Das Ende der Abschlussprüfung: Warum punktuelle Compliance unter DORA nicht mehr ausreicht

Die Logik der regulatorischen Aufsicht ändert sich: Digitale Resilienz bedeutet heute mehr als nur periodische Tests oder einzelne Release-Gates. Vielmehr ist eine dauerhafte Nachweisfähigkeit entscheidend. In Zukunft müssen Finanzunternehmen jederzeit nachweisen können, dass ihre Systeme stabil, kontrolliert und regelkonform arbeiten.

Björn Eckmayer

FOTO: MOHAMED_HASSAN/PIXABAY

Über Jahre hinweg setzte die Versicherungsbranche auf ein IT-Denkmodell, das lange Zeit als verlässlich galt: die Abschlussprüfung als zentraler Kontrollmechanismus. Regulatorische Anforderungen wurden am Ende eines Projekts oder unmittelbar vor der Bereitstellung geprüft. Compliance fungierte dabei als nachgelagerte Instanz zwischen Entwicklung und Betrieb.

Dieses Modell gerät zunehmend unter Druck. Der Perspektivwechsel ist fundamental: Die Frage lautet nicht mehr „War das Release compliant?", sondern „Ist der laufende Betrieb jederzeit nachweislich compliant?". DORA wirkt dabei weniger wie ein weiteres Regelwerk, sondern vielmehr wie ein struktureller Einschnitt in Governance- und IT-Steuerungslogiken.

Das alte Prüfmodell entstand in einer Zeit mit langen Release-Zyklen, stabilen Kernsystemen und klar getrennten Verantwortlichkeiten zwischen den Bereichen Entwicklung, Betrieb und Kontrolle. In der Praxis kamen manuelle Checklisten, dokumentationsbasierte Nachweise und sequenzielle Übergaben zum Einsatz. Ein praktikables Modell, jedoch nur, solange Änderungen selten und IT-Landschaften überschaubar sind.

Heute bewegen sich Versicherer in hybriden Architekturen, die aus Legacy-Systemen, Cloud-Anwendungen, Komponenten von Drittanbietern sowie KI-gestützten Prozessen bestehen. Releases erfolgen häufiger, Produkte gewinnen an Komplexität und regulatorische Anforderungen werden dynamischer. Gleichzeitig steigen die Erwartungen von Kunden und Aufsichtsbehörden. In diesem Umfeld darf Agilität kein leeres Versprechen bleiben, sondern muss sich in stabilen, kontrollierten Prozessen widerspiegeln. Genau hier entsteht ein Zielkonflikt: Punktuelle Prüfungen treffen auf kontinuierliche Veränderung und verlieren so an Wirksamkeit.

DIE VERSICHERUNGSWIRTSCHAFT IST BESONDERS BETROFFEN

Während Banken ihre Prüfprozesse bereits stark professionalisiert haben, stehen viele Versicherer noch vor dem strukturellen Umbau ihrer Governance-Logik. In der Regel nutzen sie langlebige Kernsysteme, die nur schrittweise aktualisiert werden. Eine „Big-Bang-Ablösung" ist teuer, komplex und riskant. Wichtige Transformationsinitiativen wie die Migration in die Cloud, die Öffnung von APIs oder die datengetriebene Produktentwicklung müssen dagegen mit deutlich höherem Tempo neben dem eigentlichen Kernsystem weiterentwickelt oder sogar gänzlich neu konzipiert werden.

Hinzu kommt, dass ein erheblicher Teil der eingesetzten Software extern bezogen wird. Das heißt: Während die zentralen Geschäftsprozesse häufig über Standardlösungen abgewickelt werden, kommen einzelne Sparten oder Zusatzleistungen über spezialisierte Anbieter zum Einsatz. Doch auch bei zugekaufter Software bleibt die regulatorische Gesamtverantwortung beim Versicherer. Die Nachweisfähigkeit muss unabhängig vom Hersteller gewährleistet sein. DORA trifft deshalb in vielen Unternehmen auf eine IT-Realität, die aufgrund ihrer historischen Entwicklung nicht auf kontinuierliche Prüfmechanismen ausgelegt war.

COMPLIANCE ALS DURCHGEHENDER PROZESS

„Continuous Governance" ermöglicht es, Compliance an das Tempo der modernen IT anzupassen. Regulatorische Anforderungen werden nicht mehr nur dokumentiert und am Ende geprüft, sondern als technisch überprüfbare Regeln direkt in Entwicklungs- und Betriebsprozesse integriert. Das bedeutet konkret, dass Prüfungen bereits in CI/

Klassische Compliance-Logik vs. Continuous Governance

Dimension	Klassische Compliance-Logik	Continuous Governance
Grundverständnis	Compliance als Pflichtübung und Kontrollinstanz	Compliance als integrierter Bestandteil des Entwicklungs- und Betriebsprozesses
Zeitpunkt der Prüfung	Nachgelagert (Abnahme, Release-Gate, Audit)	Kontinuierlich bei jeder Codeänderung / in jeder CI/CD-Pipeline
Prüfmechanismus	Manuelle Reviews, Checklisten, Freigaben	Automatisierte Policies, regelbasierte Prüfungen, technische Kontrollmechanismen
Nachweisführung	Dokumentationsbasiert (Berichte, Protokolle)	Systemisch erzeugte Audit-Trails, versionierbar und reproduzierbar
Organisationslogik	Trennung von Dev, Ops und Compliance	Verzahnung von IT, QA, Compliance und Betrieb
Rollenverständnis	Compliance prüft am Ende	Compliance wirkt von Anfang an mit („Shift Left")
Audit-Vorbereitung	Ad-hoc-Taskforces, Vorbereitungsphasen	„Audit-ready by design"
Wirtschaftliche Wirkung	Compliance als Kostenblock	Compliance als Stabilitäts- und Effizienzhebel

CD-Pipelines stattfinden, noch bevor Code produktiv wird. Dabei werden Vorgaben nicht mehr als Textdokumente abgelegt, sondern als maschinenlesbare Richtlinien formuliert. Jede Codeänderung durchläuft automatisiert diese Prüfinstanzen. Parallel dazu entstehen lückenlose, versionierbare Audit-Trails, die jederzeit nachvollziehbar machen, welche Anforderung zu welchem Zeitpunkt erfüllt wurde.

