CASE STUDY · FINANZDIENSTLEISTUNGEN

Was tragen soll, wächst von unten

Wie ein Finanzunternehmen sein IKT-Risikomanagement auf die Anforderungen der DORA umstellt, nachdem eine Konzernprüfung die Lücken benannt hat.

„Ein Keimling bildet zuerst die Wurzel. Erst wenn sie hält, geht er in die Höhe."

ZUM GELEIT

Das Prinzip der tragenden Wurzel

Ein Keimling wächst nicht zuerst in die Höhe. Er treibt eine Wurzel, lange bevor oben etwas zu sehen ist. Das kostet Zeit, in der nichts passiert, was von außen beeindruckt. Es ist trotzdem die einzige Reihenfolge, in der später etwas stehen bleibt.

Regulatorische Rahmenwerke lassen sich in derselben Ordnung am besten erfüllen. Vorgeschrieben ist sie nicht, die DORA nennt ihre Anforderungen ohne Rangfolge. Bewährt hat sich trotzdem, mit der Kenntnis der eigenen Informations- und IKT-Assets zu beginnen: was gehört dazu, wovon hängt es ab, wie kritisch ist es. Diese Case Study zeigt, wie ein Finanzunternehmen diese Wurzel nachträglich angelegt hat, unter Zeitdruck und mit Feststellungen bereits im Haus.

INHALT

01 · ÜBER DEN KUNDEN

Ein Haus, auf das sich andere Häuser verlassen

Unser Kunde ist ein Finanzunternehmen mit einigen hundert Mitarbeitenden. Er ist Teil eines größeren Verbunds und erbringt zugleich IKT-Leistungen für Banken und Finanzinstitute, die dort kritische oder wichtige Funktionen stützen. Diese Doppelrolle bestimmt alles, was in dieser Case Study folgt.

Denn sie führt zu einer doppelten Betroffenheit. Als Finanzunternehmen fällt der Kunde unmittelbar unter die DORA, die seit dem 17. Januar 2025 gilt. Als IKT-Dienstleister wird er zusätzlich an den Anforderungen gemessen, die seine Kunden ihrerseits vertraglich weitergeben müssen.

DORA | IKT-Risikomanagement | Konzernverbund | Hochreguliert

KUNDENPROFIL

BRANCHE	Finanzdienstleistungen
GRÖSSE	Einige hundert Mitarbeitende
ROLLE	Finanzunternehmen + IKT-Dienstleister für Institute
RAHMEN	DORA, Verordnung (EU) 2022/2554

BRANCHEN-KONTEXT

Ein IKT-Dienstleister im Finanzsektor verkauft mit jeder Leistung auch seine Prüfbarkeit. Was er nicht nachweisen kann, kann sein Kunde in seiner eigenen Aufsichtsbeziehung nicht verantworten. Wer Institute beliefert, wird deshalb zweimal an derselben Verordnung gemessen: einmal für sich selbst und einmal durch die Augen der Häuser, die ihn beauftragen.

02 · DER KONTEXT

Eine Ordnung, die nach altem Maß gebaut war

Der Kunde stand nicht bei null. Seine Sicherheitslandschaft war nominell strukturiert und weitgehend an den bankaufsichtlichen IT-Anforderungen ausgerichtet, die für ihn bis dahin maßgeblich waren. Es gab Richtlinien, es gab Verantwortlichkeiten, es gab ein ISMS. Auf dem Papier sah das ordentlich aus.

Was fehlte, war die Umstellung auf das neue Maß. Die DORA ordnet den Stoff anders: IKT-Risikomanagement, Vorfallmeldung, Resilienztests und das Management des IKT-Drittparteienrisikos, dazu der Informationsaustausch nach Artikel 45, der freiwillig bleibt. Die BaFin unterscheidet dabei sechs wesentliche Regelungsbereiche, weil sie den Überwachungsrahmen für kritische IKT-Drittdienstleister gesondert führt. Die Umstrukturierung auf diese Systematik wurde versäumt. Sichtbar wurde das nicht durch einen Vorfall, sondern durch eine Konzernprüfung, die Feststellungen hinterließ.

01

Vorhanden

Strukturen, Richtlinien und ein ISMS waren nominell aufgestellt.

02

Verschoben

Die Umstrukturierung auf die DORA-Systematik hatte nicht begonnen.

