FINANZIERUNG
LEASING
FACTORING
FLF

5

SEPTEMBER 2022 · 69. JAHRGANG

Foto: Adobe Stock/Timelynx

DIGITALER SONDERDRUCK

Regulationsmanagement ganzheitlich gedacht

IT-Unterstützung durch Referenzmodell

Prof. Dr. Henning Herzog und Dr. Felix Timm, beide Mitglieder des Instituts für Regulation & Management e. G. (QIRM)

Regulationsmanagement ganzheitlich gedacht

IT-Unterstützung durch Referenzmodell

Finanzdienstleister sehen sich immer mehr regulatorischen Vorgaben ausgesetzt. Entsprechend muss das interne Regulationsmanagementsystem stetig angepasst und erweitert werden. Das bedeutet einen nicht zu unterschätzenden Mehraufwand für sämtliche Finanzinstitute unabhängig von deren Größe. Um weiterhin genügend Ressourcen für das Kerngeschäft zur Verfügung zu haben, hat das Forschungsinstitut für Regulation & Management einen ganzheitlichen Managementansatz entwickelt, der den betroffenen Instituten einschlägige Mehrwerte bietet. (Red.)

Leasing-, Factoring- und Absatzfinanzierungsinstitute (nachfolgend „Institute" genannt) sind stets daran interessiert, das Kerngeschäft der Finanzdienstleistungen zu optimieren und die eigenen Kompetenzen auszubauen. Gleichzeitig treibt der Gesetzgeber im Zuge der weltweiten Finanz- und Wirtschaftskrisen sowie der weiterhin auffallend zahlreichen Verfehlungen im Bereich der Compliance, Geldwäsche oder sonstiger strafbarer Handlungen die Regulierung der Banken-, Finanzdienstleistungs- und Versicherungsbranche weiterhin zügig voran.

Vor diesem Hintergrund sehen sich Institute einer permanent zunehmenden Regulationsdichte und -intensität ausgesetzt. Die damit steigenden regulatorischen Anforderungen bedingen die stetige Ausweitung und Anpassung ressourcenbindender Sicherungsmaßnahmen, welche Institute in Form eines Regulationsmanagementsystems umsetzen.

Status quo bei Instituten

Als Konsequenz agieren Institute im Spannungsfeld zwischen stetiger Geschäftsentwicklung mit einhergehender Optimierung wertschöpfender Prozesse auf der einen und der Umsetzung sowie Verwaltung stetig steigender regulatorischer Anforderungen auf der anderen Seite. Im Letzteren verdeutlichen sich organisatorische Mehraufwände, denen betroffene Institute entgegenblicken. Trotz geltendem Proportionalitätsprinzip nehmen Gesetzgeber und Wirtschafts- beziehungsweise IT-Prüfer auch kleine und mittelständische Institute in die Pflicht, die umfangreichen Anforderungen wie zum Beispiel Geldwäscheprävention, Compliance, Risikomanagement oder Auslagerungsmanagement in voller Gänze umzusetzen.

Dabei steigen auch die Sicherheitsanforderungen an genutzte Informationssysteme. So verlangt die letzte Novelle der Bankaufsichtlichen Anforderungen an die IT (BAIT) vom August 2021 ein ausgeweitetes Informationssicherheitsmanagement und IT-Notfallmanagement auch von Finanzdienstleistungsinstituten. Zwar gibt der Gesetzgeber einen Ergebniszustand vor, lässt die Art und Weise wie Institute diesen erreichen jedoch häufig offen. Zunehmend orientieren sich diese Vorgaben an umfangreichen Managementsystemen wie Informationssicherheit nach ISO 27001, ISO 9001 oder Notfallmanagement nach BSI 100-4. Deren Implementation verlangt jedoch einen großen Ressourceneinsatz.

Folgende Situation lässt sich daher in der Praxis beobachten: Institute schaffen innerhalb ihrer Organisation verantwortliche Stellen, welche ausschließlich bestimmte regulatorische Themen in der Organisation umsetzen (zum Beispiel Geldwäsche-, Risiko- oder Notfallbeauftragter). Dabei stellt das Berichtswesen eine zentrale Aufgabe dar, da Berichte die Grundlage für Prüfungen bilden. Termin- und ereignisgetrieben werden somit eine Vielzahl verschiedener Dokumente erstellt – oft auf Basis von vorhandenen Vorjahresberichten. Sie dokumentieren Richtlinien, etablier-

Foto: Tobias Kruse/Ostkreuz

PROF. DR. HENNING HERZOG

ist Mitglied des Instituts für Regulation & Management e. G. (QIRM), Berlin.

