# Bestehende IT-Regulierungen schaffen eine Basis für die effektive Umsetzung der DORA-Anforderungen

Auf Basis eines von unseren Experten durchgeführten umfassenden Abgleichs von DORA mit bestehenden Regularien, ist eine hohe Übereinstimmung erkennbar. Dennoch: Es existieren **wesentliche erweiterte und auch neue Anforderungen**, welche die vorhandenen europäischen und nationalen Vorgaben konkretisieren, verschärfen oder gänzlich ersetzen.

**Abgleich DORA vs. MaRisk/BAIT (Auszug)**

**DORA** - Anforderungen auf Einzelebene — **MaRisk / BAIT** = Wesentliche **neue Anforderungen** und Anpassungsbedarf sowie Auswirkung

| Artikel | DORA - Anforderungen | MaRisk/BAIT Referenz | Wesentliche Neuerung | Impact |
|---|---|---|---|---|
| **Kap III Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle** | | | | |
| **Artikel 17** Prozess für die Behandlung IKT-bezogener Vorfälle | Finanzunternehmen müssen angemessene Verfahren und Prozesse zur Erkennung, Behandlung und Meldung von IKT-bezogenen Vorfällen einrichten und anwenden, einschließlich Frühwarnindikatoren, Kategorisierung und Klassifizierung, Zuweisung von Funktionen und Zuständigkeiten sowie Pläne für die Kommunikation und Reaktionsmaßnahmen. | BAIT Tz 3.10 Inforiskmgmt.<br>BAIT Tz 4.7 - 4.10 ISMS<br>BAIT Tz 5.3; 5.5 OpInfoSec<br>BAIT Tz 8.6 IT-Betrieb<br>MaRisk AT 7.2.4 Tech.-org. Ausstattung | - Einsatz von Frühwarnindikatoren zur Erkennung, Behandlung und Meldung von Vorfällen<br>- Zuweisung von Funktionen und Zuständigkeiten für alle Arten von IKT-bezogenen Vorfällen<br>- Erstellung von Kommunikationsplänen für Personal, externe Interessenträger, Medien, Kunden und andere Finanzunternehmen<br>- Einführung von Prozessen zur Information an die Geschäftsleitung bei schwerwiegenden Vorfällen mit Erläuterung der Auswirkungen, Maßnahmen und zusätzlichen Kontrollen<br>- Definition von Reaktionsmaßnahmen zur Minderung der Auswirkungen von IKT-Vorfällen und Sicherstellung der zeitnahen Verfügbarkeit und Sicherheit der Dienste | **High** |
| **Artikel 18** | Finanzunternehmen klassifizieren IKT- | BAIT Tz 4.7 ISMS | - Erweiterung der Analyse von IKT-bezogenen Vorfällen, um die Anzahl betroffener Kunden, | |

*Abb.: Abgleich DORA Anforderungen und MaRisk/BAIT*

Mit der **BAIT-Novelle 2021** wurden neue Anforderungen im Bereich des Informationssicherheitsmanagements auf Basis der *EBA-Guidelines on ICT and Security Risk Management* eingeführt, die bereits viele Elemente von DORA aufgreifen. Unter anderem wurden in den Vorgaben zur „Operativen Informationssicherheit" bereits Anforderungen im Bereich der Cyber Security definiert.

Aufbauend auf einem umfassenden Abgleich auf Ebene der einzelnen Anforderungen aus DORA, mit den bestehenden Vorgaben aus MaRisk und BAIT, ergeben sich einzelne Überschneidungen sowie Neuerungen. **Die konkreten Neuerungen, wie auch eine Einschätzung der Umsetzungsauswirkungen, haben wir analysiert und aufbereitet**.

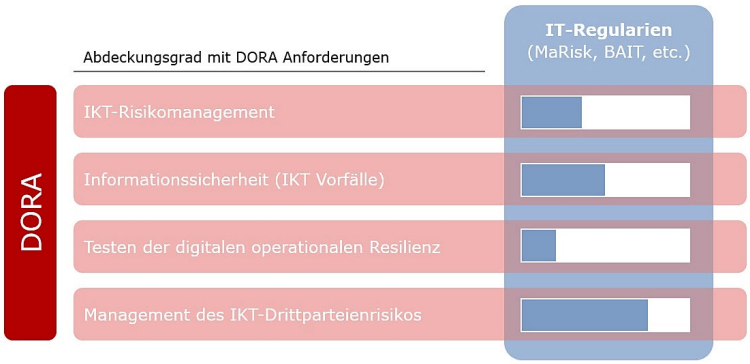



*Abb.: Abdeckungsgrad DORA vs. IT-Regulation (MaRisk, BAIT)*

# Unsere Services – Ihr Nutzen

Für eine effektive Umsetzung der DORA-Vorgaben haben wir **effiziente und ressourcenschonende Vorgehensweisen** entwickelt. Diese berücksichtigen Best-Practices aus der **prüfungssicheren Umsetzung** von IT-Compliance Lösungen sowie die individuellen Rahmenbedingungen der Organisation gleichermaßen.

