



1+1=3

Wie das Compliance - Management effizienter gestaltet werden kann

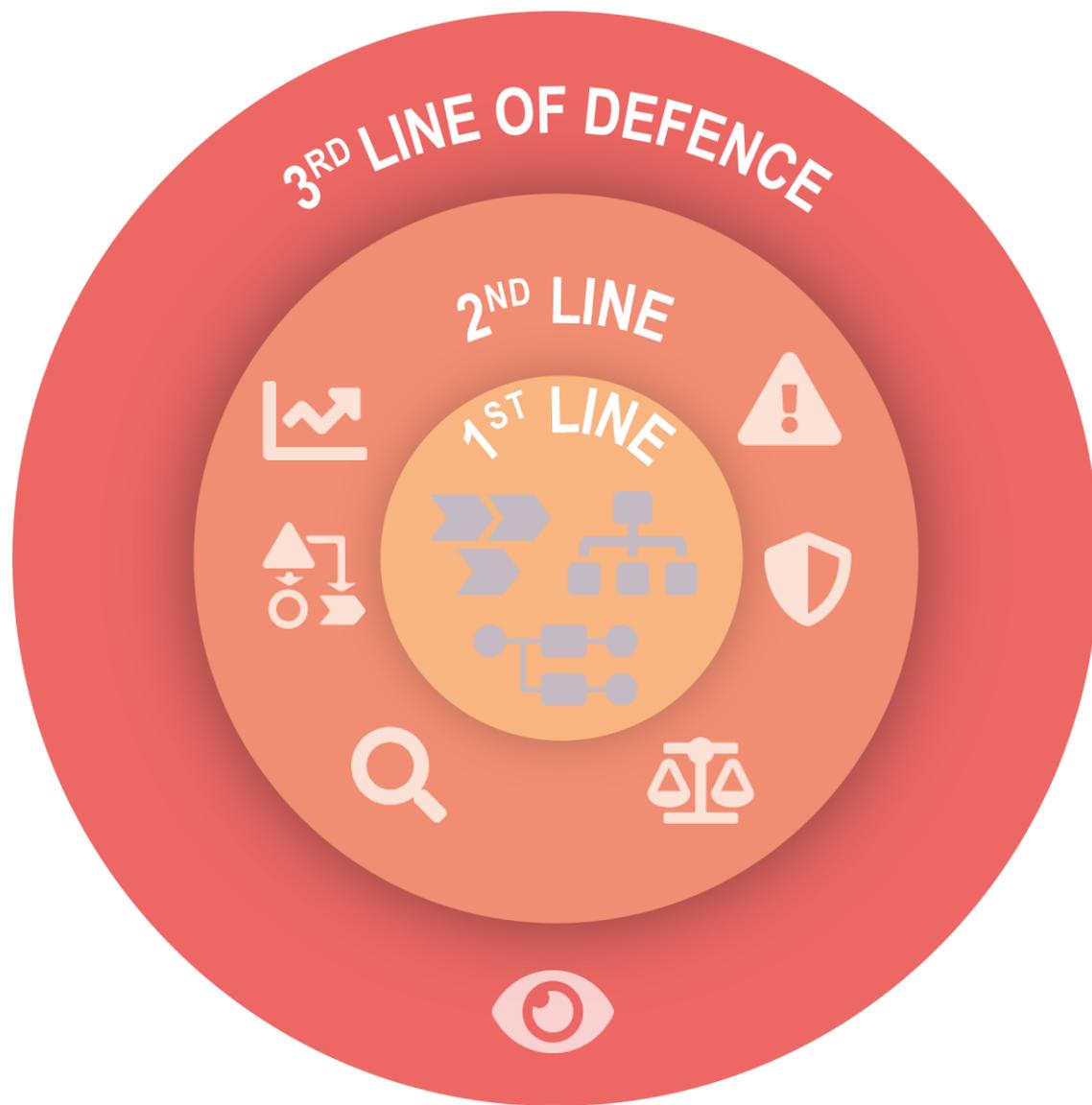
BOC Group
Thomas Müllner

A person wearing a white lab coat is shown from the chest down, carefully stacking wooden blocks. The person's right hand is in the process of placing a block on top of a stack. The stack consists of several layers of rectangular wooden blocks, with the top layer having two blocks. The background is a plain, light-colored wall.

Das Ganze ist mehr als die Summe der einzelnen Teile.

(Aristoteles)