03

Benannt

Eine Konzernprüfung hatte die Abweichungen bereits dokumentiert.

■ vorhanden · verschoben · benannt ■

WARUM DAS KEIN VERSÄUMNIS DER SUBSTANZ WAR

Ein Rahmenwerk, das für ein anderes Regelwerk gebaut wurde, ist nicht falsch. Es ist nur nicht mehr das, was verlangt wird.

03 · DER SCHMERZPUNKT

Gewachsene Strukturen in einem engen Zeitfenster

Am Verständnis lag es nicht. Der CISO wusste sehr genau, was die Verordnung verlangt. Das Problem saß eine Ebene tiefer: Die Organisation hatte zu spät begonnen, und die vorhandenen Strukturen ließen sich nicht ergänzen, sie mussten **aufgebrochen** werden. Abweichungen zwischen den veralteten und den neuen Anforderungen mussten erst einmal präzise benannt werden, bevor irgendetwas behoben werden konnte.

Manches ließ sich nicht anpassen, weil es noch gar nicht existierte. Die DORA verlangt Prozesse, Zuständigkeiten und Strukturen, die in dieser Tiefe neu zu definieren waren. Dazu kam die Alltagsrealität eines Hauses dieser Größe: verschiedene Abteilungen, sehr unterschiedlicher Kenntnisstand zur Verordnung, ein knappes Zeitfenster und ein weiterer beteiligter Dienstleister, der zeitweise nicht verfügbar war.

DAS KERNRISIKO

Für ein Haus, das Institute beliefert, geht es bei dieser Frage nicht um ein Projekt, sondern um die eigene Eignung als Dienstleister. Wer sie verliert, verliert die Geschäftsgrundlage. Sanktionen kommen dann noch dazu.

BRANCHEN-INSIGHT · ANWENDUNG + SANKTION

600+

schwerwiegende IKT-Vorfälle meldeten die beaufsichtigten Institute im ersten DORA-Jahr 2025 an die BaFin. Die Verordnung ist im Alltag angekommen.

Art. 50

Die DORA gibt Mindestbefugnisse und Abhilfemaßnahmen selbst vor und verlangt Sanktionen, die wirksam, verhältnismäßig und abschreckend sind. Die Ausgestaltung liegt bei den Mitgliedstaaten.

04 · DIE ZIELSETZUNG

Ein Rahmenwerk, das eine Prüfung trägt

Das Ziel war nicht, ein Zertifikat zu erreichen, sondern einen Zustand, in dem jede Anforderung der Verordnung einer benannten Struktur zugeordnet ist. Vier Leitziele gaben die Richtung vor.

01
Vermessen
Reifegrad und bestehende Strukturen vollständig aufnehmen, Lücken zur Verordnung präzise benennen.

02
Verankert
Das IKT-Risikomanagement auf vollständige Asset- und Abhängigkeitsinventare gründen, nicht auf eine Annahme.

03
Geregelt
Maßnahmenkatalog, Richtlinien und Meldewesen auf die neue Systematik bringen.

04
Nachweisbar
Kontrollen, Kennzahlen und ein dokumentierter IKT-Risikomanagementrahmen, der einer Prüfung standhält.

AUS ZIELEN WIRD EIN WEG

01 Vermessen → 02 Verankert → 03 Geregelt → 04 Nachweisbar

05 · UNSER ANSATZ

Erst vermessen, dann bauen

Wir haben nicht mit der Lösung angefangen, sondern mit der Vermessung. Bestehende Strukturen und Prozesse wurden detailliert analysiert, der Reifegrad erhoben und jede Abweichung zur Verordnung einzeln festgehalten. Das geschah sukzessiv und gemeinsam mit weiteren Dienstleistern, die bereits im Haus tätig waren.

◆ Methodik · Gap-Analyse + Rahmenwerk

WARUM DIESE REIHENFOLGE

Diese Reihenfolge ist unbequem, weil sie am Anfang nichts vorzeigt. Nach unserer Erfahrung ist sie trotzdem die sinnvollste. Ohne vollständige **Asset- und Abhängigkeitstransparenz** lassen sich Kritikalität und IKT-Risiken nicht belastbar bewerten.

