Strategisches IT-Management am Beispiel von DORA

Von reaktiver Anpassung zu proaktiver Planung

Abstract | Executive Summary

Dieses Paper macht deutlich, dass DORA nicht nur eine regulatorische Herausforderung darstellt, sondern auch die Chance bietet, durch proaktives IT-Management langfristige Wettbewerbsvorteile zu erzielen. Es werden zentrale Aspekte hervorgehoben – darunter Risikominimierung, Effizienzsteigerung und die Notwendigkeit einer umfassenden IT-Strategie. Letztere sollte nicht nur aktuelle regulatorische Vorgaben erfüllen, sondern auch die digitale Resilienz des Unternehmens stärken.

Digitale Resilienz als Erfolgsfaktor

Finanzinstitute stehen in einer zunehmend digitalen Welt vor wachsenden Herausforderungen. Die Abhängigkeit von stabilen IT-Infrastrukturen und der Schutz vor Cyberangriffen rücken mehr denn je in den Vordergrund. Mit dem Digital Operational Resilience Act (DORA) reagiert die EU auf diese Bedrohungen, indem sie Finanzunternehmen dazu verpflichtet, ihre digitale Widerstandsfähigkeit deutlich zu stärken. Doch diese regulatorischen Vorgaben sollten nicht als bloße Last verstanden werden. Vielmehr eröffnet DORA den Finanzinstituten eine strategische Chance, ihre IT-Infrastruktur nicht nur sicherer, sondern zugleich effizienter und wettbewerbsfähiger aufzustellen.

Ziel des Whitepapers

Der Fokus dieses Whitepapers liegt darauf, wie Finanzinstitute die Anforderungen von DORA nicht nur erfüllen können, sondern durch strategische und proaktive IT-Planung langfristige Wettbewerbsvorteile erzielen. Ein Wechsel von reaktiven zu proaktiven Ansätzen ermöglicht es, die Komplexität der IT-Systeme zu reduzieren, die operative Effizienz zu steigern und gleichzeitig die Widerstandsfähigkeit gegenüber künftigen Bedrohungen zu erhöhen.

Nutzen für die Zielgruppe

Als Zielgruppe gelten IT-Entscheider, Compliance-Verantwortliche und Unternehmensleiter in Finanzinstituten. Das Whitepaper liefert praxisnahe Empfehlungen, wie durch die Umsetzung von DORA sowohl IT-Systeme gestärkt als auch strategische Wettbewerbsvorteile gesichert werden können. Der proaktive Umgang mit IT-Risiken ermöglicht es Unternehmen, über die bloße Erfüllung gesetzlicher Vorgaben hinauszugehen und ihre Marktposition langfristig zu festigen.

Wesentliche Empfehlungen

Das Whitepaper legt dar, wie Finanzinstitute ihre IT-Strategien so ausrichten sollten, dass DORA nicht als einmalige Compliance-Aufgabe, sondern als integraler Bestandteil einer nachhaltigen IT- und Geschäftsstrategie betrachtet wird. Die wichtigsten Empfehlungen sind:

- **Proaktive IT-Planung:** Unternehmen sollten Risiken nicht nur erkennen, sondern ihnen aktiv zuvorkommen. Das bedeutet, IT-Systeme von vornherein flexibel und anpassungsfähig zu gestalten, um zukünftigen Herausforderungen gewachsen zu sein.

- **Integration von Best Practices:** Bewährte Verfahren aus IT-Sicherheit und Risikomanagement sollten konsequent in die IT-Infrastruktur eingebunden werden, um langfristige Resilienz sicherzustellen.

- **Optimierung der Zusammenarbeit mit Drittanbietern:** Da viele Finanzinstitute stark auf externe IT-Dienstleister angewiesen sind, sollte ein besonderes Augenmerk auf das Management von Drittanbieter-Risiken gelegt werden, um potenzielle Schwachstellen frühzeitig zu erkennen und zu minimieren.

Content | Inhaltsverzeichnis

Robin Haak

Consultant für IT Service Management &

Regulatorische Compliance

e:ndlich
in der IT zu Hause

LinkedIn

20.01.2026

1 | Einleitung

Die steigende digitale Abhängigkeit von Finanzinstituten und die daraus resultierende Notwendigkeit robuster IT-Strategien bilden den Ausgangspunkt dieses Whitepapers. Genau hier setzt der Digital Operational Resilience Act (DORA) der EU an. Er reagiert auf wachsende Cyberbedrohungen und die immer komplexeren digitalen Infrastrukturen, indem er klare Regeln für die digitale Resilienz im Finanzsektor definiert. Viele Unternehmen setzen bislang auf reaktive IT-Ansätze – das Whitepaper zeigt, warum ein strategischer, proaktiver IT-Plan notwendig ist, um neben der reinen Compliance auch langfristige Widerstandsfähigkeit zu gewährleisten.

2 | Regulatorischer Hintergrund: Der Wandel durch Krisen

Regulatorische Eingriffe im Finanzsektor entstehen in der Regel als Reaktion auf Krisen, die Schwächen in den bestehenden Systemen aufdecken. Historisch wurden viele Regulierungen – von den Basel-III-Richtlinien bis zur Datenschutz-Grundverordnung (DSGVO) – erst nach Krisenereignissen formuliert, um zukünftige Risiken zu minimieren. Solche Vorschriften dienen nicht nur dazu, Schäden zu begrenzen, sondern tragen auch dazu bei, das Vertrauen der Marktteilnehmer und der Öffentlichkeit in die Stabilität und Integrität des Finanzsystems wiederherzustellen.

In einer zunehmend digitalisierten Welt rückt ein Bereich besonders in den Fokus: die Informationstechnologie (IT). Mit dem exponentiellen Wachstum digitaler Dienste und der Abhängigkeit von komplexen IT-Infrastrukturen gewinnen IT-Risiken wie Cyberangriffe, Datenverluste und Systemausfälle massiv an Brisanz. Regulierungsbehörden weltweit erkennen inzwischen, dass die Stabilität des Finanzsystems ohne robuste IT-Infrastruktur nicht mehr gewährleistet werden kann.

3 | Die Dualität der Regulatorik: Missverstandene Notwendigkeit

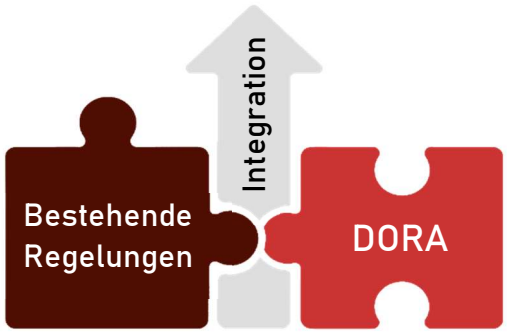
In vielen Unternehmen wirken neue Vorschriften auf den ersten Blick wie eine zusätzliche Last: Sie kosten Zeit, binden Ressourcen und können den operativen Betrieb erschweren. Im Kern sind sie jedoch weit mehr als nur formale Pflichten. Versteht man sie richtig, stellen sie einen klaren Kriterienkatalog dar, der entscheidend dazu beiträgt, IT-Systeme sicher und verlässlich zu halten. Für einen Prüfer der Aufsichtsbehörde – etwa der BaFin – bedeutet das, dass eine Prüfung nicht bloß der Nachweis der Einhaltung gesetzlicher Vorschriften ist. Vielmehr bewertet der Prüfer, wie wirksam und angemessen die implementierten Maßnahmen für Sicherheit und Betriebsstabilität sind.

