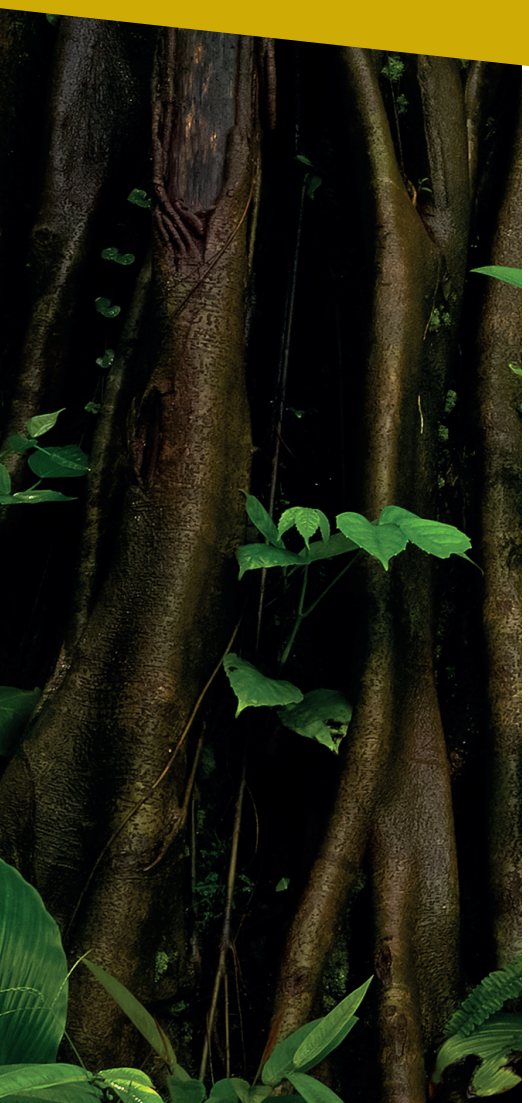
BPM FÜR GOVERNANCE, RISK & COMPLIANCE

Gezielter durch den GRC-Dschungel

Finanzinstitute verbinden mit Governance, Risk & Compliance oft eine Hassliebe: einerseits lästige Pflicht, andererseits sinnvolles Regelwerk für resiliente Strukturen und Arbeitsabläufe. Dabei bergen regulatorische Anforderungen auch Potenzial für Effizienzsteigerungen. Den Weg dahin ebnen BPM-Tools. Sie bilden die Organisation und ihre Prozesse transparent ab und helfen, GRC-Anforderungen besser zu erkennen und einzuhalten, während gleichzeitig die Komplexität reduziert wird.



Viele Finanzinstitute sind in Bezug auf das Management von Governance, Risk & Compliance-Anforderungen (oder kurz: dem GRC-Management) fragmentiert aufgestellt. Das zeigt sich vor allem in der Nutzung vieler verschiedener IT-Systeme zur Datenablage und Dokumentation.

Aber auch in der Vorgehensweise und Kommunikation zwischen der 1st-Line-of-Defence, also den Fachbereichen, und der 2nd-Line-of-Defence – z. B. den Compliance- oder Datenschutzbeauftragten – zeigt sich: Der Fachbereich (1st-Line) empfindet die Vorgaben und Anforderungen der 2nd-Line oft als lästig und behindernd, während die Beauftragten (2nd-Line) über die mangelnde Einsicht der Fachbereiche in die Notwendigkeit der Regelungen Unverständnis äußern.

Was fehlt, ist eine vernetzte Sicht auf ein integriertes GRC-Management für die Fachbereiche und die einzelnen Beauftragtenfunktionen. Der fehlende ganzheitliche Ansatz führt zu hoher Komplexität, Effizienzverlusten und einem erhöhten Risiko, da die Gefahr von Regelverstößen durch parallel geführte Datenbestände und Medienbrüche steigt.

Die Finanzinstitute sollten daher einen Perspektivwechsel im GRC-Management anstreben, um mit einem ganzheitlichen Ansatz über die fachlichen Silos hinweg langfristig Stabilität und Resilienz in einem immer enger werdenden regulatorischen Umfeld zu gewährleisten. Denn mit einer singulären Sicht auf die Anforderungen pro Fachbereich ist dieses Ziel dauerhaft nicht zu erreichen.

