

Willkommen zum

# GRC Day 2024

---

Deep Dive into the World of  
Governance, Risk, and Compliance



**Christian Buechler**  
*GRC Consulting & Training*



# Folgen Sie uns auf LinkedIn!

Es erwarten Sie Neuigkeiten, Trends und Informationen rund um das Thema GRC.



<https://linkedin.com/company/gbtec-group>

# Agenda des GRC Day 2024



# Agenda des GRC Day 2024



**Martin Tanzer**  
GRC Solution Architect  
**Matthias Singer**  
Sales Specialist & Account Manager

**BIC Security GRC:**  
Umfassender Schutz Ihrer  
gesamten Unternehmenswerte

13:30 – 14:10

14:10 – 14:50

## Success Story:

Umfassende Integration von  
ISMS & BCM bei DEW21, dem  
Energie- und Wasserversorger  
der Stadt Dortmund

**Jens Feistel**  
Informationssicherheits-Beauftragter,  
DEW21



## Pause & Networking

14:50 – 15:10

15:10 – 15:40

## Expert Talk:

Verschiedene Aspekte einer  
gelungenen Unternehmensstrategie

**Kaspar Kühl, Samuel Brandstätter,  
Philipp Strokosch, Christian Buechler**



**Samuel Brandstätter &  
Christian Buechler**

**Key Takeaways &  
Verabschiedung**

15:40 – 16:00



## **Samuel Brandstätter**

*Head of Product Line GRC &  
Managing Director GBTEC Austria*



# Governance, Risk, and Compliance

---

Innovative Lösungen für Top Performance

Samuel Brandstätter

# Vereinbaren Sie ein unverbindliches Gespräch mit uns!

Stellen Sie uns kostenlos Ihre Fragen rund  
um Governance, Risk und Compliance



[https://outlook.office365.com/  
owa/calendar/GRCSales@gbtec.com  
/bookings/](https://outlook.office365.com/owa/calendar/GRCSales@gbtec.com/bookings/)





**Philipp Strokosch**  
*Head of Sales GRC*



# GRC-Solutions

---

Umfassende Abdeckung vielfältiger GRC-Bereiche

**Philipp Strokosch**

# Agenda

- 01 Neueste Trends auf dem Markt für GRC-Tools
- 02 Mit BIC GRC Schritt für Schritt den Reifegrad verbessern
- 03 Integrated GRC: Die nächste Stufe für Ihren Reifegrad
- 04 Zusammenfassung und Ausblick

# Neueste Trends auf dem Markt für GRC-Tools

## Single- und Multiple-Point GRC-Solutions

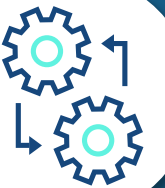
- Speziell für einzelne GRC-Anwendungsfälle entwickelt
- Keine Verknüpfung oder Integration mit anderen GRC-Systemen
- Geringe Konfigurierbarkeit / Anpassungsfähigkeit
- Begrenzte Möglichkeiten zur Workflow Steuerung