Die geprüften Kriterien basieren auf bewährten Praktiken (Best Practices) der Industrie. Diese Standards wurden nicht willkürlich festgelegt, sondern haben sich über die Zeit als sinnvoll und zweckmäßig erwiesen, weil sie sich in der Praxis bewährt haben. Ähnlich wie in der Natur, in der Organismen sich durch fortlaufende Optimierung immer besser an ihre Umwelt anpassen, entwickeln sich auch Best Practices durch kontinuierliche Verbesserung und Anpassung an reale Herausforderungen. Sie sind das Ergebnis von Verfahren und Prozessen, die sich in der Praxis als effizient und effektiv erwiesen haben und heute als verlässliche Maßstäbe gelten.
Die Integration entsprechender bewährter Verfahren bringt Unternehmen weit mehr als nur das Bestehen von Audits. Sie führt zu einer robusteren IT-Infrastruktur, stärkt das Vertrauen von Kunden und Partnern in die Zuverlässigkeit des Unternehmens und sorgt für gleiche Wettbewerbsbedingungen. Ein erfolgreich absolvierter Prüfvorgang durch die Aufsicht sollte daher lediglich als positiver Nebeneffekt betrachtet werden.

4 | DORA: Die neue Ära der digitalen Resilienz

Digitale Risiken und ihre potenziellen Folgen haben in den letzten Jahren zunehmend die Aufmerksamkeit der Regulierungsbehörden auf sich gezogen. Groß angelegte Cyberangriffe auf Finanzinstitute haben deutlich gemacht, wie anfällig das Finanzsystem gegenüber digitalen Bedrohungen ist. Dies führte zu einem Umdenken – vergleichbar mit der Reaktion auf die Finanzkrise 2008, die tiefgreifende Reformen und striktere Regulierungen nach sich zog.
Mit der Einführung von DORA werden nun konkrete Maßnahmen ergriffen, um die digitale Widerstandsfähigkeit des Finanzsektors zu stärken. Finanzinstitute werden angehalten, ihre IT-Systeme robuster zu gestalten und ihre Cyberabwehr zu optimieren. Risiken sollen künftig

frühzeitig erkannt und abgewehrt werden. Auch Risiken aus Drittanbieter-Beziehungen, die im Finanzsektor eine zentrale Rolle spielen, rücken stärker in den Fokus. DORA setzt auf eine umfassende Überprüfung der digitalen Infrastrukturen, um die Einhaltung aller Anforderungen sicherzustellen. Wie schon bei den Vorgaben des Kreditwesengesetzes (KWG) und den MaRisk-Richtlinien zur Risikominimierung wird auch hier großer Wert auf praktische Umsetzung und kontinuierliche Überprüfung gelegt. Dieser verschärfte Fokus auf digitale Resilienz erfordert von Finanzinstituten eine proaktive Vorbereitung.



Einige Kernpunkte von DORA greifen bestehende Regelungen auf und verstärken sie, um den aktuellen Herausforderungen gerecht zu werden. Etablierte Vorschriften werden teilweise integriert und erweitert. Ziel ist es dabei nicht nur, die Widerstandsfähigkeit der Institute zu erhöhen, sondern auch eine europaweite Harmonisierung der Anforderungen zu erreichen und einen einheitlichen Rahmen zu schaffen.

5 | Von reaktiver Anpassung zu proaktiver Planung: Eine neue Denkweise

Der Titel dieses Whitepapers **„Von reaktiver Anpassung zu proaktiver Planung“** bringt es auf den Punkt: Unternehmen müssen ihre IT-Strategien grundlegend überdenken. Anstatt auf Bedrohungen erst zu reagieren, nachdem sie bereits eingetreten sind, verlangen strategische Ansätze wie DORA ein vorausschauendes Handeln.

Proaktive Planung bedeutet, nicht nur die Mindestanforderungen der Regulierung zu erfüllen, sondern darüber hinaus eigene Wege zu finden, die IT-Systeme auf zukünftige Herausforderungen vorzubereiten. Dies beginnt bei der Identifikation potenzieller Schwachstellen und reicht bis zur kontinuierlichen Verbesserung der digitalen Infrastruktur sowie der gezielten Schulung von Mitarbeitenden in IT-Sicherheitsfragen. Das Ziel ist eine IT-Landschaft, die nicht nur den heutigen Anforderungen gewachsen ist, sondern auch künftigen Bedrohungen standhält. DORA stellt dabei den Rahmen bereit, den Unternehmen für die Entwicklung einer solchen langfristigen IT-Strategie benötigen. Die strikten Vorgaben und die Betonung kontinuierlicher Überwachung und Verbesserung bieten eine klare Orientierung, um das IT-Management zukunftssicher auszurichten.

20.01.2026

Die Einführung von DORA ist mehr als eine weitere regulatorische Vorgabe – sie markiert den Beginn einer neuen Ära des IT-Managements im Finanzsektor. Unternehmen, die diese Herausforderung annehmen, haben die Chance, ihre IT-Infrastruktur nicht nur widerstandsfähiger, sondern auch zukunftssicherer zu gestalten. Der Wandel von reaktiver Anpassung zu proaktiver Planung wird somit nicht nur zum Wettbewerbsvorteil, sondern zur Voraussetzung, um in einer immer digitaleren Welt zu bestehen.

6 | Problemanalyse

Die zentrale Herausforderung bei der Umsetzung von DORA liegt in der bislang verbreiteten reaktiven Herangehensweise im IT-Management. Angesichts wachsender digitaler Bedrohungen und komplexer regulatorischer Vorgaben reicht ein rein reaktiver Ansatz nicht mehr aus. Probleme wie mangelnde Datenqualität und fragmentierte IT-Landschaften erschweren die Umsetzung. Nur durch proaktive, strategische Planung lassen sich langfristig Compliance, Sicherheit und Effizienz sicherstellen.

