





# „GRC als integratives Managementsystem“

Risk Management Congress, 17. Mai 2022

Tobias Schöffel, Schleupen SE & Alexander Hilsbos, Insel Gruppe AG

# AGENDA

1. Vorstellung
2. Integrative GRC Systeme
3. Fallbeispiel Insel Gruppe AG
4. Zusammenfassung
5. Diskussion & Fragen

# Referenten



**Tobias Schöffel**

**Bereichsleiter Markt**

Schleupen SE, Ettlingen

Deutschland



**Alexander Hilsbos**

**Leiter Risk Management**

Insel Gruppe AG, Bern

Schweiz

# Schleupen SE

**Gründung 1970**  
durch Leo Schleupen



**Umsatz 2021**  
64,8 Mio. Euro



**5 Standorte**

Ettlingen (Hauptsitz), Moers,  
Dresden, Wunstorf, Altbeken



**Mitarbeiter**  
bundesweit rund 470



**Softwarelösungen**  
Governance, Risk & Compliance  
Energie- und Wasserwirtschaft



**Businessunit GRC**

Seit 2000

Mehr als 600 Kundenprojekte



## 2. Integrative GRC Systeme

# Themenvielfalt GRC

RISIKOMANAGEMENT

INFORMATIONSSICHERHEIT

INTERNES KONTROLLSYSTEM

ISMS

COMPLIANCE MANAGEMENT

AUDIT

DATENSCHUTZ

FRAGEBOGEN

MULTIDIMENSIONALE BEWERTUNG

RICHTLINIENMANAGEMENT

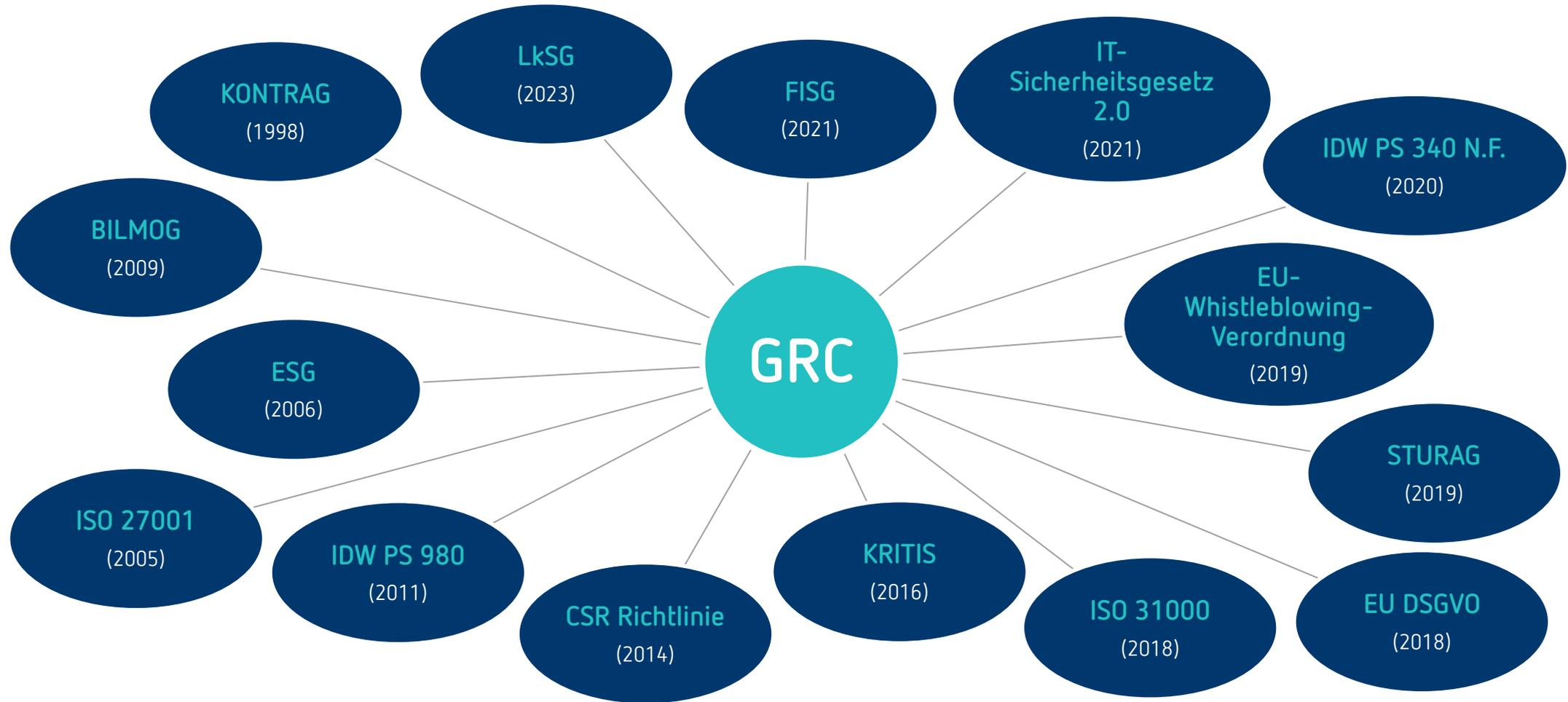
TAX COMPLIANCE

WHISTLEBLOWING

MELDE- UND HINWEISGEBERSYSTEM

SCHADENMANAGEMENT

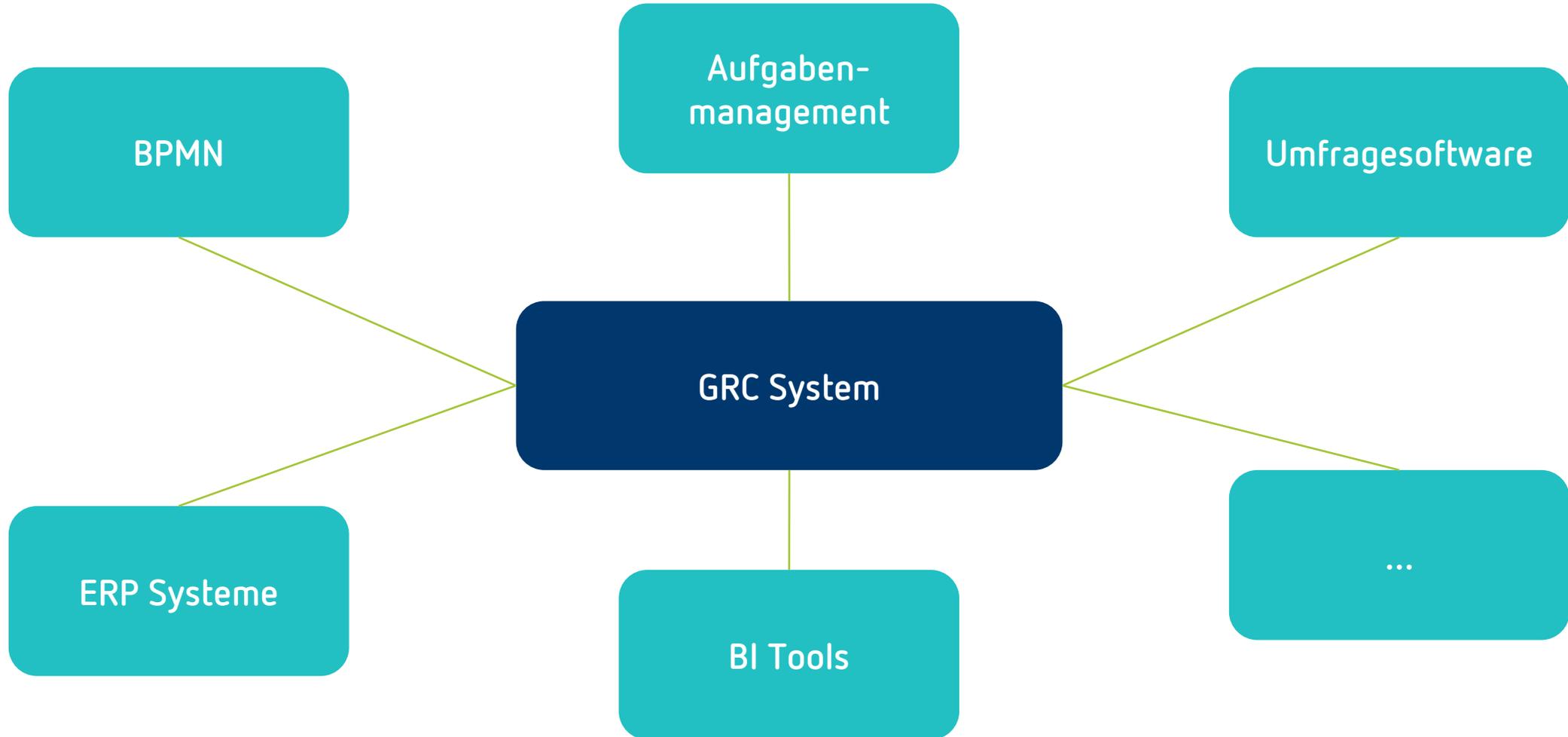
# Gesetzliche und regulatorische Anforderungen nehmen zu



