DORA im Jahr vor dem Inkrafttreten

Inhalte, Herausforderungen, Strategien

IT-GRC Kongress 2024, Hamburg

04.06.2024

ISACA Germany Chapter

Fachvortrag aus der Fachgruppe IT-Compliance im Finanz- und Versicherungswesen

Dr. Christian Schwartz

Head of Security in Finance

usd AG

Dr. Frank Innerhofer

Geschäftsführer

Innerhofer Risk Management GmbH

Die von Digital Operational Resilience Act (DORA) betroffenen Unternehmen müssen die neuen Anforderungen bis zum Januar 2025 umgesetzt haben.

Ausgangssituation

- Die DORA ist seit Januar 2023 in Kraft und Entwürfe / finalisierte Versionen der RTS / ITS sind inzwischen veröffentlicht.
- Die DORA wird ab Januar 2025 angewendet.
- Die (meisten) betroffenen Unternehmen haben Umsetzungsprojekte gestartet.

Herausforderung

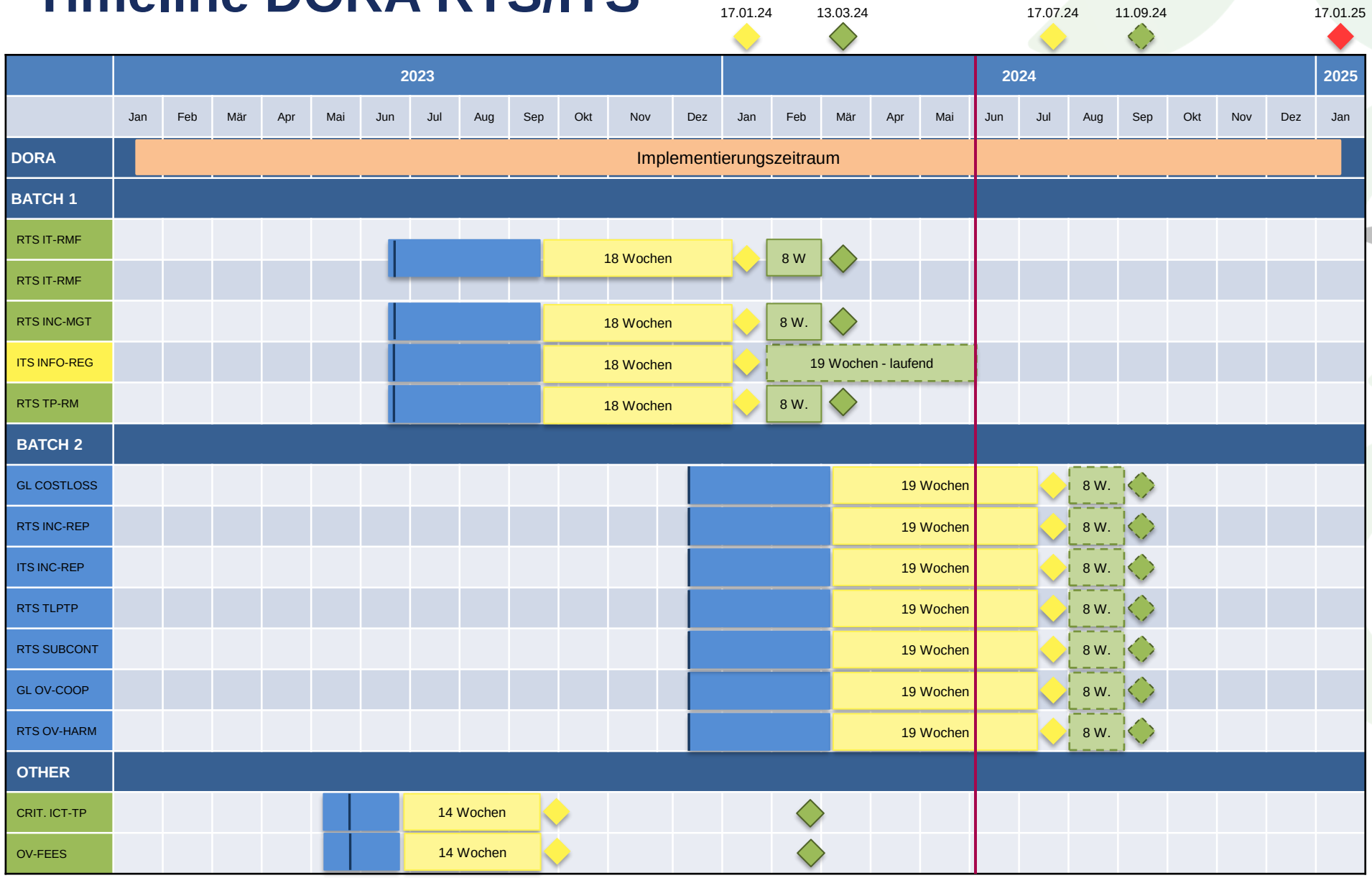
- Trotzdem sind die finalen Versionen aller Anforderungen noch immer nicht vollständig bekannt.
- Die verbleibende Zeit für die Umsetzung der Anforderungen ist knapp.
- Die Umsetzung ist fachlich komplex und enthält viele Abhängigkeiten.