6.1 | Herausforderung regulatorischer Anforderungen

Die fortschreitende Digitalisierung der Finanzindustrie hat das regulatorische Umfeld tiefgreifend verändert. Mit dem Digital Operational Resilience Act soll gewährleistet werden, dass Finanzinstitute über robuste und widerstandsfähige IT-Systeme verfügen, die den wachsenden Risiken der digitalen Welt standhalten. DORA geht über frühere Regelwerke hinaus, indem es spezifische Vorgaben für das Management von IKT-Risiken einführt, die umfassende organisatorische und technische Anpassungen erfordern.

Viele Unternehmen sind zwar bereits mit grundlegenden regulatorischen Anforderungen vertraut, doch DORA bringt neue Dimensionen an Vielschichtigkeit und Präzision mit sich. Finanzinstitute sind gezwungen, ihre IT-Management-Strategien grundlegend zu überdenken und anzupassen. Die Verordnung setzt nicht nur auf Compliance im klassischen Sinne, sondern zielt darauf ab, die digitale Resilienz zu stärken und damit die Funktionsfähigkeit des gesamten Finanzsystems vor Bedrohungen wie Cyberangriffen, Systemausfällen und IT-Drittanbieter-Risiken zu schützen.

6.2 | Das Problem reaktiver IT-Management-Ansätze

Historisch gesehen neigen viele Finanzinstitute dazu, Bedrohungen oder Compliance-Lücken erst reaktiv anzugehen – sie reagieren also erst, wenn Probleme bereits aufgetreten sind. Was in der Vergangenheit funktionierte, wird den Anforderungen der heutigen digitalen Bedrohungslandschaft jedoch nicht mehr gerecht.

Ein überwiegend reaktiver Ansatz bringt mehrere zentrale Probleme mit sich:

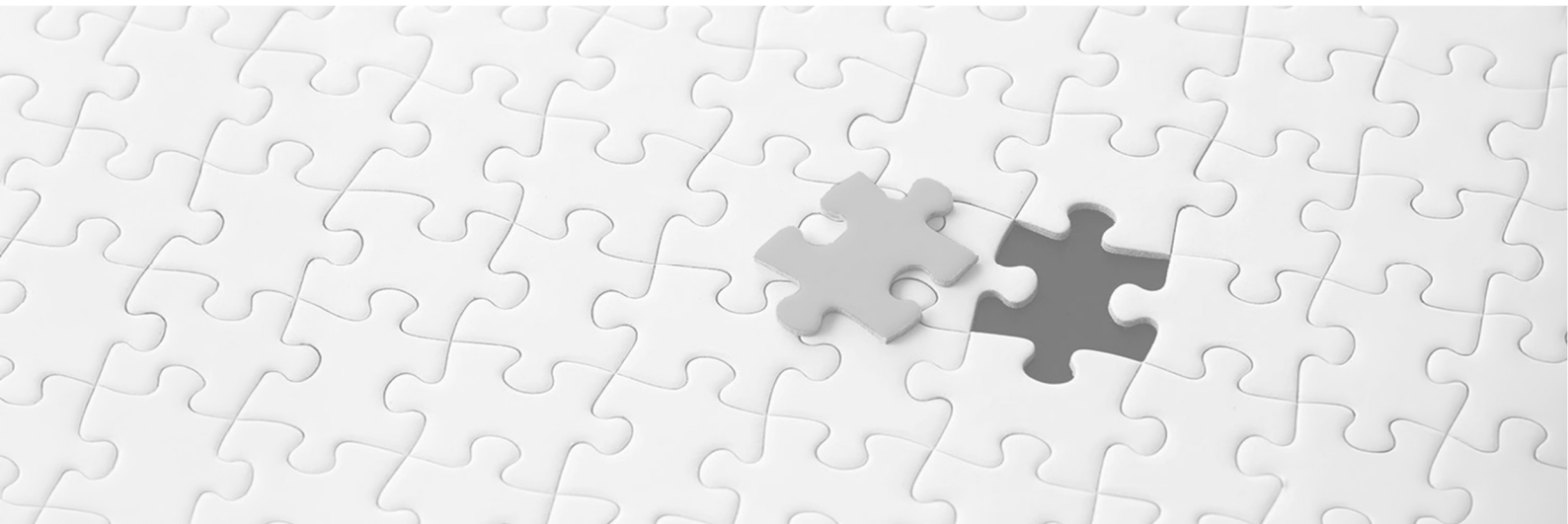
Hohe Betriebskosten und Ineffizienz

Finanzinstitute, die vor allem reaktiv agieren, sehen sich oft mit erhöhten Betriebskosten konfrontiert. Sicherheitslücken oder regulatorische Mängel werden meist erst entdeckt, wenn es bereits zu Ausfällen oder Verstößen gekommen ist. Die Folge sind teure und ineffiziente Ad-hoc-Maßnahmen, anstatt von vornherein proaktive und kosteneffiziente Lösungen umzusetzen.

Erhöhte Sicherheitsrisiken

Reaktive Maßnahmen halten mit der Geschwindigkeit und Komplexität moderner Cyberbedrohungen kaum Schritt. In einer Welt immer ausgefeilterer Angriffe ist reines Reagieren oft zu spät. Finanzinstitute, die sich auf reaktive Ansätze verlassen, sind daher anfälliger für Cyberattacken und Datenverluste – schlicht, weil sie häufig erst handeln, wenn ein Vorfall bereits eingetreten ist.

Ein solcher reaktiver Ansatz führt zwangsläufig zu einer fragmentierten IT-Landschaft: Statt einer ganzheitlichen, strategischen Planung werden immer wieder kurzfristig Ad-hoc-Lösungen implementiert. Die IT-Systeme werden dadurch immer komplexer und schwerer zu verwalten – was nicht nur die Sicherheit gefährdet, sondern auch die Effizienz des gesamten Unternehmens beeinträchtigt.



6.3 | Die Komplexität von DORA

DORA stellt Finanzinstitute vor eine Reihe von Anforderungen, die tiefgreifende organisatorische und technische Veränderungen notwendig machen. Ein zentrales Element ist dabei ein umfassendes, kontinuierliches Management von IKT-Risiken. Finanzinstitute müssen all ihre IT-Assets, Abhängigkeiten und Geschäfts-prozesse detailliert erfassen, dokumentieren und regelmäßig überprüfen. Ein konkretes Beispiel bietet Artikel 8 von DORA, der die Identifizierung und Bewertung von IT-Risiken vorschreibt. Finanzinstitute müssen sämtliche IT-gestützten Geschäfts-prozesse und deren Abhängigkeiten systematisch analysieren und dokumentieren. Es geht dabei nicht nur um die Erfassung der physischen IT-Infrastruktur, sondern auch um die Wechselwirkungen zwischen verschiedenen IT-Komponenten und deren Bedeutung für die Geschäfts-kontinuität.

Dazu gehören unter anderem:

Identifizierung von IT-Risiken

Alle potenziellen Risiken im Zusammenhang mit der IT-Infrastruktur müssen kontinuierlich erkannt werden. Dies umfasst technische Risiken (z. B. Sicherheitslücken in Systemen) ebenso wie organisatorische Risiken (z. B. Abhängigkeiten von externen IT-Dienstleistern).

