Trusted Governance
Bringing GRC to the next level

In volatilen Zeiten wird Vertrauen zur wichtigsten Konstante und das Risikomanagement, wenn richtig verzahnt, zur Schlüsselfigur bei dessen Schutz und Aufbau

Risk Management Congress, München, Mai 2022

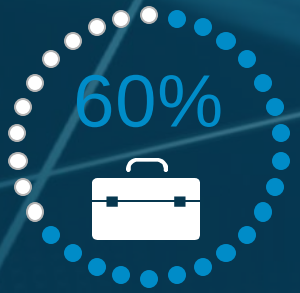
Daniel Cassel
Kai Rumphorst

Die Vertrauenskrise – laut dem Edelmann Trust Barometer befinden wir uns 2022 im “Cycle of Distrust”…

der Befragten sorgen sich, von **Unternehmensführungen** bewusst getäuscht zu werden[1]

Dabei gaben die Befragten an, folgende Entscheidungen vom Werteversprechen eines Unternehmens abhängig zu machen

Kauf-entscheidung



Arbeitgeber-entscheidung

Investment-entscheidung

[1] Edelmann Trust Barometer 2022

… doch was hat das mit dem Risikomanagement zu tun?

Die offizielle Definition der OCEG von GRC:

*GRC is the **capability**,*
*or **integrated collection** of **capabilities**,*
*that **enables** an organization to*
***reliably achieve objectives**,*
***address uncertainty**,*
*and **act with integrity**;*
including the governance, assurance and management of performance, risk, and compliance.[1]

[1] OCEG Homepage - Link

Die Herausforderung: Schutz des Vertrauens in einer beispiellos dynamischen und vernetzten Risikolandschaft

77% der befragten

Risikomanager gaben an, dass die Risikolandschaft komplexer, vernetzter und dynamischer denn je ist.

Die Befragung stammt aus 2019![1]

Trusted Governance
Ein integrierter Ansatz zur Steuerung von Risiken

- ✓ Risikomanagement als „Connector“ und nicht nur „Collector“ von Informationen
- ✓ Bessere Integration als Prämisse für eine bessere Übersicht und mehr Agilität
- ✓ Klare Ausrichtung der Risikomanagementaktivitäten an den Unternehmenszielen
- ✓ Nutzung vorhandener Risikomanagementaktivitäten
- ✓ Fokus mitigierender Maßnahmen auf Risiken, die wirklich wesentlich sind

[1] 2019 Global Risk Management Study, Accenture

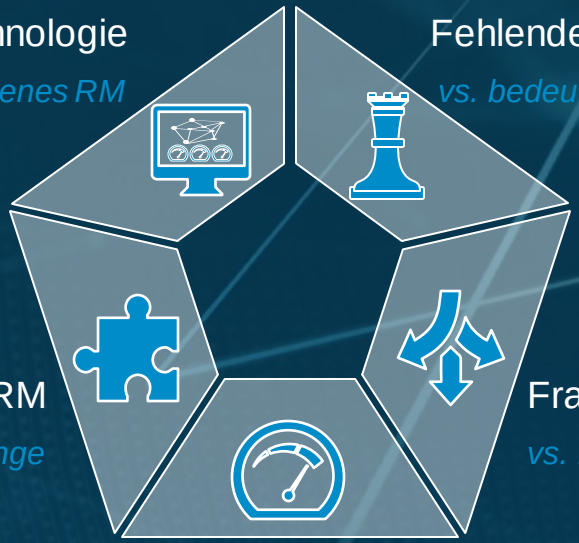
Aus unserer Erfahrung gibt es jedoch typische Fallstricke beim Verzahnen von Risikomanagementaktivitäten

