Empowering Success
The Global Transformation of Third-Party Risk Management
AVANTEC Cyber Threat Exchange Liechtenstein

Schaan, 26.09.2023, Jousry Abdel-Khalek

Solide in die Zukunft: Zahlen und Fakten (per 30.6.2023)

Mitarbeitende
(teilzeitbereinigt)

1'168 Mitarbeitende

Standorte

3 Heimmärkte

Konzernergebnis

CHF 88.7 Mio.

Kundenausleihungen

CHF 14.9 Mia.

Assets under Management

CHF 87.4 Mia.

Eigenkapital
nach Gewinnverwendung

CHF 2.1 Mia.

Einführung

Was ist Third Party Risk Management und wo ist der Zusammenhang mit Outsourcing

Zusammenarbeit mit Dritten bringt Chance aber auch Risiken, daher benötigt es ein Third Party Risk Management insbesondere bei Auslagerungen und Cyber Resilience

- Untertitelzunehmender Globalisierung und Abhängigkeit von Lieferanten ist das Management der Risiken essentiell.
- Das Outsourcing von Dienstleistungen an Dritte kann Geld und Zeit sparen. Aber Dritte bringen auch eine Reihe von Risiken mit sich, welche dann zu den eigenen Risken werden.

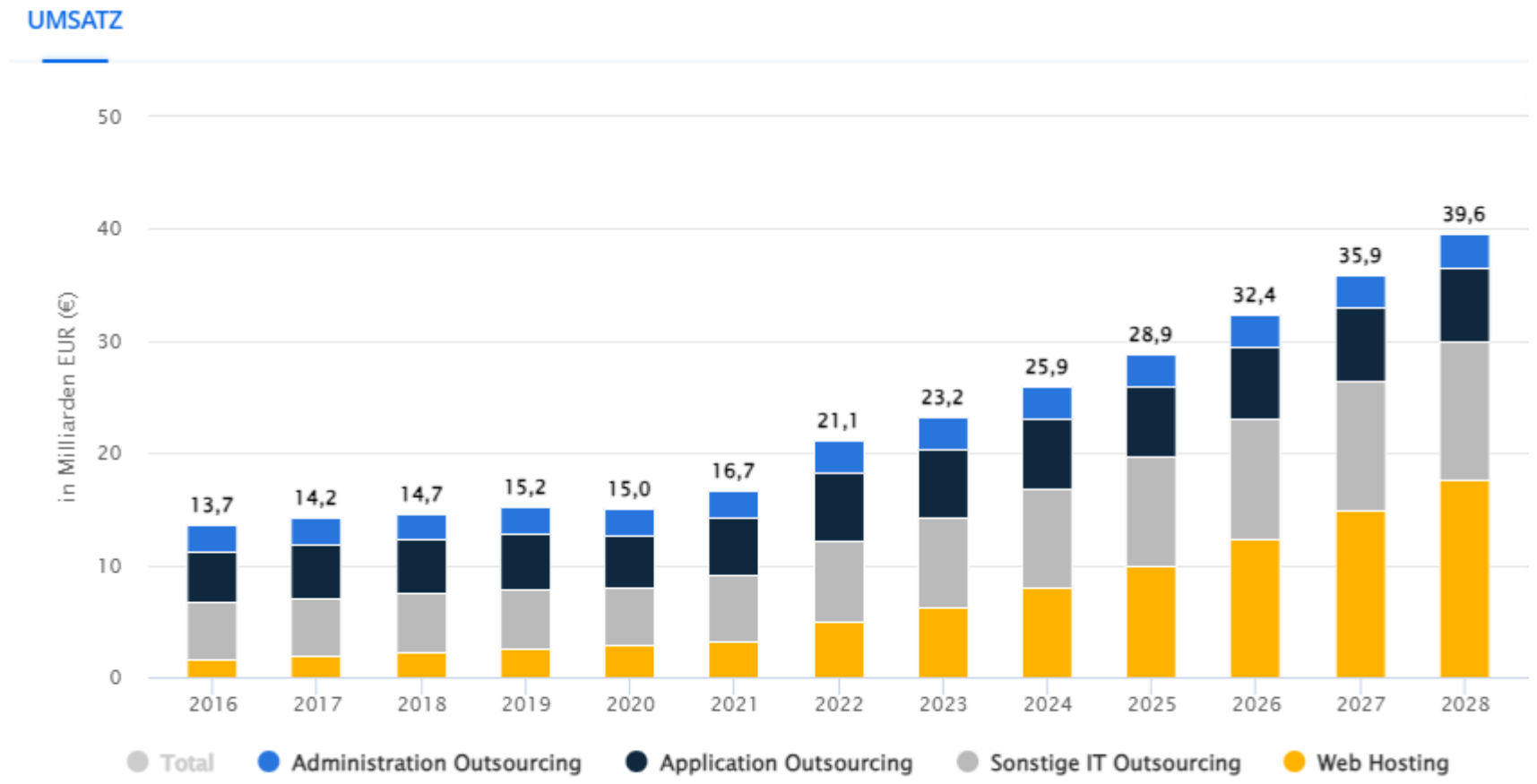
Strategisches Risiko	Compliance Risiko	Operationelles Risiko	Finanzielles Risiko	Cybersecurity Risiko	Reputations Risiko	Geopolitisches Risiko
Helfen Lieferanten die strategischen Ziele zu erreichen	Einhaltung der regulatorischen Vorschriften	Ausfall durch den Dienstleister mit	Erhöhte Aufwände beim Dritten können weiter verrechnet werden	Schwachstellen beim Zulieferer können ausgenutzt werden	Schaden am eigenen Ruf wenn Daten bei Dienstleister offen gelegt werden	Wirtschaftsstandorte sind nicht mehr erreichbar z.B. durch Krieg oder Schutzmassnahmen