**BIC**GRC

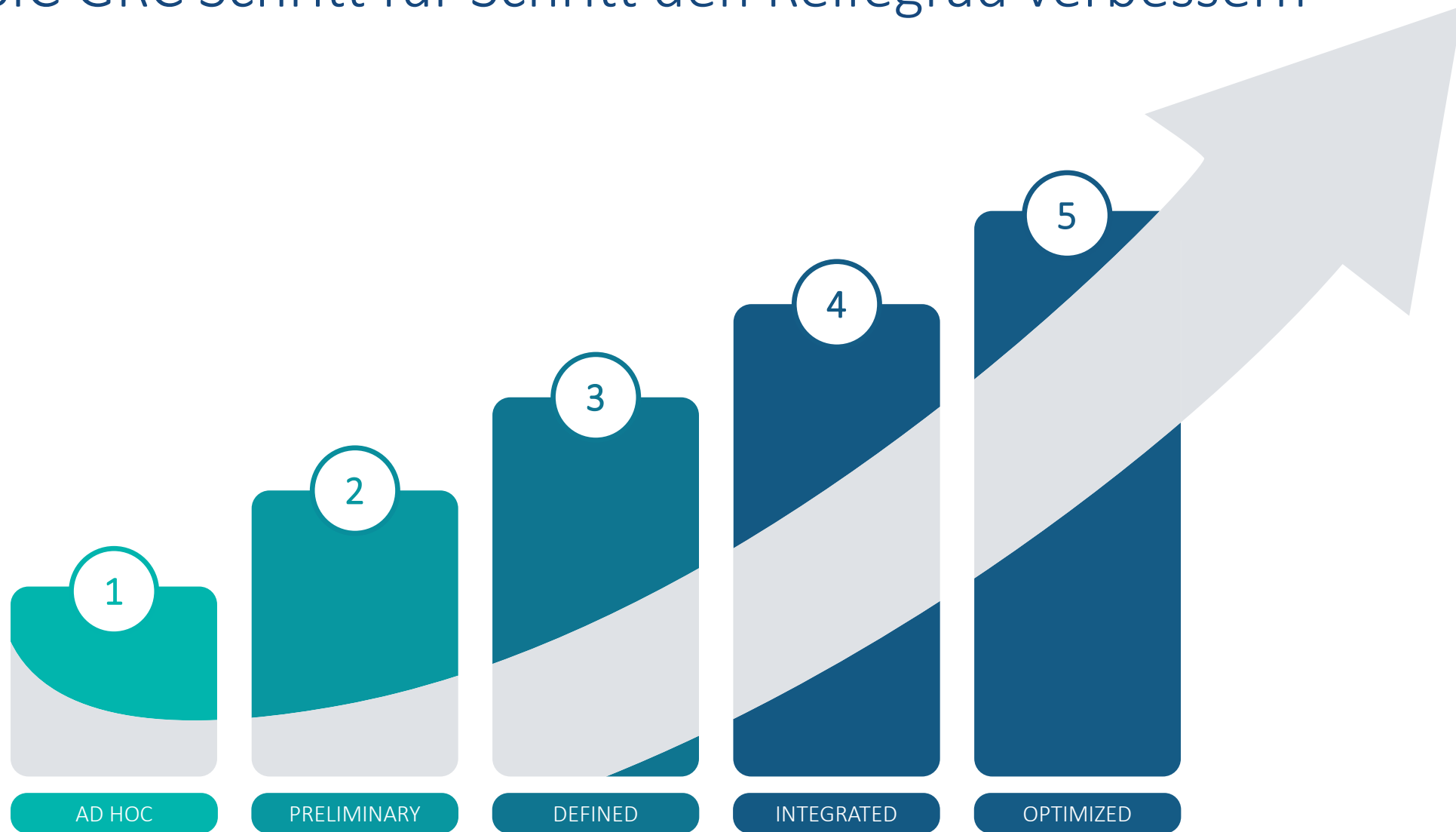
Integrierte &  
plattformbasierte  
GRC-Lösungen

## GRC-Plattformen

- Mehrere GRC-Anwendungsfälle auf einer Plattform
- Integriertes GRC mit Verknüpfungsfunktionen
- Hoher Grad an No-Code / Low-Code Anpassungsfähigkeit
- Umfassende Berichterstattungsfunktionen
- Integration in weitere Unternehmensanwendungen



# Mit BIC GRC Schritt für Schritt den Reifegrad verbessern



Stimmen Sie jetzt ab!