Begrenzte Nutzung von Technologie

vs. vorausschauendes, datengetriebenes RM

Fehlende Verzahnung mit Strategie & Zielen

vs. bedeutsames, wertstiftendes RM



Heterogenes, inkonsistentes RM

vs. Transparenz über Zusammenhänge

Fragmentierte, unklare Governance

vs. Integration durch Föderalismus

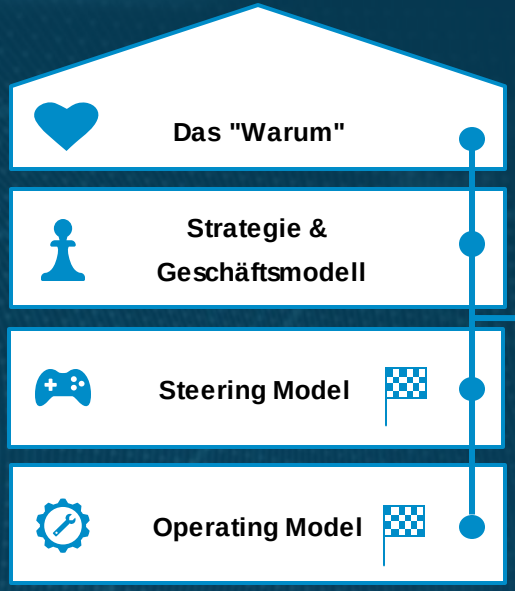
„Überkontrolle“ unkritischer Risiken

vs. Management relevanter Risiken, um Ziele besser zu erreichen

Wenn Unternehmensziele an den Werten und der Strategie ausgerichtet sind, warum nicht auch Risiken?

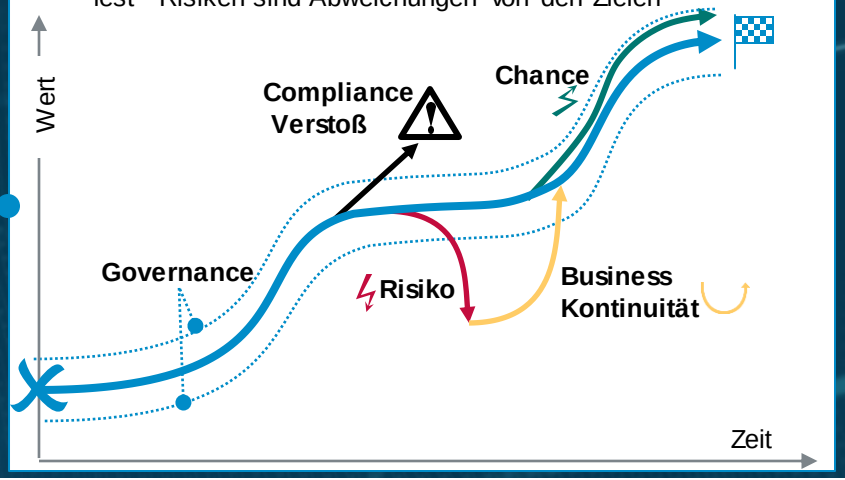
… schließlich sind Risiken Abweichungen von Zielen!

Wertebasiert ...



… das Wesentliche mit dem RM verknüpfen

- Das Risikomanagement muss zum "Warum" beitragen...
- Strategien legen Maßnahmen zur Erreichung von Zielen fest - Risiken sind Abweichungen von den Zielen



Ein integrierter Risikomanagement-Ansatz wird dazu beitragen, dass die Ziele zuverlässiger erreicht werden und gleichzeitig die vorher festgelegten Grenzen eingehalten werden.

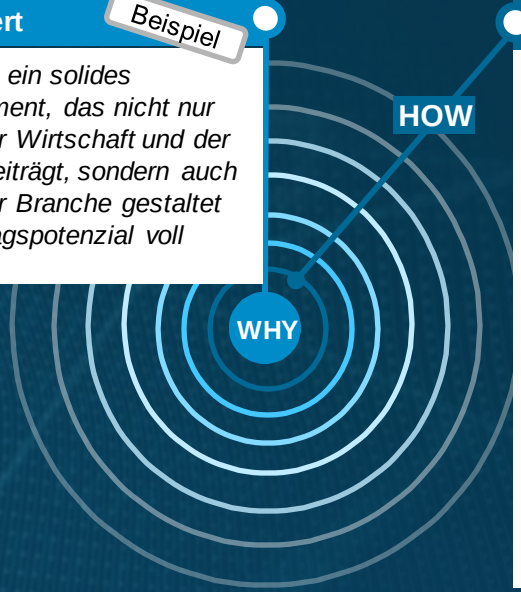
Das gemeinsame „Warum“ legt den Grundstein der Integration, das „Wie“ hängt von der Governance ab

… der Fokus liegt auf der Schaffung von Konsistenz, nicht dem Ersetzen von bereits Vorhandenem!