Prozess- und GRC-Exzellenz in Gleichklang bringen

Mit einer abteilungsübergreifenden Betrachtung des GRC-Managements wird über eine Vernetzung der einzelnen Verteidigungslinien, dem Three-Lines-of-Defence-Modell, die Zusammenarbeit erleichtert. Dabei sollten folgende Ziele erreicht werden:

- Eine Prozess- und GRC-Evidenz aufbauen,
- prozessorientiertes Denken stärken und
- Orte der Wahrheit schaffen.

Prozess- und GRC-Evidenz entsteht durch die systematische Vernetzung der verschiedenen GRC-Daten mit den Prozessen und Strukturen der Organisation. Das erfordert häufig eine Neuausrichtung des etablierten Prozessmanagements. Hierfür ist der Einsatz eines modernen Business Process Management (BPM) Tools hilfreich, das die dafür notwendigen umfangreichen Funk-

tionalitäten bietet. Darüber hinaus sollte im Auftrag der Geschäftsführung eine Überwachungsinstanz für die Einhaltung von GRC-Transparenz und -Vollständigkeit eingerichtet werden, die somit zum „Hüter der GRC-Exzellenz“ wird.

Prozessorientiertes Denken bricht das Silo-Denken auf und ermöglicht es der Mitarbeiterschaft und den Führungskräften, eine ganzheitliche Sichtweise auf das eigene Haus einzunehmen. Dies hilft der Belegschaft auch, die umfangreichen Regeln, Risiken und Kontrollen besser zu verstehen, da diese typischen GRC-Anforderungen oft unmittelbar oder zumindest mittelbar einen Prozessbezug haben. Die Etablierung dieses Denkens ist eine zentrale Führungsaufgabe, die von den Führungskräften erklärt und gelebt werden muss. Die Vorteile der Prozessorientierung sollten auch immer wieder an konkreten Beispielen aufgezeigt werden (z. B. „Die Kundenzufriedenheit im Kundenprozess X ist gestiegen.“).

„Orte der Wahrheit“ schaffen bedeutet, dass möglichst alle Prozess- und GRC-Informationen an einer Stelle bzw. in einem System abgelegt werden. Hier können vor allem aktuelle BPM-Tools eingesetzt werden, um Prozess- und GRC-Daten transparent und prozessbezogen abzulegen. Über Reporting- und Dashboard-Funktionen stellt die Software die Daten für Auswertungs- und Analysezwecke übersichtlich dar. Damit wird auch das Ziel der Prozess- und GRC-Evidenz unterstützt.

GRC-Exzellenz mit BPM-Tools erreichen

Für den BPM-Marktüberblick 2023 wurden die sechs gängigsten BPM-Tools (ADONIS, Aeneis, BIC Platform, Ibo, iGrafx und SAP Signavio) für die Finanzindustrie untersucht. Zu den Bewertungskriterien zählte auch der Funktionsumfang im Umfeld des GRC-Managements (siehe Kasten). Darüber hinaus erfolgte eine Analyse der Standardanforderungen an ein leistungsfähiges Prozessmanagement. Das sind z. B. die Funktionen

- zur revisionssicheren Versionierung,
- für eine einfache und intuitive Prozessmodellierung,
- für ein Dokumenten- und Content-Management,
- für Benutzerfreundlichkeit,
- zur Erstellung von Organigrammen,
- für einfache und anpassbare Freigabe-Workflows zur Veröffentlichung,
- Werkzeuge zur Auswertung (Dashboards und Reporting-Funktionen), sowie die Unterstützung von Automatisierungsinitiativen.

Diese Tools bieten teilweise weit mehr Funktionalitäten als die reine Risiko- und Kontrolldokumentation und ermöglichen den Instituten den Übergang von einer fragmentierten zu einer einheitlichen und prozessorientierten Governance, Risk & Compliance. Die Anwendungen sind in der Lage, die gesetzlichen Anforderungen an ein Internes Kontrollsystem (IKS) ebenso zu erfüllen wie die Integration eines Business Continuity Managements (BCM), eines Information Security Management Systems (ISMS) oder die Abbildung von Datenschutzanforderungen.