- In ihrem Statusbericht zu den vor Ort Prüfungen in 2022 stuft die EZB Auslagerungen als eine der Hauptschwachstellen in den geprüften Banken und Finanzdienstleister ein.
- IT-Auslagerungen sind von wachsender Bedeutung, auch gemessen an den Ausgaben und bleiben daher auch weiter ein Schwerpunktthemen der EZB.

Quelle: ECB presentation "IT and cyber risk –key observations"

Marktsituation beispielhaft anhand Deutschland im Bereich des IT-Outsourcings

- Umsatzschätzung für das Jahr 2023 etwa 23,2Mrd. €
- Jährliche Wachstumsrate (CAGR* 2023-2028) von 11,32% → prognostiziertes Marktvolumen von 39,6Mrd. € im Jahr 2028
- Durchschnittlichen Ausgaben je Arbeitnehmer liegt im Jahr 2023 voraussichtlich bei 533,90 €
- Im globalen Vergleich wird der größte Teil des Umsatzes in den USA erwartet (157,7Mrd. € im Jahr 2023)



*Compound Annual Growth Rate

Deep Dive Outsourcing

Was ist Outsourcing?

Bei Outsourcing handelt es sich um einen Spezialfall des Third Party Managements. Im Allgemeinen ist die teilweise oder vollständige, andauernde oder wiederholte Erbringung von Tätigkeiten, Prozessen oder Funktionen durch einen spezialisierten Dienstleister, die vom auslagernden Unternehmen ansonsten realistischerweise selbst erbracht würden, gemeint.

Beispiele für Outsourcing:

- Gruppeninterne Auslagerung des IT-Betriebs (z.B. Tochter- an Muttergesellschaft)
- Auslagerung des Drucks und Versands von Kundenoutput an eine Druckerei
- Bezug einer Software, die in einer Cloud betrieben wird ("Software as a Service")

Kein Outsourcing ist u.a. :

- Bezug von Marktinformationen (z.B. Bloomberg)
- Leistungen, die aus rechtlichen Gründen durch Externe erbracht werden müssen (z.B. Durchführung der Jahresabschlussprüfung)
- Nutzung globaler Netzwerkinfrastruktur (z.B. Visa und MasterCard)

Die Gründe für eine Zusammenarbeit mit Dritten sind vielfältig!