# Treiber für die Verbesserung des Reifegrads



Mangelnde **Datensicherheit** und **-integrität**



Hohe manuelle **Aufwände** und **Fehleranfälligkeit**



Fehlende **Automatisierung** und **Workflow-Unterstützung**



Unzureichendes Commitment von Kollegen wegen **abschreckender Excel-Tapeten**



Begrenzte **Skalierbarkeit** und **Anpassungsfähigkeit**



Fehlende **Kollaborationsmöglichkeiten** und ungewisse **Datenaktualität**

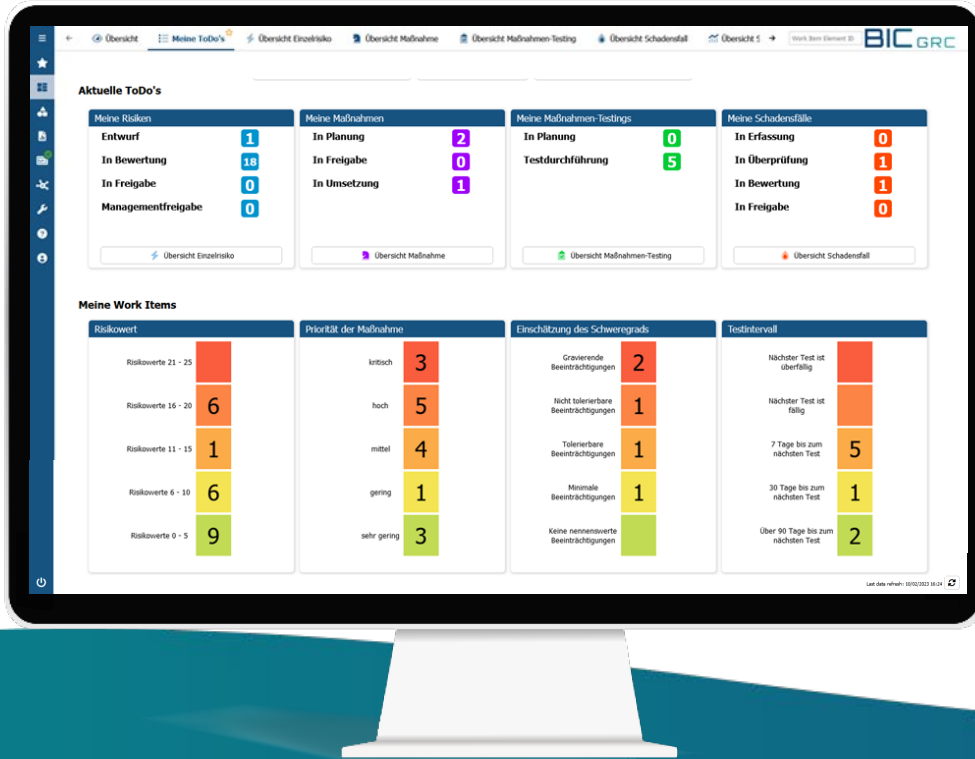


Inkompatible **Berichts-** und **Analysefunktionen**



Unzureichende Möglichkeit der Darstellung **finanzieller Auswirkungen** für Vorstand

# Mit BIC GRC zur risikoorientierten Unternehmenssteuerung



Risikomanagement inklusive Simulation



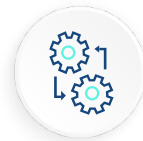
Internes Kontrollsystem und Internal Audit



ISMS nach ISO 27001 sowie BSI-Grundschutz



Datenschutz nach EU-DSGVO



Business Continuity Management



Blueprints für viele Bereiche (z.B. Compliance, etc.)

## BIC Benefits



Rasch einsetzbare, branchen-unabhängige Standard Solutions nach gängigen Standards und Best-Practice-Ansätzen.



Zukunftsfähigkeit und Skalierbarkeit durch Ausbaumöglichkeiten hinsichtlich Use Cases, Standards und Normen.



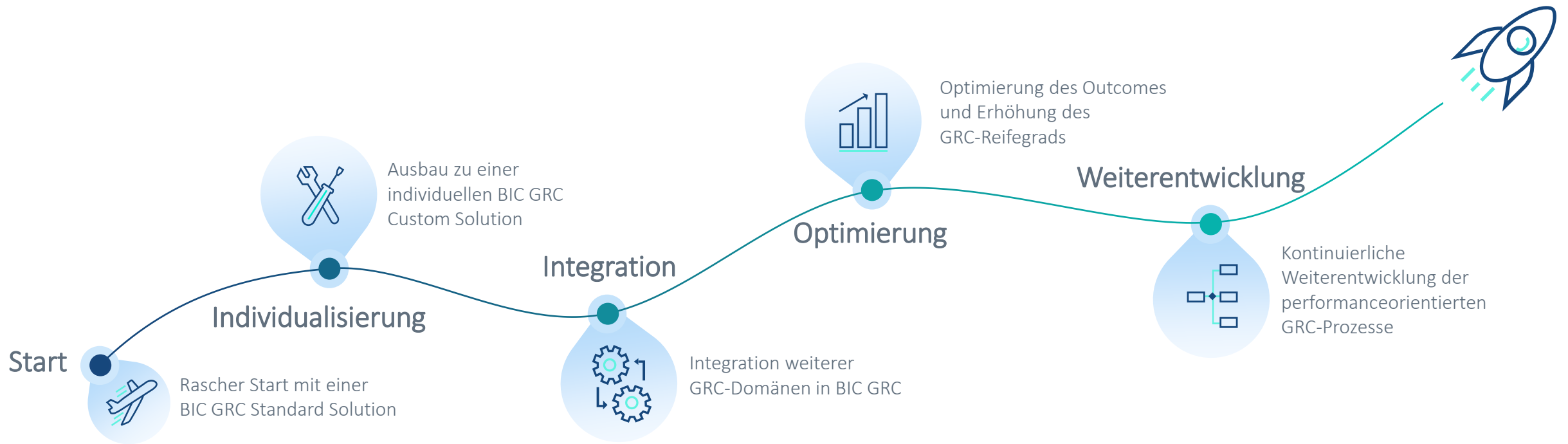
100% individuelle, passgenau zugeschnittene Custom-Solutions entsprechend Ihrer aktuellen und zukünftigen GRC-Prozesse.



