



DORA praxisorientiert meistern: Effizienz durch Nutzung genossenschaftlicher Standards

Lösungsansätze für alle Genossenschafts- und
Privatbanken mit Einsatz von **agree21**

Hilfreiche Good-Practice-Impulse

Seit Januar 2025 gilt DORA verbindlich für alle Institute der genossenschaftlichen Finanzgruppe. Viele Häuser haben Prozesse, Rollen und Dokumentationen angepasst und neue Anforderungen umgesetzt. Doch bleibt eine Frage offen: Wie wird die Aufsicht den Umsetzungsstand künftig bewerten?



André Rapp
Partner bei der
ECG Eurogroup Consulting AG
E-Mail: andré.rapp@
eurogroupconsulting.de



Christian Störck
Senior Manager bei der
ECG Eurogroup Consulting AG
E-Mail: christian.storck@
eurogroupconsulting.de

DORA ist mehr als eine regulatorische Pflicht. Die Anforderungen eröffnen die Chance, IKT-Strukturen systematisch zu prüfen, digitale Resilienz als Querschnittsaufgabe zu verankern und Risiken ganzheitlich zu steuern. Unterstützung liefern genossenschaftliche Standards wie die BVR-Prozesslandkarte, ZAM-Datenpakete oder Musterarbeitsanweisungen der Verbände. Entscheidend ist die qualifizierte Umsetzung im eigenen Haus. Fünf Good-Practice-Impulse können hilfreich sein, damit dies angemessen und nachhaltig gelingt.

Richtlinienkonforme Strukturen verankern

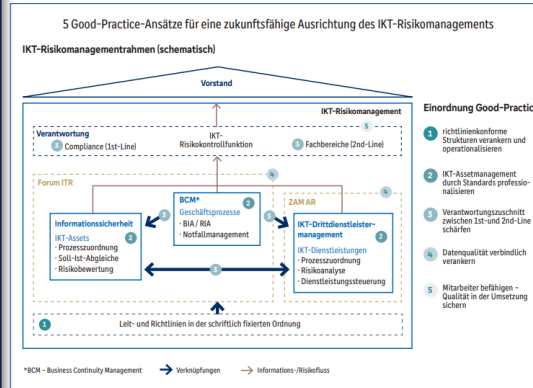
Die wirksame Umsetzung von DORA beginnt mit einer klar strukturierten, regulatorisch konformen Richtlinienlandschaft entlang der Mindestanforderungen von EBA und BaFin. Die Musterarbeitsanweisungen der Regulatorverbände bieten dabei eine wertvolle Grundlage, müssen jedoch individuell angepasst und konsistent in das jeweilige Organisations- und Kontrollumfeld eingebettet werden.

Entscheidend ist vorab deren vollständiger Abgleich mit der bestehenden schriftlich fixierten Ordnung (sFO) der Bank (Soll-/Ist-Abgleich), um das konkret notwendige Veränderungsmaß für die Organisation abzuleiten. Nur wenn Leit- und Richtlinien sowie die tatsächliche Praxis – überprüft etwa durch Stichproben oder Interviews – dann auch übereinstimmen, kann die Umsetzung erfolgreich sein.

Ein belastbares IKT-Assetmanagement bildet das Herzstück der DORA-Umsetzung und der IKT-Risikosteuerung. Es entsteht, wenn IKT-Assets und Dienstleistungen konsequent aus den Prozessen abgeleitet, darüber verzahnt und letztlich auch in deren

IKT-Assetmanagement professionalisieren

Ein belastbares IKT-Assetmanagement bildet das Herzstück der DORA-Umsetzung und der IKT-Risikosteuerung. Es entsteht, wenn IKT-Assets und Dienstleistungen konsequent aus den Prozessen abgeleitet, darüber verzahnt und letztlich auch in deren



Kontext bewertet werden. So wird die Basis für fundierte Schutzbedarfsbewertungen und Steuerung gelegt.