Mit unseren **DORA Services** unterstützen wir Finanzinstitute und IT-Dienstleister in der **fokussierten Analyse** bis hin zur **Umsetzung von maßgeschneiderten Lösungen und kompetenter Beratung** in allen Schwerpunktthemen der IT-Organisation.

| Service | Umfang |
|---|---|
| **Gap-Analyse (moderiert)** | ▪ Prüfung des Umsetzungsstandes der DORA-Anforderungen<br>▪ Moderierte Workshops zu den Bereichen der IT-Compliance<br>▪ Erarbeitung der IST-Situation und eines Zielbildes (Soll)<br>▪ Aufzeigen von **Handlungsbedarf** und konkreter **Umsetzungsplanung** |
| **Webinare / Training** | ▪ Transparenz über Schwerpunkte der **DORA-Anforderungen**<br>▪ **Abgleich** mit IT-Compliance Vorgaben<br>▪ Praktische Handlungshinweise und Prüfungserfahrungen<br>▪ Adressatengerechte **Sensibilisierungsschulungen** |
| **IKT-Risiko-management** | ▪ Etablierung eines **IKT-Risikomanagements** und dessen Verzahnung mit bestehenden Verfahren (u.a. OpRisk)<br>▪ Aufnahme und Bewertung des Risiko-Portfolios<br>▪ Erstellung von **Risikoberichten**<br>▪ Awareness-Training für Mitarbeiter und (Senior-)Management |
| **Cyber-Security** | ▪ Konzeption und Etablierung von IT-Asset-Management-Lösungen (CMDB)<br>▪ Prüfung und Optimierung von Verfahren zur Cyber-Security<br>▪ Etablierung eines **Cyber-Security**-Vorfallmanagements inkl. Reaktionsplänen |
| **Outsourcing Management** | ▪ Erstellung von Auslagerungsstrategien, Richtlinien und Verfahren zum Auslagerungsmanagement<br>▪ Konzeption und Durchführung von Risiko- und Vertragsanalysen, laufendes Auslagerungscontrolling, Exit-Strategien<br>▪ Regulatorische Begleitung und Absicherung von Auslagerungsvorhaben (u.a. Cloud Outsourcing)<br>▪ Unterstützung von IT-Dienstleistern zur regulatorisch-konformen Ausgestaltung von IT-Services |

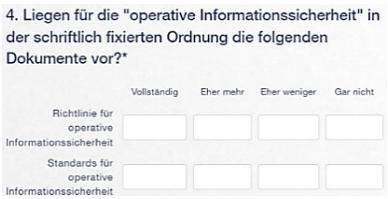
# DORA Gap-Analyse – schnell und zuverlässig den Reifegrad der IT-Organisation ermitteln

Um **schnell und zuverlässig** einen Überblick über den Reifegrad der eigenen IT-Organisation zu erhalten und **konkreten Handlungsbedarf** zur Umsetzung der DORA-Anforderungen zu ermitteln, unterstützen wir zielgerichtet mit einem **praxiserprobten DORA Toolset**:

**A**

**Aufbau**

- Mehr als 400 Prüfungsfragen zu allen relevanten Themenbereichen (von IT-Strategie bis Security Testing)
- Erkenntnisse aus externen Prüfungen und laufenden Aufsichtsgesprächen
- Quantitativer und qualitativer Ansatz




**B**

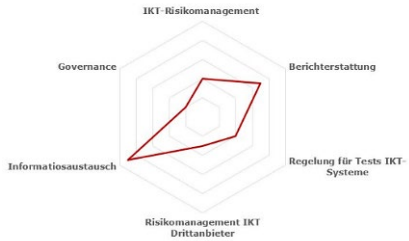
**Durchführung**

- Modulares Assessment, um den Erfüllungstand effektiv zu bewerten und Lücken aufzudecken
- Fokussierte Einbindung der betroffenen Bereiche (u.a. IT-Governance, IT-Security, Auslagerungs-Management)
- Vorbereitete Checkliste für zielgerichtete Interviews und Workshops erleichtern die Analyse


**C**

**Auswertung**

- Einwertung der Antworten anhand von Best-Practices und Prüfungsstandards
- Auswertung je Themengebiet (Detailreport) und gesamthaft (Management Report)
- Praxisnahe Vorschläge für konkrete Handlungsmaßnahmen je Themengebiet als Basis für die individuelle Umsetzungsplanung




Zur Unterstützung des Quick-Checks und der Analyse haben wir Webinare zu verschiedenen Themenstellungen, die einen tieferen Einblick in die neuen Anforderungen bieten.