- Fokus auf **Kernkompetenzen**
- Nutzung von gruppeninternen **Synergieeffekten**

- **Mangel** an Personal / Fachkräften
- Zugang zu **Spezialisten**
- **Kostensenkung** (z.B. für spezifische Weiterbildungen von eigenen Mitarbeitenden)

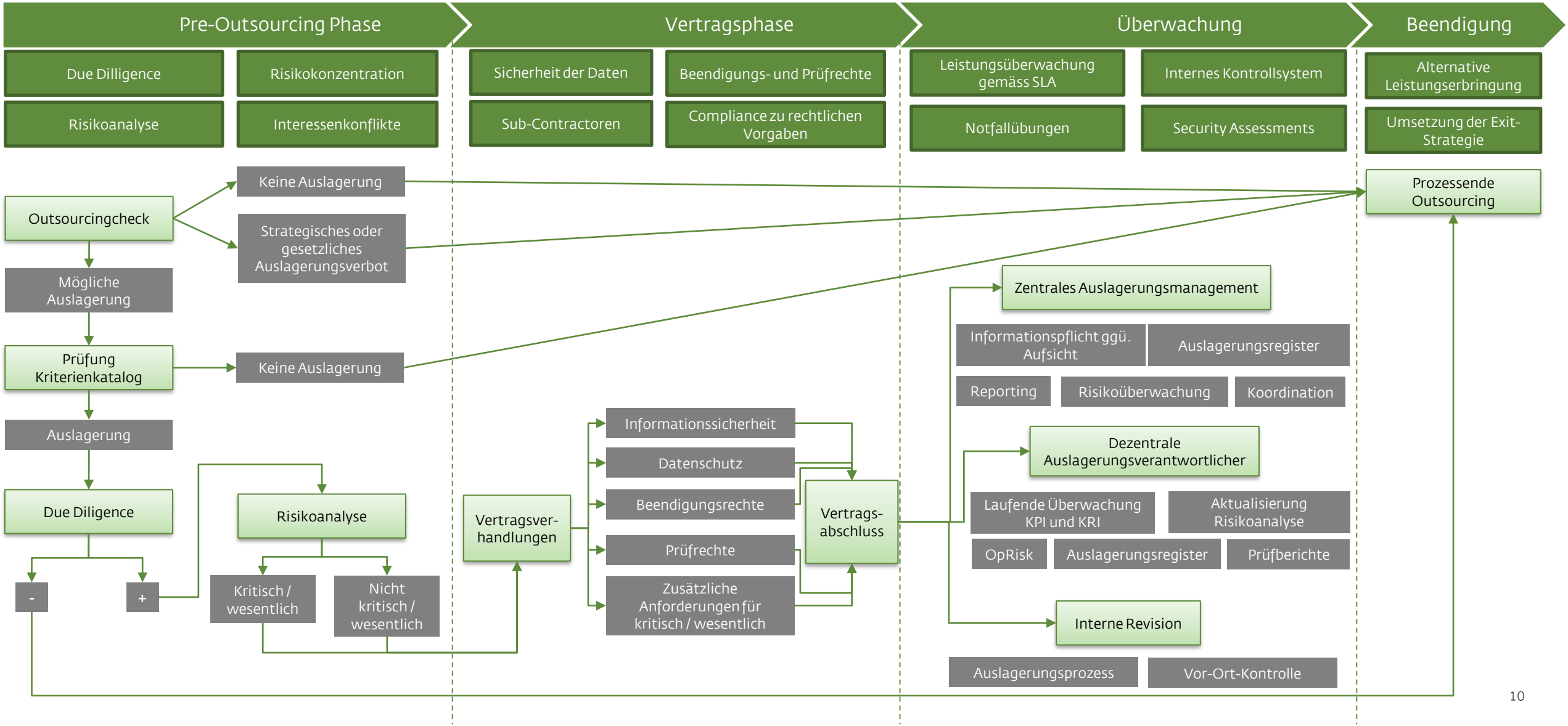
- Identifizierung von Entwicklungs- und Verbesserungspotenzial durch **Erfahrung und Vergleich** mit anderen Kunden
- Zwang zur Weiterentwicklung und des Angebots **moderner Lösungen** durch den Markt