Die BVR-Prozesslandkarte bietet hierfür ein stabiles Fundament, da sie eine einheitlich etablierte Struktur vorgibt. Die Vorschlagsdaten der ZAM inklusive des Banken-Sollmaßnahmenkatalogs (BaSo) ergänzen diese Sicht durch eine Zuordnung von Anwendungen und Dienstleistungen zu Prozessen. Hiermit können direkte Synergien für das Asset Management erzeugt werden.

Werden diese Daten systematisch ins GRC-Tool (Governance Risk & Compliance) integriert und mit konsistenten Verantwortlichkeiten verbunden,

können Banken profitieren: Die Datenqualität steigt, regulatorische Nachweise werden einfacher und der individuelle Dokumentationsaufwand sinkt spürbar.

Verantwortungszuschnitt schärfen
DORA verlangt klare Verantwortlichkeiten. Es empfiehlt sich eine organisatorische Klarstellung:

- Wer agiert in der operativen Verantwortung (1st Line)?
- Wer ist in der Kontrolle (2nd Line)?
- Und wie sehen die konkreten Aufgaben dahinter aus?

Besonders im IKT-Assetmanagement sollten diese Linien mit Rollen, Prozessen und Informationswegen unterlegt werden. Dies schafft Transparenz und unterstützt bei internen und externen Prüfungen. DORA ist der geeignete Zeitpunkt, um etablierte Verantwortungsmodelle zu schärfen und auf Effizienz

auszurichten. Dazu gehören insbesondere Themen wie die Zentralisierung von Aufgaben.

Die Verantwortung sollte sowohl aufbauorganisatorisch, vor allem aber ablauforganisatorisch verankert werden. Hierzu ist die detaillierte Ableitung von Prozessen im Management von IKT-Assets und IKT-Dienstleistungen, gestützt über eine gute Ausgestaltung des zentralen GRC-Tools (beispielsweise Forum, ZAM-ARI, erforderlich. Diese dient nicht nur der Beschreibung, sondern auch der Verankerung risikoorientierter Verhaltens- und Arbeitsweisen.

Datenqualitätsstandards verbindlich verankern

Die Qualität von Daten eines wirksamen IKT-Assetmanagement beginnt mit der Sicherstellung einer reibungslosen Vollständigkeit des IKT-Inventars. Hier ergeben sich regelmäßig Bestandslücken durch unzureichende Bewer-



BAFIN-
INFOS
ZU DORA

Gerade weil regulatorische Vorgaben häufig Interpretationsspielräume lassen und noch keine abschließenden Prüfstandards vorliegen, ist eine einheitliche Bewertung unverzichtbar.

tyssystematiken oder mangelnde Transparenz in der Bank.

Entscheidend ist, dass klare Datenstrukturen in den GRC-Tools definiert und konsistent über alle relevanten Teilbereiche hinweg angewendet werden – von Prozessen über Anwendungen bis hin zu den damit verbundenen Dienstleistungen. Nur so lassen sich Abhängigkeiten transparent darstellen und bewerten.

Asset-Daten müssen zudem vollständig, korrekt und aktuell sein. Verbindlich benannte Asset-Verantwortliche sorgen dafür, dass Vorgaben eingehalten und Aktualisierungen zeitnah mit fachlicher Expertise umgesetzt werden. Hierbei können vor allem Vorschlagsdaten der ZAM wertvolle Orientierung bieten und zugleich für eine einheitliche Terminologie im Verbund sorgen.

Mitarbeiterinnen und Mitarbeiter befähigen

Die Qualität der DORA-Umsetzung hängt vor allem von der fachlichen Substanz und konsistenten Durchführung von Analysen ab. Dafür ist es entscheidend, die verantwortlichen Stakeholder – von der 1st-Line bis zum Vorstand – gezielt zu befähigen. Mitarbeiter müssen nicht nur verstehen, wie Prozesse, Assets,

Ebenso wichtig sind definierte Prozesse zur dauerhaften Pflege und Qualitätssicherung. Regelmäßige Plausibilitätsprüfungen – idealerweise verankert im IKS des Instituts, abgestimmte Schnittstellen zu Fachbereichen und eine konsistente Dokumentation im GRC-Tool – verhindern Medienbrüche und Doppelarbeiten. So wird Datenqualität nicht als punktuelle Aufgabe verstanden, sondern als kontinuierlicher Steuerungsprozess – und damit zum zentralen Erfolgsfaktor.