Möglichkeit des Ausbaus bis hin zur umfassenden, integrierten GRC-Plattform sowie Anbindung an BIC BPM Software.



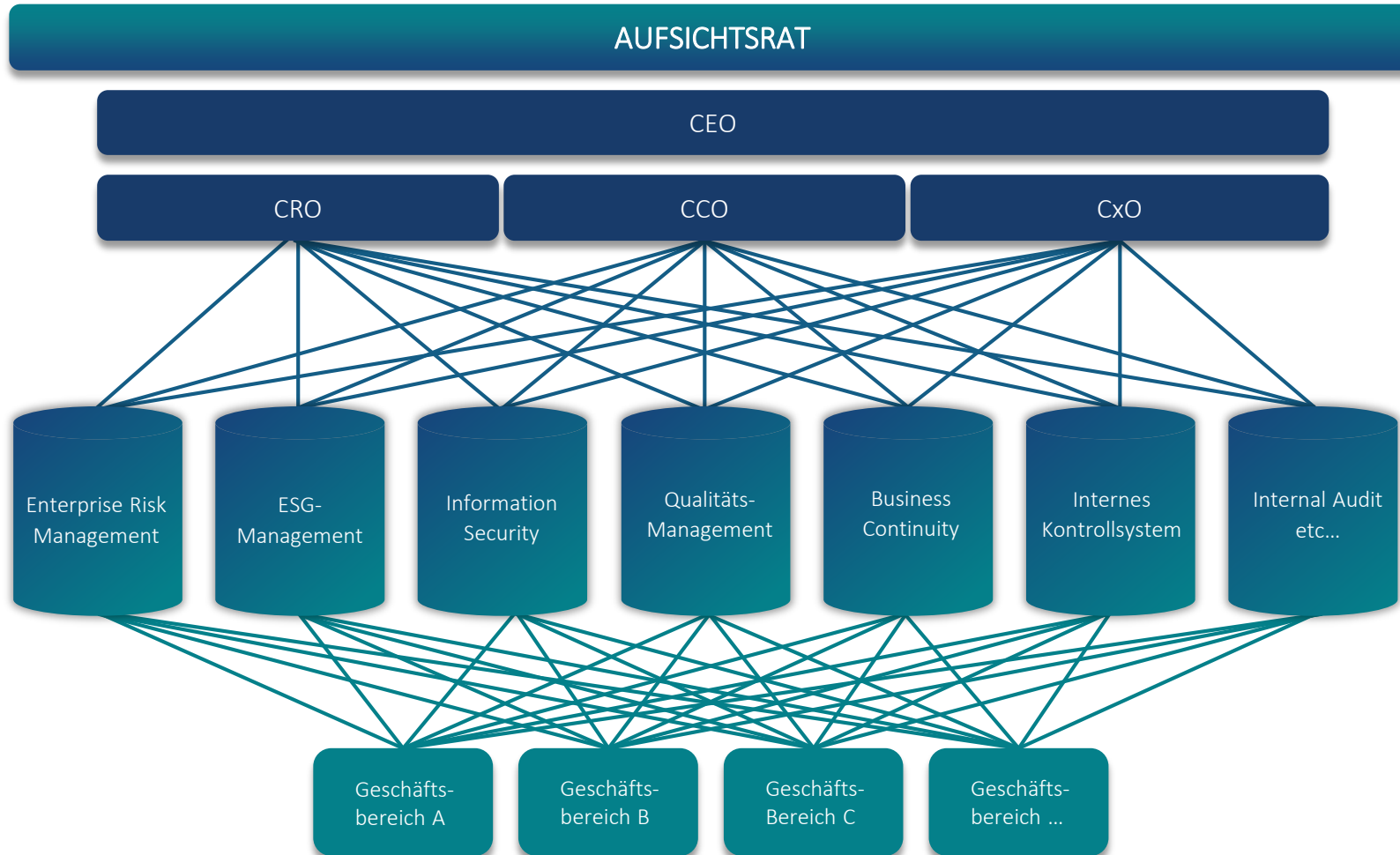
# Ihre Erfolgsgeschichte mit BIC GRC





## Volle Flexibilität mit BIC GRC

- ✓ BIC GRC ist die Basis für Ihr zukunftsicheres GRC - wir begleiten Sie auf dem Weg zu wertorientierten GRC-Prozessen.
- ✓ Erhöhen Sie kontinuierlich den Reifegrad Ihrer GRC-Prozesse und erweitern Sie BIC GRC je nach Ihren Anforderungen.
- ✓ Starten Sie mit einer Best Practice Standard Solution oder einer individuell angepassten Custom Solution.
- ✓ GBTEC ist einer der wenigen Software-Anbieter, die alle Stufen der digitalen Transformation abdecken.

# Die Folge fragmentierter Management-Systeme



## Herausforderungen

-  Redundante Datenhaltung
-  Mehrfache Abfragen in Fach- / Geschäftsbereichen
-  Inkonsistente Berichterstattung
-  Uneinheitliche Nachverfolgung von Maßnahmen & Aufgaben
-  Redundante Kontroll-Nachweise
-  Hohe Betriebs-Aufwände

# Integrated GRC – Die nächste Stufe für ERM & IKS

## Effizientere interne Kontrollprozesse

Ein großes Handelsunternehmen mit Filialen in mehreren Ländern muss sicherstellen, dass alle Prozesse ordnungsgemäß und effizient ablaufen.



Reduzierung von  
redundanten  
Kontrollen



Automatisierung von  
Kontrollprozessen



Verbesserte  
Transparenz und  
Berichterstattung

# Integrated GRC – Die nächste Stufe für ERM & IKS

## Verbesserte Risikosteuerung und Compliance

Ein Unternehmen der Lebensmittelindustrie sah sich mit komplexen regulatorischen Anforderungen und vielfältigen Risiken konfrontiert.



