BEST PRACTICE BIBLIOTHEK FÜR REGULATORY COMPLIANCE

Modulbasiertes Referenzmodell für Nutzende des BOC Management Office

ADONIS
Business Transformation Suite

ADOIT
Enterprise Architecture Suite

ADOGRC
Your professional GRC Suite

WEBINAR

MATTHIAS PUTZLER
Management Consultant
BOC Group

DR. FELIX TIMM
Regulatory Compliance Consultant
QIRM Institut für Regulation & Management e.G.

Über QIRM

Das QIRM - Institut Regulation & Management (QIRM) konzentriert sich seit 2014 auf die praxisnahe Forschung und Entwicklung von anwendungsorientierten Standards, Referenzmodellen und IT-gestützten Lösungen für die aktuellen, vielfältigen Managementherausforderungen in regulierten Märkten. QIRM setzt sich aus Experten der Finanzmarktregulation sowie Fachleuten aus der Wissenschaft zusammen.

Gesellschaft

- Gegründet 2014 in Berlin
- 7 Genossenschaftsmitglieder

Referenzen

- Forschungsprojekt: IT gestützte Compliance im Finanzsektor | Bitkom e. V.
- BCM – Berufsverband der Compliance Manager

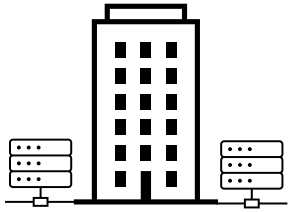
Regulation im Finanzsektor – Auswirkung auf Finanzinstitute und IT-Dienstleister

QIRM - Institut für Regulation & Management

Finanzinstitut

Übertragung der Anforderungen

Auslagerungsvertrag



IT-Dienstleister

Sicherstellung

Weiterverlagerung

Sub-Provider
(extern oder intern)

Gesetzliche Anforderungen:

- EBA-Richtlinien
- KWG, VAG, ZAG
- MaRisk, MaGo
- BAIT, VAIT, ZAIT
- GwG, DSGVO
- DORA

Anforderungen an IT-Dienstleister

- Risikomanagement
- Auslagerungsmanagement
- IT-Sicherheit, ISMS
- (IT-) Notfallmanagement
- Revision
- Reporting
- ISAE 3402 Report

Weiterverlagerung managen

- Leistungsabhängige Spiegelung der Anforderungen Richtung Provider
- Sicherstellung der Erfüllung durch Provider
- Regelmäßiges Monitoring

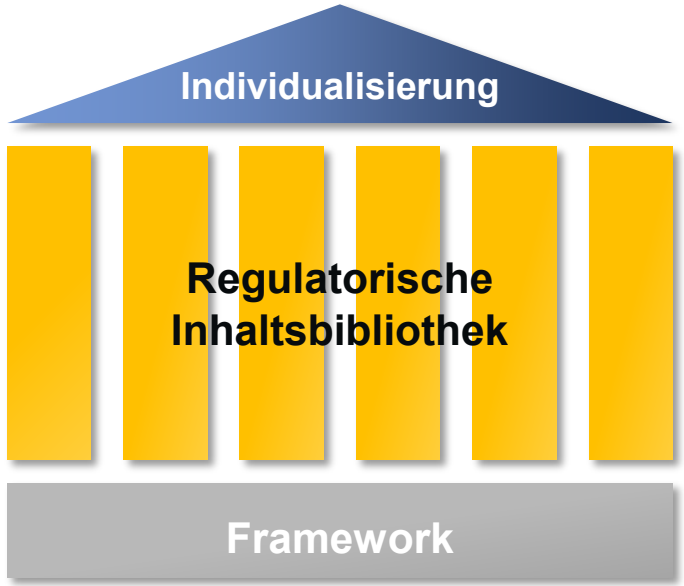
Auswirkung auf

- Aufbauorganisation
- Prozessorganisation
- Berichtswesen

GRC-Service: Integriertes Referenzmodell für Regulationsmanagement

QIRM - Institut für Regulation & Management

Ein Referenzmodell vereint alle notwendigen Managementprozesse für Governance, Risk and Compliance (GRC):



Module des Referenzmodells

z.B. Risk-Mgmt, BCM, Auslagerungen, ISMS, Geldwäsche, etc.