E-Mail:
henning.herzog@qirm.org

Foto: Thomas Rahr

DR. FELIX TIMM

ist Mitglied des Instituts für Regulation & Management e. G. (QIRM), Berlin.

E-Mail:
felix.timm@qirm.org

te Prozesse, genutzte IT-Systeme und anderweitig geforderte Nachweise.

An vielen Stellen existieren Schnittstellen zwischen den einzelnen Regulationsanforderungen. Dennoch ist es eine große Herausforderung, diese Schnittstellen zu identifizieren und miteinander abzustimmen. Auch wenn am Markt Software angeboten wird, die konkrete Bereiche wie das Risikomanagement unterstützt, fehlt eine integrierte Sicht auf das Regulationsmanagement. Dies führt zu redundanten Informationen, die oftmals unabhängig voneinander gepflegt werden. Schlussendlich entstehen somit regulatorische Inkonsistenzen, die nicht mehr verwaltbar sind und deren Klärung hohen Aufwand bedarf. Kurz gesagt – die meisten der heute in den Instituten gelebten Regulationsmanagementsysteme sind ineffizient.

An der Stelle knüpft dieser Beitrag an, indem ein ganzheitlicher Ansatz für Regulationsmanagement vorgestellt wird. Der Ansatz wurde vom Forschungsinstitut für Regulation & Management e. G. (QIRM) entwickelt. Er basiert auf langjährigen praktischen Erfahrungen im Bereich Governance, Risk und Compliance der Finanzindustrie, welche in verschiedenen anwendungsorientierten Forschungsprojekten verprobt wurden. Grundlage bildet das Konzept der Unternehmensmodellierung, welches komplexe organisatorische Sachverhalte darstellbar und Managementsysteme verwaltbar macht.

Ganzheitliches Regulationsmanagement

Schlussfolgernd stehen regulierte Institute heute vor der Aufgabe, ein System zur effektiven, aber auch effizienten Umsetzung regulatorischer Anforderungen aufzubauen. Solch ein Regulationsmanagementsystem muss das Ziel verfolgen, mit minimaler Ressourcenbindung regulatorische Anforderungen proaktiv sicherzustellen und zu managen. Nur so können Institute weiterhin den Fokus auf das Kerngeschäft legen. Anhand dieser Anforderung ergibt sich die Fragestellung, wie solch ein Regulationsmanagementsystem gestaltet sein muss.

Bei genauerer Analyse einzelner Gesetze lässt sich feststellen, dass sich die Anforderungen auf Organisationsstruktur, Prozessgestaltung, Informationssysteme sowie Berichtswesen auswirken. Dies lässt sich am Beispiel des Notfallmanagements nach Mindestanforderungen an das Risikomanagement (MaRisk) und den BAIT kurz verdeutlichen: Neben der Entwicklung eines Notfallkonzepts und einer Notfallorganisation sind Institute zusätzlich dazu verpflichtet, ein Berichtswesen des Notfallmanagements (unter anderem Schulungsdokumentation, Notfalltests, Notfallbericht) sowie einen Notfallmanagementprozess zu etablieren, welcher sich zum Ziel setzen muss, das implementierte Notfallmanagement kontinuierlich zu verbessern (siehe MaRisk AT 7.3 sowie BAIT II.10).