- Deckung des Ressourcenbedarfs, **wenn nötig** (z.B. im Projektumfeld)
- **Skalierbarkeit** (z.B. Nutzung von Hyper-Scalern)

Key-Aspekte des Managements von Outsourcing

1. **Klare Definition→** Ein strukturierter Kriterienkatalog ermöglicht die effiziente Einordnung eines Vorhabens als Outsourcing. Entscheidend sind hierbei Transparenz und Dokumentation, auch für den Fall, dass das Ergebnis negativ ausfällt. Der Kriterienkatalog sollte auch Abfragen enthalten, die klar untersagte Outsourcingvorhaben offenlegen (gesetzliche oder strategische Verbote).
2. **Kritische oder wesentliche Funktionen→** Betrifft ein Outsourcing kritische oder wesentliche Funktionen, muss das Kontrollframework entsprechend strikter ausgestaltet sein (bspw. realistische Pläne zur Reintegration der Tätigkeit im Bedarfsfall). Kritische und wesentliche Funktionen sind hierbei vor allem solche, mit einem materiellen Impact auf die Geschäftstätigkeit bzw. das Risikoprofil.
3. **Solide Governance→** Die Verantwortung für die Compliance mit gesetzlichen Vorgaben verbleibt beim Unternehmen. Hierfür sind die Zuständigkeiten für die Dokumentation, das Management und die Kontrolle eines Outsourcings klar zu definieren. Des Weiteren gilt es angemessene Ressourcen sicherzustellen und eine zentrale Instanz mit entsprechender Seniorität zu etablieren, die unmittelbar für das zugehörige Risikomanagement verantwortlich ist.
4. **Drittländer→** Das Outsourcing in Drittländer (ausserhalb der EU und CH) darf nur erfolgen, sofern die Sicherheit der Daten sowie der rechtliche Rahmen vergleichbar mit denen innerhalb der Region ist. Die Prüfung des Drittanbieters durch die Aufsichtsbehörden darf nicht behindert sein und das Risiko darf sich nicht signifikant erhöhen.

Die Verantwortung des Managements erstreckt sich über alle Phasen des Outsourcing-Lifecycles