Wertebasiert

Beispiel

Wir glauben an ein solides Risikomanagement, das nicht nur zum Aufbau der Wirtschaft und der Gesellschaft beiträgt, sondern auch den Wandel der Branche gestaltet und unser Ertragspotenzial voll ausschöpft.



EIN integratives Rahmenwerk über die Organisation für Konsistenz

Wir nennen dieses Rahmenwerk **„Trusted Governance“:**

- Ein integrativer Rahmen für **alle Aktivitäten zur Steuerung von Risiken** und somit zur **zuverlässigeren Erreichung von Zielen**

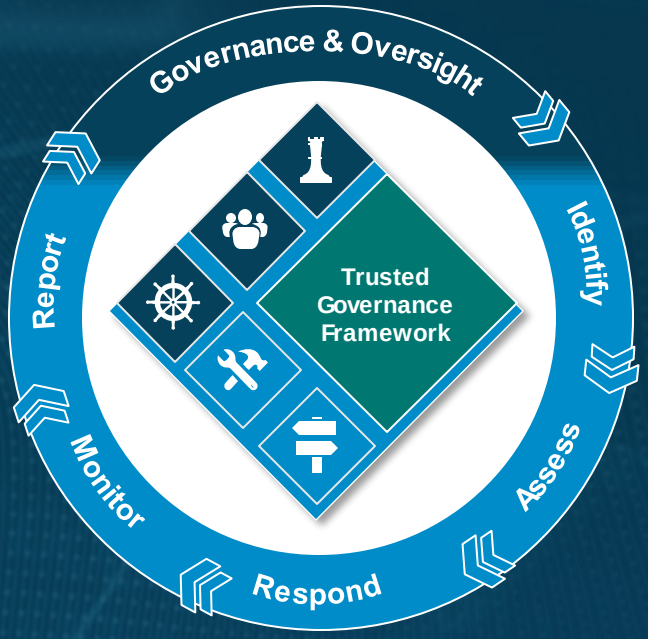
Konsistenz durch Subsidiarität:

Dieser Rahmen bildet **kein Korsett**, sondern vielmehr eine **Grundlage** für **konsistente Risikomanagementaktivitäten**

- Klare **Mindeststandards** entlang der Elemente des Rahmens für **Konsistenz**
- **Freiheit**, auf diesen aufbauend, **bestehende Methoden** und **Strukturen** zu nutzen

Risiken werden Stand heute an vielen Stellen gesteuert, sowohl explizit als auch implizit…

… denn wo Ziele verfolgt werden, werden auch Maßnahmen zu deren Erreichung eingeleitet!



Everyone is a risk manager…

- … jeder identifiziert und steuert tagtäglich Risiken
- … dabei wird stets eine Art „PDCA“-Zyklus durchlaufen
- … dies geschieht häufig im Kontext des Risikos und ohne es explizit „Risikomanagement“ zu nennen
- … Risiken sollten möglichst dort gesteuert werden, wo sie anfallen – für eine effektive und schnelle Steuerung