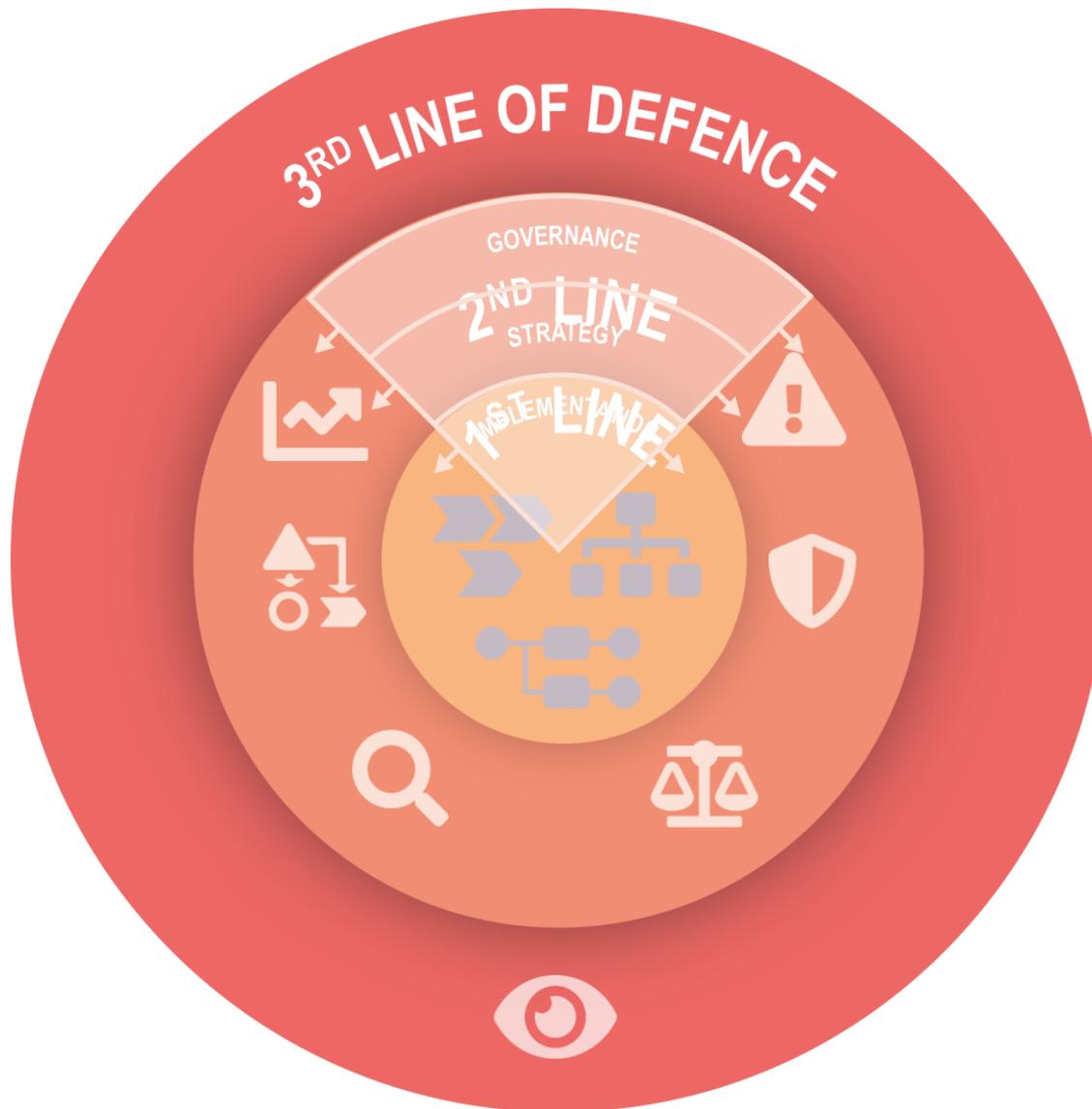
Integriertes GRC im Kontext der 3 LoD



- Prozessstruktur
- Organisationsstruktur
- Prozessabläufe

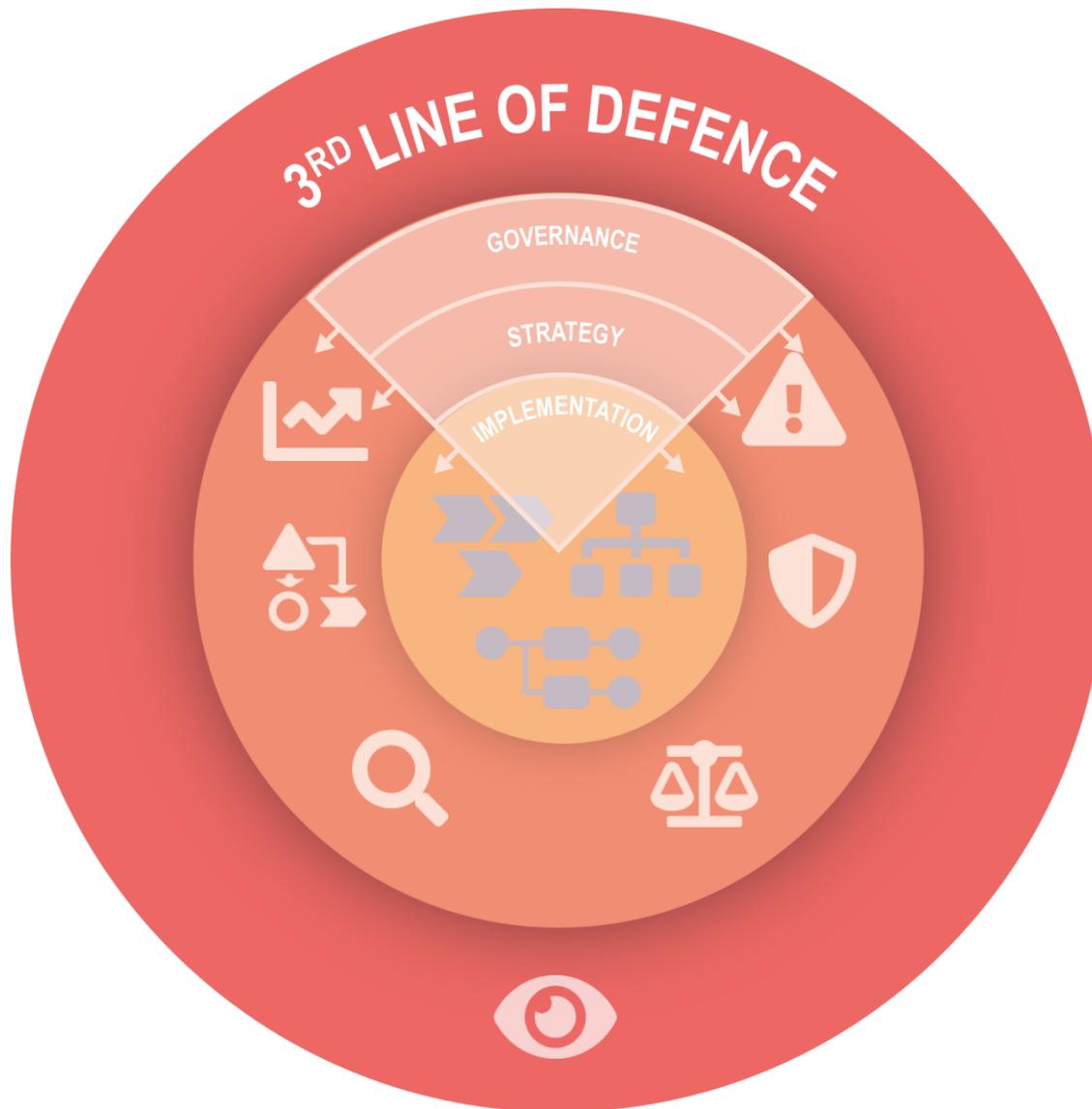
- Compliance-Management
- Sicherheitsmanagement
- Qualitätsmanagement
- Internes Kontrollsystem
- Risikomanagement
- Prozessmanagement