Ziel des Vortrags

- Die aktuellen Weiterentwicklungen der DORA-Anforderungen sollen bekannt sein.
- Für die Umsetzung verfügbare Kapazitäten sollen priorisiert eingesetzt werden können.
- Mögliche Stolpersteine bei der Umsetzung sollen vermieden werden können.

ISACA Germany Chapter

Timeline DORA RTS/ITS



- Consultation Paper
- Final Draft
- Delegierte Verordnungen

ISACA Germany Chapter

Überblick wesentlicher Änderungen aus RTS/ITS Batch 1

	RTS IKT-Risikomanagementrahmen	RTS Leitlinie Nutzung von IKT-Dienstleistungen von kritischen oder wichtigen Funktionen	RTS Kriterien zur Klassifizierung IKT-bezogener Vorfälle
Wesentliche Änderungen nach Konsultation	**Verhältnismäßigkeit:** […] Größe und Gesamtrisikoprofil des Finanzunternehmens sowie die Art und der Umfang seiner Dienstleistungen, Tätigkeiten und Geschäfte und die Elemente berücksichtigt, die deren Komplexität erhöhen oder verringern […]		
	Artikel weggefallen: "Provisions on Governance" und "ICT and information security awareness and training" wurden gestrichen	**Due Diligence:** Erweiterung der zu berücksichtigenden Elemente und Anforderung nach Möglichkeit mehr als eines anzuwenden	**Änderung des Klassifizierungsansatzes:** Einstufung als erhebliche Vorfälle
	Technologiespezifische Anforderungen: Technologie-spezifische Anforderungen zu Cloud Computing gestrichen	**Vertragsklauseln:** Präzisierungen im Hinblick auf Audits und Zertifizierungen	**Klassifizierungskriterien:** Anpassung der Schwellenwerte
	Streichungen: Anforderungen zu mindestens jährlichem Review und Aktualisierung von Dokumenten	**Exit:** Anforderung zu dokumentiertem Ausstiegsplan, Berückschtigung bei Tests	**Klassifizierung wiederholter Vorfälle:** Eintritt zweimal in 6 Monaten und die Kriterien kumulativ erfüllen sowie offensichtlich dieselbe Ursache haben
Keine wesentlichen Änderungen nach finalen Entwüfen	Redaktionelle Änderungen, bessere Strukturierung.		
	Ausgliederung von Erläuterungen zu einzelnen Unterpunkten.		
			Änderungen in der Struktur durch Zusammenfassung von Artikeln.

ISACA Germany Chapter

Elemente, die bestimmt und bewertet werden müssen, wenn für IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, Subunternehmer eingesetzt werden.

Der RTS enthält konkretisierte Anforderungen

- zu der Risikobewertung von Subdienstleistern,
- zu den Kriterien, nach denen eine Unterauftragsvergabe für kritische oder wichtige Funktionen (kwF) zulässig ist,
- wie Subdienstleister überwacht werden müssen,
- wie mit wesentlichen Änderungen an der Unterauftragsvergabe umgegangen werden muss und
- wann Finanzunternehmen das Recht haben Verträge mit IKT-Dienstleistern auf Grund von Unterauftragsvergaben beendigen zu dürfen.

