# TPRM
# und
# DORA, Kap. V

CISO360

SECURE THE PRESENT, ENABLE THE FUTURE

CISO360 GmbH

ciso360.de

# Third-Party Risk Management (TPRM)

## Definition und Bedeutung von TPRM

TPRM bezieht sich auf die systematische Identifikation, Bewertung, Kontrolle und Dokumentation von Risiken, die aus der Zusammenarbeit mit Drittanbietern entstehen. Für Unternehmen, insbesondere im Finanzsektor, ist TPRM von entscheidender Bedeutung, da es die betriebliche Resilienz stärkt und sicherstellt, dass externe Partnerschaften nicht zu Sicherheits- oder Compliance-Verstößen führen. Die Abhängigkeit von Drittanbietern erhöht das Risiko von Cyberangriffen, operationellen Störungen und Verstößen gegen regulatorische Vorgaben.

TPRM ist für Unternehmen wichtig, weil es hilft, Risiken durch Drittparteien wie Lieferanten oder Dienstleister zu identifizieren und zu managen. Dadurch können Unternehmen potenzielle Sicherheitslücken, Compliance-Verstöße und finanzielle Verluste vermeiden. Ein effektives TPRM stärkt die Resilienz und schützt die Reputation des Unternehmens.

## Risiken in der Zusammenarbeit mit Drittanbietern

Die Zusammenarbeit mit Drittanbietern birgt eine Vielzahl von Risiken. Zu den häufigsten gehören Cyberrisiken, wie Datenlecks oder Hackerangriffe, die durch Sicherheitslücken bei Dienstleistern verursacht werden können. Operationelle Risiken entstehen, wenn Drittanbieter aufgrund von Ausfällen oder Fehlfunktionen ihrer Systeme die Geschäftsabläufe eines Unternehmens negativ beeinflussen. Darüber hinaus besteht ein erhebliches regulatorisches Risiko, wenn Drittanbieter die strengen Anforderungen von Gesetzen und Verordnungen wie DORA nicht einhalten, was zu Sanktionen oder Reputationsverlusten führen kann.

-

**D**igital
**O**perational
**R**esilience
**A**ct

BaFin
Bundesanstalt für Finanzdienstleistungsaufsicht

## TPRM in DORA

Mit der Einführung der neuen Verordnung „Digital Operational Resilience Act“ (DORA), die ab dem 17. Januar 2025 in Kraft tritt, stehen Finanzdienstleister in der Europäischen Union vor der Herausforderung, die Verwaltung ihrer IKT umfassend zu managen.

Ein Teil der neuen Verordnung DORA betrifft das "Management des IKT-Drittparteienrisikos", auch bekannt als Third-Party Risk Management (TPRM).

So sind im weltweit etablierten Standard ISO/IEC 27001:2022 bereits folgende Anforderungen enthalten

- Information security in supplier relationships (A.5.19)
- Addressing information security within supplier agreements (A.5.20)
- Managing information security in the supply chain (A.5.21)
- Monitoring, review and change management of supplier services (A.5.21)
- Information security for use of cloud services (A.5.22)

Neu hingegen sind das Erarbeiten und Testen dedizierter Exitstrategien für kritische IKT-Dienstleister, sowie das Identifizieren von "Konzentrationsrisiken".

In Bild 1 befindet sich ein grober Überblick über die einzelnen Schritte, die zur Umsetzung von DORA erforderlich sind, die jeweiligen Referenzen zum Verordnungstext, der ISO/IEC 27001:2022 und den jeweiligen Challenges.

| DORA-Steps | Organisation | Registrierung und Klassifizierung | Risikobewertung | Vertragsanpassungen | Exit Strategien | Konzentrations–Risiken |
|---|---|---|---|---|---|---|
| Output | Strategie und Leitlinie | Information Register | Fragebögen, Riskoregister | Neue / aktualisierte Verträge | Business Continuity Pläne | Liste kritischer Dienstleister |
| Referenz | Art. 28 (2) | Art. 28 (4) | Art. 28 (4) c) | Art. 28 (5) und Art. 30 | Art. 28 (8) | Art. 29 |
| Komplexität | Niedrig - Mittel | Mittel | Hoch | Hoch | Mittel | Niedrig |
| Challenge | Einpassung in bestehende Vorgaben | Durchforsten der Lieferanten–landschaft | Handling einer Vielzahl von Fragen und Anworten | Kommerzielle Auswirkungen / Verhandlungen | Aufbau BCM | Setzen der Schwellwerte |
| ISO/IEC 27001:2022 | A.5.19 | - | A.5.21, A.5.22, A5.23 | A.5.20 | | |

*Bild 1: DORA Steps zum IKT-Drittparteienrisikomanagement*

# Strategien zur Implementierung von TPRM im Einklang mit DORA

## Identifikation/Gap-Analyse

Die Durchführung einer Gap-Analyse ist ein wesentlicher erster Schritt, um sicherzustellen, dass bestehende Third-Party Risk Management (TPRM)-Prozesse den Anforderungen der DORA-Verordnung entsprechen. Diese Analyse identifiziert Diskrepanzen zwischen den aktuellen Praktiken und den neuen regulatorischen Vorgaben. Dabei werden alle relevanten Prozesse, Richtlinien und Kontrollen auf ihre Konformität mit DORA überprüft, um festzustellen, welche Bereiche angepasst oder verbessert werden müssen. Die Ergebnisse dieser Analyse bilden die Grundlage für die anschließende Implementierung von Maßnahmen zur Schließung der identifizierten Lücken.