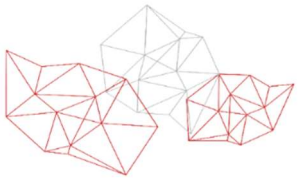
Bewertung von Drittanbieter-Risiken

Angesichts der starken Nutzung von Drittanbietern im IT-Bereich verlangt DORA auch die Identifizierung und Bewertung der Risiken, die von externen Dienstleistern ausgehen. Viele Institute setzen auf externe Cloud-Dienste, Datenverarbeitung oder IT-Support – was zusätzliche Komplexität und potenzielle Schwachstellen mit sich bringt.

Artikel 8 mag nur ein einzelner Paragraph sein, doch er entfaltet weitreichende Wirkung und bringt unerwartete Komplexität mit sich. Im Kern geht es um den sogenannten *Informationsverbund* – das zentrale Anliegen besteht darin, ein umfassendes, integriertes Gesamtbild der gesamten IT-Umgebung zu schaffen.

Artikel 8

Ein vollständiges Bild der IT-Landschaft zu zeichnen bedeutet weit mehr, als nur einzelne Configuration Items (CIs) zu verwalten. Es gilt, die komplexen Verbindungen und Abhängigkeiten zwischen den Komponenten der IT-Infrastruktur vollständig zu erfassen. Das beginnt bei einzelnen Elementen wie Servern, Datenbanken und Applikationen und umfasst deren Interaktionen sowie ihre Rolle bei der Bereitstellung von Geschäftsservices.



Ein einziger Business-Service hängt oft von mehreren CIs ab, die ihrerseits miteinander vernetzt sind und voneinander abhängen. Diese Abhängigkeiten können sowohl technischer als auch organisatorischer Natur sein. So funktionieren bestimmte Applikationen nur dann ordnungsgemäß, wenn sie Zugriff auf spezifische Datenbanken haben, die auf bestimmten Servern betrieben werden.

Ebenso spielen die Beziehungen zu Drittanbietern im Gesamtbild eine wichtige Rolle. Externe Dienstleister und Lieferanten sind über Verträge eingebunden, wodurch die Leistungsfähigkeit und Verfügbarkeit mancher Dienste von Dritten abhängt. Um Transparenz über solche Abhängigkeiten zu schaffen, müssen Verträge zentral verwaltet und deren Inhalte auswertbar gemacht werden.

Die Herausforderung beim Thema Informationsverbund liegt häufig darin, dass für Vertragsmanagement, CMDB und Asset-Management unterschiedliche Systeme im Einsatz sind, die nicht optimal miteinander integriert sind. Steht dann eine Prüfung an, kommt es oft zu unangenehmen Überraschungen – Lücken in der Dokumentation und die fehlende Integration dieser Systeme treten schlagartig zutage.

6.4 | Problematik der Datenqualität

Eine hohe Datenqualität sicherzustellen, ist eine der zentralen Herausforderungen bei der Erfüllung der DORA-Anforderungen. Finanzinstitute müssen verlässliche und vollständige Daten über ihre IT-Assets, Geschäftsprozesse und Drittanbieter verwalten, um sowohl regulatorische Vorgaben als auch betriebliche Effizienz zu gewährleisten. Häufig arbeiten Unternehmen jedoch mit fragmentierten Systemen, in denen verschiedene Datenbanken und Tools nicht ausreichend integriert sind.

Dies führt zu zwei Hauptproblemen:

Fehlende Transparenz

Wenn Daten in isolierten Silos gespeichert sind, wird es schwierig, ein klares und vollständiges Bild der IT-Infrastruktur zu erhalten. Diese Intransparenz erschwert nicht nur die Erfüllung regulatorischer Anforderungen, sondern erhöht auch die Anfälligkeit für Fehler und Sicherheitslücken.

Mangelhafte Datenqualität

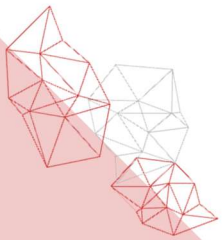
In vielen Fällen sind die vorhandenen Daten inkonsistent, unvollständig oder veraltet. Schlechte Datenqualität kann gravierende Auswirkungen auf das Risikomanagement haben, da falsche oder fehlende Informationen zu Fehlentscheidungen führen.

Datenqualität hat jedoch nicht nur regulatorische, sondern auch operative Bedeutung. Zuverlässige Informationen sind die Grundlage für fundierte operative und strategische Entscheidungen. Dieses Niveau an Datenqualität zu erreichen, ist oft mit erheblichem Aufwand verbunden – selbst wenn gepflegte Datenbanken vorhanden sind. Die kontinuierliche Pflege und Überwachung von Daten auf Korrektheit, Vollständigkeit und Aktualität ist essenziell. Ohne robuste Prozesse verliert selbst eine gut strukturierte Datenbank schnell an Wert.

Ein weiteres Problem: Unstrukturierte Datenablagen, wie etwa Dokumente auf Fileservern

- Schwer zugänglich
- Nicht systematisch auswertbar
- Bieten keine Mechanismen, um die Datenqualität sicherzustellen

Dadurch entstehen deutliche Informationslücken. Fehlende oder unzureichende Prozesse im Datenmanagement verschärfen diese Probleme zusätzlich. Ohne klare Richtlinien und Verfahren können selbst gut konzipierte Systeme nicht effektiv arbeiten.
Besonders heikel wird es, wenn Daten über Systemgrenzen hinweg ausgetauscht werden müssen. Jede Schnittstelle birgt das Risiko von Konvertierungsfehlern oder unvollständigen Übertragungen– was die Datenqualität weiter beeinträchtigen kann.



6.5 | Risiken reaktiver Umsetzungen

Ein weiteres häufiges Problem im Umgang mit neuen regulatorischen Anforderungen ist eine kurzfristige, reaktive Umsetzung. Viele Unternehmen beginnen erst mit der Implementierung von Vorgaben, wenn die Compliance-Fristen näher rücken. Das führt oft zu hektischen und ineffizienten Projekten. Dabei sind viele regulatorische Änderungen lange im Voraus absehbar – häufig liegen Entwürfe von Gesetzen oder Richtlinien Jahre vor ihrem Inkrafttreten vor. Wird diese Vorlaufzeit nicht genutzt, geraten Institute unnötig unter Zeitdruck und schaffen vermeidbare Risiken:

Fragmentierte IT-Landschaften

Unternehmen, die Anforderungen in letzter Minute umsetzen, neigen dazu, neue Tools oder Systeme ad hoc einzuführen. Das Ergebnis ist eine fragmentierte IT-Landschaft mit schlecht integrierten Insellösungen, steigender Komplexität und hohen Wartungskosten.