# Mitarbeiter werden mit der Themenvielfalt konfrontiert



# Unterschiedliche Werkzeuge werden in Unternehmen eingesetzt



# Neue gesetzliche Anforderungen bringen unterschiedliche Themen zusammen

Bsp. LkSG



# Neue gesetzliche Anforderungen bringen unterschiedliche Themen zusammen

Bsp. LkSG

Richtlinien

Governance

Lieferanten-  
management

Risiko-  
management

Beschwerde-  
verfahren

Verantwortlich-  
keiten

The screenshot shows a software interface titled 'Eingabedialog' (Input Dialog) with a sidebar on the left and a main form area. The sidebar contains a navigation menu with items like 'Allgemein', 'Exogene Daten', 'Sanktionslistenp', 'Verknüpfte Elemente', 'Risiken', and 'Maßnahmen'. The main form area is divided into several sections: 'Allgemein' (General) with fields for 'Namenskürzel', 'Vollständiger Name', 'Logo', 'Als Meldestelle v', 'Beschreibung', 'Zeitpunkt', 'Betroffener Mandant', 'Betroffene Unternehme', and 'Entdeckung'; 'Sofortmaßnahmen' (Immediate Measures) with a table showing 'Anzahl: 1'; and 'Weitere Angaben' (Further Information) with a table showing 'Anzahl: 1'. The 'Allgemein' section also includes a list of dropdown menus: 'Recht auf Kollektivverhandlungen', 'Angemessener Lebensstandard', 'Schutz vor Folter', 'Freiheit von Sklaverei und Zwangsarbeit', 'Umweltbezogene Pflichten', 'Vereinigungsfreiheit', 'Unversehrtheit von Leben und Gesundheit', 'Schutz vor Kinderarbeit', and 'Gerechte Arbeitsbedingungen' (set to 'Ja').

# Zusammenfassung der Ausgangslage

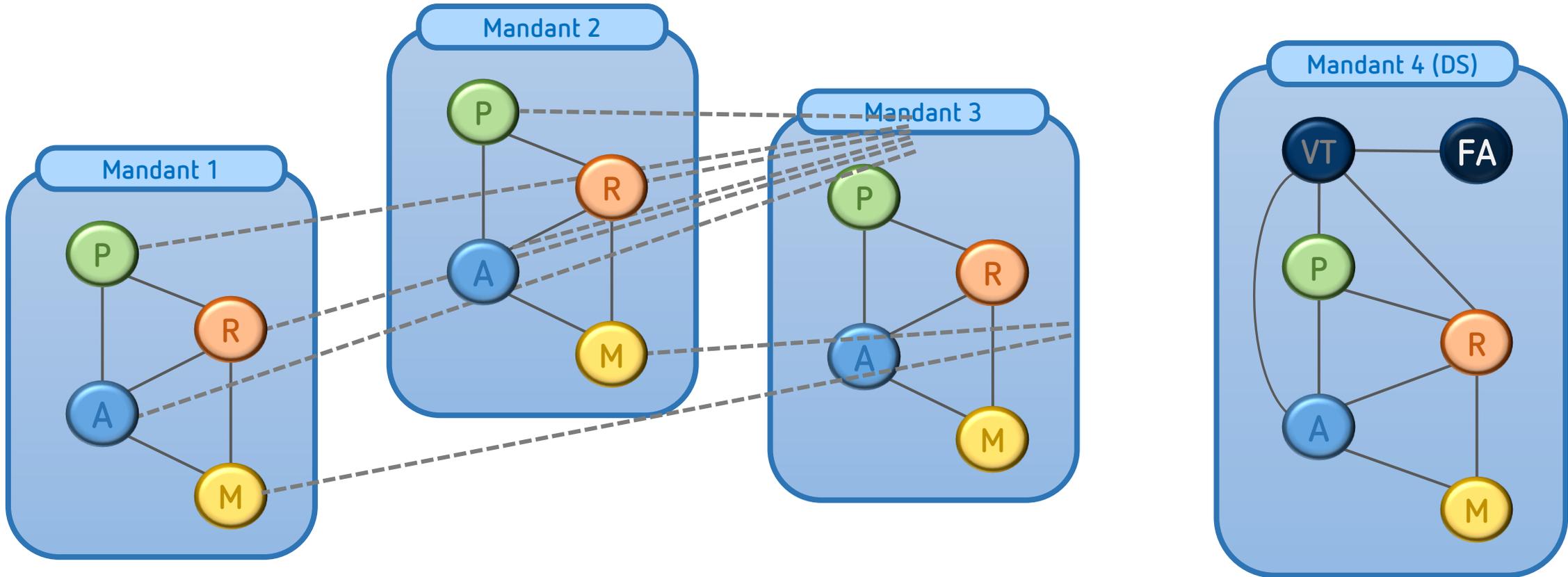


- Regulatorische Anforderungen nehmen weiter zu
- Es müssen immer mehr Governance-Themen durch die gleichen Ansprechpartner im Unternehmen bearbeitet werden
  - RiskOwner (ERM) – ControlOwner (ICS) – RiskOwner (Sec)
- Komplexität steigt
  - Bsp. IDW PS 340 n.F.
- Unterschiedliche Informationen werden pro Thema abgefragt
- Unterschiedliche Systeme sollen miteinander verzahnt werden
  - Informationen nicht doppelt pflegen
  - Experten-Tools

# Wie können digitale, integrative GRC-Lösungen unterstützen?

- **Nutzung vorhandener Informationen**
  - Erhobene Daten können miteinander „verzahnt“ werden und müssen nicht mehrfach erfasst werden
- **Integration von Experten-Tools**
  - Immer mehr wird gefordert vorhandenen Lösungen anzubinden (z.B. BPMN-Lösungen oder Reporting-Tools etc.)
- **Komplexitätsreduktion**
  - Dialoge passen sich je nach Thema an, um die Komplexität zu reduzieren und nur die geforderten Informationen anzuzeigen
- **Höhere Transparenz**
  - In integrierten Lösungen können alle Themen zentral ausgewertet werden

# Verbindung unterschiedlicher Disziplinen, Bsp. Datenschutz und ISMS



**A** = Asset

**P** = Prozess

**M** = Maßnahme

**R** = Risiko

**VT** = Verarbeitungstätigkeit

**FA** = Datenschutz-  
Folgenabschätzung

# Wie können digitale, integrative GRC-Lösungen unterstützen?

- Nutzung vorhandener Informationen
  - Erhobene Daten können miteinander „verzahnt“ werden und müssen nicht mehrfach erfasst werden
- Integration Drittsystemen (Experten-Tools)
  - Immer mehr wird gefordert vorhandenen Lösungen anzubinden (z.B. BPMN-Lösungen oder Reporting-Tools etc.)
- Komplexitätsreduktion
  - Dialoge passen sich je nach Thema an, um die Komplexität zu reduzieren und nur die geforderten Informationen anzuzeigen
- Höhere Transparenz
  - In integrierten Lösungen können alle Themen zentral ausgewertet werden