## Risikobewertung und Due Diligence

Eine gründliche Risikobewertung und Due Diligence sind entscheidend, um sicherzustellen, dass Drittanbieter den DORA-Anforderungen gerecht werden. Dies beinhaltet eine umfassende Bewertung der potenziellen Risiken, die mit jedem Drittanbieter verbunden sind, wie etwa Cyberrisiken, operationelle Risiken und regulatorische Risiken. Im Rahmen dieser Bewertung sollten Unternehmen standardisierte Kriterien und Checklisten verwenden, um die Risiken systematisch zu erfassen und zu bewerten. Eine sorgfältige Due Diligence hilft dabei, nur solche Drittanbieter auszuwählen, die die notwendigen Sicherheits- und Resilienzanforderungen erfüllen.

## Überwachung und Kontrolle

Nach der Risikobewertung ist es unerlässlich, robuste Überwachungs- und Kontrollmechanismen zu implementieren, um die fortlaufende Einhaltung der DORA-Vorgaben sicherzustellen. Diese Mechanismen sollten regelmäßige Audits, kontinuierliche Risikobewertungen und Echtzeit-Überwachung von Drittanbietern umfassen. Durch den Einsatz von Technologien wie Automatisierung und Echtzeit-Datenanalyse können Unternehmen potenzielle Risiken schneller identifizieren und entsprechende Maßnahmen ergreifen, bevor diese zu erheblichen Problemen führen.

## Automatisierung durch TPRM-Tools

Um die notwenigen Fristen einzuhalten und den Aufwand in einem vertretbaren (Kosten)rahmen zu halten, ist eine Automatisierung unerlässlich! Hier bieten sich TPRM-Tools an, die durch die Zusammenarbeit mit externen Dienstleistern und Partnern entstehen. Dies geschieht beispielsweise durch standardisierte Fragebögen mit vorgegebenen Antworten, die ein schnelles Ausfüllen und automatisiertes Auswerten erlauben.

## Vertragsanalyse per KI

Um alle bestehenden Verträge auf Dora Compliance zu prüfen zu lassen, ist ab einer bestimmten Menge der Einsatz von KI unerlässlich. Hierzu ist es notwendig den richtigen Kontext und das richtige Trainingsset zu wählen, um zu guten Ergebnissen zu kommen. Zum Beispiel gibt es in DORA detaillierte Vorgaben, wie die Auditklauseln geregelt sollen, siehe Art. 30 e) i). Nur dieses eine Merkmal manuell herauszufinden bei 1000+ Verträgen und 100.000+ Seiten Text gleicht einer Sisyphos Arbeit.

## Fazit

Third Party Risk Management ist seit je her ein essenzieller Bestandteil einer Cyber Security Architektur und in den gängigen Standards beschrieben. Mit dem Digital Operational Resilience Act (DORA) kommt jedoch eine neue Breite und Tiefe an regulatorischen Anforderungen auf die betroffenen Unternehmen zu. So werden in der Praxis beispielsweise hunderte von Lieferanten mit umfangreichen Fragebögen kontaktiert, die dann manuell ausgewertet werden müssen. Hier versprechen TPRM-Tools durch ihren integrierten Ansatz einen hohen Effizienzgewinn, während KI-Tools in der Vertragsanalyse erste Wahl sind.

## Links


[BaFin - DORA]: https://www.bafin.de/DE/Aufsicht/DORA/DORA_node.html

[LinkedIn Beitrag Daniel Hallen]: https://www.linkedin.com/posts/daniel-hallen-a5a71336_dora-tprm-activity-7238905296566251520-QP_O?utm_source=share&utm_medium=member_desktop

[Prevalent]: https://www.onetrust.com/solutions/third-party-management/

[Process Unity]: https://www.processunity.com/third-party-risk-management/

[SecurityScorecard]: https://securityscorecard.com/blog/complete-third-party-risk-management-guide/

Jeroen Erné, (2023). *The Artificial intelligence handbook for contract administrators*


CISO360

**SECURE THE PRESENT, ENABLE THE FUTURE**


**Autoren**:

Daniel Hallen

Maximilian Modes

**Kontakt**:

dhallen@ciso360.de