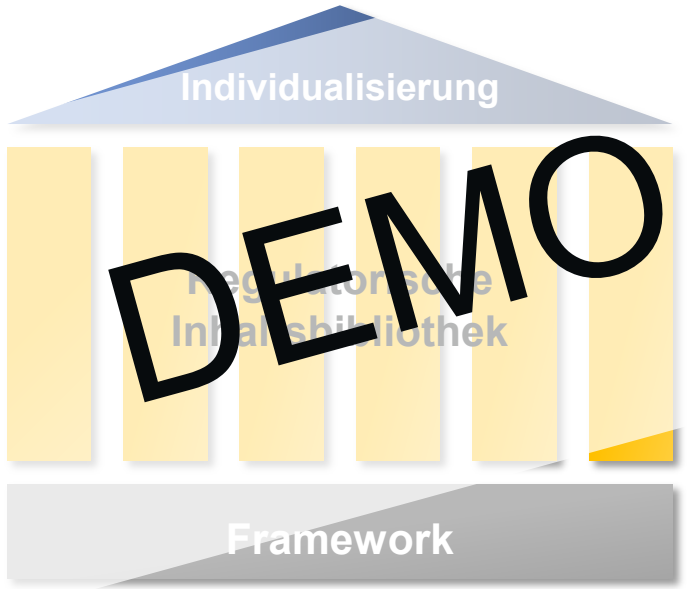
Auf Basis von: ADOIT Enterprise Architecture Suite

- „Single Source of Truth“ für Umsetzung regulatorischer Anforderungen
- „BaFin-ready“: Prüfungs- und Investitionssicherheit externer Audits
- Synergieeffekte zur Effizienzsteigerung nutzen
- Bereitstellung regulatorischer Templates & Reporting
- Pflege & Anpassung an neue Anforderungen

GRC-Service: Integriertes Referenzmodell für Regulationsmanagement

QIRM - Institut für Regulation & Management

Ein Referenzmodell vereint alle notwendigen Managementprozesse für Governance, Risk and Compliance (GRC):



Module des Referenzmodells

z.B. Risk-Mgmt, BCM, Auslagerungen, ISMS, Geldwäsche, etc.

DEMO im Tool

- „Single Source of Truth“ für Umsetzung regulatorischer Anforderungen
- „BaFin-ready“ Prüfungs- und Investitionssicherheit externer Audits
- Synergieeffekte zur Effizienzsteigerung nutzen
- Bereitstellung regulatorischer Templates & Reporting
- Pflege & Anpassung an neue Anforderungen

Auf Basis von: ADOIT Enterprise Architecture Suite

GRC-Service: Stakeholder und Nutzen

QIRM - Institut für Regulation & Management

Für wen ist der GRC-Service gedacht?

Stakeholder

Finanzinstitut

- Nutzung von Synergieeffekten dank integriertem Ansatz
- Kickstart bei Erfüllung neuer Anforderungen (z.B. DORA)
- Stakeholder-bezogenes Reporting

IT-Dienstleister

- Sicherheit bei der Schließung von IT-Auslagerungsverträgen
- Effiziente Umsetzung regulatorischer Anforderungen von Finanzkunden
- Nutzung praxiserprobter Vorlagen
- Kundenspezifisches Reporting