In der Risikobewertung für Subdienstleister muss *unter anderem* bewertet werden

- ob der IKT-Dienstleister Subdienstleister so auswählen und bewerten kann, dass diese den Anforderungen des Finanzunternehmens (insb. auch bezüglich Tests und Reporting von Vorfällen) genügen
- was der Einfluss von Ausfällen von Subdienstleistern auf kritische oder wichtige Dienste des Finanzunternehmens ist und
- ob ein IKT-Konzentrationsrisiko besteht.

Wenn eine IKT-Dienstleistung eine kwF unterstützt, muss das Finanzunternehmen die vollständige Subdienstleistungskette überwachen.

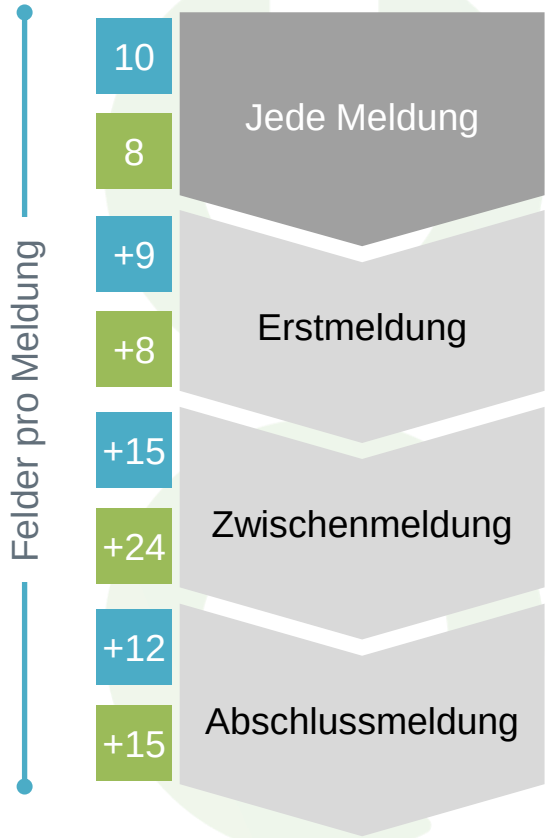
ISACA Germany Chapter

Inhalt und zeitliche Grenzen für die Meldung von schwerwiegenden IKT-bezogenen Vorfällen und erheblichen Cyberbedrohungen.

Der RTS enthält Anforderungen an die einzuhaltenden Fristen und notwendigen Inhalte zur Meldung von schwerwiegenden IKT-bezogenen Vorfällen, insbesondere der

1. Erstmeldung,
2. Zwischenmeldung und
3. Abschlussmeldung.

Der RTS enthält außerdem Anforderungen an die Inhalte für eine (freiwillige) Meldung von erheblichen Cyber-bedrohungen.



ISACA Germany Chapter

Inhalt und zeitliche Grenzen für die Meldung von schwerwiegenden IKT-bezogenen Vorfällen und erheblichen Cyberbedrohungen.

Der R
Friste
schwe
insbes

1

2

3

Der R
für ein
bedro

3.40 – Indicators of Compromise *(Zwischen- und Abschlussbericht)*

The IoC provided by the financial entity may include, but not be limited to, the following categories of data:

- IP addresses;
- URL addresses;
- Domains;
- File hashes;
- Malware data (malware name, file names and their locations, specific registry keys associated with malware activity);
- Network activity data (ports, protocols, addresses, referrers, user agents, headers, specific logs or distinctive patterns in network traffic);
- E-mail message data (sender, recipient, subject, header, content);
- DNS requests and registry configurations;
- User account activities (logins, privileged user account activity, privilege escalation);
- Database traffic (read/write), requests to the same file.