Sicherheitsrisiken

Überstürzte Implementierungen können dazu führen, dass Schwachstellen und Sicherheitslücken übersehen werden. Die IT-Infrastruktur wird dadurch verwundbarer für Cyberangriffe.

7 | Lösungsansätze und Best Practices

Um den skizzierten Herausforderungen zu begegnen, werden im Folgenden zentrale Lösungsansätze und Best Practices vorgestellt. Diese reichen von agilen Management-Prinzipien über technische Architekturmaßnahmen bis hin zu kulturellen Aspekten und sollen Finanzinstituten helfen, DORA proaktiv und strategisch umzusetzen.

Übersicht

- Agile Weitsicht
- Selbstoptimierende Prozesse
- Effektive Kommunikation als Schlüssel agiler Praktiken
- „Fail Fast“-Prinzip
- Systemarchitektur und Rahmenbedingungen
- Integrative Systeme

7.1 | Agile Weitsicht

Zielsetzung

Eine IT-Strategie etablieren, die langfristige Unternehmensziele unterstützt und dennoch flexibel genug bleibt, um schnell auf Marktveränderungen und technologische Trends reagieren zu können. Das heißt, eine Balance zwischen Stabilität und Agilität zu finden, sodass planvolles Vorgehen und Anpassungsfähigkeit gleichermaßen möglich sind.

Strategie

Die Umsetzung dieser Vision beruht auf zwei wesentlichen Komponenten. Zum einen werden klare Rahmenbedingungen und Leitlinien festgelegt, die für Stabilität sorgen und sicherstellen, dass alle IT-Aktivitäten konsequent auf die übergeordneten Unternehmensziele ausgerichtet sind. Zum anderen werden parallel agile Prozesse und Praktiken eingeführt, die dem IT-Betrieb die nötige Flexibilität verleihen, um auf Veränderungen und unvorhergesehene Herausforderungen schnell reagieren zu können. Diese Agilität stellt sicher, dass Anpassungen vorgenommen werden können, ohne die langfristigen Ziele aus den Augen zu verlieren.

Ergebnis

Durch die Kombination stabiler Leitplanken mit agilen Prozessen entsteht eine IT-Strategie, die sowohl zukunftssicher als auch anpassungsfähig ist. Das Unternehmen kann sich so erfolgreich auf Marktveränderungen einstellen, während die langfristigen Unternehmensziele gewahrt bleiben. Die IT-Infrastruktur bleibt stabil und zugleich flexibel genug, um auf neue Herausforderungen reagieren zu können.

Erkenntnis

Kontinuierliche Überprüfung und Anpassung der agilen Prozesse sind maßgeblich für den Erfolg. Regelmäßige Evaluierungen sowohl der Rahmenbedingungen als auch der eingesetzten Praktiken sind nötig, um neuen Anforderungen effektiv begegnen zu können. Dabei zeigt sich, dass die enge Zusammenarbeit zwischen strategischen Entscheidern und operativen Teams entscheidend ist, um die Balance zwischen Stabilität und Agilität zu halten.

7.2 | Selbstoptimierende Prozesse

Zielsetzung

IT-Prozesse nicht als starre Abläufe verstehen, sondern als flexible, dynamische Systeme, die sich kontinuierlich verbessern. Dadurch wird sichergestellt, dass Prozesse stets effizient bleiben und sich an neue Anforderungen und Herausforderungen anpassen können.

Strategie

Die Umsetzung erfolgt über iterative Feedbackschleifen. Regelmäßig eingeholte Rückmeldungen aus der Praxis fließen direkt in die fortlaufende Verbesserung der Prozesse ein. Jeder Prozessschritt wird kritisch hinterfragt und bei Bedarf angepasst, um aktuellen Anforderungen zu entsprechen und sich dynamisch weiterzuentwickeln. Ein zentraler Baustein dieses Ansatzes sind regelmäßige Retrospektiven, in denen Verbesserungspotenziale identifiziert werden. Dabei werden nicht nur die unmittelbaren Teammitglieder, sondern auch entferntere Stakeholder einbezogen, um ein möglichst breites Spektrum an Perspektiven zu erhalten. Durch die Einbindung verschiedener Blickwinkel können Prozesse flexibler auf veränderte Bedingungen reagieren und gleichzeitig sicherstellen, dass alle relevanten Anforderungen berücksichtigt sind.

Ergebnis

Durch die kontinuierliche Selbstoptimierung der IT-Prozesse entsteht eine Umgebung, in der proaktiv auf Neuerungen und Veränderungen reagiert wird. Diese fortlaufende Anpassung sorgt dafür, dass Prozesse langfristig effizient ineinandergreifen, da sie sich dynamisch weiterentwickeln und an aktuelle Bedürfnisse angleichen. Die hohe Anpassungsfähigkeit führt zu einer reaktionsschnellen IT-Infrastruktur, die den wechselnden Anforderungen des Marktes gerecht wird.

Erkenntnis

Unterschiedliche Perspektiven liefern wertvolle Einsichten, die sonst möglicherweise übersehen würden. Zudem zeigt sich, dass konsequent eingesetzte Feedbackschleifen in Kombination mit agilen Praktiken nicht nur die Effizienz steigern, sondern auch die Fähigkeit erhöhen, auf unvorhergesehene Herausforderungen flexibel zu reagieren.

7.3 | Effektive Kommunikation als Schlüssel agiler Praktiken

Zielsetzung

Aufbau einer starken Kommunikationskultur als Fundament einer agilen Organisation. Diese Kultur stellt sicher, dass Informationen frei fließen, Silos vermieden werden und alle Teammitglieder sowie Abteilungen stets auf demselben Stand sind – um effektiv und gemeinsam an den Zielen des Unternehmens zu arbeiten.

Strategie

Um eine effektive Kommunikation zu gewährleisten, werden gezielte Maßnahmen etabliert. Zunächst gilt es, verbindliche Kommunikationsstrukturen einzuführen: tägliche Stand-up-Meetings für aktuelle Aufgaben und Herausforderungen sowie wöchentliche bereichsübergreifende Abstimmungsrunden, damit alle Beteiligten up to date sind. Digitale Plattformen wie Microsoft Teams oder Confluence dienen als zentrale Informationsdrehscheiben. Wichtig ist, dass vorhandene Wissensdatenbanken gut strukturiert und fest in den Arbeitsalltag integriert sind. Nur durch klare Prozesse können solche Plattformen tatsächlich als zentrale Anlaufstelle dienen, an der sämtliche wichtigen Informationen gesammelt und für alle verfügbar gemacht werden.
Darüber hinaus sollte die Kommunikationskultur laufend gepflegt und verbessert werden – etwa durch interne Workshops und Schulungen. So wird sichergestellt, dass alle Mitarbeiter die Kommunikationskanäle effizient nutzen und den hohen Stellenwert von transparentem Informationsaustausch verstehen.