# Schnittstellen zu / Integration von Dritt-Systemen

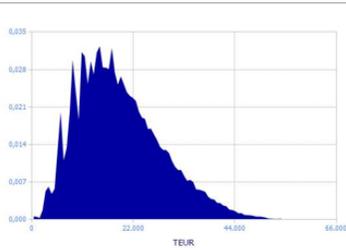
## Risikomanagement

- Spezialsoftwarelösungen zur Simulation von Risiken → Berechnung Risikotragfähigkeit

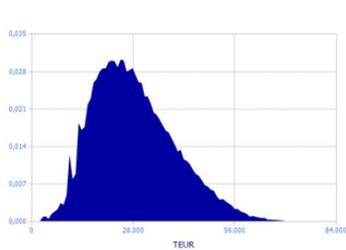
### Muster SE

Simulationsergebnisse - SIM-00000000, Konzernweites Gesamtportfolio (alle Risiken)

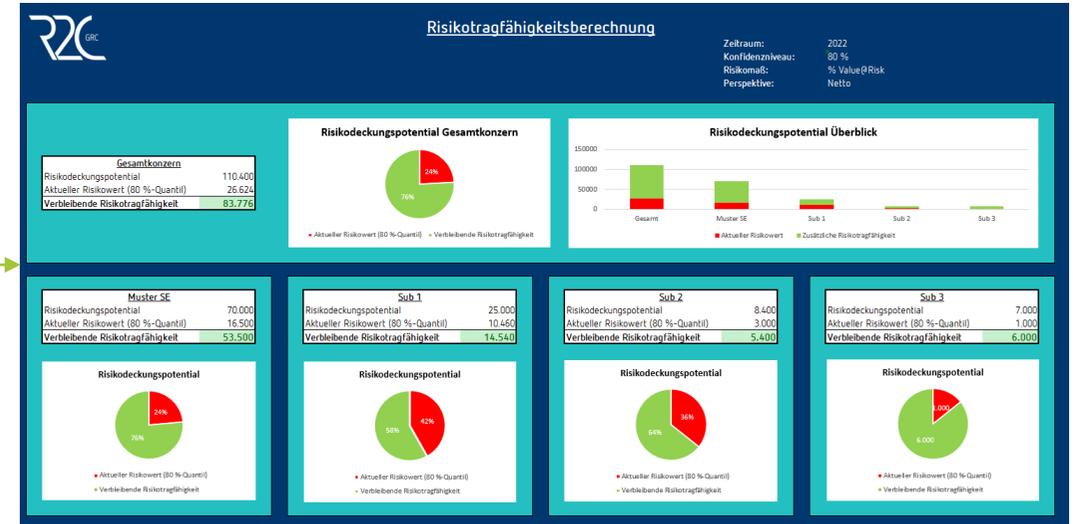
### Muster SE



2022 (Werte in TEUR)		
Konfidenzniveaus	Value@Risk	Conditional Value@Risk
50,00%	17.649	26.359
80,00%	26.624	33.325
90,00%	31.937	37.592
95,00%	36.438	41.203
99,00%	44.198	48.045
99,90%	52.834	55.741
5,00%	6.231	19.806
Erwarteter Schaden	19.050	
Standardabweichung	9.213	



2023 (Werte in TEUR)		
Konfidenzniveaus	Value@Risk	Conditional Value@Risk
50,00%	26.764	37.300
80,00%	37.707	45.696
90,00%	44.058	50.749
95,00%	49.323	55.036
99,00%	58.548	63.186
99,90%	68.964	72.306
5,00%	12.500	29.208
Erwarteter Schaden	28.229	
Standardabweichung	11.388	



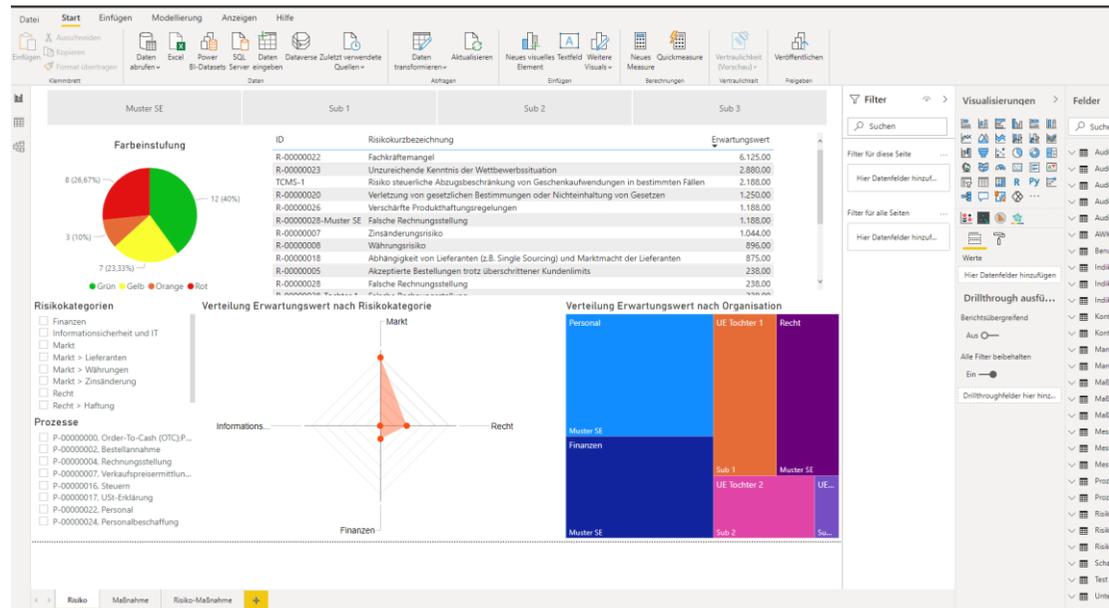


# Schnittstellen zu Dritt-Systemen

## Reporting – Microsoft PowerBI

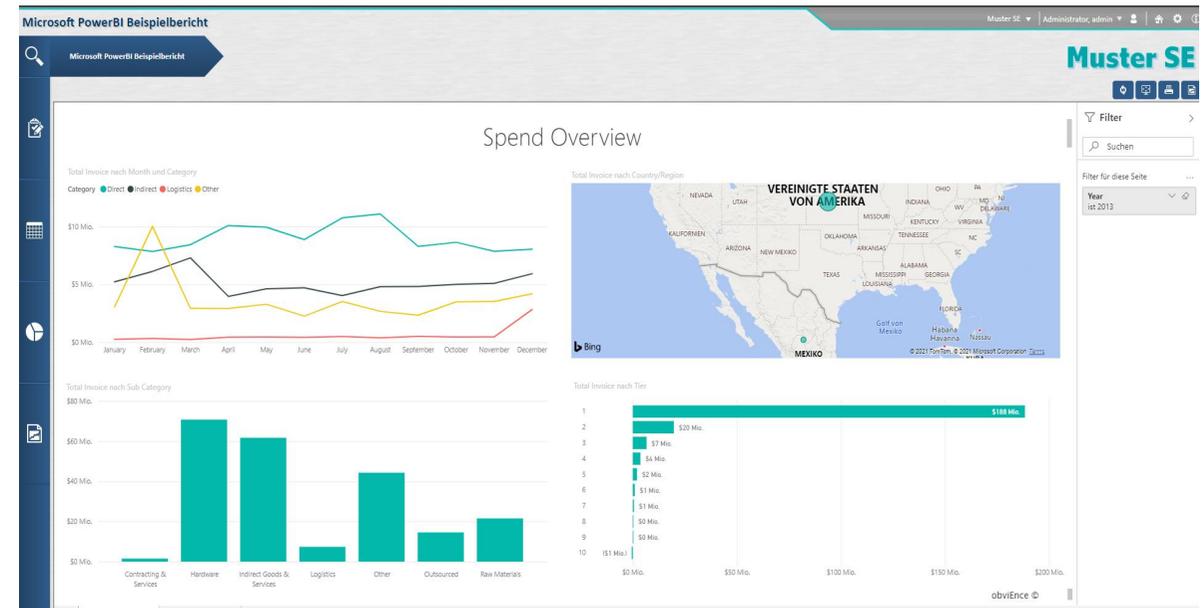
### Stand-Alone

- Nutzung per Internetzugriff auf PowerBI oder per Installation



### Integriert

- Integration in R2C



# Wie können digitale, integrative GRC-Lösungen unterstützen?

- Nutzung vorhandener Informationen
  - Erhobene Daten können miteinander „verzahnt“ werden und müssen nicht mehrfach erfasst werden
- Integration Drittsystemen (Experten-Tools)
  - Immer mehr wird gefordert vorhandenen Lösungen anzubinden (z.B. BPMN-Lösungen oder Reporting-Tools etc.)
- **Komplexitätsreduktion**
  - **Dialoge passen sich je nach Thema an, um die Komplexität zu reduzieren und nur die geforderten Informationen anzuzeigen**
- Höhere Transparenz
  - In integrierten Lösungen können alle Themen zentral ausgewertet werden