Glossar

IT-Strukturen

IT-Strukturen umfassen alle Systeme, Geräte, Software und Netzwerke, die für die Informations- und Kommunikationstechnologie innerhalb einer Organisation oder der Gesellschaft verwendet werden.

DORA

Die Abkürzung sFO in einer Bank steht für schriftlich fixierte Ordnung, ein umfassendes Dokumentationssystem für den Aufbau- und Ablauforganisation sowie die internen Richtlinien und Prozesse, das von der deutschen Aufsichtsbehörde BaFin gefordert wird, um Transparenz und Compliance sicherzustellen.

Banken-Sollmaßnahmenkatalog (BaSo)

Der BaSo ist ein zentrales Umsetzungsinstrument der genossenschaftlichen Finanzgruppe, bereitgestellt über die ZAM eG, zur Erfüllung regulatorischer Anforderungen aus dem Digital Operational Resilience Act (DORA). Er unterstützt Banken dabei, Soll-Zustände für ihre IT-Sicherheit und Resilienz zu definieren, Maßnahmen abzuleiten und deren Umsetzung strukturiert zu dokumentieren. Damit erleichtert der BaSo den Nachweis gegenüber Aufsichtsbehörden und schafft Vergleichbarkeit innerhalb der Finanzgruppe. Banken erhalten übergreifende Sicherheitsrichtlinien sowie auf Einzel-Ebene konkrete Maßnahmenvorschläge, deren Anwendungen in der Organisation zu bewerten sind (SOLL-/IST-Abgleich).

Risiken, Notfallmanagement und Risikovororge zusammenhängen, sondern auch, welche eigenen Gestaltungsräume sie haben. Ein klar strukturiertes Onboarding und kontinuierliche Sensibilisierung legen hierfür die Basis.

Risikobewertungs- und Meldeprozess, dessen Ergebnisse quantitativ belastbar und qualitativ nachvollziehbar sind. So entsteht eine realistische Risikovorlage, die Eigenkapital schont und operative Risiken absichert.

Gerade weil regulatorische Vorgaben häufig Interpretationsspielräume lassen und noch keine abschließenden Prüfstandards vorliegen, ist eine einheitliche Bewertung unverzichtbar. Einheitliche Kriterien – etwa zur Identifikation von IKT-Assets oder kritischen Funktionen – verhindern Unsicherheit und fördern Vergleichbarkeit. Unterstützt durch Befähigungskonzepte wird nicht nur die Qualität der Analysen gesichert, sondern auch die Ergebnisumsetzung in den Häusern gestärkt.

DORA als Impulsgeber

Ziel einer erfolgreichen DORA-Umsetzung ist ein vollständiger und sauber dokumentierter

DORA ist damit nicht nur Regulierung, sondern Impulsgeber: für mehr Transparenz, Verantwortungsbewusstsein und ein aktiveres Risikomanagement. Die Good-Practice-Impulse können helfen, Anforderungen in nachhaltigen Mehrwert zu übersetzen.

Eine Prüfung der bisherigen Umsetzung gegen diese Ansätze kann Handlungsbedarfe aufzeigen, regulatorische Konformität erhöhen und eine konsistente Risikosituation erzeugen. Genossenschaftliche Standards und Instrumente bieten dafür die Basis. Richtig eingesetzt, schaffen sie nicht Bürokratie, sondern Effizienz, Struktur und Sicherheit.



