1.1 - Hardware/Software/Telekommunikation	0,223	2 - möglich	3 - hoch
Shop	... „Zugangssteuerung - Vergabe und Änderungsprozess“	G 0.25 Ausfall von Geräten oder Systemen	6.1.1 - Hardware/Software/Telekommunikation	0,250	2 - möglich	1 - niedrig
I-Rating	... „Zugangssteuerung - dokumentiertes Berechtigungskonzept“	G 0.25 Ausfall von Geräten oder Systemen	6.1.1 - Hardware/Software/Telekommunikation	0,250	2 - möglich	2 - mittel
Datentransfer	... „Zugangssteuerung - Regelungen und Konzepte“	G 0.25 Ausfall von Geräten oder Systemen	6.1.1 - Hardware/Software/Telekommunikation	0,194	3 - wahrscheinlich	2 - mittel
M365	... „Zugangssteuerung - Regelungen und Konzepte“	G 0.25 Ausfall von Geräten oder Systemen	6.1.1 - Hardware/Software/Telekommunikation	0,194	3 - wahrscheinlich	2 - mittel
Banking	... „Anforderungen an die Anwendungssicherheit - Elektronische Bestell- und Zahlungsanwendungen“	G 0.27 Ressourcenmangel	6.1.1 - Hardware/Software/Telekommunikation	0,194	2 - möglich	2 - mittel
I-Rating	... „Zugangssteuerung - dokumentiertes Berechtigungskonzept“	G 0.27 Ressourcenmangel	6.1.1 - Hardware/Software/Telekommunikation	0,250	2 - möglich	2 - mittel
Datentransfer	... „Zugangssteuerung - Regelungen und Konzepte“	G 0.27 Ressourcenmangel	6.1.1 - Hardware/Software/Telekommunikation	0,194	3 - wahrscheinlich	2 - mittel
M365	... „Zugangssteuerung - Regelungen und Konzepte“	G 0.27 Ressourcenmangel	6.1.1 - Hardware/Software/Telekommunikation	0,194	3 - wahrscheinlich	2 - mittel
Banking	... „Anforderungen an die Anwendungssicherheit - Elektronische Bestell- und Zahlungsanwendungen“	G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen	6.1.1 - Hardware/Software/Telekommunikation	0,932	2 - möglich	2 - mittel
Datentransfer	... „Zugangssteuerung - Regelungen und Konzepte“	G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen	6.1.1 - Hardware/Software/Telekommunikation	0,932	3 - wahrscheinlich	2 - mittel
M365	... „Zugangssteuerung - Regelungen und Konzepte“	G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen	6.1.1 - Hardware/Software/Telekommunikation	0,932	3 - wahrscheinlich	2 - mittel
Banking	... „Anforderungen an die Anwendungssicherheit - Elektronische Bestell- und Zahlungsanwendungen“	G 0.32 Fehlerhafte Administration von Kommunikationsverbindungen	6.1.1 - Hardware/Software/Telekommunikation	0,194	2 - möglich	2 - mittel
eBanking	... „Anforderungen an die Anwendungssicherheit - Elektronische Bestell- und Zahlungsanwendungen“	G 0.32 Fehlerhafte Administration von Kommunikationsverbindungen	6.1.1 - Hardware/Software/Telekommunikation	0,167	1 - unwahrscheinlich	4 - sehr hoch
IDA	... „Anforderungen an die Anwendungssicherheit - Elektronische Bestell- und Zahlungsanwendungen“	G 0.32 Fehlerhafte Administration von Kommunikationsverbindungen	6.1.1 - Hardware/Software/Telekommunikation	0,167	2 - möglich	2 - mittel
I-Rating	... „Zugangssteuerung - dokumentiertes Berechtigungskonzept“	G 0.32 Fehlerhafte Administration von Kommunikationsverbindungen	6.1.1 - Hardware/Software/Telekommunikation	0,250	2 - möglich	2 - mittel
Datentransfer	... „Zugangssteuerung - Regelungen und Konzepte“	G 0.32 Fehlerhafte Administration von Kommunikationsverbindungen	6.1.1 - Hardware/Software/Telekommunikation	0,194	3 - wahrscheinlich	2 - mittel