# Neue gesetzliche Anforderungen bringen unterschiedliche Themen zusammen

Es müssen immer mehr Themen durch die gleichen Ansprechpartner im Unternehmen bearbeitet werden

Dialoge müssen sich den GRC-Themenfeldern automatisch anpassen

Themenfestlegung:

Eingabedialog Mandant

Mandant  
\* Muster - ERM

Allgemein  
Namenskürzel \* Muster - ERM  
Vollständiger Name \* Muster - ERM  
Verantwortlicher  
Logo  
Beschreibung  
Risikodeckungspotenzial TEUR

Zusatzinformationen  
Art \* 2- ERM

Untergeordnete Mandanten  
Namenskürzel Übergeordneter M

Anzahl: 0 25

Dokumente  
Kurzbezeichnung Dateiname Link

Speichern Abbrechen Übernehmen Übernehmen und Parallelmandant anlegen Übernehmen und Untermandant anlegen

Dialog passt sich bei der Erfassung eines Elements automatisch an (Bsp. Risikobewertung):

Anzahl: 0

Risikobewertung  
Bewertungsschema \* Quantitativ  
Manuelle Bewertung

Eintrittsw. \* 10 % Auswirkung \* 50.000 TEUR

Risiko-  
management

Personenschäden sehr gering

Beeinträchtigung der Reputation hoch

Beeinträchtigung der Geschäftsprozesse sehr gering

Auswirkungen auf die Umwelt sehr gering

Internes Kontroll  
System

# Neue gesetzliche Anforderungen bringen unterschiedliche Themen zusammen

Es müssen immer mehr Themen durch die gleichen Ansprechpartner im Unternehmen bearbeitet werden

## Informationen je Adressatenkreis einblenden

Festlegung der Rechte / Rollen:



Informationen werden (nicht) angezeigt angezeigt:

Detailansicht: R-0000022, Fachkräftemangel

2023

Simulationsergebnisse

2022

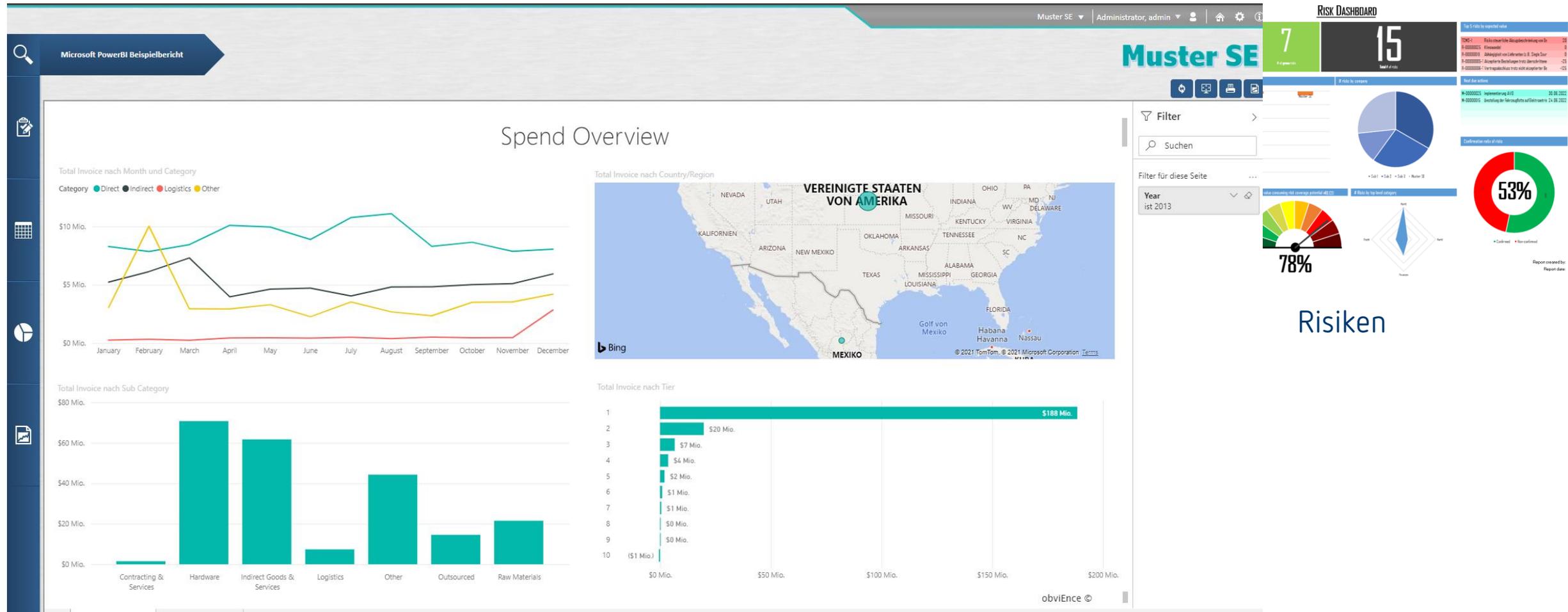
Konfidenzniveau	Value@Risk
50 %	0 TEUR
80 %	0 TEUR
90 %	100 TEUR
95 %	100 TEUR
99 %	100 TEUR
99,9 %	100 TEUR

# Wie können digitale, integrative GRC-Lösungen unterstützen?

- Nutzung vorhandener Informationen
  - Erhobene Daten können miteinander „verzahnt“ werden und müssen nicht mehrfach erfasst werden
- Integration Drittsystemen (Experten-Tools)
  - Immer mehr wird gefordert vorhandenen Lösungen anzubinden (z.B. BPMN-Lösungen oder Reporting-Tools etc.)
- Komplexitätsreduktion
  - Dialoge passen sich je nach Thema an, um die Komplexität zu reduzieren und nur die geforderten Informationen anzuzeigen
- Höhere Transparenz
  - In integrierten Lösungen können alle Themen zentral ausgewertet werden