NetCon 2025 – Gemeinsam auf Kurs

„Leinen los!“ heißt es am 28. Oktober bei der NetCon 2025! Begleiten Sie uns auf einer inspirierenden Reise durch die zentralen Themen des Digitalen Customer Journey Managements. Die NetCon 2025 bietet Ihnen wertvolle Impulse, praxisnahe Lösungen und strategische Antworten auf Ihre Herausforderungen von morgen. Erleben Sie, wie smarte Strategien, neue Technologien und clevere KI-Lösungen Ihre Bank zukunftsfest machen.

Freuen Sie sich auf einen ganzen Tag voller Innovation, Inspiration und Interaktion – online, live und praxisnah.

Melden Sie sich jetzt an.
<https://netcon.vr-networld.de>



Wir machen Digital.
Erfolgreich.

DORA treibt herausfordernde Prioritäten für Regional- und Privatbanken

Ziele sind Stabilität, Effektivität und Effizienz sowie Wertschöpfung

Herausfordernde Prioritäten

Nachhaltige Ziele und erstrebenswerte Ambitionsniveaus

**Vollständige
Operationalisierung
regulatorischer Vorgaben**



Stabilität

Regulatorische Anforderungen werden durch eine konsistente Zuordnung aller IKT-Assets und -Dienstleistungen zu Geschäftsprozessen sowie der Ableitung von Abhängigkeiten, Kritikalität und Risiken erfüllt. Ein DORA-konformes Richtlinienwesen und dessen Operationalisierung bilden diese Anforderungen praxisnah ab.

**Optimierung der Abläufe
innerhalb des Rahmens für
das IKT-Risikomanagement**



Effektivität und Effizienz

Durch einen nachhaltigen Verantwortungszuschnitt für Prozesse, IKT-Assets und -Dienstleistungen sowie eine klare Ablauforganisation zur effizienten Bearbeitung der DORA-Anforderungen wird die operative Informationssicherheit gestärkt und der Sicherstellungsaufwand reduziert.

**Generierung und Gestaltung
von organisatorischen
Chancen aus den Regularien**



Wertschöpfung

Durch Befähigung der Organisation und Nutzung von etablierten Standards erfolgt eine valide Ableitung sowie Bewertung von IKT-Risiken, mit dem Ziel eine angemessene Risikovorsorge mit optimaler Balance des Risikoappetits zu betreiben.

Zur Erreichung der zentralen Ziele sollten 4 wesentliche Fragen für die Organisation beantwortet werden können:

1.

Wie klar und vollständig ist eine funktionierende Governance auf Basis von DORA-Anforderungen im Haus definiert und etabliert?

2.

Wie gut ist die notwendige übergreifende Transparenz zu Geschäftsprozessen und den IKT-Assets sowie -Dienstleistungen, die diese unterstützen?