Beispiel

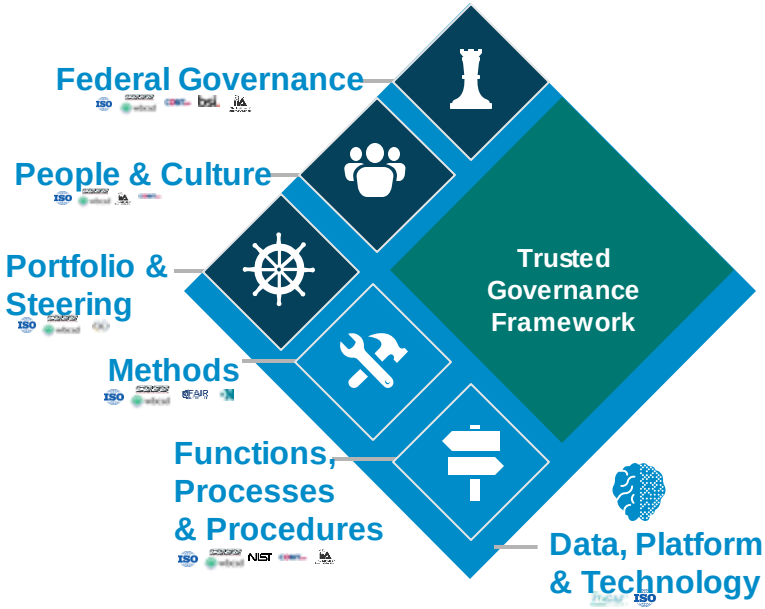
Mitarbeiterfluktuation

Kundenzufriedenheit

CO_2 Einsparungen

… ein integrativer Rahmen verzahnt bestehende Praktiken und schafft Konsistenz

… folgende Elemente bilden das Fundament für die Risikomanagementaktivitäten einer Organisation!



- ✓ **„Kleinster gemeinsamer Nenner“**

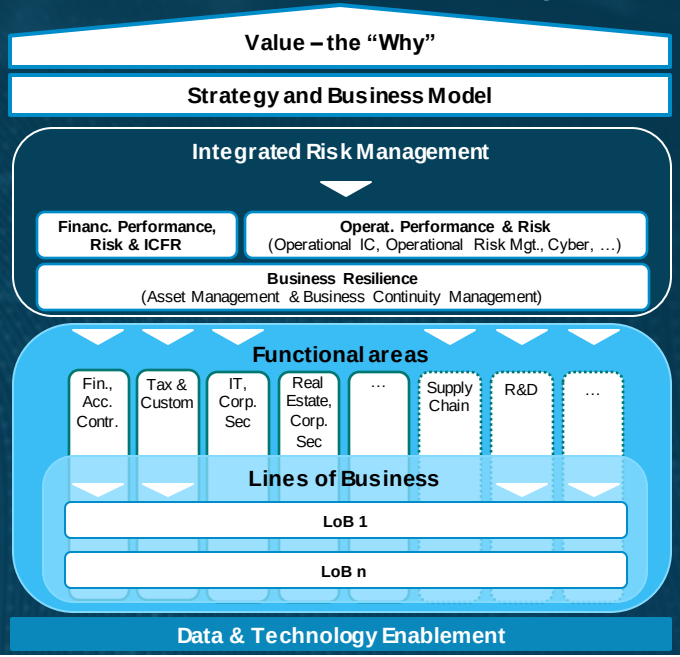
  Durch eine verbindliche Definition von Mindestanforderungen in jedem dieser Elemente wird der „kleinste gemeinsame Nenner“ für Konsistenz geschaffen

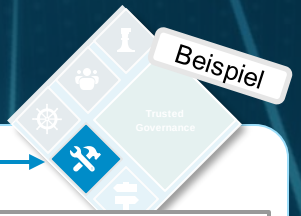
- ✓ **Flexibilität durch Subsidiarität**

  Darauf aufbauend können Risikomanagementpraktiken dezentral weiter auf individuelle Bedürfnisse ausspezifiziert werden, im Sinne der Subsidiarität

Die organisatorische Verzahnung des Rahmenwerks setzt ein klares Verständnis der Governance voraus

… am Beispiel der Methodik zeigt sich, wie aus dem Prinzip der Subsidiarität eine integrative Plattform wird!