# Wie können digitale, integrative GRC-Lösungen unterstützen?

## ■ Zusammenhänge erkennen – Transparenz schaffen



# Welche Vor- und Nachteile lassen sich ableiten?

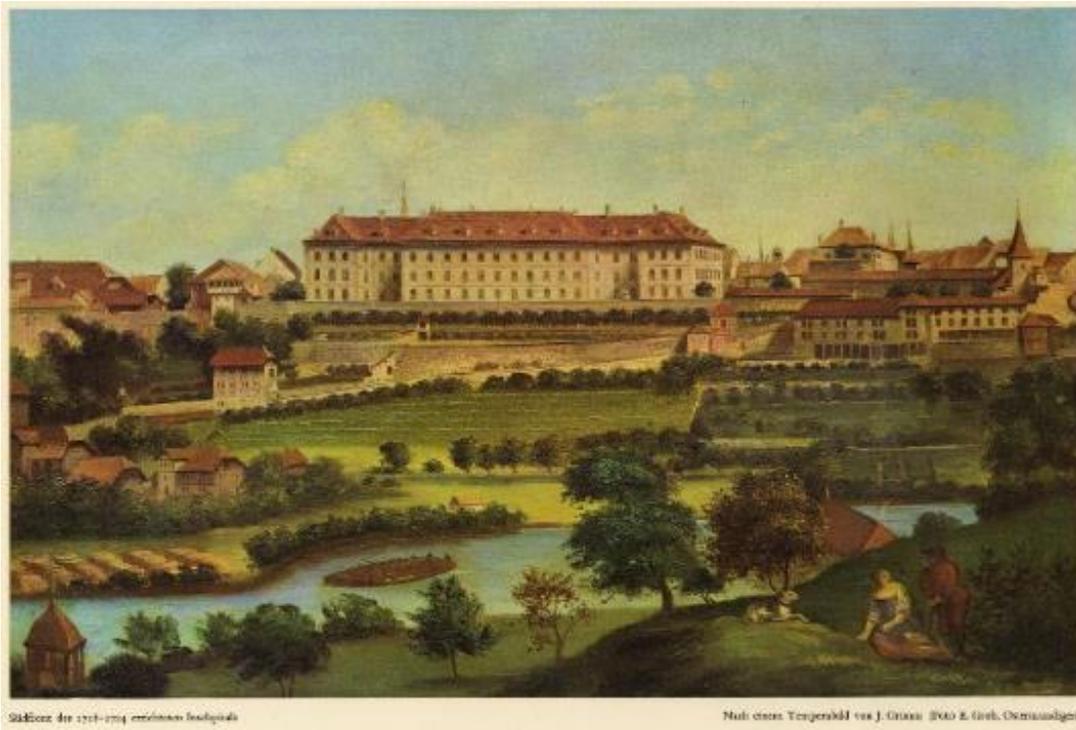
Chancen	Risiken
<ul style="list-style-type: none"><li>▪ Geforderte Funktionalitäten einzelner Themen können auch in anderen Disziplinen Anwendung finden<ul style="list-style-type: none"><li>▪ Kontrollen zur Risikosteuerung</li><li>▪ Fragebögen z.B. zur Ermittlung geeigneter Verteilungsfunktionen</li><li>▪ ...</li></ul></li><li>▪ Vorhandene Informationen können angebunden und übergreifend genutzt werden<ul style="list-style-type: none"><li>▪ Meldungen z.B. als Indikatoren nutzen</li></ul></li></ul>	<ul style="list-style-type: none"><li>▪ Gefordert Funktionsvielfalt kann zu überfrachteten Eingabedialogen führen</li><li>▪ Kognitive Überforderung der Benutzer</li></ul>

# 3. Fallbeispiel Insel Gruppe AG

Alexander Hilsbos, Leiter Risk Management

# Die Insel Gruppe

## Geschichtliches



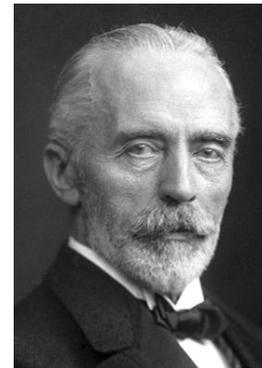
Bildquelle: <http://www.inselgruppe.ch/de/die-insel-gruppe/geschichte-des-inselspitals/>

# INSELGRUPPE

Die älteste Organisation in der Schweiz,  
die seit dem Jahr

# 1354

im gleichen Geschäft tätig ist.



Theodor Kocher  
Nobelpreis für Medizin 1909

Bildquelle: [https://de.wikipedia.org/wiki/Theodor\\_Kocher](https://de.wikipedia.org/wiki/Theodor_Kocher)

# Die Insel Gruppe

## Struktur heute

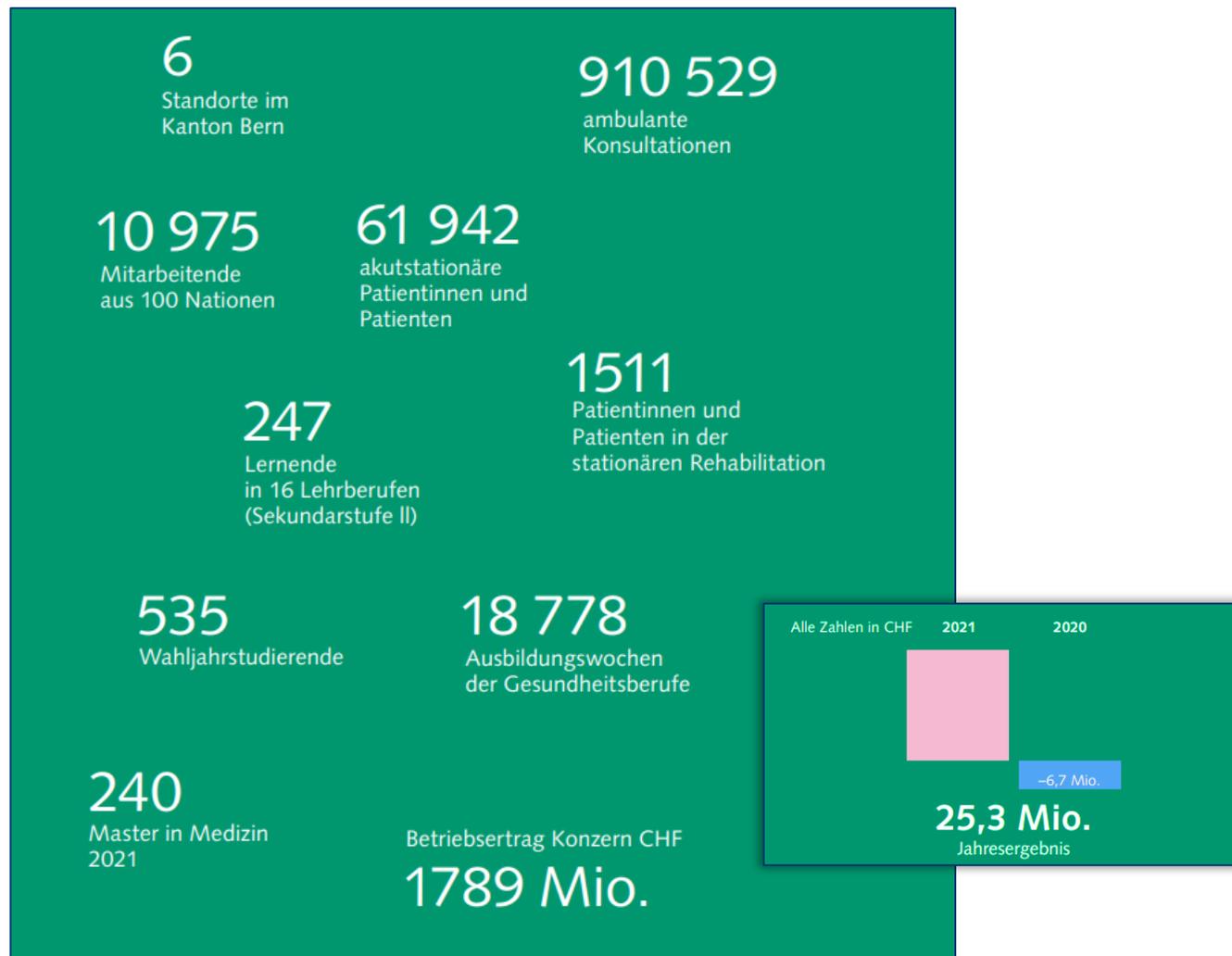
- Grösstes medizinisches Leistungszentrum in der Schweiz
- Universitätsspital der medizinischen Fakultät der Uni Bern
- Mehr als 42 Universitätskliniken in 11 Medizinbereichen, internationale Forschungstätigkeit
- Eigene Betriebsfeuerwehr, 7 Restaurants, Bewachstation, Areal etwa gleich gross wie die Berner Altstadt



Bildquelle: [www.inselgruppe.ch/de/die-insel-gruppe/](http://www.inselgruppe.ch/de/die-insel-gruppe/)