VON DER BESTANDSAUFNAHME ZUM BELASTBAREN RAHMENWERK

A
Ist-Aufnahme

B
Gap-Analyse

C
Kritikalität

→

ERGEBNIS
Ein Rahmenwerk, das trägt

UNSER PRINZIP

Konformität ist kein Dokument, sondern ein Zustand, den ein Dokument beschreibt. Wir bauen erst den Zustand.

06 · DIE UMSETZUNG

In vier Meilensteinen zum IKT-Risikomanagementrahmen

01 **Ist-Aufnahme + Gap-Analyse** — belastbares Lagebild

Die bestehenden Sicherheitsstrukturen und der Reifegrad wurden detailliert analysiert, Lücken und Abweichungen zu den Anforderungen der Verordnung präzise identifiziert, sukzessiv und gemeinsam mit weiteren Dienstleistern.

02 **IKT-Risikomanagement neu ausgerichtet** — auf vollständigen Inventaren

Erweiterung des Scopes, Vervollständigung der Asset- und Abhängigkeitsinventare sowie Klassifizierung und Kritikalitätsbewertung der Informations- und IKT-Assets.

03 **Regelwerk + Meldewesen aktualisiert** — eine Sprache in allen Dokumenten

Inhaltliche Überarbeitung des Bedrohungs- und Sollmaßnahmenkatalogs sowie der übergeordneten ISMS-Richtlinien. Parallel wurden das operative Meldewesen an die Behörden und die internen ISM-Reporting-Strukturen angepasst.

04 **Kontrollframework + Dokumentation** — prüfbar gemacht

Ein neues Prüf- und Kontrollframework mit IS-Kennzahlen und Messprozessen wurde implementiert. Den Abschluss bildete die Dokumentation, Genehmigung und Inkraftsetzung des IKT-Risikomanagementrahmens.

HÜRDE + LÖSUNG

Der unterschiedliche Kenntnisstand der beteiligten Abteilungen war die größere Bremse als die Fachfrage. Ein gemeinsames Briefing und eine Kurzschulung haben alle auf denselben Stand gebracht. Wo Termindruck und Abwesenheiten die Abstimmung erschwerten, halfen die enge Taktung mit dem CISO und die Regel, jede Entscheidung sofort zu dokumentieren.

07 · DIE LÖSUNG

Ein Rahmenwerk, das seine Assets und Abhängigkeiten kennt

Am Ende steht kein Ordner, sondern ein Zusammenhang. Die Asset- und Abhängigkeitsinventare sind vollständig, jedes Informations- und IKT-Asset ist **klassifiziert und in seiner Kritikalität bewertet**. Darauf setzen Risikoanalyse und Risikoinventar auf, und beide werden fortlaufend nachgeführt. Eine Erhebung einmal im Jahr ersetzt das nicht.

IKT-RISIKOMANAGEMENTRAHMEN — In Kraft

BEREICH	GRUNDLAGE	TAKT	STATUS
Asset-Inventare	Klassifizierung + Kritikalität	fortlaufend	vervollständigt
Risikoinventar	Risikomanagementrahmen	laufend	umgesetzt
Maßnahmenkatalog	IKT-Risikobewertung + Risikobehandlung	überarbeitet	in Kraft
Meldewesen	Aufsicht + ISM-Reporting	ereignisbezogen	angepasst
Kontrollframework	IS-Kennzahlen + Messung	periodisch	implementiert

PROJEKT-TICKER | Erfasst → **bewertet** → geregelt → gemeldet → **nachgewiesen**

etabliert · angepasst

▪ Schematische Darstellung des Wirkprinzips

WIRKPRINZIP

01 Erfassen → 02 Bewerten → 03 Regeln → 04 Melden → 05 Nachweisen

DER NACHWEISPUNKT

Was als Risiko erkannt wird, findet sich im Maßnahmenkatalog wieder. Was als Maßnahme gilt, wird über eine Kennzahl gemessen. Was gemessen wird, steht im dokumentierten IKT-Risikomanagementrahmen, und zwar so, dass ein Prüfer den Weg vom einzelnen Asset bis zur Kennzahl nachvollziehen kann.

08 · ERGEBNIS + WIRKUNG

Ein Fundament, das weiterträgt

Inventare vollständig

Die Asset- und Abhängigkeitsinventare sind vollständig, die Kritikalitätsbewertung neu ausgerichtet.