- Interne Revision



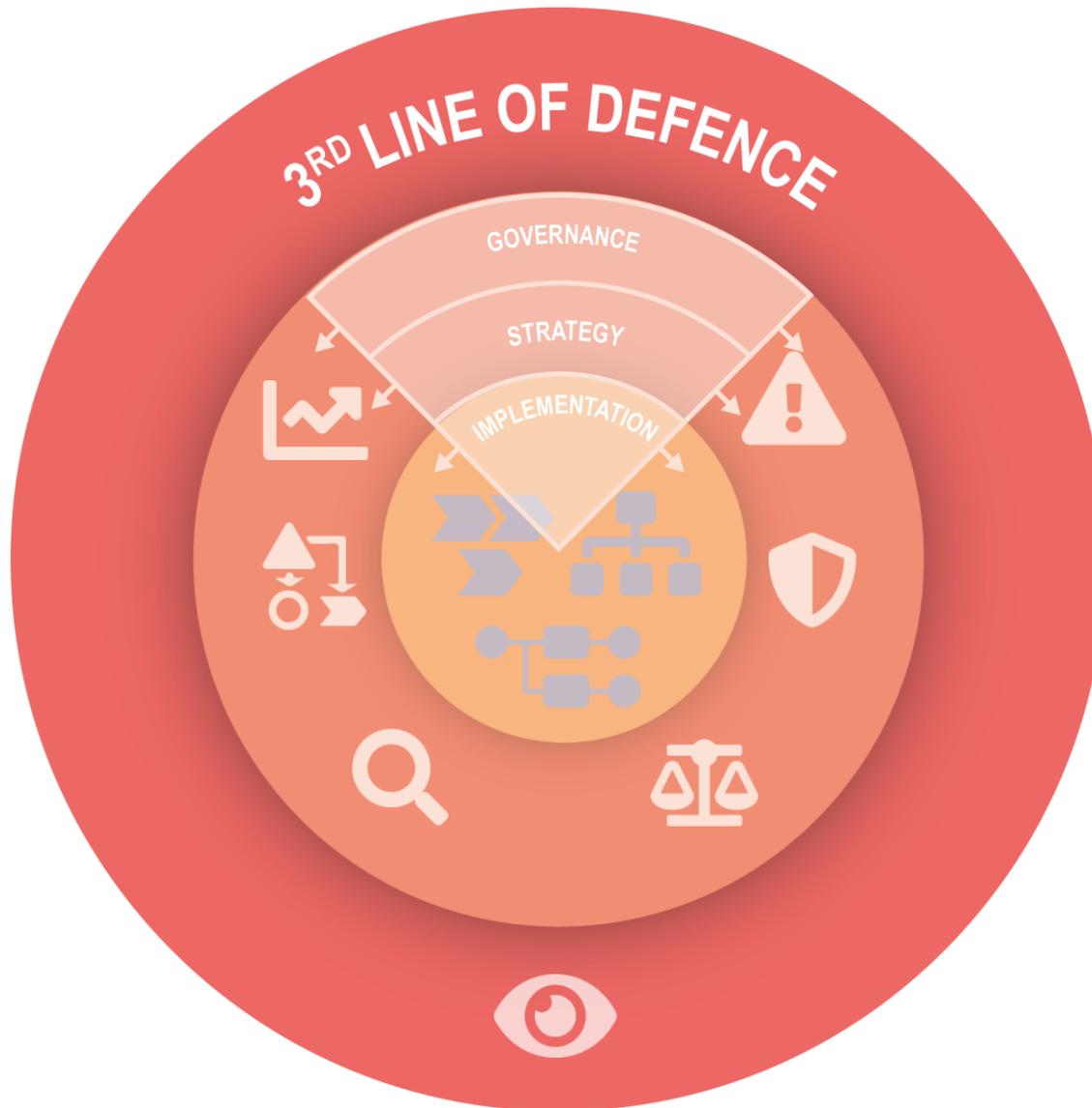
Governance

- ✓ Begriffe und Definitionen festlegen
- ✓ Bezug zu normativen Referenzen (ONR 192050, ISO 19600, ISO 37001) herstellen
- ✓ Scope mittels Compliance-Risiko-Bewertung definieren
- ✓ CMS im integrierten GRC einordnen (Bezug zu RM, IKS, GPM,...)