# Die Insel Gruppe in Zahlen

Geschäftsjahr 2021



## Personalbestand nach Berufsgruppen in Vollzeiteinheiten 100%: 8444 ohne Auszubildende (73% Frauen; 27% Männer)



36,7%  
Pflegepersonal:  
3096



2,1%  
Technischer  
Dienst: 179



18,2%  
Ärztinnen/  
Ärzte: 1534



3,2%  
Akademisches  
Personal: 274



8,2%  
Medizinisch-  
technisches  
Personal: 697



0,8%  
Sozialdienst,  
Seelsorge, Kita:  
66



3,6%  
Medizinisch-  
therapeutisches  
Personal: 303



9,5%  
Hauswirtschaft:  
805



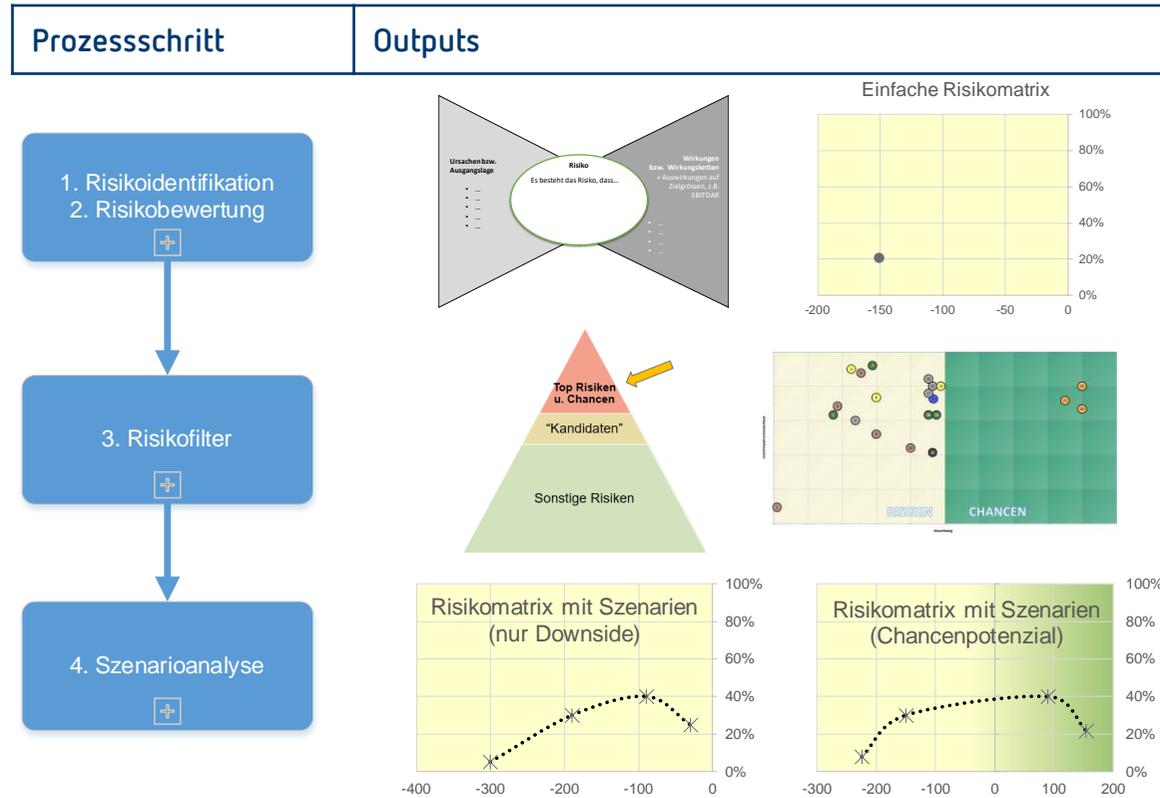
17,3%  
Verwaltung:  
1464



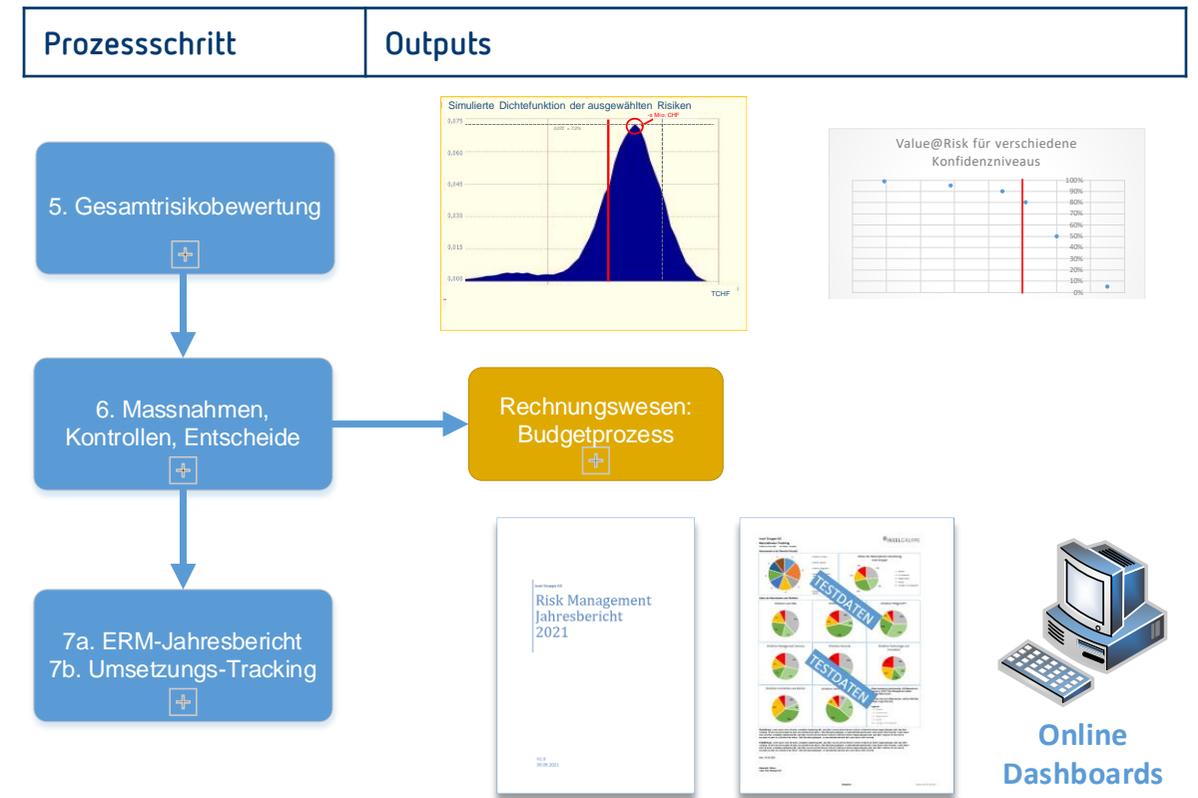
0,3%  
Nachtwachen:  