Rahmenwerk verankert

Ein IKT-Risikomanagementrahmen und ein umstrukturiertes BIA-Framework tragen die Bewertung.

Rahmen nachweisbar

Aktualisierter Maßnahmenkatalog, implementiertes Kontrollframework sowie dokumentierter und in Kraft gesetzter IKT-Risikomanagementrahmen.

NACHHALTIGE WIRKUNG

Der Kunde hat deutliche Schritte in Richtung DORA-Konformität zurückgelegt und damit die Voraussetzung dafür gesichert, weiter als IKT-Dienstleister für Banken und Finanzinstitute zu arbeiten. Der eigentliche Gewinn liegt in der Struktur: Kommt die nächste Anforderung, muss nicht wieder alles aufgebrochen werden. Sie wird eingehängt.

09 · STIMME DES KUNDEN

> **Wir wussten, was die Verordnung von uns verlangt. Was uns fehlte, war die Ordnung dahinter, und die ließ sich nicht nebenbei nachziehen. Heute kann ich jede Anforderung auf eine Struktur zeigen, die es bei uns wirklich gibt. Das ist der Unterschied, der in einer Prüfung zählt.**

Chief Information Security Officer, Finanzunternehmen

10 · KEY ACHIEVEMENTS

Was bleibt

- Bestehende Sicherheitsstrukturen und Reifegrad detailliert analysiert
- IKT-Risikomanagementrahmen überarbeitet, Erweiterung des Scopes umgesetzt
- Kritikalitätsbewertung neu ausgerichtet, BIA-Framework umstrukturiert
- Bedrohungs- und Sollmaßnahmenkatalog sowie ISMS-Richtlinien überarbeitet
- Prüf- und Kontrollframework mit IS-Kennzahlen implementiert
- Lücken und Abweichungen zur DORA präzise identifiziert und dokumentiert
- Klassifizierungs- und Kritikalitätsbewertung der Informations- und IKT-Assets durchgeführt
- Asset- und Abhängigkeitsinventare vervollständigt, Risikoinventar etabliert
- Meldewesen an die Behörden und internes ISM-Reporting angepasst
- Dokumentierten IKT-Risikomanagementrahmen einschließlich der zugehörigen Strategien, Richtlinien und Verfahren erstellt, genehmigt und in Kraft gesetzt

FAZIT · AUS ABLAGE WIRD RAHMENWERK

Aus einer Ordnung nach altem Maß wurde ein Rahmenwerk, das die Verordnung in der Sprache des Hauses beantwortet.

WIE DER KEIMLING IM BODEN

Die Arbeit, die zuerst niemand sieht, entscheidet darüber, was später stehen bleibt.

11 · FAZIT

Konformität wächst von unten.