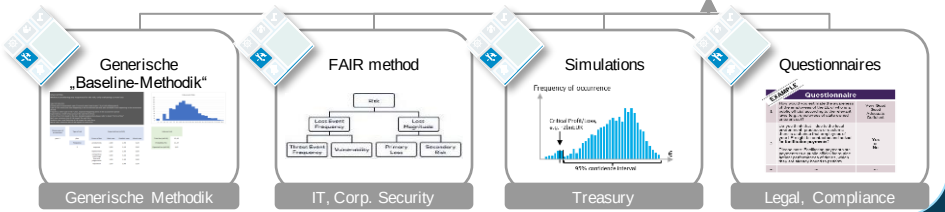


Beispiel für **„Methods, Treatments & Controls"**

- ✓ Risikobewertung mittels vordefinierter, konsistenter Skalen
- ✓ Methoden können variiert werden, solange Überleitbarkeit gegeben ist

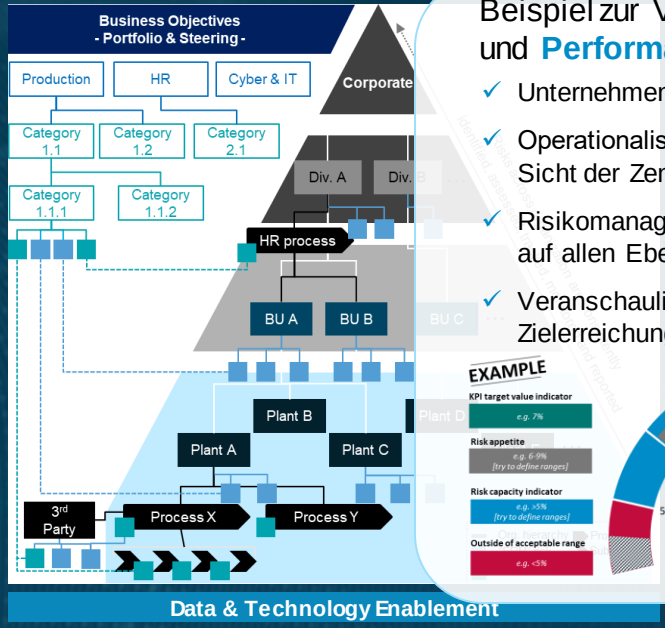
Konsistente Berichterstattung

Prinzip Subsidiarität bei der Risikobewertung



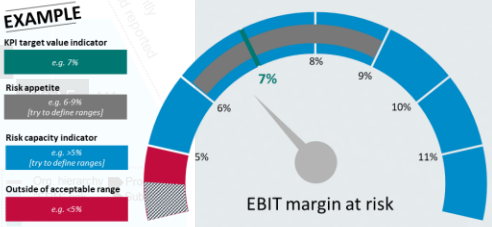
Die Ausrichtung an den Zielen und der Organisation verknüpft Risiko- und Performance Management

… Risikomanagement im Kontext des Risikos - für eine größere Transparenz über die Zielerreichung!

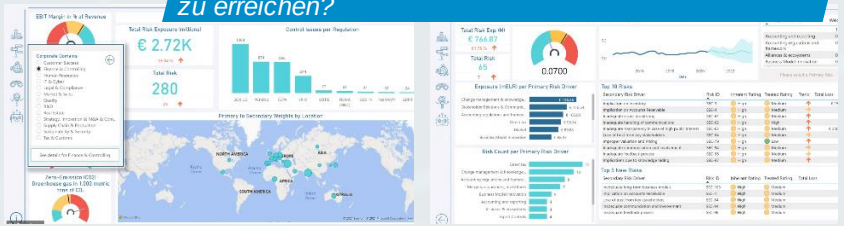


Beispiel zur Verzahnung von **Risikomanagement** und **Performance Management**

- ✓ Unternehmensziele im Einklang mit der Strategie
- ✓ Operationalisierung durch "Herunterbrechen" aus Sicht der Zentral- und Geschäftsfunktionen
- ✓ Risikomanagement identifiziert und steuert Abweichungen auf allen Ebenen der Organisation
- ✓ Veranschaulichung des prognostizierten Zielerreichungsgrades auf konsolidierter Ebene