Strategie

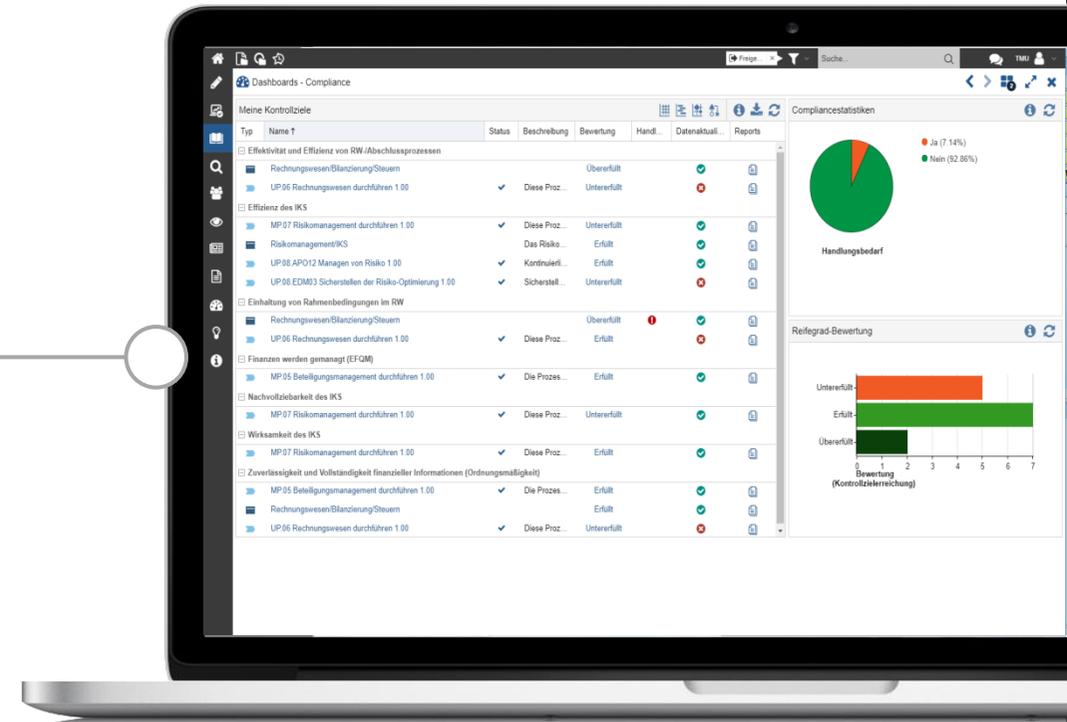
- ✓ CMS planen und umsetzen (Aufbau- und Ablauforganisation, Handlungsanweisungen)
- ✓ Normenverzeichnis erstellen und aktuell halten
- ✓ Operative Einheiten unterstützen (Trainings,...)
- ✓ Einhaltung der Handlungsanweisungen (mittels Stichproben) überwachen
- ✓ Schadensfälle managen
- ✓ Wirksamkeit des CMS sicherstellen
- ✓ Intern sowie extern kommunizieren und berichten



Umsetzung

- Handlungsanweisungen in Prozesse integrieren
- Handlungsanweisungen befolgen und nachweislich dokumentieren
- Verfehlungen melden und Schadensfälle erfassen
- Ideen zur Verbesserung mit Compliance Officer teilen

Compliance-Management mit der GRC-Suite von ADONIS



Umfassend

Transparent

Rollenbasiert

Integriert

Compliance-relevante Vorgänge identifizieren

Scoping mittels Prozesslandkarte (1)

ADOMONEY BANK Prozesslandkarte

Prozesseigner: Power Adonis (ado)
Status: In Bearbeitung
Gültig ab:

Managementprozesse

- MP.01 Strategiemangement durchführen
- MP.02 Produktionsmanagement durchführen
- MP.03 Ertrags- und Kostenmanagement durchführen
- MP.04 Vertriebsmanagement durchführen
- MP.05 Beteiligungsmanagement durchführen
- MP.06 Compliancemanagement durchführen
- MP.07 Risikomanagement durchführen
- MP.08 Revisions- und Auditmanagement durchführen
- MP.09 HSEQ Management durchführen
- MP.10 Prozess- und Organisationsmanagement durchführen

Kernprozesse

- KP.01 Kunden beraten
- KP.02 Finanzierung durchführen
- KP.03 Giro/Zahlungsverkehr durchführen
- KP.04 Veranlagungen tätigen
- KP.05 Wertpapiergeschäfte umsetzen
- KP.06 Vermittlungsgeschäfte umsetzen

Unterstützungsprozesse

- UP.01 Werbung und Marketing durchführen
- UP.02 Infrastruktur bereitstellen
- UP.03 Meldewesen und Raising durchführen
- UP.04 Projekt- und Maßnahmenmanagement durchführen
- UP.05 Rechtsberatung bereitstellen
- UP.06 Rechnungswesen durchführen
- UP.07 Personalmanagement durchführen
- UP.08 IT Management durchführen
- UP.09 Betrugs- und Fraud Management
- UP.10 Verbesserungs- und Change Management durchführen

Compliance-relevante Vorgänge identifizieren



Scoping mittels Prozesslandkarte (2)

Prozesslandkarte ADOmoney Bank 1.01

Prozesseigner: Power Adonis (ado)
 Status: In Bearbeitung
 Gültig ab: -----

[Kontrollziel (Compliance) | KP.02 Finanzierung durchführen, KP.03 Giro/Zahlungsverkehr durchführen, KP.04 Veranlagungen tätigen, KP.05 Wertpapiergeschäfte umsetzen, KP.06 Vermittlungsgeschäfte umsetzen, UP.03 Meldewe...