Darüber hinaus werden Möglichkeiten zur Vernetzung der drei Verteidigungslinien geschaffen. Das System stellt somit den operativen Einheiten als erste Verteidigungslinie, den Beauftragtenfunktionen als zweite Verteidigungslinie und der internen Revision als dritte Verteidigungslinie alle relevanten Daten und Informationen anwendergerecht zur Verfügung.

Darüber hinaus können automatisierte Workflows zur Analyse und Bewertung der verschiedenen GRC-Anforderungen, etwa im Umfeld der Risiken und Kontrollen, erstellt und Handlungsempfehlungen aufgezeigt werden.

Durch die Vernetzung der GRC-Daten aller Beauftragtenfunktionen in Kombination mit den Auswertungsmöglichkeiten entsteht ein GRC-Managementsystem, das die relevanten Daten und Informationen benutzerfreundlich, d. h. mit Analysefunktionen, Dashboards und Reports, zur Verfügung stellt. Darüber hinaus zeigt das System Handlungsbedarf und Handlungsempfehlungen auf.

MEHR ALS RISIKO- UND KONTROLLDOKUMENTATION

Die im Rahmen der Marktübersicht untersuchten Software-Lösungen zeichnen sich im GRC-Management durch folgende Merkmale aus:

- ADONIS ist ein umfassendes Tool für die Finanzindustrie, das standardisierte Funktionen des Internen Kontrollsystems (IKS) unterstützt, indem Risiken und Kontrollen innerhalb von Prozessen und Prozessschritten hinterlegt und mit dem Rollenmodell verknüpft werden können. Für anspruchsvollere GRC-Anforderungen können Kunden mit dem Zusatzmodul ADOGRC ein vollständiges GRC-Management aufbauen.
- Bei Aeneis trifft Benutzerfreundlichkeit auf ein hohes Individualisierungspotenzial. Fachliche GRC-Anforderungen können kundenspezifisch umgesetzt werden. Das Tool unterstützt auch die notwendigen regelmäßigen Überprüfungen, z. B. von Risiken und Kontrollen. Die Ergebnisse lassen sich in Diagrammen zusammenfassen.
- Die BIC Platform ist ein intuitives Tool mit Lösungen für viele Anforderungen und bietet ein benutzerfreundliches und sehr leistungsfähiges Modul für das GRC-Management. Es enthält Lösungen für typische GRC-Anforderungen wie IKS, Enterprise Risk Management, BCM, ISMS, Datenschutzmanagement und Auditmanagement.
- ibo hat sich als ausgereiftes Werkzeug für das klassische Prozessmanagement erwiesen. Der Anbieter hat eine Lösung für das klassische Risikomanagement entwickelt und kontinuierlich verbessert. Im Modul ibo Prometheus Risk werden alle in den Prozessen und Aufgaben auftretenden Risiken und Kontrollen dokumentiert, bewertet und zusammengefasst.
- iGrafx ist ein funktionsreiches Tool mit hohem Individualisierungsgrad und stellt umfangreiche Risikomanagement-Funktionalitäten zur Verfügung. Bei der Auswertung können individuelle Reports und Dashboards mit Informationen für die jeweiligen Stakeholder konfiguriert werden.
- Mit SAP Signavio stellt der Anbieter ein leistungsfähiges Tool für Process Mining zur Verfügung und bietet damit auch eine Erweiterung eines bereits implementierten IKS-Management-Tools. Mit den Produkten „SAP Signavio Process Manager“ und „SAP Signavio Process Governance“ kann eine Verbindung zwischen Ist- und Soll-Geschäftsprozessmodellen und dem internen Risiko- und Kontrollmanagement hergestellt werden.