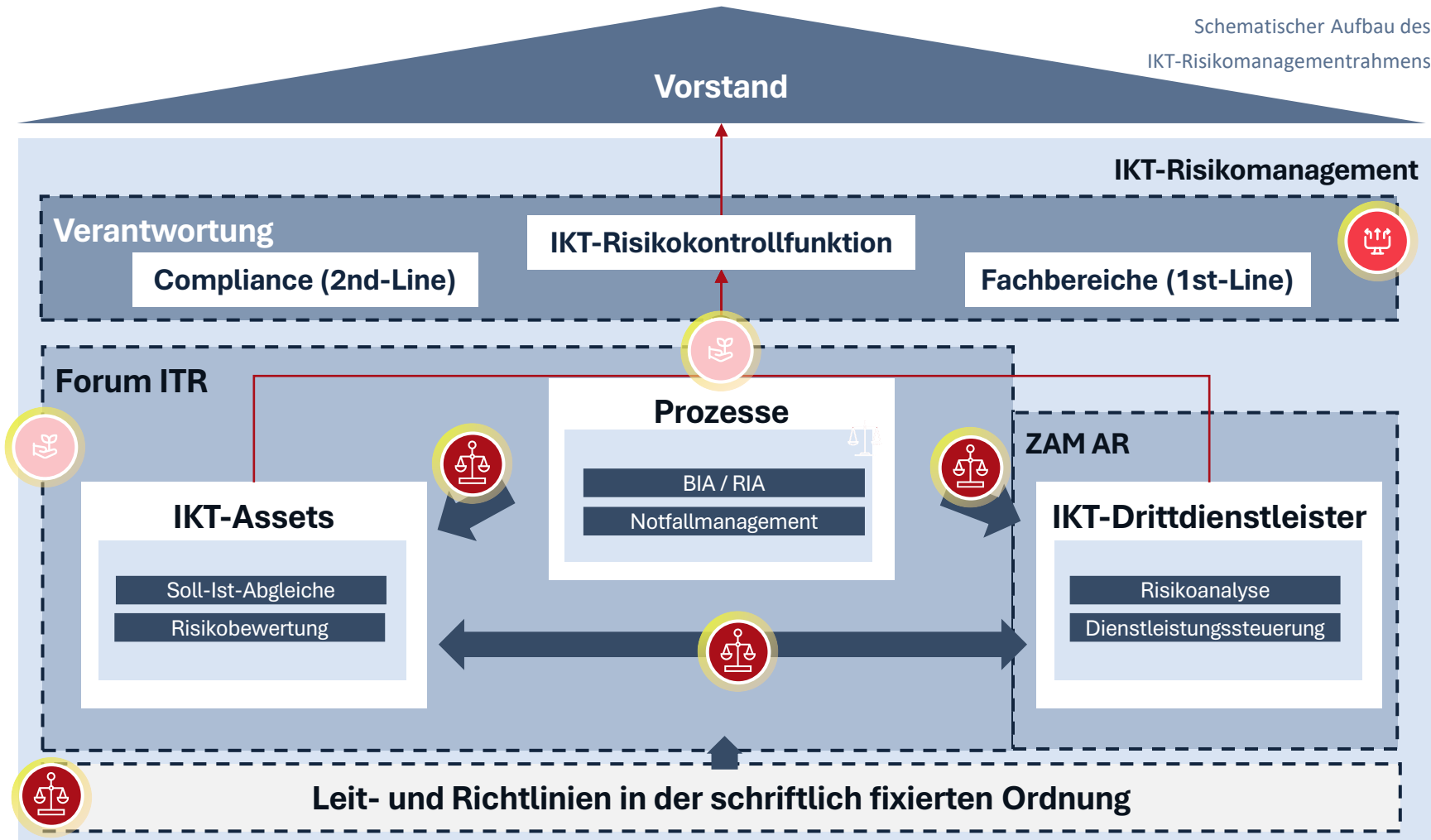
3.

Wie gut und klar sind Prozesse zur Operationalisierung von Anforderungen über die Gesamtorganisation geregelt, befähigt und etabliert?

4.

Wie ganzheitlich vernetzt werden zentral zur Verfügung stehende technische und organisatorische Standards (z.B.: ZAM, Forum ITR, etc.) eingesetzt, sofern sie überhaupt bekannt sind?

Der IKT-Risikomanagementrahmen liefert Antworten zur Erreichung nachhaltiger DORA Compliance



→ Risikofluss

Nachhaltige Ziele im Fokus



Stabilität

Das IKT-Assetmanagement macht Zusammenhänge und Abhängigkeiten transparent



Effektivität und Effizienz

Klare Verantwortung und Zusammenarbeit sind definiert sowie etabliert.



Wertschöpfung

Standards und eine befähigte Organisation stützen die Risikosteuerung.

Mit etablierten Standards*...