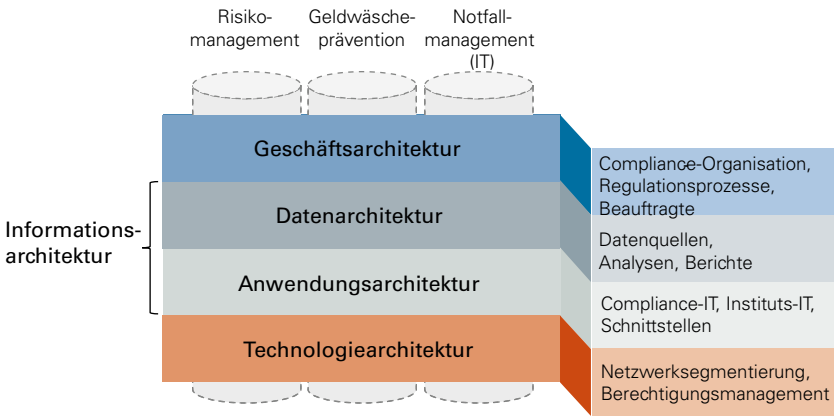
Ähnliche Anforderungen ergeben sich aus anderen Bereichen der MaRisk und BAIT (etwa Risiko- oder Auslagerungsmanagement und Informationssicherheit) sowie der Mindestanforderungen an die Compliance, dem Geldwäschegesetz oder der Datenschutz-Grundverordnung. Die Regulationssituation von Instituten lässt sich daher folgendermaßen zusammenfassen:

- gesetzliche Anforderungen sind heterogen und werden stetig erweitert,
- die konkrete Ausgestaltung von teilweise undeutlichen Anforderungen obliegt den Instituten,
- benannte Anforderungen wirken auf Organisationsstruktur, wertschöpfende und unterstützende Geschäftsprozesse der IT-Infrastruktur und erfordern ein Berichtswesen,
- Instituten fehlt eine integrierte Umsetzung der verschiedenen Normen und Gesetzen.

Um Institute bei diesen Herausforderungen zu unterstützen, wird ein ganzheitliches und wissenschaftlich gestütztes Regulationsmanagement vorgestellt, welches folgendes übergeordnetes Ziel verfolgt: Statt eine organisatorische Optimierung einzelner Normen voranzutreiben, muss das Ziel sein, standardisierte, revisions- und investitionssichere Lösungen zur strukturierten und proaktiven Übersetzung von Normen in organisatorische und informationstechnologische Maßnahmen zu entwickeln.

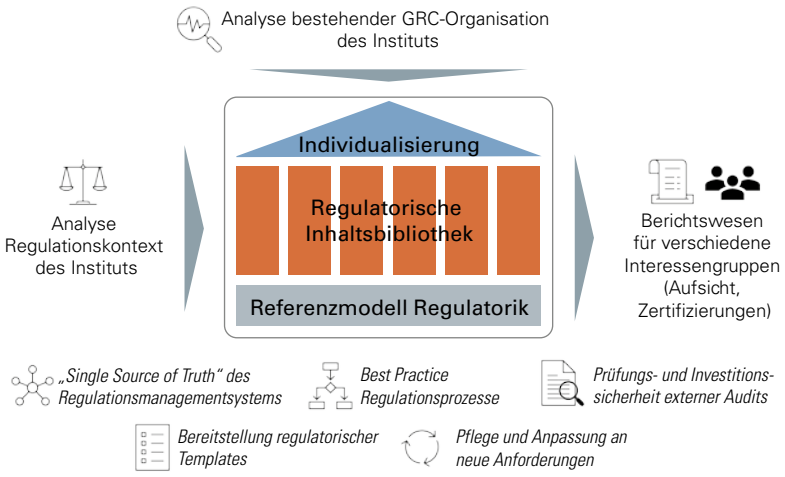
Solch ein ganzheitlicher Ansatz darf regulatorische Anforderungen nicht nur in aufbau- und ablaufbezogene Aufgaben übersetzen, sondern muss relevante Daten und unterstützende Informationssysteme mit ihnen in Beziehung setzen. Diese Herangehensweise beseitigt die aktuellen Probleme der Institute, der Bankenaufsicht und von Marktteilnehmern wie IT-Anbietern; vielmehr wird dadurch deren Zusam-

Abbildung 1: Perspektiven auf eine Organisation



Quelle: QIRM

Abbildung 2: Individuelle Anpassung des Referenzmodells



Quelle: QIRM

menarbeit gefördert. Für das einzelne Institut bedeutet dies effektive Umsetzung von Anforderungen, transparente Dokumentation sowie die Freisetzung von Kapazitäten für das Kerngeschäft.