Nutzen

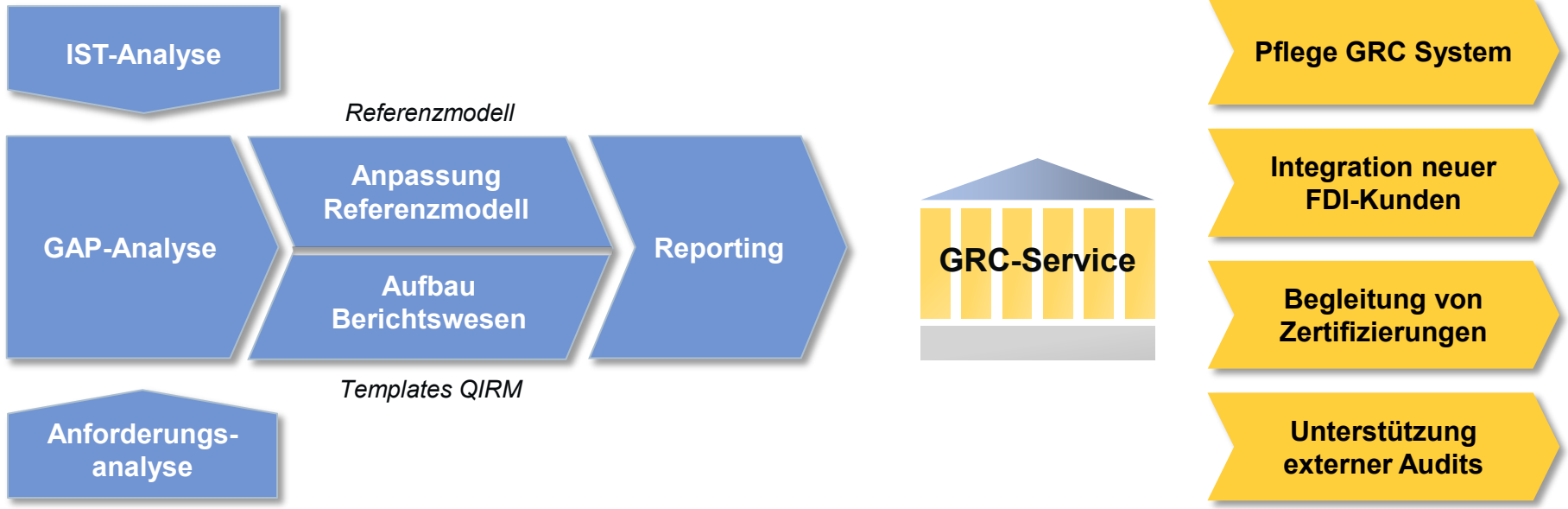
GRC-Service: Umsetzung + Bereitstellung

QIRM - Institut für Regulation & Management

Finanzinstitut

Was sind Triggerpunkte für Kunden?

IT-Dienstleister



Use Case: Digital Operational Resilience Act (DORA)

QIRM - Institut für Regulation & Management

Ziele

Harmonisierung	Schaffung eines einheitlichen und detaillierten Rahmenwerks für digitale Betriebsstabilität von EU-Finanzunternehmen
Resilienz	Stärkung der Sicherheit und operationalen Resilienz des gesamten europäischen Finanzsektors

Adressaten

u.a. Kreditinstitute, Zahlungsinstitute, Kontoinformationsdienstleister, E-Geld-Institute, Wertpapierfirmen, Anbieter von Krypto-Dienstleistungen, Versicherungsunternehmen, Ratingagenturen, IKT-Drittdienstleister

→ **ca. 3.600 (20.000) Finanzunternehmen in Deutschland (Europa) betroffen**

Anforderungen

IKT-Risikomanagement
Aufbau eines (vereinfachten) Risikomanagementrahmens

Management IKT-Drittparteien
Strategie für und Steuerung von IT-Drittdienstleistern

Testen der dig. op. Resilienz
Testprogramm zur digitalen operationalen Resilienz

IKT-Vorfallmeldewesen
Prozess zur Klassifikation von IT-Vorfällen, einheitliches Meldewesen

Kritische IKT-Drittdienstleister
direkte Überwachung erfordert GRC-Prozesse bei kritischen IKT-Dienstleistern

Informationsaustausch
Prozesse zum Informations- und Erkenntnisaustausch unter den Instituten

Use Case: Implikationen durch DORA

QIRM - Institut für Regulation & Management

Die DORA-Anforderungen erfordern die Anpassung und Erweiterung von bestehenden GRC-Prozessen.

Das Referenzmodell kennt diese Implikationen.

DORA-Anforderung

- IKT-Risikomanagement
- IKT-Vorfallmeldung
- op. Resilienz
- IKT-Drittparteien

Finden Sie alle Informationen im BOC Marketplace!

https://www.boc-group.com/de/newsletter/

- Bleiben Sie über aktuelle Nachrichten auf dem Laufenden
- Erhalten Sie Insider-Tipps
- Erfahren Sie als Erste:r von brandneuen Releases und neuen Produkten
- Werden Sie Teil von mehr als 15.000 aktiven Abonnenten