	BWG	Einhaltung KYC-Erfordernisse (Geld...	ESAEG	FM-GWG	GMSG	WAG 2018
KP.02 Finanzierung durchführen 0.01	■	■				
KP.03 Giro/Zahlungsverkehr durchführen 0.01	■	■		■		
KP.04 Veranlagungen tätigen 0.01	■	■	■			■
KP.05 Wertpapiergeschäfte umsetzen 0.01		■				■
KP.06 Vermittlungsgeschäfte umsetzen 0.01	■	■				
UP.03 Meldewesen und Rating durchführen 0.01					■	

Compliance-Risiken analysieren und Kontrollen festlegen



Risikoanalyse und Kontrolldokumentation basierend auf betrieblichen Abläufen

The screenshot displays the ADOMONEY BANK process map software. The top window shows the process map for 'ADOMONEY BANK Prozesslandkarte' with a search bar and navigation icons. The bottom window shows a detailed risk analysis table for the 'Kontrolle-Risiko-Prozess'.

	Auskünfte / Bonität einholen	Identifizieren von Anspruchsgruppen für ...	Kontrolle und Genehmigung durch ...	Prüfung durch interne Revision / Wirtschafts...	Quartalsweise Sichtung der Kreditbewilligungen	Risikoprüfung durchführen	Zuweisen von Störungen an releva...
KP.02 Finanzierung durchführen 0.01		07.07.03.03 Kundenaufnahme un...	07.01.01.01 Nicht gemeldete Transaktio...	07.04.01.09 Angemessenheit, Off...		07.05.01.03 Katastrophen und an...	
KP.03 Giro/Zahlungsverkehr durchführen 0.01	07.04.04.02 Überschreitung des K...		07.01.01.01 Nicht gemeldete Transaktio... 07.01.02.12 Diebstahl und Betrug durch Mit...	07.01.02.12 Diebstahl und Betrug durch Mit... 07.04.04.02 Überschreitung des K...	07.04.04.02 Überschreitung des K...	07.04.04.02 Überschreitung des K... 07.05.01.03 Katastrophen und an...	
KP.04 Veranlagungen tätigen 0.01						07.05.01.03 Katastrophen und an...	
KP.05 Wertpapiergeschäfte umsetzen 0.01			07.01.02.12 Diebstahl und Betrug durch Mit...	07.01.02.12 Diebstahl und Betrug durch Mit...		07.05.01.03 Katastrophen und an...	
KP.06 Vermittlungsgeschäfte umsetzen 0.01						07.05.01.03 Katastrophen und an...	

Compliance-Risiken regelmäßig bewerten



Workflowbasierte Risikobewertung

Meine Risikobewertungen

Alle Objekte anzeigen

Typ	Name ↑	Status	Aktionen	Eskaliert	Zugeordnetes Risiko	Fehlerhäufigkeit	Auswirkung	Entdeckbarkeit	Risikoerwartung	Häufigkeit der Risikobewertung	Bewertung gesteuert	Nächste geplant
Freigegeben	07.01.01.04 Positive Kreditentscheidung entgegen interner Richtlinien	✓			▲ 07.01.01.04 Positive Kreditentscheidung entgegen interner Richtlinien	Häufig (4 - 12 Mal pro Jahr)	Hoch	Moderat	144	Jahr	26.08.2019	31.10.2019
Freigegeben	07.01.02.03 Veruntreuung von Vermögenswerten	✓			▲ 07.01.02.03 Veruntreuung von Vermögenswerten	Selten (einmal alle 1 - 5 Jahre)	Gering	Sehr hoch	18	Jahr	05.02.2019	31.12.2019
Freigegeben	07.01.02.06 Scheckbetrug	✓			▲ 07.01.02.06 Scheckbetrug	Möglich (einmal alle 1 - 2 Jahre)	Moderat	Moderat	64	Jahr	05.02.2019	01.01.2020
Freigegeben	07.03.01 Ereignisse in Verbindung mit Arbeitnehmern	✓			▲ 07.03.01.03 Sonstige Ereignisse in Verbindung mit Arbeitnehmern	Möglich (einmal alle 1 - 2 Jahre)	Mittel	Sehr hoch	40	Jahr	06.02.2019	01.01.2020
Freigegeben	07.03.02 Sicherheit des Arbeitsumfeldes	✓			▲ 07.03.02.05 Allg. Sicherheit des Arbeitsumfeldes	Selten (einmal alle 1 - 5 Jahre)	Hoch	Sehr gering	108	Jahr	06.02.2019	01.01.2020
Freigegeben	07.04.02 Unzulässige Geschäfts- oder Marktpraktiken	✓			▲ 07.04.02.07 Unzulässige Geschäfts- oder Marktpraktiken	Unwahrscheinlich (5 Jahre oder länger)	Gering	Hoch	18	Jahr	06.02.2019	01.01.2020
Freigegeben	07.04.05 Beratungstätigkeiten	✓			▲ 07.04.05.03 Beratungstätigkeiten	Möglich (einmal alle 1 - 2 Jahre)	Mittel	Moderat	135	Jahr	06.02.2019	01.01.2020
Freigegeben	07.07.04 Kundenkontoführung	✓										
Freigegeben	07.07.05 Geschäftspartner im Handel	✓										
Freigegeben	KP.01.00 Neukunde anlegen - Geldwäsche	✓										
Freigegeben	KP.01.00.01 - Überschreitung des Kundengesamtlimits	✓										
Freigegeben	KP.02.02-P2 Antragsentscheidung durchführen - Überschreitung des Kundengesamtlimits	✓										

[Risikobewertungen (Auswirkung - Fehlerhäufigkeit) | 07.01.01.04 Positive Kreditentscheidung entgegen interner Richtlinien, 07.01.02.03 Veruntreuung von Vermögenswerten, 07.01.02.06 Scheckbetrug]