Risiken proaktiv  
identifizieren und  
bewerten



IKS-Maßnahmen  
zielgerichtet  
implementieren



Kontinuierliche  
Verbesserung des  
Risikomanagements

# Integrated GRC – Die nächste Stufe für ERM & IKS

## Effektive Entscheidungsfindung in komplexen Situationen

Ein global agierendes, schnell wachsendes Unternehmen stand vor der Herausforderung, komplexe Entscheidungen in einem volatilen Marktumfeld zu treffen.



Risikobasierte  
Entscheidungen



Verbesserte  
Szenarioanalyse



Nachvollziehbare und  
transparente  
Entscheidungen

# Integrated GRC – Die nächste Stufe für ISMS, DPMS und BCM

## Sichere und effiziente Wiederherstellung nach Betriebsunterbrechungen

Ein Produktionsunternehmen ist von einer hohen Verfügbarkeit seiner IT-Systeme abhängig.



Detailliertere **Business Impact Analysen** durchführen



Notfallpläne & Wiederherstellungsstrategien erstellen



Schnelle **System-Wiederherstellung** gewährleisten

# Integrated GRC – Die nächste Stufe für ISMS, DPMS und BCM

## Förderung einer Kultur der Compliance und Sicherheit

Ein Unternehmen in der Gesundheitsbranche legt großen Wert auf die Einhaltung von Compliance-Anforderungen und die Sicherheit von Patientinnen und Patienten sowie Mitarbeitenden.



Verankerung von  
Compliance-Prinzipien



Verbesserung der  
DSGVO-Prozesse



Einfache Integration  
und Nutzung von  
branchenspezifischen  
Sicherheitsstandards

# Integrated GRC – Die nächste Stufe für ISMS, DPMS und BCM

## Verbessertes Management von Informationssicherheitsrisiken

Ein Unternehmen im Finanzsektor verarbeitet große Mengen sensibler Kundendaten.