Ergebnis

Eine starke Kommunikationskultur stellt sicher, dass Informationen reibungslos und effektiv ausgetauscht werden und keine Wissenssilos entstehen. Dies verbessert die bereichsübergreifende Zusammenarbeit und erhöht die Qualität der Arbeitsergebnisse, da alle Teammitglieder stets den gleichen Wissensstand haben und kontinuierlich Ideen sowie Feedback austauschen. Durch regelmäßigen Austausch sinkt außerdem die Gefahr von Doppelarbeit, was die Effizienz steigert. In einer agilen Umgebung – in der schnelle Anpassungsfähigkeit an neue Herausforderungen entscheidend ist – bildet eine solche Kommunikationskultur das Rückgrat des Erfolgs.

Erkenntnis

Eine wichtige Erkenntnis aus der Umsetzung einer intensiven Kommunikationskultur ist, dass kontinuierlicher Informationsaustausch nicht nur die Qualität der Arbeit verbessert, sondern auch die Teamdynamik und das gegenseitige Verständnis stärkt. Es hat sich gezeigt, dass die Förderung sowohl der Kommunikation innerhalb einzelner Teams als auch abteilungsübergreifend unerlässlich ist, damit wirklich alle an einem Strang ziehen.

7.4 | „Fail Fast“-Prinzip

Zielsetzung

Eine Kultur der Innovation fördern, in der Teams ermutigt werden, Neues auszuprobieren und kalkulierte Risiken einzugehen. Die „Fail Fast“-Mentalität soll sicherstellen, dass Innovationen nicht aus Angst vor dem Scheitern unterdrückt werden. Fehler werden stattdessen als wertvolle Lernchancen betrachtet und neue Ideen können schnell auf ihre Tragfähigkeit getestet werden.

Strategie

Die Förderung dieser Kultur umfasst mehrere Elemente:

- **Ermutigung zum Experimentieren:** Teams werden dazu angehalten, neue Ideen und Ansätze zügig auszuprobieren – ohne Angst vor Rückschlägen. Dies schafft Raum für kreative Lösungen und fördert die Bereitschaft, unbekannte Wege zu gehen.
- **Positive Fehlerkultur:** Fehler gelten nicht als Scheitern, sondern als wertvolle Gelegenheit zu lernen. Es wird ein Umfeld geschaffen, in dem Fehler offen angesprochen und analysiert werden, um daraus wichtige Erkenntnisse für zukünftige Projekte zu gewinnen.
- **Konstruktives Feedback:** Regelmäßiges, konstruktives Feedback ist fest im Arbeitsablauf verankert. Es ermöglicht den Teams, aus misslungenen Versuchen zu lernen und ihre Ansätze kontinuierlich zu verbessern. Dadurch wird eine stetige Weiterentwicklung sichergestellt.

Ergebnis

Eine Fail Fast-Kultur fördert nicht nur die schnelle Umsetzung neuer Ideen, sondern auch kontinuierliche Verbesserungen durch Lernen aus Fehlern. So entstehen praxisnahe, effektive Lösungen in einem agilen, lernbereiten Arbeitsumfeld. Innovationsprozesse beschleunigen sich, weil Teams fähig sind, rasch Anpassungen vorzunehmen und die vielversprechendsten Ansätze konsequent weiterzuverfolgen.

Erkenntnis

Fail Fast funktioniert nur in Kombination mit einer ausgeprägten Fehlerkultur und einem etablierten Feedback-Prozess. Mut zum Risiko und die Bereitschaft, aus konstruktiver Kritik zu lernen, führen zu schnellerer und erfolgreicherer Entwicklung. Außerdem zeigt sich, dass Teams, die diese Mentalität verinnerlicht haben, widerstandsfähiger und anpassungsfähiger sind – sie ziehen aus jedem Rückschlag wertvolle Lehren und lassen diese in zukünftige Vorhaben einfließen.

7.5 | Systemarchitektur und Rahmenbedingungen

Zielsetzung

Die Stabilität und Skalierbarkeit der IT-Infrastruktur langfristig sicherzustellen. Eine klar definierte Systemarchitektur mit eindeutigen Rahmenbedingungen und gut beschriebenen Schnittstellen bildet die Grundlage dafür. Ziel ist es, durch konsequente Einhaltung der Architekturvorgaben und regelmäßige Überprüfungen die Datenqualität hochzuhalten und einen robusten Informationsverbund zu gewährleisten.

Strategie

Die Sicherstellung einer stabilen und skalierbaren IT-Architektur umfasst mehrere Elemente:

- **Klare Architekturvorgaben:** Es werden präzise, dokumentierte Leitlinien für die Systemarchitektur und die Schnittstellen zwischen den Systemen festgelegt. Darin sind die technischen und funktionalen Anforderungen definiert, die für Stabilität und Skalierbarkeit nötig sind.
- **Enterprise Architecture Management (EAM):** Das EAM ist für die Erstellung und Pflege dieser Vorgaben verantwortlich. Es sorgt dafür, dass Schnittstellen, Prozesse und Dokumentationen klar definiert und in die Gesamtarchitektur integriert werden.

- **Regelmäßige Reviews und Anpassungen:** Die definierten Architekturvorgaben und -prozesse sollten in regelmäßigen Abständen überprüft und bei Bedarf angepasst werden. So kann gewährleistet werden, dass sie veränderten Anforderungen und neuen Technologien gerecht bleiben. Diese Überprüfungen sichern die Einhaltung der Vorgaben und ermöglichen rechtzeitige Nachjustierungen.
- **Kontinuierliche Überwachung und Nachbesserung:** Die Einhaltung der Architekturvorgaben muss laufend überwacht werden. Sobald Abweichungen oder Optimierungsbedarf festgestellt werden, sind umgehend Korrekturmaßnahmen einzuleiten, um die Datenqualität und die Systemstabilität sicherzustellen.

Ergebnis

Die konsequente Anwendung der Architekturvorgaben und regelmäßige Überprüfungen sorgen für eine langfristig stabile und skalierbare IT-Infrastruktur. Dies verbessert die Datenqualität und schafft eine solide Basis für einen integrierten Informationsverbund. Die IT-Systeme lassen sich effizienter verwalten und gezielt auf Änderungen ausrichten, was die Gesamteffizienz und Leistungsfähigkeit der IT-Landschaft deutlich steigert.

Erkenntnis

Das Enterprise Architecture Management (EAM) trägt die Hauptverantwortung für die Definition und Pflege der Architekturvorgaben. Um eine hohe Datenqualität zu gewährleisten, sind jedoch ebenso regelmäßige Überprüfungen und eine lückenlose Dokumentation erforderlich. Die festgelegten Vorgaben müssen konsequent eingehalten und bei Bedarf aktualisiert werden, damit eine stabile und skalierbare Infrastruktur ihren Zweck erfüllen kann.