Risikobewertung:

- 07.01.01.04 Positive Kreditentscheidung entgegen interner Richtlinien
- 07.01.02.03 Veruntreuung von Vermögenswerten
- 07.01.02.06 Scheckbetrug
- 07.03.01 Ereignisse in Verbindung mit Arbeitnehmern
- 07.03.02 Sicherheit des Arbeitsumfeldes
- 07.04.02 Unzulässige Geschäfts- oder Marktpraktiken
- 07.04.05 Beratungstätigkeiten
- 07.07.04 Kundenkontoführung
- 07.07.05 Geschäftspartner im Handel
- KP.01.00 Neukunde anlegen - Geldwäsche
- KP.01.00.01 - Überschreitung des Kundengesamtlimits
- KP.02.02-P2 Antragsentscheidung durchführen - Überschreitung des Kundengesamtlimits

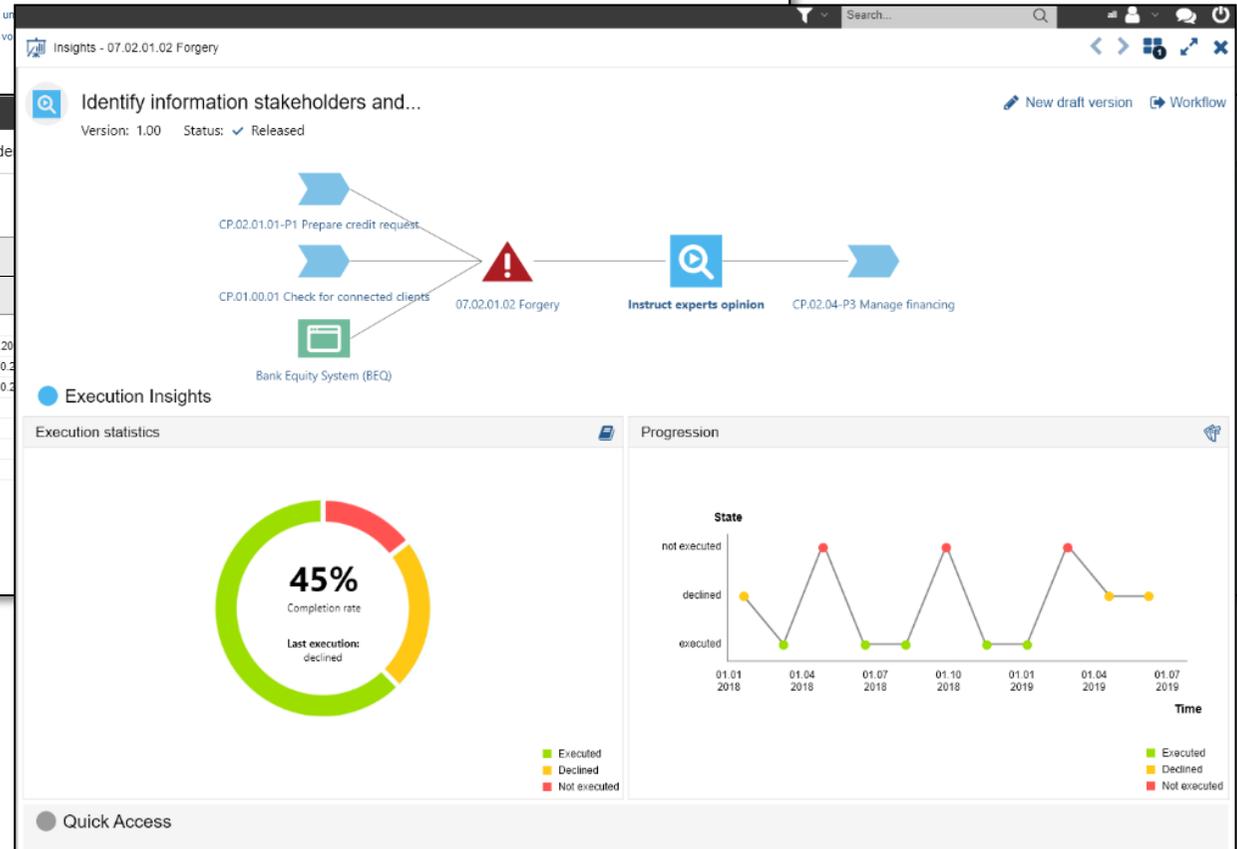
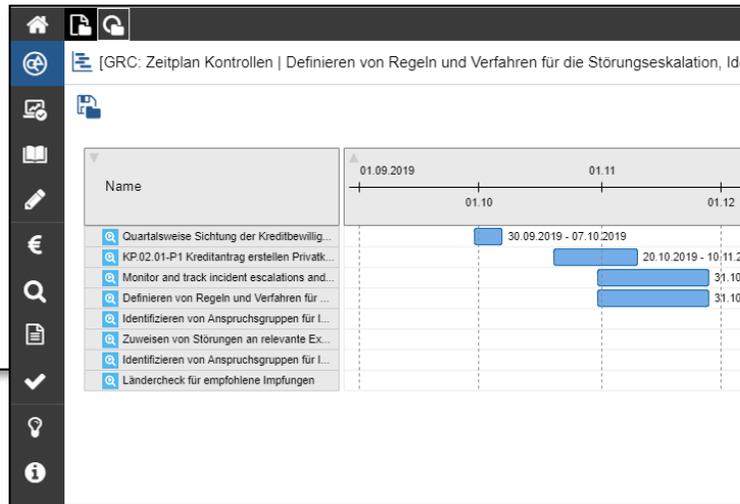
Einhaltung der Handlungsanweisungen überwachen