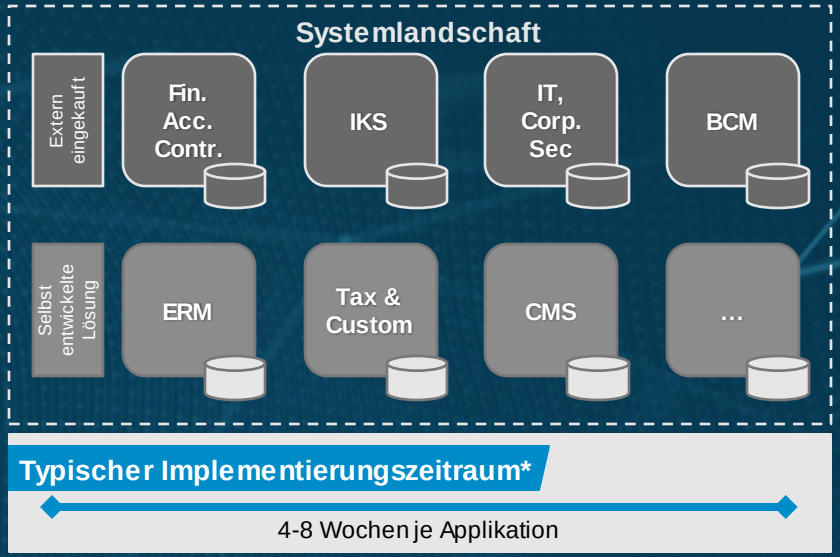


Was sind z. B. die wichtigsten Treiber, die mich daran hindern, meine Ziele (EBIT-Marge, CO2-Emissionen,…) zu erreichen?

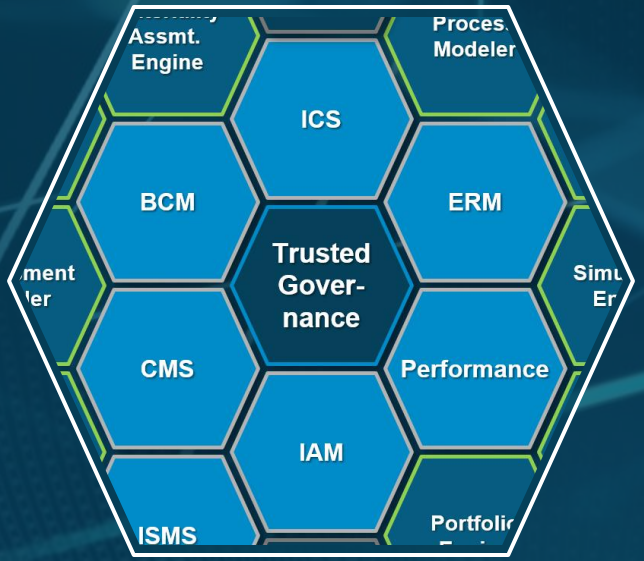


Der Plattformgedanke steht und fällt mit der technologischen Basis

Applikationen für einzelne Funktionen zu entwickeln oder einzukaufen, ist einfach …



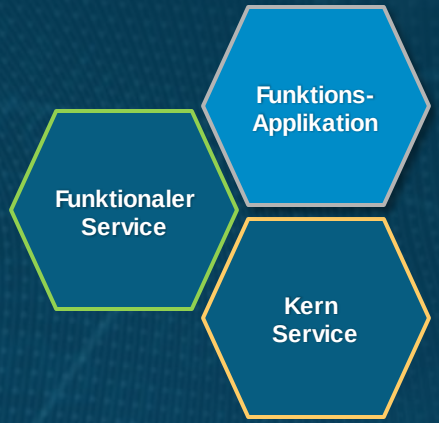
… doch für eine *Trusted Governance* benötigt es Applikationen, die zusammenarbeiten