M365	... „Zugangssteuerung - Regelungen und Konzepte“	G 0.32 Fehlerhafte Administration von Kommunikationsverbindungen	6.1.1 - Hardware/Software/Telekommunikation	0,194	3 - wahrscheinlich	2 - mittel
Banking	... „Anforderungen an die Anwendungssicherheit - Elektronische Bestell- und Zahlungsanwendungen“	G 0.39 Schadprogramme	6.1.1 - Hardware/Software/Telekommunikation	0,006	2 - möglich	2 - mittel
NAVIGATO Vermögensplanung	... „Rückgabe von Werten - Außerbetriebnahme“	G 0.39 Schadprogramme	6.1.1 - Hardware/Software/Telekommunikation	0,003	1 - unwahrscheinlich	1 - niedrig
eBanking	... „Anforderungen an die Anwendungssicherheit - Elektronische Bestell- und Zahlungsanwendungen“	G 0.39 Schadprogramme	6.1.1 - Hardware/Software/Telekommunikation	0,005	1 - unwahrscheinlich	4 - sehr hoch
IDA	... „Anforderungen an die Anwendungssicherheit - Elektronische Bestell- und Zahlungsanwendungen“	G 0.39 Schadprogramme	6.1.1 - Hardware/Software/Telekommunikation	0,005	2 - möglich	2 - mittel
I-Rating	... „Zugangssteuerung - dokumentiertes Berechtigungskonzept“	G 0.39 Schadprogramme	6.1.1 - Hardware/Software/Telekommunikation	0,008	2 - möglich	2 - mittel
Datentransfer	... „Zugangssteuerung - Regelungen und Konzepte“	G 0.39 Schadprogramme	6.1.1 - Hardware/Software/Telekommunikation	0,006	3 - wahrscheinlich	2 - mittel
M365	... „Zugangssteuerung - Regelungen und Konzepte“	G 0.39 Schadprogramme	6.1.1 - Hardware/Software/Telekommunikation	0,006	3 - wahrscheinlich	2 - mittel
Banking	... „Anforderungen an die Anwendungssicherheit - Elektronische Bestell- und Zahlungsanwendungen“	G 0.39 Schadprogramme	6.1.1 - Hardware/Software/Telekommunikation	0,006	2 - möglich	2 - mittel
NAVIGATO Vermögensplanung	... „Rückgabe von Werten - Außerbetriebnahme“	G 0.39 Schadprogramme	6.1.1 - Hardware/Software/Telekommunikation	0,003	1 - unwahrscheinlich	1 - niedrig
eBanking	... „Anforderungen an die Anwendungssicherheit - Elektronische Bestell- und Zahlungsanwendungen“	G 0.39 Schadprogramme	6.1.1 - Hardware/Software/Telekommunikation	0,005	1 - unwahrscheinlich	4 - sehr hoch
IDA	... „Anforderungen an die Anwendungssicherheit - Elektronische Bestell- und Zahlungsanwendungen“	G 0.39 Schadprogramme	6.1.1 - Hardware/Software/Telekommunikation	0,005	2 - möglich	2 - mittel
I-Rating	... „Zugangssteuerung - dokumentiertes Berechtigungskonzept“	G 0.39 Schadprogramme	6.1.1 - Hardware/Software/Telekommunikation	0,008	2 - möglich	2 - mittel
Datentransfer	... „Zugangssteuerung - Regelungen und Konzepte“	G 0.39 Schadprogramme	6.1.1 - Hardware/Software/Telekommunikation	0,006	3 - wahrscheinlich	2 - mittel
M365	... „Zugangssteuerung - Regelungen und Konzepte“	G 0.39 Schadprogramme	6.1.1 - Hardware/Software/Telekommunikation	0,006	3 - wahrscheinlich	2 - mittel
Datentransfer	... „Zugangssteuerung - Regelungen und Konzepte“	G 0.11 Ausfall oder Störung von Dienstleistern	6.1.3 - Störung eines externen Dienstleisters	0,932	3 - wahrscheinlich	2 - mittel
M365	... „Zugangssteuerung - Regelungen und Konzepte“	G 0.11 Ausfall oder Störung von Dienstleistern	6.1.3 - Störung eines externen Dienstleisters	0,932	3 - wahrscheinlich	2 - mittel