Standardisierte Prozesslandkarte

01

Bildet alle banktypischen Prozesse ab und stellt Musterbewertungen zur Geschäftskritikalität zur Verfügung

Muster-Richtlinien

02

Bilden alle Anforderungen der DORA und weitere IT-Regulatorik ab und werden regelmäßig aktualisiert

Standardisiertes GRC-Tool

03

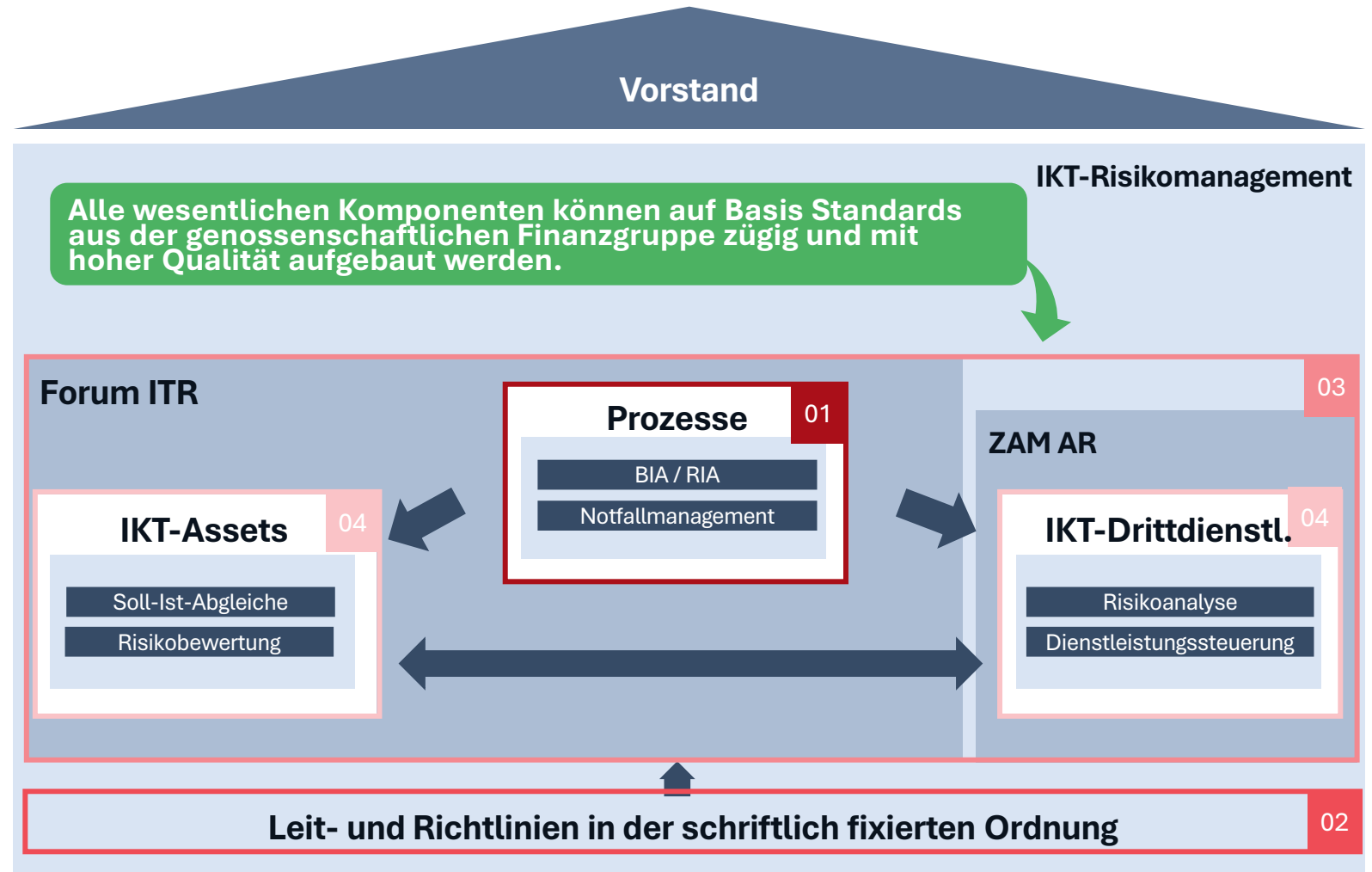
Stellt einen etablierten Rahmen zur Verfügung, der die Anforderungen an Struktur und Inhalte abdeckt. Es interagiert mit den Musterbewertungen.