IT-gestütztes Referenzmodell

Eine zentrale Herausforderung bei der Umsetzung der komplexen Regulationslandschaft ist die ganzheitliche Verortung innerhalb eines Instituts. Um einzelne gesetzliche Anforderungen in die Praxis von Instituten übersetzbar zu machen, wurde ein IT-gestütztes Referenzmodell für Regulationsmanagementsysteme in der Finanzindustrie entwickelt.

Referenzmodelle sind ein bewährter Ansatz aus dem Forschungsfeld der Wirtschaftsinformatik, um für bestimmte Anwendungsgebiete den typischen oder empfohlenen Aufbau von Unternehmensstrukturen und deren Zuordnung zu IT-Lösungen zu definieren. Beispiele sind das Referenzmodell für die Telekommunikationsindustrie[1)] oder die Referenzarchitektur für Industrie-4.0-Lösungen[2)]. Referenzmodelle unterstützen dabei, die Kosten der Organisationsentwicklung zu senken und die Effizienz sowie Qualität von Abläufen zu erhöhen. So muss eine Organisation nicht mehr komplett eigenständig eine für sich geeignete Lösung entwickeln, sondern kann eine Referenz als Bauplan verwenden. Dieser Bauplan wird dann auf die individuellen Bedarfe einer einzelnen Organisation angepasst. Stark regulierte Branchen wie die Finanzdienstleistungsbranche eignen sich gut für den Einsatz von Referenzmodellen, um notwendige Strukturen neben dem Kerngeschäft erfolgreich zu implementieren.

Auf Basis von Praxis- und Projekterfahrungen sowie wissenschaftlichen Erkenntnissen interpretiert das Referenzmodell gesetzliche Anforderungen und kann diese auf die Bedürfnisse von regulierten Instituten überführen. Dabei beantwortet das Referenzmodell Fragen, die bei der Umsetzung neuer Gesetze und Normen relevant sind:

- Welche organisatorischen Rollen muss das Institut definieren?
- Welche Prozesse müssen implementiert werden und wie sind diese auszugestalten?
- Welche Anforderungen ergeben sich für das Berichts- und Meldewesen?
- Welche IT-Systeme helfen bei der Umsetzung?
- Welche Synergien existieren zwischen verschiedenen Gesetzesvorgaben?

Um diese Fragestellungen systematisch zu beantworten und dieses Wissen zeitstabil festzuhalten, genügt ein klassisches Prozessmanagement nicht mehr. Daher nutzt das Referenzmodell ArchiMate®. Diese standardisierte und in der Praxis bereits etablierte Modellierungssprache ermöglicht es, über den Tellerrand von Prozessmanagement zu schauen und integriert oben skizzierte Fragestellungen in einem Unternehmensmodell. Solch ein Modell dient dazu, das Zusammenspiel zwischen organisatorischen und geschäftlichen Tätigkeiten in Unternehmen mit den informationstechnischen Abläufen und Strukturen zu planen.[3)]

Dabei hat es sich bewährt, verschiedene Perspektiven auf eine Organisation zu unterscheiden (Abbildung 1): Die Geschäftsarchitektur enthält die zentralen Geschäftsprozesse und deren Verankerung in den Organisationstrukturen. Die Informationsarchitektur beschreibt, wie die geschäftlichen Tätigkeiten durch die IT unterstützt werden und welche Informationen sowie Formulare genutzt werden müssen. Die Informationsarchitektur ist daher in Daten- und Anwendungsarchitektur unterteilt. Während die Anwendungsarchitektur Softwarekomponenten und notwendige Schnittstellen dokumentiert, analysiert die Datenarchitektur die für die geschäftliche Architektur erforderlichen Daten und deren Verarbeitung. Die Technologiearchitektur enthält die technische Infrastruktur mit Netzwerken, Serversystemen und Kommunikationskomponenten.

Innerhalb und vor allem auch zwischen allen Architekturebenen bestehen Verknüpfungen, die die gegenseitige Abhängigkeit der Ebenen ausdrücken und mittels Regeln konkretisiert werden können. Auf diese Weise verortet das Referenzmodell die organisatorischen Anforderungen verschiedener Gesetze, Normen und Richtlinien und kann Potenziale für Synergien herausstellen. Die geschilderten Zusammenhänge lassen sich visuell greifbar machen. Darüber hinaus verbirgt sich im Hintergrund ein wissendes System, welche alle existierenden Beziehungen kennt und somit analysierbar macht.