26

# Risk Management System der Insel Gruppe

## Hauptprozess mit Outputs



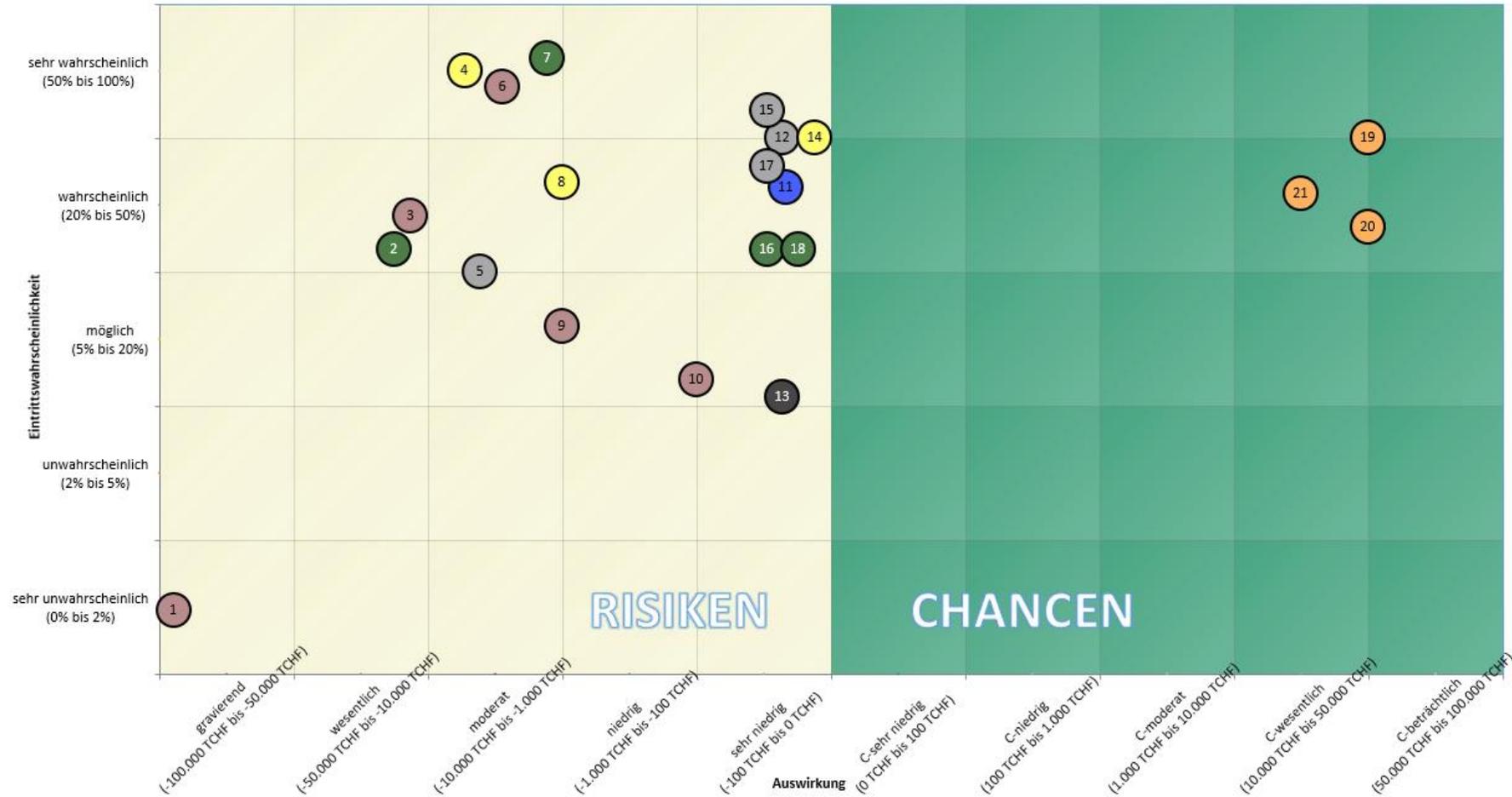
- An die ISO 31000 angelehnt
- Kombination von klinischen, technischen und betriebswirtschaftlich-administrativen Risiken



- Scope: Gesamte Insel Gruppe; alle Direktionen und Medizinbereiche
- Rollenkonzept mit Risikoeigner, Risikofachperson, Massnahmeneigner

# Risk Management System der Insel Gruppe

## Risiko- / Chancenmatrix

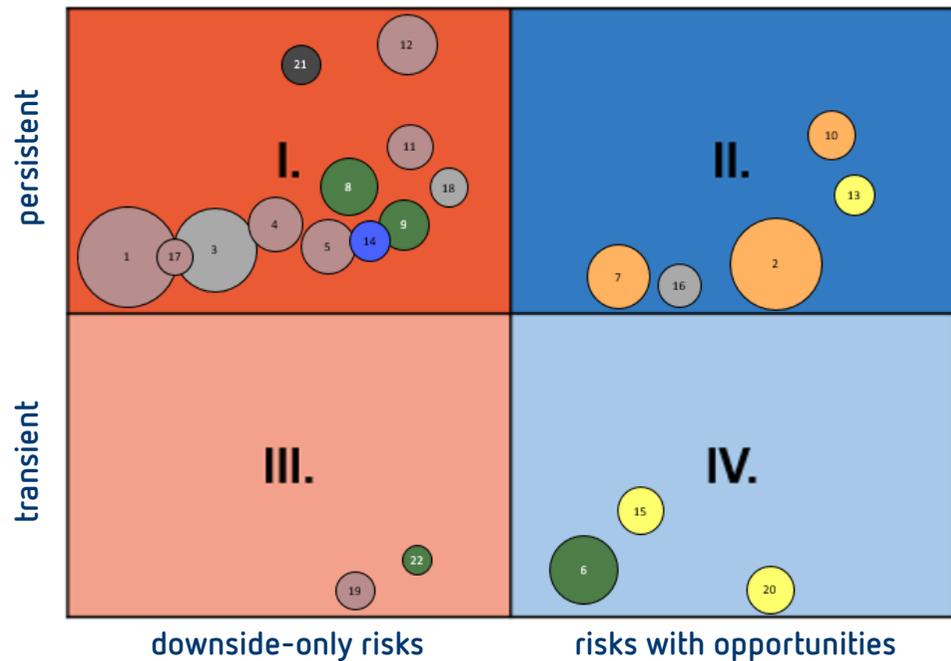


RISIKEN

CHANCEN

# Alternative Risikomatrix

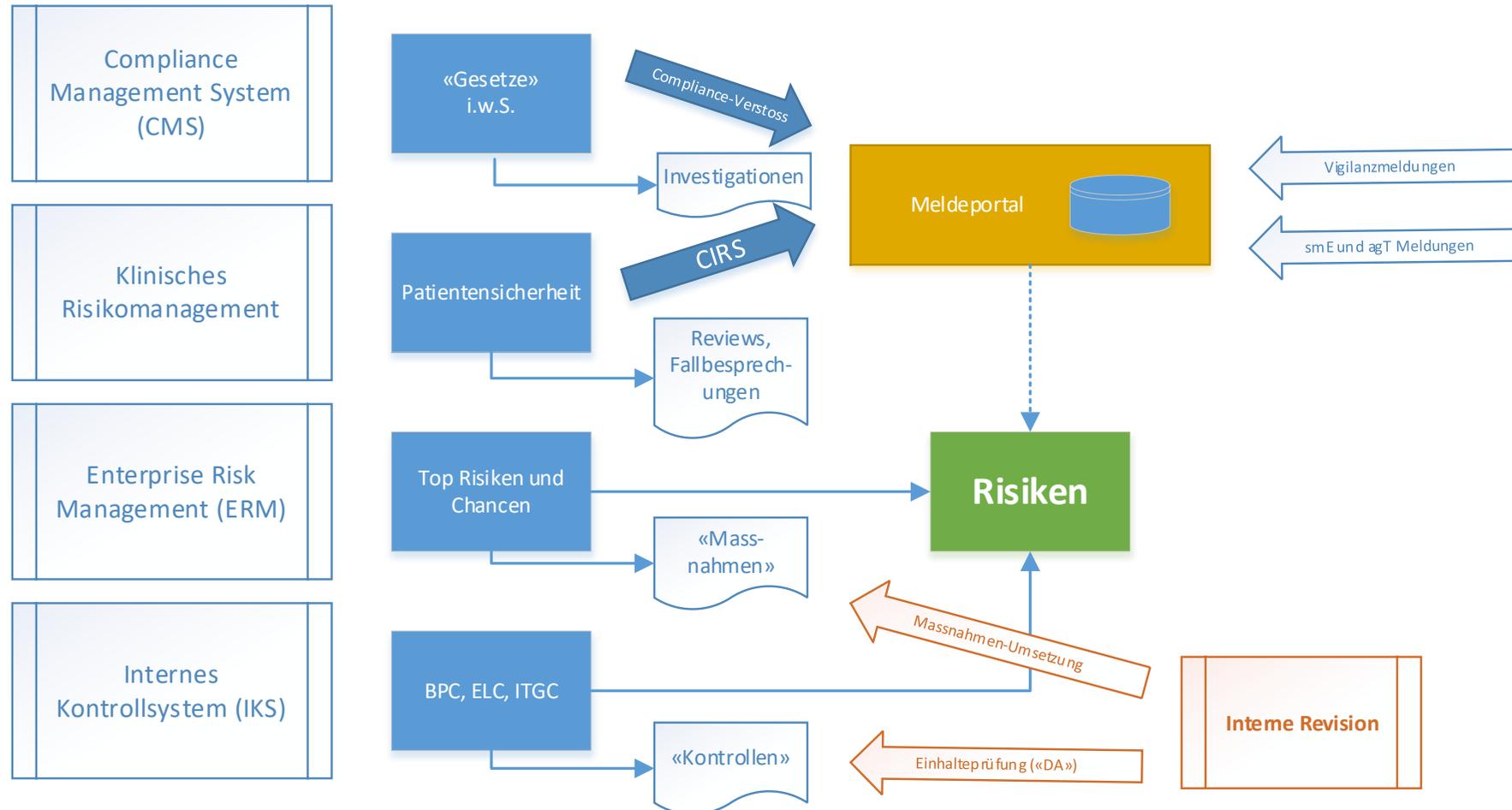
Risiken im Gesundheitswesen sind dauerhafter Natur