Bewertung von Assets & Dienstleistungen

04

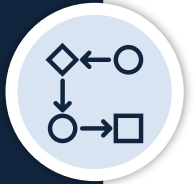
Für alle IKT-Assets und Dienstleistungen werden Musterbewertungen für Risikoanalysen zur Verfügung gestellt

...lässt sich der IKT-Risikomanagementrahmen mit allen Elementen aufbauen und Ziele erreichen



* Standards liegen in der genossenschaftlichen Finanzgruppe für alle Aspekte vor

Echte Ergebniswirkungen sind für eine prüfungssichere und effektive IT-Compliance nach DORA-Anforderungen zu erwarten



GFG-konforme Strukturbasis implementieren

Zukunftsfähige Strukturen auf Basis eines etablierten GFG-Standards (u.a. PLK der Genossenschaftsbanken) aufbauen und Prozesse, IKT-Assets und Dienstleistungen konsequent ausrichten



IKT-Assetmanagement vollständig und valide auf- bzw. ausbauen

Zusammenhänge zwischen Prozessen, IT-Assets und Dienstleistungen auf Basis PLK erzeugen sowie Inventar durch Einsatz von Vorschlagsdaten und Individualinformationen ausbauen



ZAM AR und Forum ITR praxisorientiert ausgestalten

Standards für die Nutzung und die Datenqualität definieren sowie Klarheit zur ablauforganisatorischen Nutzung entlang klarer Verantwortungsregelungen etablieren



Schriftlich fixierte Ordnung DORA-konform operationalisieren

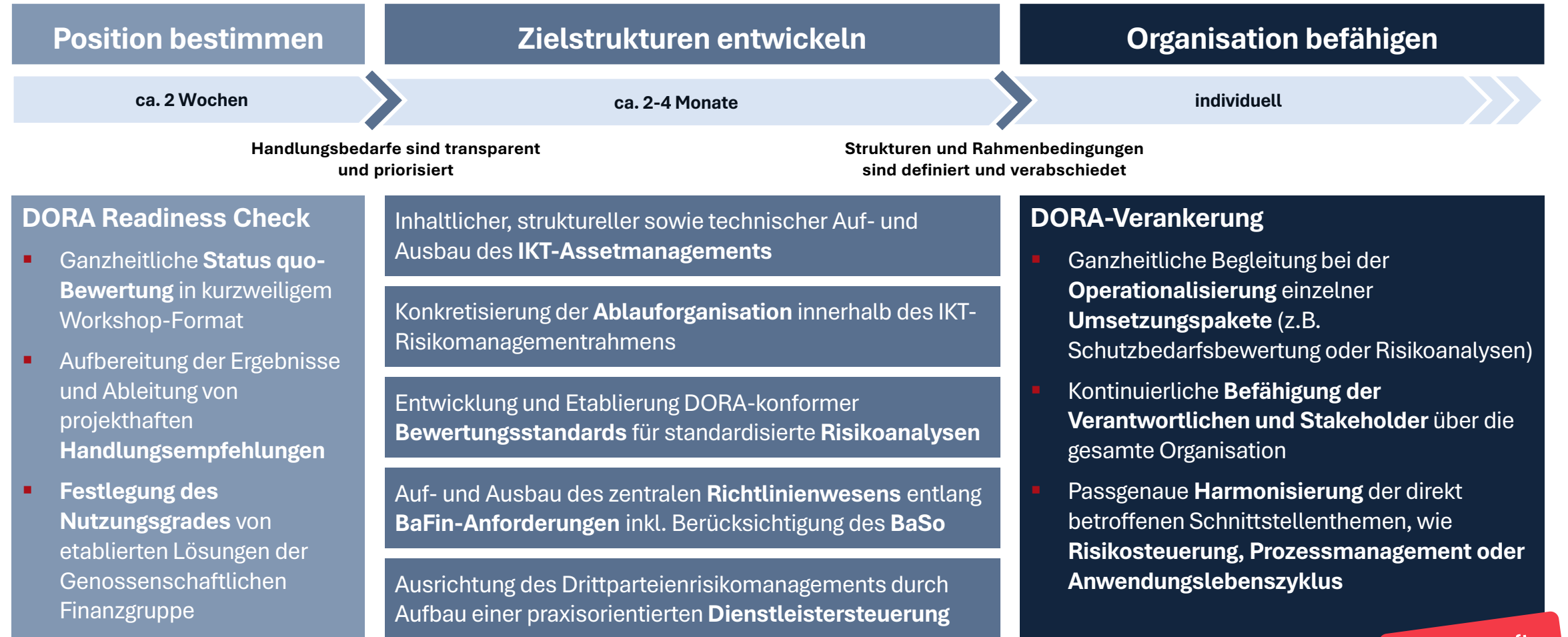
Geforderte Richtlinien und organisatorische Maßnahmen werden im SOLL passend für die Bank definiert und in einen klaren, risikoorientierten Umsetzungsplan zur Erreichung im IST überführt