7.6 | Integrative Systeme

Zielsetzung

Eine effiziente und konsistente IT-Landschaft sicherstellen, indem neue Systeme nahtlos und sinnvoll in die bestehende Infrastruktur integriert werden können. Klare Regelungen und Standards sollen die Kompatibilität gewährleisten und verhindern, dass eine unübersichtliche, heterogene Systemlandschaft entsteht.

Strategie

Die erfolgreiche Integration neuer Systeme umfasst mehrere wesentliche Aspekte:

- **Klare Vorgaben für neue Systeme:** Einheitliche Standards und Richtlinien für die Auswahl und Einführung neuer Lösungen stellen sicher, dass alle Neusysteme die gleichen technischen und funktionalen Anforderungen erfüllen und miteinander kompatibel sind.
- **Sorgfältige Prüfung der Kompatibilität:** Jedes neue System muss gründlich auf seine Verträglichkeit mit der bestehenden IT-Landschaft geprüft werden. Werden Abweichungen oder Lücken festgestellt, sind Anpassungen vorzunehmen oder alternative Lösungen zu suchen, um eine reibungslose Integration sicherzustellen.
- **Frühe Einbindung aller Stakeholder:** Wichtige Beteiligte – von IT-Architekten über Endanwender bis hin zu Vertretern angrenzender Bereiche – sollten frühzeitig in den Beschaffungsprozess eingebunden werden. So lassen sich Anforderungen abstimmen und sicherstellen, dass neue Systeme sowohl funktional passen als auch mit den vorhandenen Anwendungen harmonieren.

Ergebnis

Durch die frühe Einbindung aller relevanten Stakeholder wird sichergestellt, dass neue Systeme passgenau auf die bestehenden Anforderungen abgestimmt und nahtlos in die vorhandene IT-Infrastruktur integriert sind. Dies fördert die Auswahl von Lösungen, die funktional zusammenpassen und harmonisch miteinander arbeiten. Unnötige Schnittstellen werden vermieden und die Komplexität der Systemlandschaft reduziert. Die IT-Umgebung bleibt stabil und effizient, da die Systeme reibungslos zusammenwirken und somit ein unterbrechungsfreier Datenfluss und eine konsistente Funktionalität gewährleistet sind.

Erkenntnis

Eine frühe Einbindung aller Beteiligten ermöglicht es, potenzielle Risiken und Herausforderungen rechtzeitig zu erkennen und proaktiv anzugehen. Besonders die Abhängigkeiten zwischen neuen und bestehenden Systemen dürfen nicht unterschätzt werden. Wenn diese nicht richtig identifiziert und gemanagt werden, können Integrationsprobleme oder Leistungseinbußen die Folge sein. Daher ist es essenziell, diese Abhängigkeiten frühzeitig zu analysieren und entsprechende Gegenmaßnahmen einzuleiten.

8 | Fazit

Dieses Whitepaper macht deutlich, dass die Anforderungen des Digital Operational Resilience Act (DORA) nicht nur als regulatorische Pflicht gesehen werden sollten, sondern als Chance, die IT-Infrastruktur von Finanzinstituten nachhaltig zu verbessern. Institute, die ihre IT-Management-Strategien von reaktiven Ansätzen auf proaktive, langfristig ausgerichtete Konzepte umstellen, profitieren von einer robusteren, widerstandsfähigeren und effizienteren IT-Landschaft.
Durch die Stärkung der Datenqualität, die Einführung eines kontinuierlichen IT-Risikomanagements und die engmaschige Überwachung von Drittanbietern können Unternehmen nicht nur die DORA-Vorgaben erfüllen, sondern auch ihre digitale Resilienz deutlich erhöhen. Der Einsatz von Best Practices, eine klare IT-Strategie und innovative Technologien wie Automatisierung und KI-gestützte Bedrohungserkennung stellen sicher, dass die IT-Landschaft nicht nur den aktuellen, sondern auch zukünftigen Herausforderungen gewachsen ist.
Abschließend lässt sich festhalten: Der Schlüssel zur erfolgreichen Umsetzung von DORA liegt in frühzeitiger und strategischer Planung. Finanzinstitute, die DORA als Impuls für eine umfassende Transformation ihrer IT-Infrastruktur nutzen, werden langfristig nicht nur alle regulatorischen Auflagen erfüllen, sondern dank einer agilen und resilienten IT-Landschaft auch nachhaltige Wettbewerbsvorteile erzielen.

8.1 | Branchenweite Erkenntnisse

In der Praxis belegen Studien, dass proaktive IT- und Compliance-Strategien langfristig erhebliche Vorteile bringen. Eine Deloitte-Studie aus dem Jahr 2021 (Deloitte, „Global Risk Management Survey“, 2021) ergab beispielsweise, dass Organisationen, die in RegTech (regulatorische Technologien) investieren, ihre Compliance-Kosten um bis zu 30 % senken konnten. Dies gelang durch die Integration von Automatisierung, KI-gesteuerten Überwachungssystemen und Blockchain-basierten Prozessen, welche eine frühzeitige Identifizierung von Risiken ermöglichen und gleichzeitig den Aufwand für die Berichterstattung reduzieren.
Darüber hinaus zeigte eine Untersuchung der Oesterreichischen Nationalbank (OeNB) aus 2020 (OeNB, „AuRep – Automated Reporting for Banks“, 2020), dass österreichische Banken, die eine gemeinsame Datenplattform für die regulatorische Berichterstattung nutzen, ihre Kosten um mehr als 30 % verringern konnten. Diese Plattform – bekannt als „Basic Cubes“-Lösung – erlaubt es den teilnehmenden Banken, ihre Meldedaten gemeinsam zu bündeln. So werden Effizienzgewinne erzielt und die Datenqualität erhöht.

Auch im Versicherungssektor ist dieser Effekt zu beobachten. Eine PwC-Studie aus 2022 (PwC, „Digital Transformation in Insurance“, 2022) stellte fest, dass Versicherungsunternehmen, die proaktiv digitale Transformation in ihre Compliance-Prozesse integrieren, ihre Betriebskosten um etwa 20 % senken konnten. Diese Einsparungen resultierten vor allem aus der Automatisierung von Risikomanagement-Prozessen und dem Einsatz von cloudbasierten Plattformen.