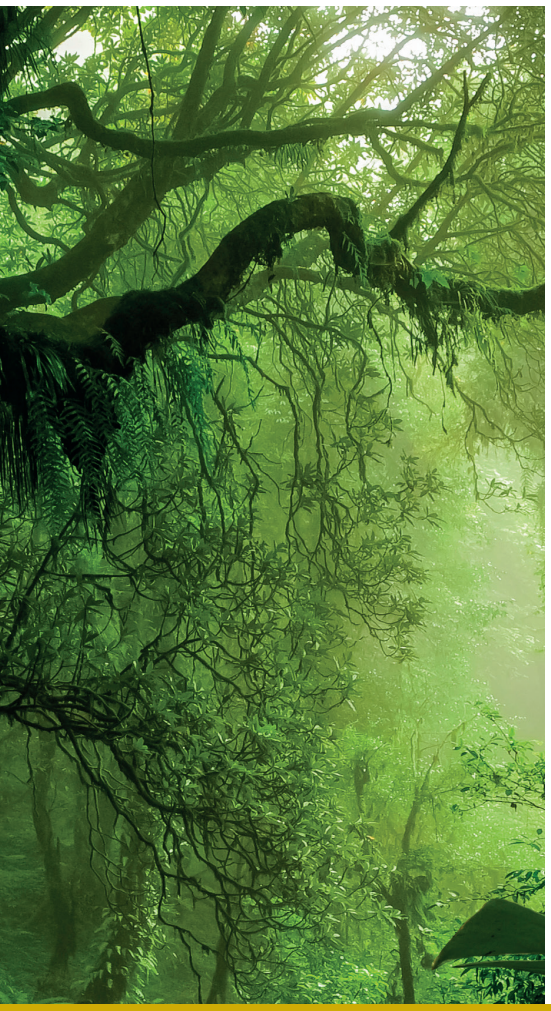
So gelingt ein ganzheitliches GRC-Management

Die untersuchten BPM-Tools bilden zwar alle grundlegenden IKS-Funktionalitäten ab, unterscheiden sich aber im Detail erheblich. So bieten einige der betrachteten Tools weitergehende Funktionen für ein ausgeprägtes GRC-Management, was wiederum den Einsatz zusätzlicher Anwendungen mit Einzelfunktionen, beispielsweise für Datenschutz oder Compliance, überflüssig macht. Dies spart Kosten bei der Anschaffung, Implementierung und Wartung der Systeme. Die Abbildung ▸ **1** fasst die untersuchten Tools in einem Netzdiagramm zusammen, das die unterschiedlichen Schwerpunkte der einzelnen BPM-Software-Lösungen verdeutlicht. Die Studie belegt, dass die Hersteller zunehmend ihre Tools um leistungsfähige GRC-Funktionen erweitern.

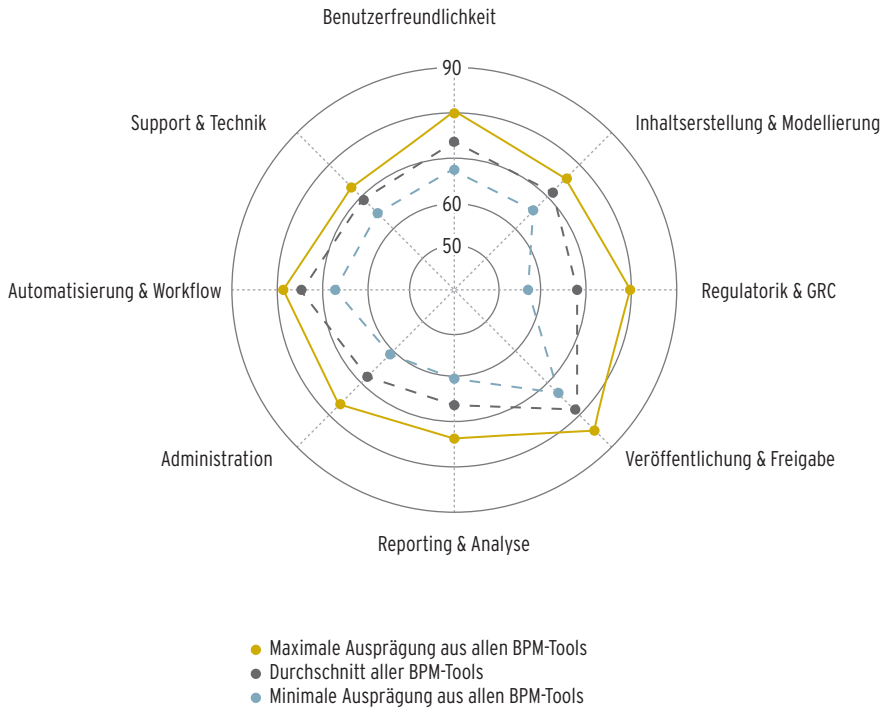
Finanzinstitute, die ein BPM-Tool nutzen, um Prozess- und GRC-Exzellenz zu erreichen, sollten im ersten Schritt einen möglichst vollständigen GRC-Datenhaushalt aufbauen. Dort werden die relevanten Daten als Objekte oder Attribute an den Prozessen und Aktivitäten hinterlegt. Anschließend sollten der systematische Aufbau und die Implementierung der GRC-Funktionalitäten im BPM-Tool erfolgen. Damit wird ein „Ort der Wahrheit“ für alle Stakeholder geschaffen.