Für jeden Regulationsbereich existieren die beschriebenen Betrachtungsweisen und Querverbindungen. Beispielsweise hängt das Risikomanagement von Ergebnissen anderer Bereiche wie Auslagerungs-, Informationssicherheit- und Notfallmanagement ab. Während Gesetzestexte diese Verbindungen nur erwähnen, lassen sich die Zusammenhänge verständlich als Unternehmensmodell darstellen. Das Referenzmodell kennt diese Zusammenhänge.

Umsetzung in der Praxis

Mithilfe des Referenzmodells kann ein IT-gestütztes Regulationsmanagement für einzelne Institute abgeleitet werden. Das Referenzmodell wird im Rahmen einer Ist-Analyse auf das Institut angepasst. Dies geschieht auf Basis des individuellen regulatorischen Kontexts und den bereits existierenden Regulationspraktiken des Instituts. Dabei kann auf eine Vielzahl sogenannter Bibliotheken einzelner Regulationsthemen aus MaRisk, BAIT oder Geldwäschegesetz zurückgegriffen werden, welche je nach Situation des Instituts genutzt werden können. Bereits bestehende Prozessdokumentationen und Dokumente werden dabei wiederverwendet und in das System integriert. Nach der Umsetzungsphase kann das System zur Verwaltung der regulatorischen Anforderungen genutzt werden und unterstützt ein Stakeholder-spezifisches Berichtswesen.

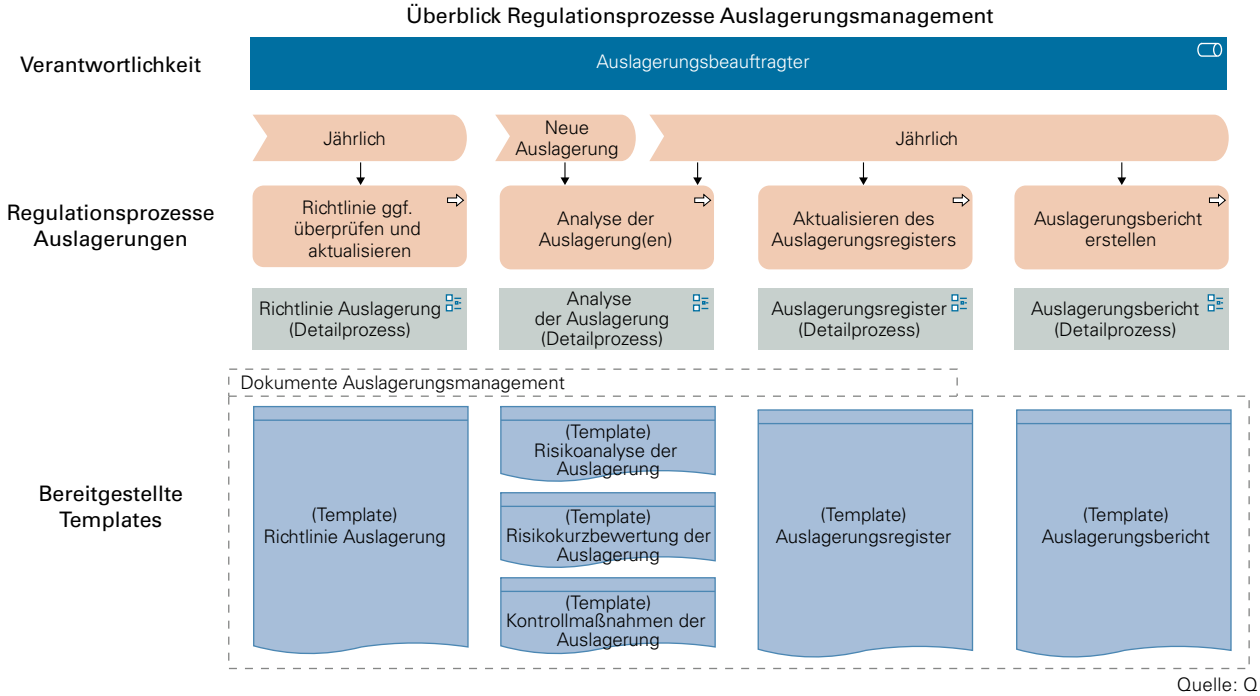
Auch wenn die institutsinterne Sichtweise im Fokus steht, bedeutet ganzheitliches Regulationsmanagement auch die Berücksichtigung externer Stakeholder und deren Anforderungen. Externe Adressaten (etwa Aufsichtsbehörden, Zertifizierungsgesellschaften, Kunden, Partner) eines Regulationsmanagementsystems werden vom Referenzmodell abgebildet. Es systematisiert daher auch konkrete Anforderungen aus Gesetzen und Normen, die ein einheitliches Vorgehen vereinfachen. Der vorgestellte Ansatz wird in Abbildung 2 vereinfacht dargestellt.