8.2 | Branchenübergreifende Trends

Branchenübergreifend zeigt sich, dass Unternehmen, die neue Technologien in ihre Compliance- und IT-Prozesse integrieren, deutlich von höherer Effizienz und geringeren Kosten profitieren. Ein markanter Trend ist die verstärkte Nutzung von künstlicher Intelligenz und Automatisierung, um regulatorische Anforderungen zu erfüllen. Laut einer McKinsey-Studie aus 2021 (McKinsey, „AI in Risk Management“, 2021) setzen bereits 40 % der befragten Unternehmen KI-basierte Lösungen ein, um ihre Compliance-Prozesse zu optimieren. Diese Unternehmen konnten den Aufwand für die Erfüllung regulatorischer Vorgaben um rund 25 % reduzieren.
Ein weiterer Trend ist der Einsatz von Cloud-Technologien. Einer Gartner-Studie von 2022 (Gartner, „Top Trends in Cloud Computing“, 2022) zufolge verwenden 60 % der untersuchten Unternehmen Cloud-Plattformen, um ihre Compliance-Prozesse zu verbessern. Diese Organisationen berichten von höherer Skalierbarkeit und Flexibilität – insbesondere im Hinblick auf die Bewältigung zukünftiger regulatorischer Anforderungen.
Zudem zeigt sich in vielen Sektoren, dass Unternehmen, die ihre IT-Architektur proaktiv an neue regulatorische Vorgaben anpassen, widerstandsfähiger gegenüber Cyberangriffen sind. Eine Accenture-Studie aus 2022 (Accenture, „State of Cyber Resilience“, 2022) ergab, dass Firmen mit proaktiven IT-Sicherheitsstrategien 50 % weniger Sicherheitsvorfälle verzeichneten als jene, die lediglich reaktiv auf Zwischenfälle reagieren.

9 | Zukunftsaussichten

Mit der fortschreitenden Digitalisierung und der zunehmenden Abhängigkeit von IT-Infrastrukturen wird die digitale Resilienz für Finanzinstitute künftig von noch größerer Bedeutung sein. Regulatorische Initiativen wie DORA sind dabei nur der Anfang. Es ist zu erwarten, dass die EU und andere internationale Regulierungsbehörden ihre Vorgaben weiter verschärfen werden, um Finanzinstitute gegen die wachsenden Bedrohungen durch Cyberangriffe, IT-Ausfälle und verstärkte Drittanbieter-Abhängigkeiten zu schützen.

Finanzinstitute werden in Zukunft nicht vermeiden können, kontinuierliche Innovation in ihre IT-Management-Strategien zu integrieren. Der Einsatz von künstlicher Intelligenz, automatisierten Überwachungssystemen und Cloud-Technologien wird dabei unverzichtbar, um die steigende Komplexität der IT-Landschaften zu bewältigen und Bedrohungen in Echtzeit zu erkennen und abzuwehren. Gleichzeitig wird die Weiterentwicklung von Cybersecurity-Lösungen und deren nahtlose Einbindung in bestehende Systeme entscheidend sein, um den Anforderungen an digitale Widerstandsfähigkeit gerecht zu werden.
Darüber hinaus wird die Zusammenarbeit zwischen Regulierungsbehörden, Finanzinstituten und Dienstleistern intensiver, um globale Standards für IT-Sicherheit und Resilienz zu schaffen. Diese Kooperation wird den Weg für eine stärkere Harmonisierung der Vorschriften ebnen und die Einführung innovativer Technologien beschleunigen.
Finanzinstitute, die diese Entwicklungen frühzeitig aufgreifen und in ihre IT-Strategien integrieren, werden nicht nur die regulatorischen Vorgaben erfüllen, sondern sich auch als Vorreiter in puncto digitale Sicherheit und Effizienz positionieren.

Die Zukunft gehört denjenigen, die Agilität, Sicherheit und Innovationskraft in ihr IT-Management einbauen und sich kontinuierlich an die wandelnde digitale Landschaft anpassen.

10 | Literaturverzeichnis

Atzema, H., & Brandwijk, N. (2023, 29. August). What can we expect from the Digital Operational Resilience Act? Deloitte Netherlands. Abgerufen von https://www.deloitte.com/nl/en/services/consulting-risk/perspectives/digital-operational-resilience-act.html (Zugriff: 20.01.2026)

Basel Committee on Banking Supervision. (2021, 31. März). Principles for operational resilience. Bank for International Settlements. ISBN 978-92-9259-480-0. Abgerufen von https://www.bis.org/bcbs/publ/d516.pdf (Zugriff: 20.01.2026)

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). (2021, 16. August). Bankaufsichtliche Anforderungen an die IT (BAIT) – Rundschreiben 10/2017 (BA) in der Fassung vom 16.08.2021. Abgerufen von https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.html (Zugriff: 20.01.2026)

Boehm, J., & Schneider, S. (2024, 28. Juni). Europe's new resilience regime: The race to get ready for DORA. McKinsey & Company. Abgerufen von https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/europes-new-resilience-regime-the-race-to-get-ready-for-dora (Zugriff: 20.01.2026)

Boston Consulting Group (BCG) Platinion. (2024, 13. Mai). DORA: Table Stakes or Strategic Investment? Abgerufen von https://www.bcgplatinion.com/insights/dora-table-stakes-or-strategic-investment (Zugriff: 20.01.2026)

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2021). BSI-Standard 200-4: Business Continuity Management (Notfallmanagement). Bonn: BSI. Abgerufen von https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/210118_BSI-Standard-200-4.html (Zugriff: 20.01.2026)

European Banking Authority (EBA). (2019a, 29. November). EBA Guidelines on ICT and security risk management (EBA/GL/2019/04). Abgerufen von https://www.eba.europa.eu/publications-and-media/publications?text=&document_type=250&media_topics=All (Zugriff: 20.01.2026)

European Banking Authority (EBA). (2019b, 25. Februar). EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02). Abgerufen von https://www.eba.europa.eu/sites/default/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf (Zugriff: 20.01.2026)

European Central Bank (ECB). (2018). Cyber resilience oversight expectations for financial market infrastructures (CROE). Frankfurt: ECB. Abgerufen von https://www.ecb.europa.eu/home/html/index.en.html (Zugriff: 20.01.2026)

European Union. (2022, 27. Dezember). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). Amtsblatt der EU, L 333, S. 1–79. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2554 (Zugriff: 20.01.2026)

European Union Agency for Cybersecurity (ENISA). (2025). ENISA Threat Landscape: Finance Sector – January 2023 to June 2024. Abgerufen von https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf (Zugriff: 20.01.2026)

National Institute of Standards and Technology (NIST). (2018, 16. April). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). Gaithersburg, MD: NIST. DOI: 10.6028/NIST.CSWP.04162018. Abgerufen von https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (Zugriff: 20.01.2026)

PricewaterhouseCoopers (PwC). (2025, 30. Juni). DORA: Laying the groundwork for digital resilience and transformation. PwC Luxembourg. Abgerufen von https://www.pwc.lu/en/digital-operational-resilience-act/dora-laying-the-groundwork.html (Zugriff: 20.01.2026)

e:ndlich
in der IT zu Hause

Robin Haak

Consultant für IT Service Management &
Regulatorische Compliance

Strategisches IT-Management am Beispiel von DORA

Von reaktiver Anpassung zu proaktiver Planung