Umfassende  
Risikoanalyse



Technische und  
organisatorische  
Schutzmaßnahmen



Schnellere Reaktion auf  
Sicherheitsvorfälle



# Alle Vorteile bereits ab Werk – die integrierten BIC GRC Solutions



Zeit- und Kostenersparnis



Klares Rollenkonzept



Vermeidung von Redundanzen



Kollaboratives Arbeiten



Konsolidierte Berichte



Gemeinsame Verwaltung



Nutzung von Synergien



Zentrale Datenadministration

# BIC GRC | Solutions Roadmap



## BIC Security GRC

- ISO 27x, BSI & DSGVO & BCM in einer Lösung
- ISMS-Implementierungsanleitung und Statusübersicht



## BIC Compliance GRC

- Third-Party-Management-Modul
- Compliance Assessments



## BIC Enterprise GRC

- Verbesserte Risiko- und Chancenbewertung
- Integration globaler Kontrollanforderungen
- Mehr Simulations-Anwendungsfälle



## BIC Enterprise Sustainability

- Nachhaltigkeitsmanagement nach ESRS
- Individuelles Scoping für Datenpunkte/Indikatoren

Stimmen Sie jetzt ab!



# Vereinbaren Sie ein unverbindliches Gespräch mit uns!

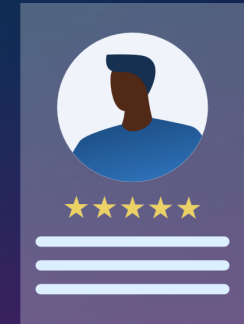
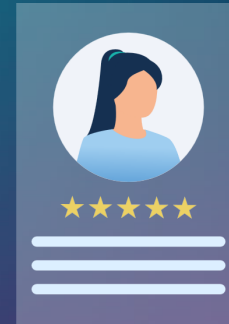
Stellen Sie uns kostenlos Ihre Fragen rund  
um Governance, Risk und Compliance



[https://outlook.office365.com/  
owa/calendar/GRCSales@gbtec.com  
/bookings/](https://outlook.office365.com/owa/calendar/GRCSales@gbtec.com/bookings/)

# Ihre Meinung ist gefragt!

Wir freuen uns über Feedback.





**Kaspar Kühl**

*Partner, greenfield Consulting*



# ESG

## (Environmental, Social, & Governance)

---

Sicher und nachhaltig in die Zukunft

Kaspar Kühl

# Agenda

- 01 Verpflichtung zur ESG-Berichterstattung
- 02 Status quo in der Unternehmenspraxis
- 03 Schritte zur optimalen Umsetzung







1,48

150

160.000.000

# ESG-Berichterstattung wird verpflichtend

		2023	2024	2025	2026
	NFRD	Kapitalmarktorientierte Unternehmen >500 MA			
	CSRD		Kapitalmarktorientierte Unternehmen >500 MA	Große Unternehmen 250 MA 50 Mio. EUR Umsatz 25 Mio. EUR Bilanzsumme	Gelistete Unternehmen 50 MA 8 Mio. EUR Umsatz 4 Mio. EUR Bilanzsumme
	EU-Taxonomie	Konformität bzgl. Umweltziel 1+2	Taxonomiequoten zur Fähigkeit & Konformität aller 6 Ziele		
	LkSG	Unternehmen >3.000 MA	Unternehmen >1.000 MA		



# Status quo



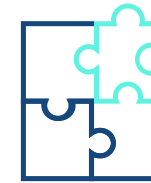
## Wissenslücke

Häufig mangelt es an Wissen über die Notwendigkeit der nachhaltigen Transformation, konkrete Umsetzung und Einhaltung der Regulatorik.