I.	<p>Dauerhafte Risiken mit Schadenspotenzial, diese verbleiben langfristig auf der Risikomatrix.</p> <p><b>Strategie:</b> Beeinflussung von Schadenshöhe u./o. Reduktion der Eintrittswahrscheinlichkeit (p). Einrichten <b>regelmässiger Kontrollen</b> bzw. <b>Nachweis der kontinuierlichen Mitigierung</b>.</p> <p><b>Beispiele:</b> Grossbrand, Cyber-Angriff, Patientenschädigung</p>
II.	<p>Dauerhafte Risiken mit Chancenpotenzial.</p> <p><b>Strategie:</b> Konsequenter Fokus auf nachhaltiges Erschliessen des Chancenpotenzials. Nachweis durch <b>Kontrollen</b>, ggf. Audits.</p> <p><b>Beispiele:</b> Angebotsstrategie, Bauprojekte, Forschungsprojekte</p>
III.	<p>Vorübergehende Risiken mit Schadenspotenzial. Nach erfolgreicher Umsetzung von Massnahmen verschwinden diese Risiken.</p> <p><b>Strategie:</b> Massnahmen zur Vermeidung u./o. Verminderung.</p> <p><b>Beispiele:</b> Rückbau BHH, Sanierung FKL</p>
IV.	<p>Vorübergehende Risiken mit Chancenpotenzial. Verschwinden durch erfolgreiche Massnahmenumsetzung oder ggf. externe Faktoren.</p> <p><b>Strategie:</b> Fallweises Erschliessen des Chancenpotenzials durch <b>Massnahmen</b> (z.B. Projekte), sofern realistisch und realisierbar. Ggf. Projekt-Audits.</p> <p><b>Beispiele:</b> EPD, KISS</p>

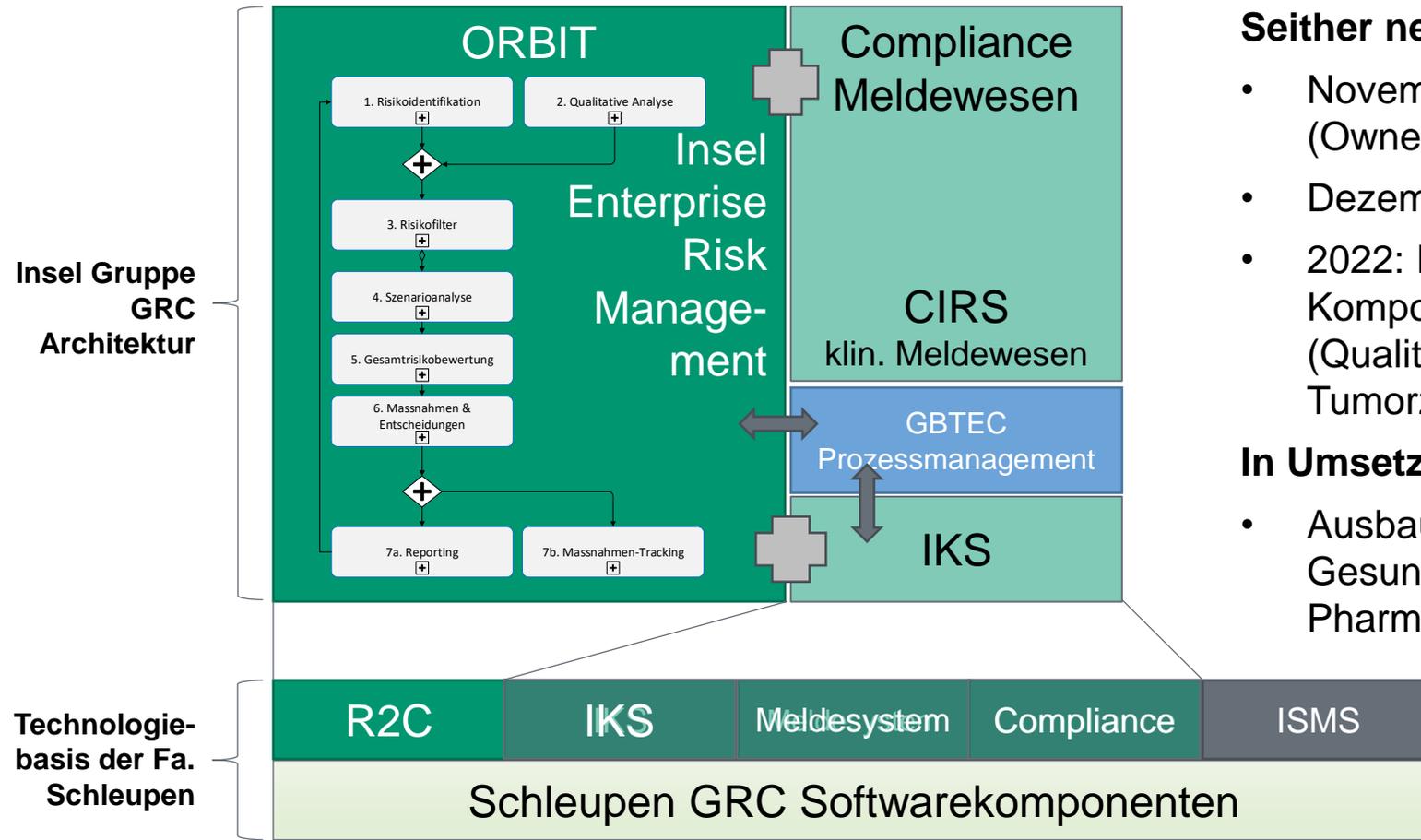
# Risk Management Prozess der Insel Gruppe

## Integrierte – risikozentrierte Perspektive



# GRC-Architektur der Insel Gruppe

## Entwicklung von April 2020 bis heute



Quelle: Schlepen Website [grc.schlepen.de](http://grc.schlepen.de)

### Seither neu hinzugekommen sind:

- November 2020: Compliance-Meldewesen (Owner: Compliance Officer)
- Dezember 2021: IKS-Modul (Owner: Leiter IKS)
- 2022: Intensive Nutzung der Risk Management-Komponente für diverse ISO-Zertifizierungen (Qualitätsmanagement, Labormedizin, Tumorzentren)

### In Umsetzung:

- Ausbau Meldewesen für Pflichtmeldungen im Gesundheitssektor (Materiovigilanz, Hämovigilanz, Pharmacovigilanz, Strahlenexposition)
- Anbindung Prozessmanagement
- Ablösung CIRS (Meldesystem für Beinahe-Unfälle, geplant)

## 4. Zusammenfassung

# Zusammenfassung

- Silo vs. Integrativ
  - Weiterhin werden in vielen Unternehmen die einzelnen Themen alleine voneinander betrachtet und bearbeitet
- „Offene GRC-Systeme“ → Integration von Drittsystemen nimmt zu
  - Reporting Werkzeuge (z.B. MS PowerBI)
  - Anbindung von Drittsystemen (BPMN Lösungen, Umfrage Tools...)
- Die Anforderungen an die Themen/Disziplinen steigen
  - Bsp. IDW PS 340 n.F.
- Neue gesetzliche Anforderungen müssen erfüllt werden
  - Bsp. LkSG

# 5. Diskussion und Fragen

**VIELEN DANK!**