In practice, this type of information may include data relating to, for example, indicators describing patterns in network traffic corresponding to known attacks/botnet communications, IP addresses of machines infected with malware (bots), data relating to “command and control” servers used by malware (usually domains or IP addresses), URLs relating to phishing sites or websites observed hosting malware or exploit kits, etc.

Data field is mandatory for the intermediate and final report if cybersecurity is selected as a type of incident in data field 3.26.

Verpflichtende Felder Bedingte Felder

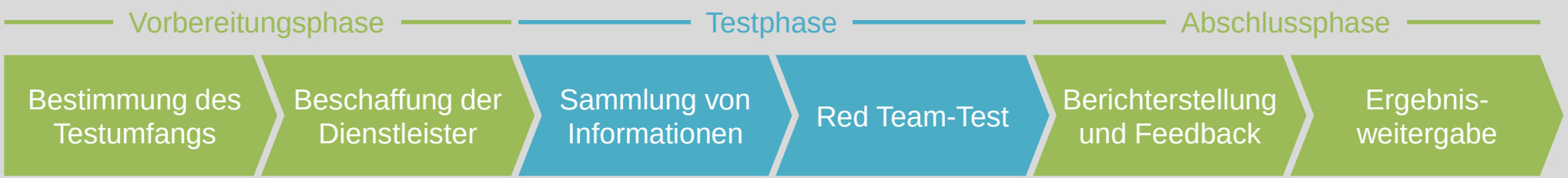
ISACA Germany Chapter

Elemente im Zusammenhang mit bedrohungsorientierten Penetrationstests.

Der RTS spezifiziert die Anforderungen an Finanzinstitute zur Durchführung von bedrohungsorientierten Penetrationstests (Threat Led Penetration Tests – TLPT) in Bezug auf

- Kriterien, für die Verpflichtung zu TLPT
- das Vorgehensmodell für TLPT und
- die Nutzung von internen Testern.

Das TLPT-Vorgehensmodell orientiert sich an **TIBER-EU**, macht aber einige optionale Punkte (z.B. Purple Teaming) verpflichtend.



ISACA Germany Chapter

Mögliche Ansätze für Priorisierungen

Klassische Ansätze:

- Wo sind technische Implementierungen nötig?
- Wo sind aufwändige Vertragsanpassungen und -verhandlungen nötig?
- Welche Maßnahmen haben eine hohe Komplexität und viele Schnittstellen?
- Wo benötigt man eigene Daten und oder Daten-Zulieferungen von IKT-Dienstleistern zur Erfüllung der Anforderungen?

Weitere Ansätze:

- Wo bestehen Berichtspflichten an die Aufsichtsbehörden?
- Wo bestehen Genehmigungs- und Berichtspflichten an das Leitungsorgan?

ISACA Germany Chapter

Berichts- und Meldepflichten an die Aufsichtsbehörden

Kritisch	Zeitlich nachgelagerte Berichte	Obligatorisch	Anfrage	Freiwillig
Meldung von IKT-bezogenen Vorfällen (Erst-, Zwischen- und Abschlussmeldung)		✓		
Bericht über die vertraglichen Regelungen der IKT-Dienste		✓		
Geplante IKT-Dienste, die kwF unterstützen, und Änderungen Kritikalität/Wichtigkeit von Funktionen		✓		
	TLPT-Feststellungen, Abhilfemaßnahmen und Dokumentation	✓		
	Benachrichtigung über erhaltene TLPT-Bescheinigung	✓		
	Benachrichtigung über die (freiwillige) Teilnahme am Informationsaustausch	✓		
Informationsregister		✓	✓	
	Änderungen nach Prüfung IKT-bezogener Vorfälle		✓	
	Bericht über Kosten und Verluste		✓	
	Informationen über IKT-Risiken und den IKT-Risikomanagementrahmen		✓	
	Überprüfungsbericht des IKT-Risikomanagementrahmens		✓	
	Meldung einer erheblichen Cyber-Bedrohung			✓