Damit verlässt Compliance ihre Rolle als nachgelagertes Gate. Systeme sind nicht erst auditfähig, wenn eine Prüfung ansteht, sondern sie sind „audit-ready by design". Künstliche Intelligenz kann diesen Prozess unterstützen, etwa bei der Ableitung von Prüfregeln oder der Analyse von Anomalien. Sie ersetzt jedoch nicht die Verantwortung. Ein „Expert-in-the-Loop"-Ansatz bleibt notwendig, um Qualität, Kontext und ethische Dimensionen zu sichern.

GESCHWINDIGKEIT DURCH STRUKTUR

Continuous Governance ist kein reines Kontrollinstrument, sondern verändert die bisherige Vorgehensweise bei Releases grundlegend. Während manuelle Freigabeschleifen früher Tage oder Wochen in Anspruch nahmen, greifen nun automatisierte Prüfmechanismen in Echtzeit. Dadurch verkürzen sich die Release-Zyklen, die Anzahl der Audit-Befunde nimmt ab und der Wiederholungsaufwand sinkt. Knappe Expertenressourcen werden dort eingesetzt, wo Urteilskraft gefragt ist, nicht dort, wo Regeln maschinell abgeprüft werden können.

Praxiserfahrungen zeigen: Unternehmen, die regulatorische Prüfungen systemisch in ihre Pipelines integrieren, gewinnen messbar an Tempo und Planbarkeit. Diese Planbarkeit ist wiederum Voraussetzung für Innovation, gerade in einem Markt, in dem Insurtechs bei Geschwindigkeit und Kundenzentrierung vorlegen. Damit wird Governance vom Kostenfaktor zur infrastrukturellen Voraussetzung für Wettbewerbsfähigkeit.

DAS RISIKO DES „DAS HABEN WIR SCHON IMMER SO GEMACHT!"

Das Festhalten an veralteten Prüfmethoden erzeugt eine trügerische Sicherheit. Wer regulatorische Anforderungen nur punktuell überprüft, verschiebt das Risiko, anstatt es zu beseitigen. In hybriden IT-Landschaften mit hoher Release-Frequenz entstehen zwischen Releases, Systemänderungen und Updates von Drittanbietern blinde Flecken, die sich nicht mehr schließen lassen. Diese Lücken werden oft erst im Audit oder im Ernstfall sichtbar, und dann ist es häufig bereits zu spät.

> **Wer regulatorische Anforderungen nur punktuell überprüft, verschiebt das Risiko, anstatt es zu beseitigen.**

Der Umgang mit ausgelagerten Cloud-Services verdeutlicht die Dimension dieses Problems. Werden Lizenzvorgaben, Sicherheitsanforderungen oder Verfügbarkeitskriterien nicht kontinuierlich überwacht, entsteht ein Risiko, das weit über formale Beanstandungen hinausreicht. Reputationsschäden, IP-Verluste und Betriebsunterbrechungen sind keine hypothetischen Szenarien, sondern dokumentierte Risiken.

DORA verschärft diese Realität noch einmal grundlegend, denn die regulatorische Verantwortung endet nicht mehr am eigenen Systemrand. Auch Drittanbieter, Schnittstellen und KI-gestützte Module fallen in den Geltungsbereich – und damit in die Nachweispflicht des Versicherers.

GOVERNANCE ALS SYSTEMFRAGE, NICHT ALS TOOLBOX

Bei Continuous Governance geht es nicht um die Einführung neuer Tools. Im Mittelpunkt steht keine neue Software, sondern eine neue Herangehensweise. Entscheidend ist, geschäftskritische Prozesse und Systeme an den Stellen zu identifizieren, an denen Betriebsstabilität und regulatorische Nachweisfähigkeit unmittelbar zusammenfallen. Genau dort muss Governance in die bestehenden Entwicklungs- und Betriebsmodelle integriert werden.

Dies setzt voraus, dass die Verantwortlichkeiten zwischen den Bereichen IT, QA und Compliance klar abgestimmt sind und die regulatorischen Anforderungen technisch prüfbar formuliert werden. Die Grundlage dafür ist Datenqualität, denn ohne sie bleiben automatisierte Kontrollen Makulatur.

Mit DORA verschiebt sich der regulatorische Maßstab dauerhaft. An die Stelle der Abschlussprüfung tritt eine kontinuierliche, systemisch integrierte Governance-Logik, die Compliance in der DNA der IT verankert. Unternehmen, die diesen Schritt vollziehen, gewinnen nicht nur an Sicherheit und Planbarkeit, sondern schaffen auch die strukturellen Voraussetzungen für Geschwindigkeit und Innovationskraft in einem zunehmend digital geprägten Wettbewerbsumfeld.

Björn Eckmayer ist Sales Director im Bereich Banking, Financial Services & Insurance beim Ingenieurs- und Technologiedienstleister Expleo