Workflowbasierte Kontrolldurchführung

Meine Kontrolldurchführungen

Typ	Name ↑	Status	Aktionen	Eskaliert	Zugeordnete Kontrolle	Bestäti...	Dokumentation der Durchführung	Häufigkeit der Kontrolldu...	Durchführung ge...	Nächste geplant...	
Durchgeführt	Definieren von Regeln und Verfahren für die Störungseskalation	✓			30.11.2018	Definieren von Regeln und Verfa...	Nein		Jahr	31.10.2018	31.10.2019
In Arbeit	Identifizieren von Anspruchsgruppen für Informationen und deren Bedarf ...					Identifizieren von Anspruchsgrup...	Nein		Jahr	21.08.2019	01.01.2020
In Arbeit	Identifizieren von Anspruchsgruppen für Informationen und deren Bedarf ...					Identifizieren von Anspruchsgrup...	Nein		Jahr	21.08.2019	11.08.2020
In Arbeit	Ländercheck für empfohlene Impfungen						Nein		Jahr	21.08.2019	15.08.2020
In Arbeit	Quartalsweise Sichtung der Kreditbewilligungen - Durchführung				02.09.2019	Quartalsweise Sichtung der Kred...	Nein		Quartal	26.08.2019	30.09.2019
In Arbeit	Zuweisen von Störungen an relevante Experten					Zuweisen von Störungen an rele...	Nein		Jahr	21.08.2019	30.06.2020
In Bearbeitung	KP.02.01-P1 Kreditantrag erstellen Privatkunde (inkonsistente Häufigkeit)					Risikoprüfung durchführen	Nein		Halbjahr	--:--	--:--
In Bearbeitung	Monitor and track incident escalations and resolutions					Überwachen un...					
In Bearbeitung	Nachweis der Durchführung Appl 1					Durchführen vo...					
In Bearbeitung	Nachweis der Durchführung Appl 2										
In Bearbeitung	Update VDV										



Schadensfälle managen



Workflowbasiertes Managen von Schadensfällen

Dashboard: Schadensfälle

Suche...

all

Typ Name ↑

- Ausfall Firmenkredit 2018.2345
- Ausfall Privatkredit 1234.5678
- Fehlbuchung Bnr 123546.7854
- KFZ-Totalschaden W-12345 A
- Mietausfall aufgrund Wasserschaden Opengasse 20b
- Schadenersatzzahlung nach Sturz eines Kunden vor Filiale 1040 Wien
- Strafzahlung nach DSGVO Art. 30
- Strafzahlung wegen Insiderhandel 2018/02
- Unautorisierter Wertpapierhandel 2018/01
- Verlust aus Rechtsstreit 23jc4ab

[SFDB: Welches Risiko führt zu welchem Schaden | Ausfall Firmenkredit 2018.2345, Ausfall Privatkredit 1234.5678, Fehlbuchung Bnr 123546.7854, KFZ-Totalschaden W-12345 A]

	KP.02 Finanzierung durchführen 0.01	KP.05 Wertpapiergeschäfte u...	MP.06 Compliancemanage...	Prozess 0.01	UP.02 Infrastruktur bereitstellen 0.01	UP.06 Rechnungswesen d...
07.03.01.04 Nichteinhaltung rechtlicher Vorgaben (Compliance-Verstöße)			Strafzahlung nach DSGVO Art. 30			
07.04.02.04 Insidergeschäfte (auf Rechnung des Arbeitgebers)		Strafzahlung wegen Insiderhandel 2018/02				
07.04.02.05 Nicht genehmigte Geschäftstätigkeit		Unautorisierter Wertpapierhandel 20...				
07.04.04.01 Versagen bei der Kundenprüfung gemäß Richtlinien	Ausfall Firmenkredit 2018.2345					
07.04.04.02 Überschreitung des Kundengesamtlimits	Ausfall Firmenkredit 2018.2345					
07.04.04.03 Mangelnde Sorgfalt bei der Vorbereitung der Kreditvergabe	Ausfall Privatkredit 1234.5678					
07.04.05.03 Beratungstätigkeiten	Ausfall Privatkredit 1234.5678					
07.04.06.01 Verletzung von Kunden					Schadenersatzzahlung nach Sturz eines Kun...	
07.05.01.04 Sachschäden an Vermögensgütern					KFZ-Totalschaden W-12345 A	
07.07.01.02 Fehler bei der Dateneingabe, -pflege oder -speicherung						Fehlbuchung Bnr 123546.7854
07.07.03.02 Rechtsdokumente fehlen/ unvollständig					Verlust aus Rechtsstreit 23jc4ab	
Risiko				Schadenfall		