ISACA Germany Chapter

Berichts- und Genehmigungspflichten Leitungsorgan

Kritisch	Zeitlich nachgelagert	Genehmigung	Berichte
Strategie für die digitale operationale Resilienz		✓	✓
Festlegung angemessene Toleranzschwelle für IKT-Risiko		✓	✓
IKT-Geschäftsfortführungsleitlinie		✓	✓
IKT-Reaktions- und Wiederherstellungspläne		✓	✓
IKT-Revisionspläne		✓	✓
Leitlinie Vereinbarungen über Nutzung von IKT-Dienstleistungen für kwF		✓	✓
Informationssicherheitsleitline		✓	✓
	Dokumentation des Umfangs des TLPT	✓	✓
	Bericht über die Überprüfung des IKT-Risikomanagementrahmens	✓	✓
Vorkehrungen IKT-Risikomanagementrahmen			✓
Risiken aus vertraglichen Vereinbarungen über Nutzung von IKT-Dienstleistungen für kwF			✓
Einleitung, Fortschritt und Risiken von IKT-Projekten mit Auswirkungen auf kwF			✓
	Bericht über Fortschritt des TLPT und der Risiken		✓

ISACA Germany Chapter

Die Umsetzung eines komplexen Projektes – wie der DORA-Harmonisierung – ist mit Stolpersteinen versehen. Diese zu erkennen erhöht die Wahrscheinlichkeit des Projekterfolges.

Die DORA-Anforderungen sind nicht vollständig bekannt.

Die für DORA relevanten Grundgesamtheiten sind nicht identifiziert.

Das Streben nach Perfektion behindert das finden einer guten Lösung.

Es gibt keinen Plan für die Zeit nach dem 17. Januar 2025.

ISACA Germany Chapter

Verantwortliche, die noch nicht die relevanten Teile der Verordnung gelesen haben, können diese auch nicht effektiv umsetzen.

Worum geht es?

Einzelne Projektmitarbeiter:innen lesen die für sie relevanten Dokumente (die DORA selbst, bzw. die abgeleiteten RTS / ITS) nicht, sondern verlassen sich bei der Umsetzung auf Synopsen oder *Konferenzvorträge*.

Warum ist es ein Projektrisiko?

Zusammenfassungen lassen immer Informationen aus und beinhalten – ggf. unbeabsichtigte – Interpretationen die den Leser:innen nicht bewusst sein können, wenn sie die Originaltexte nicht kennen.

Was können wir dagegen tun?

- Erwartungshaltung klar kommunizieren und Umsetzung einfordern,
- eine Einführung (z.B. pro Teilprojekt) in relevante Dokumente geben und
- Plattformen zum Wissensaustausch schaffen.

Bonus Stolperstein

Auf veralteten Versionen arbeiten

Veraltete Versionen enthalten teils signifikant andere Anforderungen als die finale Version, finden sich aber noch

- auf Projektlaufwerken,
- in Ergebnisdokumenten (z.B. von Gap-Analysen) oder
- Mapping-Tabellen.

ISACA Germany Chapter

Wenn die relevante Grundgesamtheit der DORA-Umsetzung nicht bekannt ist, kann auch keine vollständige Umsetzung erfolgen.

Worum geht es?

DORA-Anforderungen betreffen bestimmte Gruppen von Objekten (z.B. IKT-Systeme die kritische oder wichtige Funktionen unterstützen, IKT-Dienstleister, usw.), die genaue Grundgesamtheit ist aber nicht bekannt.

Warum ist es ein Projektrisiko?

Im Rahmen der Operationalisierung der DORA-Anforderungen müssen die geschaffenen Vorgaben auf der Grundgesamtheit umgesetzt werden. Wenn diese nicht bekannt ist, kann dies auch nicht geplant und durchgeführt werden.

Was können wir dagegen tun?

- Frühzeitig leicht überprüfbare Definitionen schaffen,
- Verantwortlichkeiten und Zeitplan für die Identifikation festlegen und
- Zeit für Qualitätssicherung und Plausibilitätsprüfung einplanen.

Bonus Stolperstein

Unbekannte oder nicht aufgelöste Abhängigkeiten

Die DORA-Anforderungen enthalten zahlreiche (fachliche und planerische) Abhängigkeiten. Wenn diese nicht beachtet werden, ist die Umsetzung

- ineffizient,
- fehlerhaft oder
- unvollständig.