OPR Schadensfallbericht 2025

Muster ohne Institutsdaten

Kapitel 3 - Schadensfälle nach Ereigniskategorien

3.3 Anzahl der Schadensfälle Level 2 (2/3) 2019 - 2024*

Ereigniskategorie Level 1	Ereigniskategorie Level 2	Normierte Poolwerte Maximum	Normierte Poolwerte Mittelwert	Institut (normiert) Mittelwert	Poolwerte Maximum	Poolwerte Mittelwert	Institut Mittelwert
6 Geschäftsunte...	Gesamt	**0,9678**	**0,0139**	**0,0000**	**7**	**0,2932**	**0,0000**
	6.1 Ausfälle der Technolo...	0,9678	0,0121	0,0000	7	0,2638	0,0000
	6.x < Keine Angabe >	0,4778	0,0018	0,0000	5	0,0294	0,0000

* Ereignisdatum 01.01.2019 – 31.12.2024; Mittelwert pro Institut (normiert: pro 100 Mio. Euro Bilanzsumme) im Jahresdurchschnitt; Maximum über gesamten Zeitraum

Zusammenfassung und Verdichtung der IKT-Risiken notwendig

Keine automatisierte Übernahme der Schätzwerte, weitere Quellen berücksichtigen

Beispiel: Ausschnitt Export-Liste aus IKT-Risikomanagement für Ereigniskategorie 6:

Bedrohung	Ereigniskategorie	JRE	Eintritts-wahrscheinlichkeit	Schadens-potenzial
G 0.18 Fehlplanung oder fehlende Anpassung	6.1.1 - Hardware/Software/Telekommunikation	0,194	2 - möglich	2 - mittel
G 0.24 Zerstörung von Geräten oder Datenträgern	6.1.1 - Hardware/Software/Telekommunikation	0,194	2 - möglich	2 - mittel
G 0.25 Ausfall von Geräten oder Systemen	6.1.1 - Hardware/Software/Telekommunikation	0,014	1 - unwahrscheinlich	3 - hoch
G 0.33 Personalausfall	6.1.4 Nichtverfügbarkeit von Arbeitskräften/Räumlichkeiten	0,932	3 - wahrscheinlich	1 - niedrig
G 0.33 Personalausfall	6.1.4 Nichtverfügbarkeit von Arbeitskräften/Räumlichkeiten	0,250	2 - möglich	1 - niedrig
G 0.08 Ausfall oder Störung der Stromversorgung	6.1.5 Ausfall von Versorgungseinrichtungen	,167	2 - möglich	- sehr hoch

1

2

3

1 **Mapping** der Bedrohung auf Ereigniskategorie in FORUM ITR bereits automatisiert vorgeschlagen

2 **Weder Übernahme noch Summation** der Werte ist sachgemäß, sie können als Scorewerte interpretiert werden.

3 Je nach Spanne der verschiedenen Schadenspotenziale ist **Verdichtung auf ein oder mehrere Risiken** sinnvoll.

Weitere Quellen zur Risikoschätzung notwendig

Würdigung weiterer Quellen: Historische Schadensfälle

Beispiel: Interne und externe Schadensfallhistorie

	Schätzung IKT-Risiken (Restrisiken)			6-jähr. Historie Institut*		6-jähr. Historie Pool**	
Ereigniskategorie	**JRE**	**Eintritts-wahrscheinlichkeit**	**Schadens-potenzial**	**Anzahl**	**Bruttoschaden-summe pro SF**	**Anzahl**	**Bruttoschaden-summe pro SF**
6.1.1 - Hardware/Software/ Telekommunikation	0,2	2 - möglich	2 - mittel	0 – 1 Fall, Mittelwert 0,3	Maximum 10.000 €, Mittelwert 5.000 €	**Ereigniskategorie 6 insgesamt:** Mittelwert: 0,2932, Maximum: 7	Mittelwert: 44.780 € 25 %-Quantil: 3.000 € Median: 6.710 € 75 %-Quantil: 22.565 €
6.1.1 - Hardware/Software/ Telekommunikation	0,2	2 - möglich	2 - mittel				
6.1.1 - Hardware/Software/ Telekommunikation	0,01	1 - unwahrscheinlich	3 - hoch				
6.1.4 Nichtverfügbarkeit von Arbeitskräften/Räumlichkeiten	0,9	3 - wahrscheinlich	1 - niedrig	0 – 4, Mittelwert 0,2	Maximum 40.000 €, Mittelwert 15.000 €		
6.1.4 Nichtverfügbarkeit von Arbeitskräften/Räumlichkeiten	0,2	2 - möglich	1 - niedrig				
6.1.5 Ausfall von Versorgungseinrichtungen	0,2	2 - möglich	4 - sehr hoch	0 – 2, Mittelwert 0,1	Maximum 60.000 €, Mittelwert 10.000 €		

* Beispielwerte **Quelle: parcIT-Schadensfallbericht 2025

Schätzung der IKT-Risiken im OpRisk-Self Assessment

Beispielhafte Schätzung für ein IKT-Risiko „6.1.1 – Hardware/Software/Telekommunikation“