Verantwortlichkeiten festigen und befähigen

Verantwortung für Prozesse validieren, Aufgaben für alle Verantwortlichkeiten explizit festlegen und Verantwortungsträger auf Basis definierter Anforderungen aus dem IKT-Risikomanagement befähigen

Das Vorgehen der EGC identifiziert klare Prioritäten und treibt eine ergebnisorientierte Umsetzung zentraler Compliance-Anforderungen



Beispielhaft

Wir liefern passgenaue Ergebnisse durch unsere umfangreiche Erfahrung aus einer Vielzahl von Projekten mit

1. Verzahnter Einsatz vorhandener Standards der genossenschaftlichen Finanzgruppe

- Prozesslandkarte der Genossenschaftsbanken als Basis im Prozess- und IKT-Assetmanagements
- Implementierung und Ausgestaltung von Muster-Arbeitsanweisungen der Verbände
- Praktische Erfahrung im Umgang mit Inhalten und Vorlagen des Verfahrenslieferanten

2. Implementierung ganzheitlich vernetzter und zentraler GRC-Tools

- Vollständiger Auf- und Ausbau von Forum ITR in der Informationssicherheit und BCM
- Integration von Forum OSM im Auslagerungsmanagement
- Integration von ZAM-AR im Auslagerungsmanagement

3. Unterstützung der genossenschaftlichen Finanzgruppe in zentralen Themen

- Entwicklung und Durchführung des ORG/IT-Benchmarking der GFG
- Praxiserprobte Erfahrung unserer Consultants im GFG-Umfeld als Banker und Berater
- Zusammenarbeit mit BVR, u.a. im Kontext Strategieagenda, Anwendungsdefinition, IT-Strategie



Unsere Experten beantworten gerne Ihre Fragen!



André Rapp
Partner

Telefon: +49 69 2475055-0
Mobil: +49 151 72042030
Mail: andre.rapp@eurogroupconsulting.de

EGC EUROGROUP CONSULTING AG
Thurn-und-Taxis-Platz 6
D-60313 Frankfurt am Main
www.eurogroupconsulting.de



Christian Storck
Senior Manager

Telefon: +49 69 2475055-0
Mobil: +49 171 3620998
Mail: christian.storck@eurogroupconsulting.de

EGC EUROGROUP CONSULTING AG
Thurn-und-Taxis-Platz 6
D-60313 Frankfurt am Main
www.eurogroupconsulting.de



Besuchen Sie uns auf
www.eurogroupconsulting.de
oder kontaktieren Sie Ihre
Ansprechpartner bei EGC!

EUROGROUP
CONSULTING