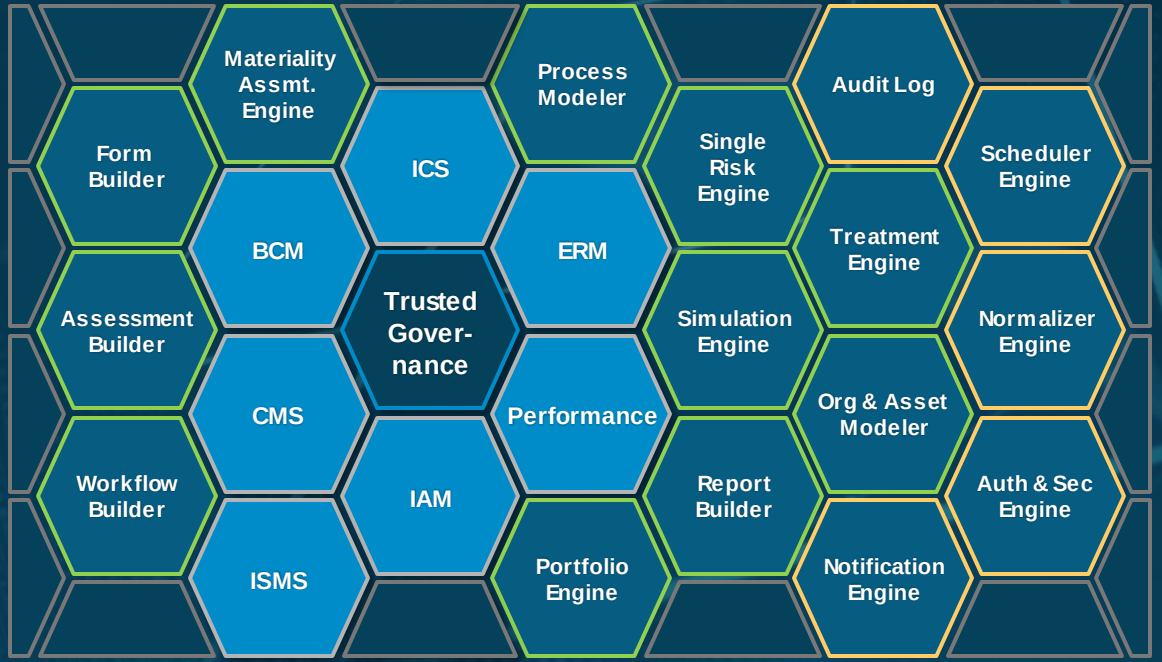


* Beispiel: Horváth CoRi ERM Module

Hierfür muss nicht nur methodisch, sondern auch technologisch eine gemeinsame Basis geschaffen werden

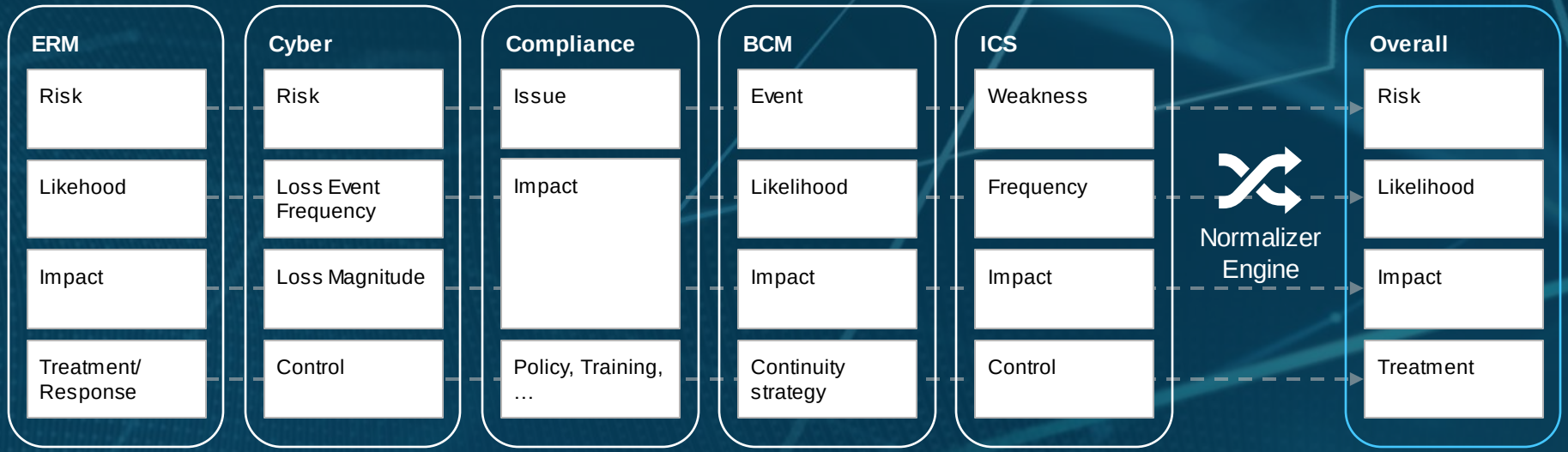
Verschiedene Services werden auf einer gemeinsamen Plattform entwickelt und können somit von allen Funktions-Applikationen genutzt werden