Webinar: DORA - Neuer EU-Rahmen für Cyber-Resilienz in Finanzunternehmen


Blog: Neue regulatorische Vorgaben rund um DORA


Auszug Präsentation VAB: Informationssicherheit im Rahmen des IKT-Risikomanagements

# Unsere Expertise in der IT- Compliance

Severn verfügt über **langjährige Erfahrungen** und **fundierte fachliche wie auch methodische Kenntnisse** in der Etablierung von IT-Management Lösungen. Dabei kombinieren wir unsere Erfahrung und **Kenntnisse der Prüfungspraxis der Aufsicht** mit **praxiserprobten Verfahren** zur Umsetzung des individuellen Handlungsbedarfs.

Wir verstehen uns als Partner der IT und konnten dies für namhafte Kunden in zahlreichen erfolgreich durchgeführten Projekten bereits unter Beweis stellen

**Referenzprojekte (Auszug):**

- **Internationales Finanzunternehmen:** Aufbau eines IT Compliance Frameworks und Umsetzung der BAIT/MaRisk sowie EBA-Vorgaben, Konzeption von Zielbildern bis Transition in die Organisation (u.a. Schulung von mehr als 200 Mitarbeitern). Durchführung einer „Audit-Simulation" zur Verprobung von Wirksamkeit und Angemessenheit.
- **Depotbank:** Nachhaltige Behebung von Feststellungen der EZB in den Bereichen: IT-Risk-Management, Identity & Access Management, Business Continuity Management, Outsourcing, Application Development / EUC, Berichterstattung an Aufsicht
- **Bank:** Behebung von Feststellungen aus IT-Sonderprüfung, Entwicklung von Zielbildern und Umsetzungsmaßnahmen in allen wesentlichen IT-Funktionen, Kommunikation mit Aufsichtsbehörden und Prüfern, Change- und Roll-out Management
- **Internationaler Börsenkonzern:** Durchführung von „Audit-Simulationen" und Prüfungsvorbereitung. Aufbau eines neuen IT Compliance Frameworks und Umsetzung der BAIT/MaRisk sowie EBA-Vorgaben nach erfolgter Sonderprüfung, Konzeption von Zielbildern und Entwicklung neuer agiler technologischer Plattformen (OpenShift).
- **Förderinstitut:** Behebung von Feststellungen im Identity & Access Management (IAM), Umsetzung von prozessualen und technischen Maßnahmen im Berechtigungsmanagement, Anbindung von Applikationen an eine zentrale IAM-Lösung
- **Landesbank:** Steuerung und Umsetzung eines Gesamtprogrammes zur Behebung von Feststellungen in der IT-Compliance, insbesondere IT-Governance, IT-Strategie, IT-Risikomanagement, Auslagerungsmanagement und IAM
- **Versicherungskonzern:** Begleitung einer IT-Sonderprüfung, Beratung und Qualitätssicherung, Unterstützung in der VAIT-Umsetzung (u.a. operative IT-Sicherheit, IDV, Ausgliederungsmanagement)

**Zu unseren Kunden zählen u.a.:**

Allianz, caceis Investor Services, RBS The Royal Bank of Scotland, eex, wüstenrot württembergische, DZ BANK, Deutsche Börse Group, ODDO BHF, Berenberg, Credit Suisse, NRW.BANK, dwpbank, Commerzbank, BNP Paribas, ABN·AMRO, UBS, NORD/LB, FONDSDEPOT BANK, SIEMENS, UniCredit, Deutsche Bundesbank Eurosystem, Helaba, Alte Leipziger ALH Gruppe, Frankfurter Sparkasse

# Ihr Partner

## Next Generation Consulting für Finanzunternehmen

Severn Consultancy ist eine auf den nationalen und internationalen Finanzmarkt spezialisierte Unternehmensberatung. Unsere besondere Expertise liegt in der effektiven Realisierung erfolgskritischer Veränderungsprozesse in der Marktfolge – dort sind wir besser als viele andere.

Exzellente Beratung und sofort wirksame Lösungen für unsere Mandanten – mit diesem Anspruch wurde Severn 1987 gegründet. Kompetente Fach- und Managementberatung gepaart mit effektivem Projektmanagement sind die Säulen des „Severn ways to get it done".

In mehr als 20 Jahren Beratungspraxis haben wir eine Vielzahl renommierter Unternehmen bei der effizienten Durchführung ihrer Projekte und der Optimierung unternehmensinterner Prozesse unterstützt. Unsere Mandanten schätzen unsere innovativen Beratungskonzepte, das methodische Know-how sowie unsere fundierten Markt- und Branchenkenntnisse.

Wir verstehen Ihre Anforderungen, kennen die Themen und unterstützen Sie schnell und flexibel mit wirkungsvollen Lösungen. Wir liefern zuverlässig konkrete Ergebnisse, die Ihnen messbaren Erfolg bringen. Nehmen Sie uns beim Wort und erleben Sie Next Generation Consulting.

**Ansprechpartner:**

Severn Consultancy GmbH
Hansa Haus, Berner Straße 74 60437
Frankfurt am Main
T +49 (0)69 / 950 900-0
info@severn.de
www.Severn.de

**Norman Nehls**
Partner