Durch die Verknüpfung der Kernelemente des Unternehmens (z. B. Organigramme, Verantwortlichkeiten, Funktionsbeschreibungen, Prozesslandkarte oder Richtlinien und Guidelines) und deren Zusammenführung mit den GRC-Anforderungen zu Risiken, Kontrollen oder Compliance-Regeln entsteht ein direkter Mehrwert.

Im letzten Schritt geht es darum, Effizienzpotenziale zu heben, indem die Möglichkeiten der Automatisierung im GRC-Umfeld ausgeschöpft werden. Ziel ist es, die Daten mithilfe des Tools so miteinander zu verknüpfen, dass automatisierte Plausibilitätsprüfungen durchgeführt und Workflows zur Bearbeitung von Risiken (z. B. Kreditausfalle oder Geldwäsche) implementiert werden können.



1 | Schwerpunkte der einzelnen BPM-Software-Lösungen



Quelle: Cofinpro.

FAZIT

Durch die Verknüpfung von GRC-Daten mit Prozessen erhalten Finanzinstitute maximale Transparenz in der Organisation und sparen durch aufeinander abgestimmte Prozesse und Datenhaushalte sowohl bei der Implementierung als auch im Regelbetrieb Zeit und Kosten. Die untersuchten BPM-Tools zeichnen sich durch ihre Flexibilität aus: Dank ihrer umfassenden Funktionalitäten sind sie ein mächtiges Werkzeug für mehr Prozess- und GRC-Exzellenz und helfen bei der Umsetzung einer vorausschauenden, kundenzentrierten und vor allem schlanken Unternehmensorganisation. Mit der Digitalisierung von GRC-Prozessen auf Basis eines strategischen Prozessmanagements können Banken mehrere Ziele gleichzeitig erreichen:

- ▷ Resilienz und Transparenz durch regelkonforme Prozesse schaffen,
- ▷ die Organisation effizienter steuern und
- ▷ kundenfreundlichere Prozesse für digitale Zugangswege etablieren.

Den Finanzinstituten bietet sich damit die Chance, ihre Organisation aktiv zu steuern und beispielsweise die notwendigen Anforderungen effektiver an den Geschäftsprozessen und -strukturen auszurichten. Grundlage für ein funktionierendes GRC-Management-System sind dabei übergreifende Anforderungen wie Revisionssicherheit, Versionierbarkeit und Wiedervorlagefunktionalitäten.

Autoren

Dominik Bollmann ist als Manager seit über zwölf Jahren im Bereich Prozessmanagement aktiv. Er ist mit bankfachlichen Themen vertraut und besitzt umfangreiche Leitungs- und konzeptionelle Kenntnisse und setzt diese in der SfO um.

Klaus Lehmann ist Senior Manager und Experte für Prozessexzellenz in der Finanzbranche. In Leitungsfunktionen bei Kreditinstituten und als externer Berater hat er umfangreiches Know-how im Prozessmanagement und den Themen Governance, Risk & Compliance erworben.

Enrico Lutz ist als Consultant und Experte im Umfeld Prozessexzellenz in der Finanzbranche tätig. Als Wirtschaftsingenieur bringt er branchenübergreifende Erfahrung im Einsatz von Prozessmanagement-Tools mit.

Alle drei arbeiten für die Cofinpro AG, Frankfurt am Main.

1 Die Studie kann kostenlos geladen werden: https://cofinpro.de/download/bpm-marktueberblick-2023/.