ISACA Germany Chapter

Das Streben nach (langfristig) perfekten Lösungen behindert das (mittelfristige) Umsetzen der DORA-Anforderungen.

Worum geht es?

Viele Anforderungen der DORA erfordern in der Umsetzung komplexe Prozesse die teils toolgestützt implementiert werden müssen. Der Zeitraum für die Implementierung bis zum 17. Januar ist hierfür aber nicht ausreichend.

Warum ist es ein Projektrisiko?

Durch die fehlende Umsetzung ergeben sich sowohl Compliance- als auch Informationssicherheitsrisiken für das Finanzunternehmen.

Was können wir dagegen tun?

- Realistisch prüfen, welche Maßnahmen fristgerecht umgesetzt werden können,
- klar kommunizieren, welche Compliance- und Informationssicherheitsrisiken entstehen können und
- sicherstellen, dass für alle nicht fristgerecht umgesetzten Maßnahmen Übergangslösungen zur Verfügung stehen.

Bonus Stolperstein

Fokus auf Einzelanforderungen verhindert die Umsetzung eines einheitlichen Zielbilds.

Wenn bei der Umsetzung der Fokus nur im Detail liegt, führt das zu

- ungenutzten Effizienzen,
- dem Verpassen von Weiter-entwicklungsmöglichkeiten und
- geringerer Risikoreduktion.

ISACA Germany Chapter

Es liegt kein Plan für die Abarbeitung von bis zum 17.01.2025 noch nicht umgesetzten Anforderungen bzw. die Operationalisierung von Vorgaben vor.

Worum geht es?

Insbesondere die Operationalisierung der DORA-Anforderungen (z.B. im IKT-Drittparteienrisikomanagement) wird bei vielen Instituten nicht im Januar 2025 abgeschlossen sein, das weitere Vorgehen muss aber geregelt werden.

Warum ist es ein Projektrisiko?

Durch die fehlende Operationalisierung ergeben sich sowohl Compliance- als auch Informationssicherheitsrisiken für das Finanzunternehmen.

Was können wir dagegen tun?

- Auf Basis der identifizierten Grundgesamtheit einen priorisierten Plan zur Operationalisierung erstellen,
- für erwartete Lücken bis zum 17. Januar 2025 Risiken transparent machen und dokumentieren und
- Erfahrungen aus der Operationalisierung nutzen, um die etablierten Prozesse anzupassen.

Bonus Stolperstein

Erzwungen erhöhte Umsetzungsgeschwindigkeit reduziert die Qualität der Umsetzung.

Umsetzungsschwächen aufgrund von erhöhtem Druck können mehr Risiken bergen als eine transparent kommunizierte leichte Verzögerung.

ISACA Germany Chapter

Was für Stolpersteine haben Sie in Ihren DORA-Umsetzungs-projekten wahrgenommen?

Die DORA-Anforderungen sind nicht vollständig bekannt.

Die für DORA relevanten Grundgesamtheiten sind nicht identifiziert.

Das Streben nach Perfektion behindert das finden einer guten Lösung.

Es gibt keinen Plan für die Zeit nach dem 17. Januar 2025.

ISACA Germany Chapter

Die Fachgruppe IT-Compliance FVW führt eine Studie zu Erfolgs- und Misserfolgsfaktoren bei regulatorischen IT-Projekten durch.

Über die Studie

Die Fachgruppe IT-Compliance im Finanz- und Versicherungswesen führt eine wissenschaftliche Studie zur Wahrnehmung von Erfolgs- und Misserfolgsfaktoren bei regulatorischen IT-Projekten durch.

- Die Umfrage dauert etwa 20 Minuten, und Ihre Daten werden streng vertraulich und anonym behandelt.
- Wenn Sie 1 CPE für Ihre ISACA-Zertifizierung(en) beantragen möchten, machen Sie bitte einen Screenshot des Dankeschön-Bildschirms als Nachweis für die Teilnahme an der Umfrage.

Zur Umfrage

ISACA Germany Chapter