Der Charakter eines IT-gestützten Regulationsmanagementsystems zeichnet sich durch folgende Aspekte aus. Das individuelle Regulationsmanagementsystem wird dem Institut dabei softwaregestützt bereitgestellt. Die Software unterstützt den oben beschriebenen Modellierungsansatz und bietet dabei unter anderem diese Funktionalitäten:

- nachvollziehbare Integration von Organisationsstruktur, Regulationsprozessen, IT-Systemen und Dokumenten,
- Überblick für Beauftragte zu regulatorischen Aufgaben,
- Überblick zu erstellender Analysen/Dokumente/Berichte,
- Bereitstellung von regulatorischen Templates,
- Verlinkung zu datenführenden Systemen wie Dokumenten- oder Risikomanagementsystemen, Meldewesen oder IT-Service-Managementtools,
- Berichterstattung aus dem System zur Unterstützung von Prüfungen.

Abbildung 3 zeigt dabei einen vereinfachten Ausschnitt des Referenzmodells aus dem Bereich Auslagerungsmanagement. Dargestellt sind ausgewählte wesentliche Prozesse des

Abbildung 3: Fokus auf das Auslagerungsmanagement



Quelle: QIRM

Auslagerungsmanagements auf höchster Ebene. Das System verortet, wer verantwortlich für die Prozesse ist, in welcher Regelmäßigkeit diese durchgeführt werden müssen und stellt passende Templates bereit. Für jeden Prozess existieren mehrstufige Detailprozesse.

Ein wesentlicher Vorteil bei diesem IT-gestützten Ansatz ist, dass gesetzliche Änderungen oder neue regulatorische Anforderungen einfach im System verortet und ohne größeren Mehraufwand umgesetzt werden können. Sollten sich gesetzliche Anforderungen ändern, lassen sich diese zwischen bereitgestelltem Referenzmodell und Institutslösung automatisch per Gap-Analyse umsetzen.

Effizienz statt Aufwand

Ob Jahresabschluss- oder IT-Prüfung – der Prüfprozess gestaltet sich oft langwierig und erfordert die Bereitstellung unzähliger Dokumente sowie Nachweise, welche oft verteilt abgelegt sind. Besonders die Sichererstellung von Auslagerungen rückt fortschreitend in den Fokus der Aufsicht. Geeignete Mittel zur Überwachung von Auslagerungsverhältnissen sind gerade vor dem Hintergrund der vermehrten Nutzung von IT-Dienstleistern notwendig. Mit dem beschriebenen IT-gestützten ganzheitlichen Ansatz lässt sich somit ein zentraler Ort zum Management von Regulationsanforderungen schaffen. Zum einen dokumentiert dieser, wie das Institut Anforderungen in der Organisation umsetzt. Zum anderen hilft er Verantwortlichen im Institut dabei, sich auf ihre wesentlichen Aufgaben zu fokussieren, indem er klare Prozesse aufzeigt und notwendige Vorlagen enthält.

Aufgrund des IT-gestützten Charakters lassen sich per Knopfdruck maßgeschneiderte Berichte über das Institutmanagementsystem erstellen, die dem Prüfer, der Aufsicht oder anderen Interessengruppen zur Verfügung gestellt werden können. Dies vereinfacht das Ausfüllen immer länger werdender Anforderungskataloge der Prüfer und unterstützt den Anspruch nach mehr Transparenz.