Exemplarischer Inhalt des Outsourcing-Registers

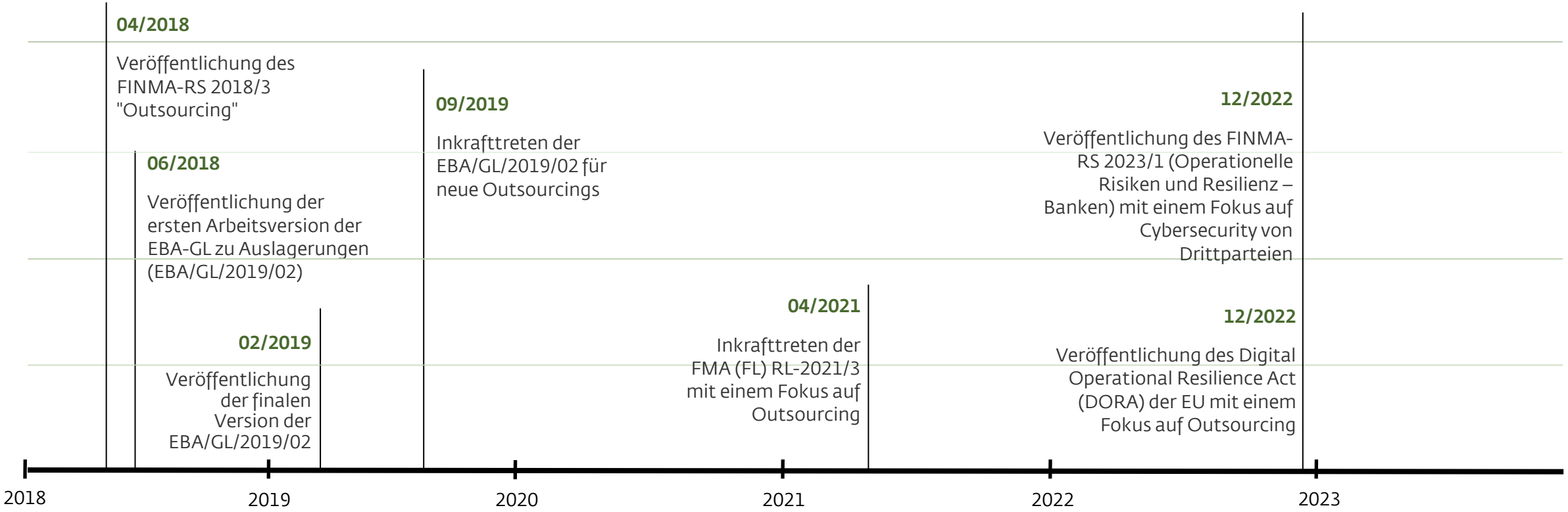
Outsourcing-Partner	Interne Informationen	Sub-Outsourcing
Name	ID	Name
Ansprechpartner	Kurzbezeichnung der Dienstleistung	Adresse
Handelsregistereintrag	Kritisch / Wesentlich	ggf. Handelsregistereintrag
Anschrift	Datenklassifizierung (z.B. CID)	ggf. Ansprechpartner
Ort der Dienstleistungserbringung	Datum erstmalige Bewertung	Ort der Dienstleistungserbringung
Ort der Datenspeicherung	Datum letzmalige Bewertung	Ort der Datenspeicherung
ggf. Cloud-Service Modell	ggf. gruppenintern oder - extern	
	Exit-Strategie	
	BCM-Relevanz	
	Status	
	Outsourcing-Verantwortlicher	

Grundsätzlich ist Outsourcing stark **interdisziplinär**. Daher besteht die Möglichkeit weitere Angaben in anderen Datenbanken zu hinterlegen (z.B. in der Revision). Im Sinne eineGrundsätzlich ist Outsourcing stark interdisziplinär. Daher besteht die Möglichkeit weitere Angaben in anderen Datenbanken zu hinterlegen (z.B. in der Revision). Im Sinne eines proaktiven und zeitnahen Risikomanagements sollten jedoch Schnittstellen zur **effizienten und flexiblen Auswertung** vorhanden sein.

Regulatorik

Welcher gesetzliche Rahmen gilt für Banken?

Beim Management von Drittanbietern handelt es sich um eine relativ junge Disziplin, die in den vergangenen Jahren in der Praxis und Regulatorik enorm an Bedeutung gewonnen hat.



Der Fokus regulatorischer Anforderungen hat sich **erweitert** um das Management von Drittanbietern.

Wesentliche Arbeitspakete in der Umsetzung DORA

Kritische IKT-Drittanbieter unterliegen einem von der Europäischen Union festgelegten Aufsichtsrahmen (Art 28 ff)

Das Arbeitspaket IKT-Drittdienstleister soll:

- Die **Outsourcing-Strategie und –Leitlinie** über- bzw. erarbeiten und diese inhaltlich mit der Geschäfts- und IT-Strategie sowie mit der Rahmenrisikopolitik koordinieren
- Entsprechende Prozesse zur regelmässigen Überprüfung und Aktualisierung der Strategie definieren
- Das **Outsourcing-Inventar** um relevante Subdienstleister erweitern und diese in das (Risiko-) Management aufnehmen
- Die Notwendigkeit und den Aufbau eines Registers der IKT-Drittdienstleister evaluieren und notwendige Arbeitspakete ableiten
- Ein Reporting (u.a. zur Risikoexposition im Outsourcing- und Lieferanten-Portfolio) etablieren
- Das **Monitoring der Dienstleister schärfen** (z.B. mittels IKS-Kontrollen, Nachweise über Pentest- und Notfalltest einfordern und evaluieren)

Notwendige Informationen der Auslagerungen sollen in den Verträgen enthalten sein:

Vertragliche Vereinbarungen zwischen Finanzinstituten und Dritten, die IKT-Dienstleistungen oder -Funktionen anbieten, müssen mindestens folgende Elemente enthalten (Art. 27)	– klare Beschreibung der zu erbringenden Funktionen und Dienstleistungen – Erfüllungsort der Funktionen und Dienstleistungen – Zugänglichkeit, Verfügbarkeit, Integrität, Sicherheit und Schutz von personenbezogenen Daten – Dienstleistungsniveau, quantitative und qualitative Leistungsziele – Berichtspflichten und Meldepflichten	– Verpflichtung zur Hilfeleistung im Falle eines IKT-Notfall – Verpflichtung des IKT-Drittanbieters zur Implementierung und Erprobung von Notfallplänen – Recht auf Überwachung des Drittanbieters – Verpflichtung zur Zusammenarbeit mit Behörden – Kündigungsrechte und Mindestkündigungsfristen – Exitstrategien

Frameworks

Wohin geht die Reise?

Risiken und Massnahmen nach dem benötigten Schutzniveau im Vorgehensmodell nach dem BSI (OPS.2.3 Nutzung von Outsourcing)

- Unzureichende Berücksichtigung der Informationssicherheit
- Auslagerung von Prozessen, die aufgrund ihrer Kritikalität oder ihres Schutzbedarfes im Institut verbleiben sollten
- Abhängigkeit zu Third Party → Vendor lock-in
- Unzureichendes Sicherheitsniveau des Dienstleisters
- Mangelhaftes Management des Dienstleisters (z.B. fehlende Instrumente zur Steuerung)
- Unzulängliche vertragliche Regelungen
- Kontroll- und Steuerverlust durch Weiterverlagerung
- Unzureichendes Notfallkonzept

Anforderungsprofil

Hohe Anforderungen

- Abschluss von ESCROW-Verträgen für softwarenahe Dienstleistungen
- Durchführung gemeinsamer Notfall- und Krisenübungen
- Einsatz von Verschlüsslung
- Sicherheits- und Eignungsprüfung von Mitarbeitenden
- Nutzung von Sandboxen für eingehende Daten vom Anbietenden

Standard-Anforderungen

- Erstellung Outsourcing-Vorhaben
- Etablierung Outsourcing Richtlinie
- Zentrales Auslagerungsmanagement
- Führung Auslagerungsregister
- Berichterstattung
- Bereitstellung Kompetenzen für die Vertragsgestaltung

Basis-Anforderungen

- Anforderungsprofile für die Tätigkeit bzw. den Prozess
- Erstellung bzw. Vorliegen Sicherheitskonzept
- Festlegung Eignungsanforderungen für Anbieter
- Festlegung Grundanforderungen für vertragliche Vereinbarungen
- Regelungen für die geplante oder ungeplante Beendigung der Dienstleistung

Weitere Frameworks

Vorgaben für die Steuerung	ISO/IEC 27001:2013 Kapitel A.15.2 "Steuerung der Dienstleistungserbringung von Lieferanten" Spezifizierung in ISO 27002:2021 Kapitel 5.19 bis 5.22 DIN ISO 37500:2015-08 "Leitfaden Outsourcing"
Rechtliche Aspekte	"Leitfaden Rechtliche Aspekte von Outsourcing in der Praxis" des Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. (Bitkom)
Auslagerung von Geschäftsprozessen	"Leitfaden Business Process Outsourcing: BPO als Chance für den Standort Deutschland" des Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. (Bitkom)
Anforderung an Anbieter von Outsourcing	National Institute of Standards and Technology (NIST) in der NIST Special Publication 800- 53 "Leitfaden Business Process Outsourcing: BPO als Chance für den Standort Deutschland" des Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. (Bitkom) Information Security Forum (ISF) Standard "The Standard of Good Practice for Information Security"

Vielen Dank!

Kontakt

Jousry Abdel-Khalek
Leiter Group Business Risk Management /
Group CISO

Telefon +423 236 85 23
jousry.abdel-khalek@llb.li