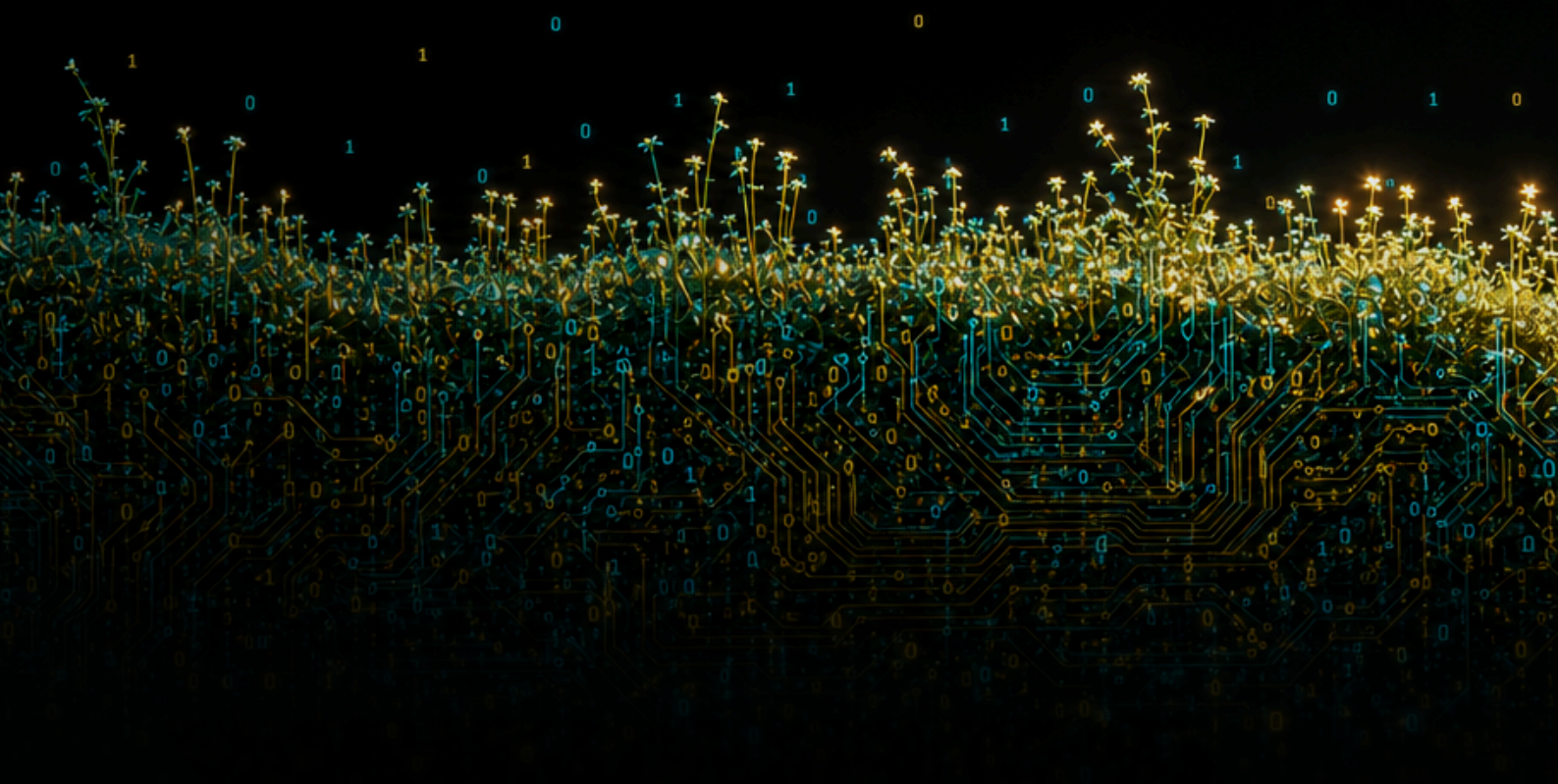
Die DORA lässt sich nicht durch Dokumente erfüllen, die über eine gewachsene Struktur gelegt werden. Sie verlangt, dass die Struktur stimmt. Ob man mit Assets, Abhängigkeiten und ihrer Kritikalität beginnt und Maßnahmen, Meldewege und Kennzahlen darauf aufsetzt, schreibt sie nicht vor. Bewährt hat es sich: Wer diese Reihenfolge einhält, braucht länger bis zum ersten sichtbaren Ergebnis und ist danach schneller, weil jede weitere Anforderung nur noch eingehängt wird.

AUSBLICK

Das Rahmenwerk trägt die kommenden Zyklen mit. Neue Systeme laufen durch dieselbe Kritikalitätsbewertung, neue Anforderungen durch denselben IKT-Risikomanagementrahmen.

ÜBERTRAGBAR

Der Ansatz aus Gap-Analyse, inventarbasiertem Rahmenwerk und nachweisfähiger Dokumentation lässt sich auf jedes Finanzunternehmen übertragen, das seine gewachsene IT-Governance auf die DORA umstellen muss.



ÜBER BASEC

Wie sicher ist Ihre Organisation wirklich?

Basec ist ein kleines, aber sehr feines Cyber-Security-Beratungshaus, persönlich, pragmatisch und auf Augenhöhe. Diese Case Study entstand im Bereich **BaseConsulting, DORA und IKT-Risikomanagement**.

IHR ANSPRECHPARTNER

Tim Will

Partnermanagement · Basec GmbH

tim.will@basec.de · +49 6326 346 3005

Erstgespräch vereinbaren →

Basec GmbH · Weinstraße 5b · 67146 Deidesheim · basec.de

Hinweis zur Erstellung. Für Grafik, Gliederung und Textbearbeitung dieser Publikation wurden generative KI-Systeme eingesetzt. Sämtliche Inhalte wurden von Basec fachlich geprüft, überarbeitet und freigegeben. Die inhaltliche Verantwortung liegt bei der Basec GmbH.