	Schätzung IKT-Risiken			6-jähr. Historie Institut*		6-jähr. Historie Pool**	
Ereigniskategorie	**JRE**	**Eintritts-wahrscheinlichkeit**	**Schadens-potenzial**	**Anzahl**	**Bruttoschaden-summe pro SF**	**Anzahl**	**Bruttoschaden-summe pro SF**
6.1.1 - Hardware/Soft-ware/Telekommunikation	0,2	2 - möglich	2 - mittel	0 – 1 Fall, Mittelwert 0,3	Maximum 10.000 €, Mittelwert 5.000 €	**Ereigniskategorie 6 insgesamt:** Mittelwert: 0,2932, Maximum: 7	Mittelwert: 44.780 € 25 %-Quantil: 3.000 € Median: 6.710 € 75 %-Quantil: 22.565 €
6.1.1 - Hardware/Soft-ware/Telekommunikation	0,2	- möglich	2 - mittel				
6.1.1 - Hardware/Soft-ware/Telekommunikation	0,01	1 - unwahrscheinlich	3 - hoch				

1

Zusammenfassen der IKT-Risiken pro Ereigniskategorie
Level 3, Level 2 oder Level 1 (je mehr Daten, desto stabiler)

2

Schätzen der Eintrittshäufigkeit:

- Minimum: 0 (immer)
- Modus: höher als Mittelwert Pool, da dort Bagatellgrenze die Anzahl drückt, eigene Historie als Basis nehmen, aktuelle Entwicklungen in Historie und IKT-Risikowerten berücksichtigen
- Maximum: hohen Wert ansetzen, z. B. 9.999, um eine unbeschränkte Poisson-Verteilung zu gewährleisten

* Beispielwerte **Quelle: parcIT-Schadensfallbericht 2025

Schätzung der IKT-Risiken im OpRisk-Self Assessment

Beispielhafte Schätzung für ein IKT-Risiko „6.1.1 – Hardware/Software/Telekommunikation“

	Schätzung IKT-Risiken			6-jähr. Historie Institut *		6-jähr. Historie Pool**	
Ereigniskategorie	**JRE**	**Eintritts-wahrscheinlichkeit**	**Schadens-potenzial**	**Anzahl**	**Bruttoschaden-summe pro SF**	**Anzahl**	**Bruttoschaden-summe pro SF**
6.1.1 - Hardware/Soft-ware/Telekommunikation	0,2	2 - möglich	2 - mittel	0 – 1 Fall, Mittelwert 0,3	Maximum 10.000 €, Mittelwert 5.000 €	**Ereigniskategorie 6 insgesamt:** Mittelwert: 0,2932, Maximum: 7	Mittelwert: 44.780 € 25 %-Quantil: 3.000 € Median: 6.710 € 75 %-Quantil: 22.565 €
6.1.1 - Hardware/Soft-ware/Telekommunikation	0,2	2 - möglich	2 - mittel				
6.1.1 - Hardware/Soft-ware/Telekommunikation	0,01	1 - unwahrscheinlich	3 - hoch				

3

3

Schätzen der Schadenshöhe:

- Minimum: 0 (immer)
- Modus: eher unter Median Pool, da dort Bagatellgrenze zu höherem Median führt, eigene Historie als Basis nehmen, Veränderungen in Historie und gg.über Vorjahr in IKT-Risikowerten berücksichtigen
- Maximum: mindestens Maximum aus Institutshistorie, Orientierung an hohen Quantilen und Top 100 aus Pool

* Beispielwerte **Quelle: parcIT-Schadensfallbericht 2025

Zu guter Letzt

Tipps für das Self-Assessment und Fazit

- Im Self-Assessment wird die Bewertung von **Eintrittshäufigkeit und Schadenshöhe** von Risiken anhand von **Minimum, Modus, Maximum** vorgenommen.
- Die **Matrix** in ORM dient lediglich der **Darstellung** der bewerteten Risiken im Bericht. Unterschiedliche Matrix-Dimensionen zwischen den Systemen sind deshalb kein Problem.

- In der Regel werden nur **neue Risiken aus dem IKT** übernommen, für bereits bekannte Risiken erfolgt nur eine Aktualisierung, ggf. Löschung bei Wegfall.

- Rückmeldung aus Validierung und von Banken und Verbänden: **Viele Einzelrisiken** führen **tendenziell zur Überschätzung** des Gesamtrisikos.
- Für Schätzungen auf historischer Basis sollten **mindestens 10, besser mehr Datensätze** in der Datenbasis vorliegen.

Fazit: Abstimmung der Betrachtungsweisen und Aggregation der Informationen führen zu einem gelungenen Übergang vom IKT-Risiko ins Operationelle Risikomanagement