Wirksamkeit mit Audits und Maßnahmen sicherstellen

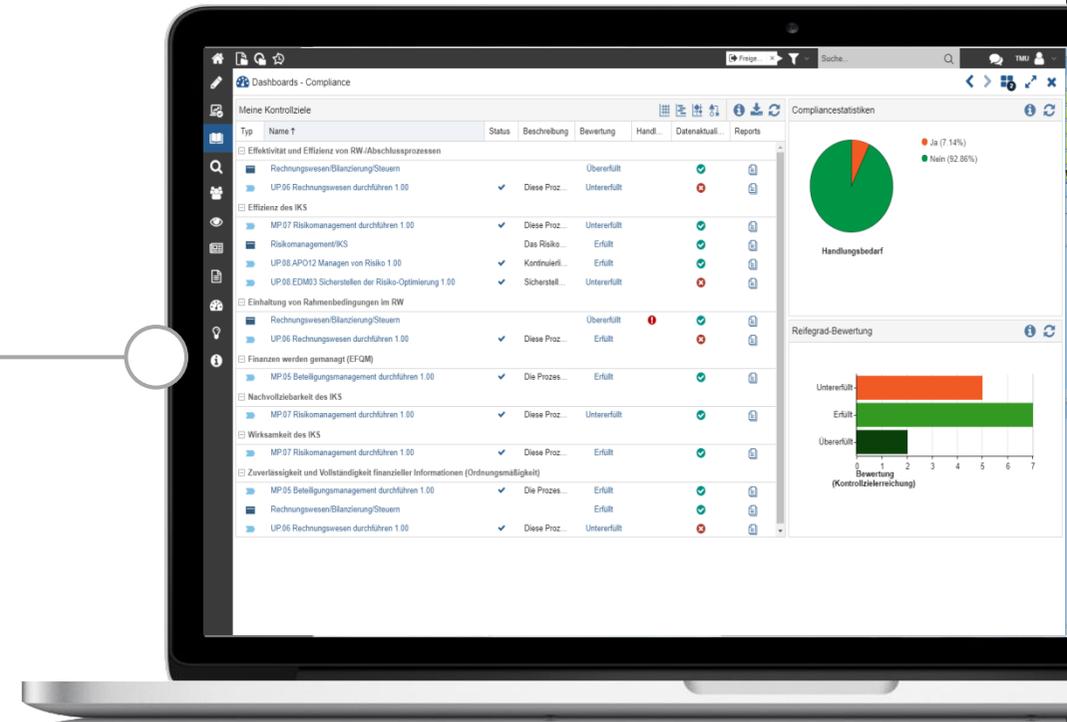


Auditplanung und -umsetzung sowie workflowbasiertes Maßnahmen-Controlling

The screenshot displays a software interface for audit planning and implementation. The top section shows a grid of categories (Business Continuity Management, Datenschutz, Dokumentation, Geschäftsprozessmanagement, IKS, Informationssicherheitsmanagementsystem, IT-Sicherheit, Physische Sicherheit, Projektentwicklung und -überwachung, Qualitätsmanagement, Risikomanagement, Umweltschutz) with corresponding task bars. The bottom section shows a Gantt chart for 'Maßnahmencontrolling (aktuelle Start-/Endtermine) | - Gantt Sicht' with a list of tasks and their timelines from 01.01.2017 to 2018.

Name	Start	End
Audit-Findings übertragen	01.01.2017	03.01.2017
Budgetcontrolling während Reise verbess...	02.01.2017	04.01.2017
CRM-Berechtigungskonzept überarbeiten	03.01.2017	05.01.2017
Direktvertrieb in Region Süd stärken	04.01.2017	06.01.2017
Dokumentation der Kontrollen im System	05.01.2017	07.01.2017
Fast Close einführen	06.01.2017	08.01.2017
Implementierung einer Systemkontrolle	07.01.2017	09.01.2017
Kennzahlen für Kernprozesse messen un...	08.01.2017	10.01.2017
Kontrolle durch vorgesetzte Rolle etablieren	09.01.2017	11.01.2017
Kunden Contact Center für Kernregionen...	10.01.2017	12.01.2017
KVP im Unternehmen aufsetzen	11.01.2017	13.01.2017
Neues Template für Detailplanung entwer...	12.01.2017	14.01.2017
Neukundenanlage: Know your customer (...)	13.01.2017	15.01.2017
Neukundenanlage: Riskoeinstufung ist zu...	14.01.2017	16.01.2017
Prozessmanagement einführen	15.01.2017	17.01.2017
Prozessreifeegrad verbessern	16.01.2017	18.01.2017
Rekrutierung neuer Schwerpunkt-Mitarbe...	17.01.2017	19.01.2017
Richtlinien zur Risiko-Prävention erarbeiten	18.01.2017	20.01.2017
Risikomanagementprozesse etablieren	19.01.2017	21.01.2017
RMLC einführen	20.01.2017	22.01.2017
Safety Officer ausbilden und Stelle etablie...	21.01.2017	23.01.2017
Schulung zu Öko-Standards durchführen	22.01.2017	24.01.2017
Tarifstruktur verschlanken und vereinheitli...	23.01.2017	25.01.2017
Verbesserung der IT-Security	24.01.2017	26.01.2017
Vertriebspartner in Region West identifize...	25.01.2017	27.01.2017
Wissensdatenbank für zukünftige Roadtri...	26.01.2017	28.01.2017
Zentrales CRM-System mit zentraler Part...	27.01.2017	29.01.2017

Compliance-Management mit der GRC-Suite von ADONIS



Single Source of Truth

Efficient Task Handling

Single Source of Information

Interessiert mehr zu erfahren?

1+1=3 – Mit den “Three Lines of Defence” zum integrierten GRC

In unserer Artikelserie erfahren Sie in 6 Teilen, wie Ihnen der Wandel zum integrierten GRC erfolgreich gelingt:

- ▶ **Prozessorientiertes GRC**
- ▶ **Schach dem (operationellen) Risik**
- ▶ **Risikoorientiertes IKS und mehr**
- ▶ **Compliance-Management Best-Practices**
- ▶ **Corporate Security Management**
- ▶ **DSGVO & Co**

Jetzt Abonnieren!

<https://discover.boc-group.com/artikel/grc/three-lines-of-defence/>



Wir danken für Ihre Aufmerksamkeit!

Für weitere Auskünfte stehen wir gerne zur Verfügung:

Mag. (FH) Thomas Müllner
Senior Management Consultant

BOC Information Technologies Consulting GmbH
Operngasse 20b, A-1040 Wien

Tel: +43-1-905 10 81-0

Fax: +43-1-905 10 81-2007

E-mail: thomas.muellner@boc-group.com