## Personallücke

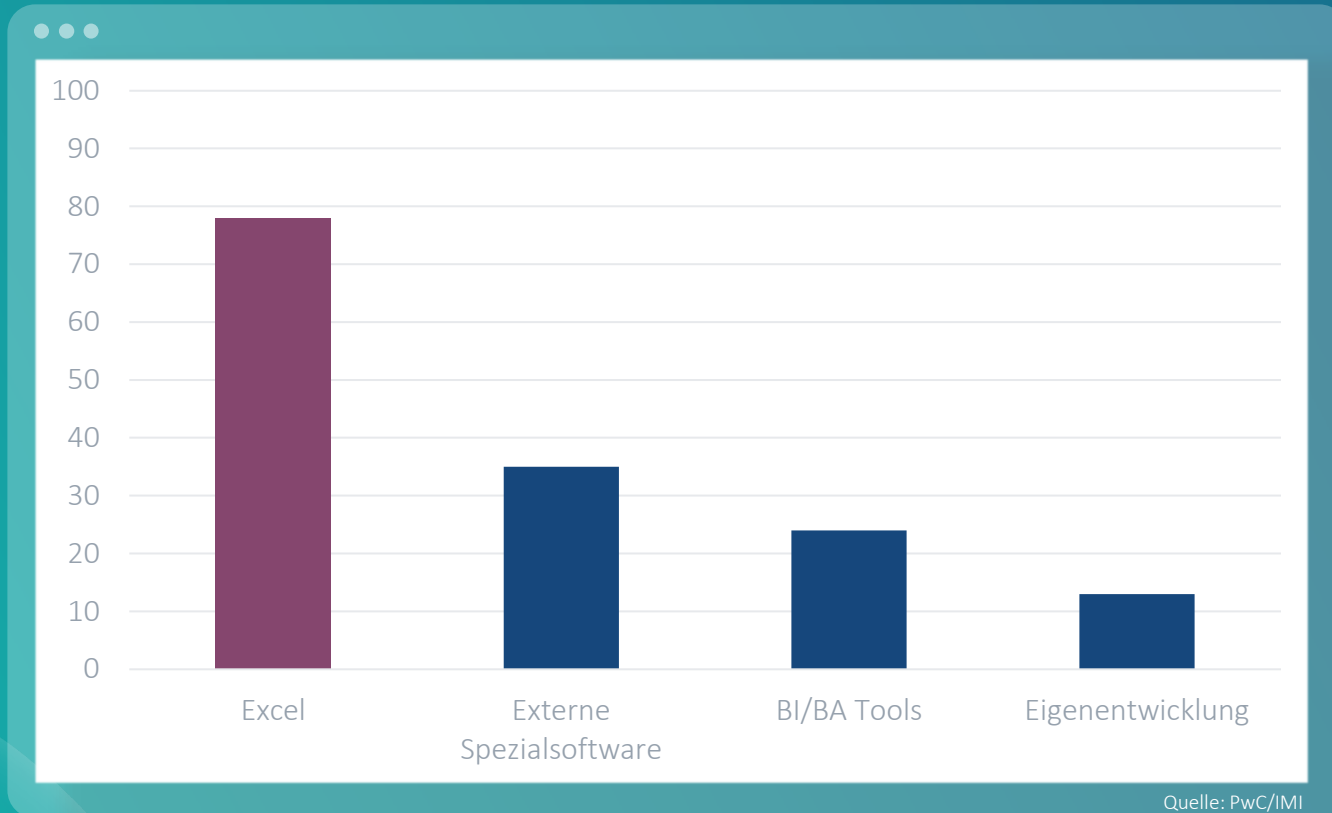
Es fehlt an qualifiziertem Personal zur Bewältigung der Aufgaben und an der notwendigen kulturellen Veränderungsbereitschaft.



## Systemlücke

Die Notwendigkeit der Erhebung und Auswertung von ESG-Daten stellt neue Anforderungen an die IT und die Datenkompetenz.

# Systemlücke konkret | ESG-Tools im Mittelstand



Revisionsicherheit?



Sicherheit / Stabilität?



Management großer Datenmengen?



Datenerhebung?



...

# Reden wir nur über Regulatorik?

“

*Wir warten erst einmal ab, bis andere etwas machen.*

”

“

*Nachhaltigkeit kostet uns sowieso nur Geld.*

”

“

*Für welche grünen Wachstumsmärkte sind wir als Organisation perfekt positioniert?*

”

“

*Was wären unsere Kunden bereit mehr zu zahlen, wenn wir ihnen helfen, selbst nachhaltiger zu werden?*

”