Auch im Bereich von IT-Auslagerungen unterstützt der Ansatz. Um das Kerngeschäft abzubilden, entscheiden sich Institute oftmals dazu, die Bereitstellung und den Betrieb von IT-Systemen an Dienstleister auszulagern. Dies hat jedoch erhebliche Konsequenzen für das Governance-, Risk- und Compliance-System (GRC). Es lässt sich ein steigender Regulationsaufwand bei der Sicherstellung von Auslagerungsverhältnissen nach MaRisk AT 9 und insbesondere den BAIT feststellen. Gerade im Bereich IT-Auslagerungen vergrößern sich die Anforderungskataloge von Aufsicht und Wirtschaftsprüfern stetig. Dies führt zu einem weiteren Verwaltungsaufwand bei den Instituten. Hinzu kommt, dass entsprechende IT-Dienstleister oftmals weder über das regulatorische Know-how noch die dafür notwendigen Regulationsprozesse verfügen, was den Beschaffungsprozess von Informationssystemen erschwert.

Zusammengefasst bietet der Ansatz folgende Mehrwerte für Institute:

- **Zeitstabilität:** integrierte Umsetzung regulatorischer Anforderungen auf Basis eines stetig gepflegten Referenzmodells, leichte Anpassbarkeit bei neuen Anforderungen,
- **Prüfungssicherheit:** bedarfsgerechtes Reporting für Audits,
- **Wissensspeicher:** Quelle für Organisationswissen bezüglich Regulationsthemen,
- **Verwaltbarkeit:** rollenabhängige Übersicht durchzuführender Aktivitäten.

Unsere Erfahrungen aus der Praxis zeigen außerdem, dass ein ganzheitlich gedachtes Regulationsmanagement dabei hilft, Mitarbeiter in den unterschiedlichen Bereichen der Regulatorik zu schulen und zu sensibilisieren. Ein wenig weitergedacht, lassen sich mithilfe des Modellansatzes auch Brücken zu wertschöpfenden Prozessen des Finanzierungsgeschäfts schlagen, um diese stetig an neue regulatorische Herausforderungen anzupassen. Darüber hinaus können andere Managementsysteme in das Regulationsmanagementsystem integriert werden, da diese ebenfalls ganzheitliche organisatorische Anforderungen stellen.

Gemeinschaftsgestützter Ansatz

Bekanntermaßen existieren am Markt bereits viele Anbieter, welche spezialisierte Produkte für verschiedene Regulationsfelder wie Geldwäscheprävention, IT-Sicherheit oder Risikomanagement anbieten. Zwar sind solche Expertensysteme notwendig, um technische Anforderungen zu erfüllen, sie sind dennoch nur ein Teil eines ganzheitlichen Regulationsmanagements. Aufgrund der Vielzahl an Gesetzen, Normen und Richtlinien ist es jedoch für Institute jeglicher Größe wichtig, Regulationsmanagement ganzheitlich zu denken und zu leben. An dieser Stelle knüpft der vorgestellte Ansatz an.

Ein wesentlicher Erfolgsfaktor des Referenzmodells liegt in der stetigen Weiterentwicklung. Diese lässt sich in verschiedenen Dimensionen denken. Auf der einen Seite wird das Referenzmodell regelmäßig um weitere Gesetze oder Richtlinien erweitert. Auf der anderen Seite werden Aktualisierungen bestehender Gesetze – siehe unter anderem BaFin Rundschreiben 10/2021 bezüglich der neuesten MaRisk-Novelle – in dem Referenzmodell gepflegt. Das Forschungsinstitut etabliert dafür eine Community für ganzheitliches Regulationsmanagement von Finanzdienstleistern. Diese Community macht es sich zum Ziel, eine Schnittstelle zwischen Anforderungen auf Aufsichtsseite und der praktischen Umsetzung auf Institutsseite aufzubauen. Das vorgestellte Referenzmodell kann als ein zentraler Baustein davon verstanden werden.

Fußnoten

1) TM Forum, https://www.tmforum.org/tm-forum-frameworx-2/

2) Heidel/Hoffmeister et al., 2017, Basiswissen RAMI4.0: Referenzarchitekturmodell mit Industrie 4.0-Komponente, in: Industrie 4.0.

3) Hanscke, 2022, Enterprise Architecture Management – einfach und effektiv. Ein praktischer Leitfaden für die Einführung von EAM; Lankhorst, 2017, Enterprise Architecture at Work: Modelling, Communication and Analysis. The Enterprise Engineering Series.