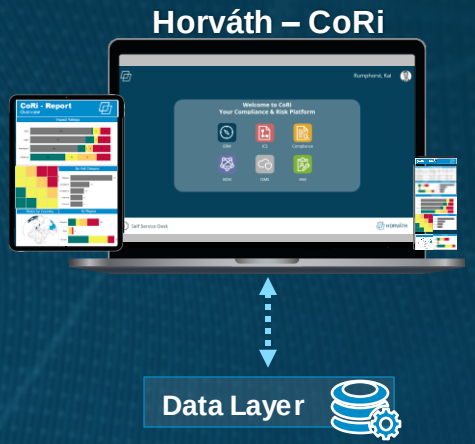
Die Kunst ist es, Flexibilität zu gestatten und trotzdem „eine Sprache“ zu sprechen

Die Applikationen je Funktion bieten spezifische Bewertungslogiken, die in der Plattform in eine gemeinsame Taxonomie überführt werden – somit können die Apps miteinander kommunizieren

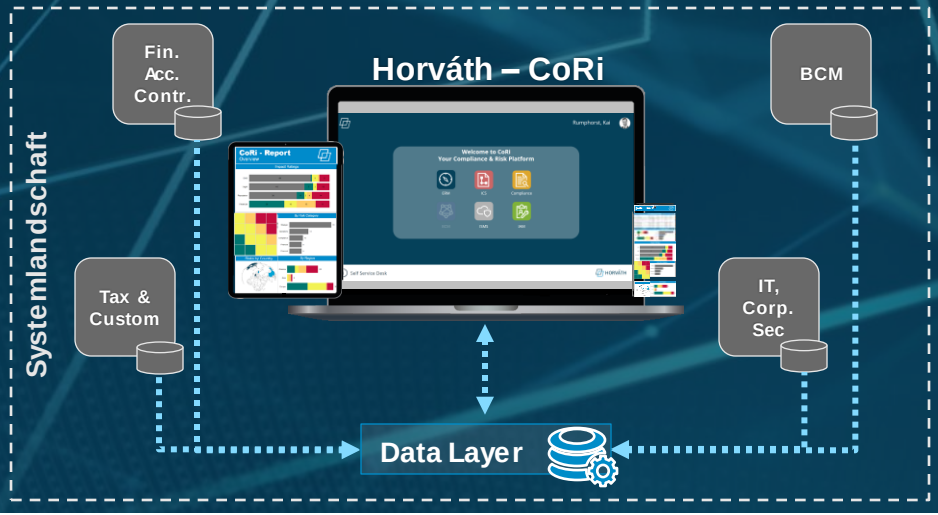


Das klare Ziel ist es, einen holistischen Blick über die Risikolandschaft zu gewinnen…

… mit Hilfe einer Solution-Plattform, die alle Funktionen bedienen kann – mit Applikationen wie aus einem Guss



… oder durch das Verzahnen bestehender Apps mittels einer Integrationsplattform



… und das idealerweise durch noch besser verzahnte Risikoinformationen, da 1+1 nicht immer 2 ist

Ihre Horváth Kontakte

Daniel Cassel

Senior Project Manager
Risk & Compliance Excellence

Mobil: +49 162 2557543
DCassel@horvath-partners.com

Kai Rumphorst

Managing Consultant
Risk & Compliance Excellence

Mobil: +49 172 6297330
KRumphorst@horvath-partners.com


HORVÁTH