15%

Deutschlands GreenTech-Weltmarktanteil

14%

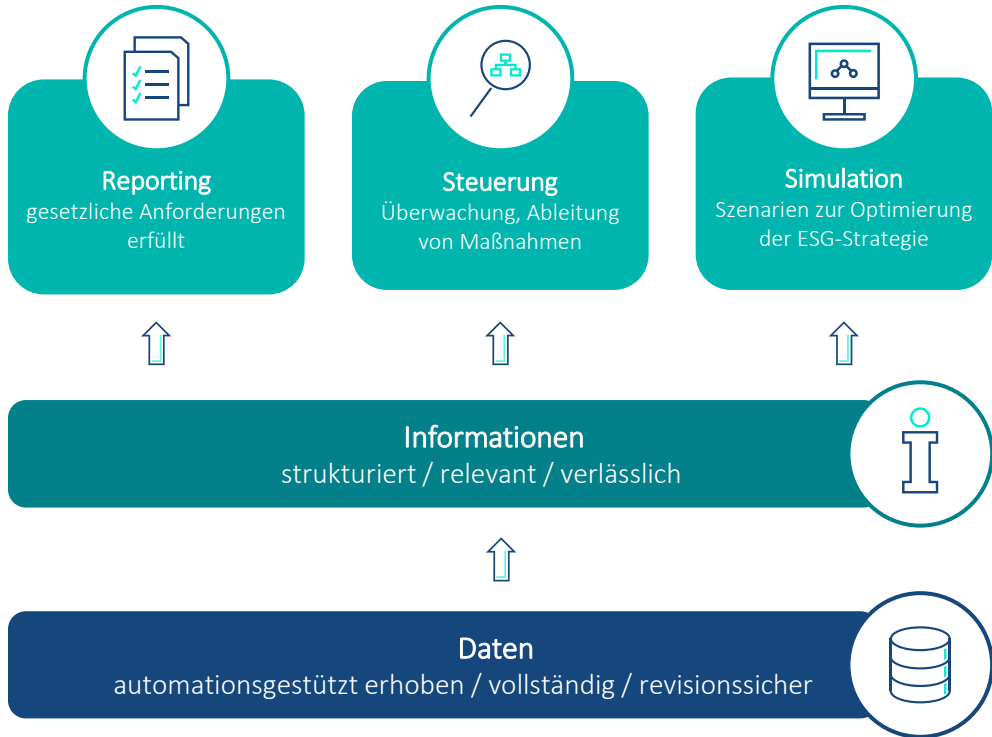
Anteil GreenTech am deutschen BIP

10%

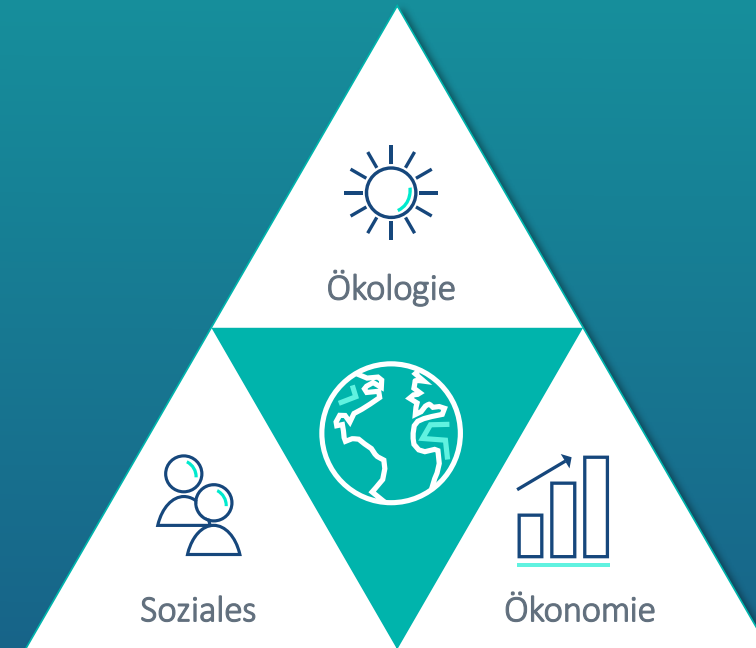
Jährliche Wachstumsrate des Markts

# Ambition lohnt sich

## Nachhaltigkeitsmanagement digitalisiert, integriert, skalierbar



## Nachhaltigkeitsprojekte abgestimmt, transparent, effizient



Strategie, Vision, Mission  
Nachhaltigkeit im Kerngeschäft verankert

# Transformation braucht ein starkes Fundament

## Process & Technology

- Standardisierte ESG-Prozesse und Tools werden in die **Kerngeschäftsabläufe** integriert
- Digitale Tools verbessern die **Effizienz** und das datengesteuerte **Risikomanagement**

## Compliance & Regulations

- **Überwachungssysteme** für Compliance-konforme Nachhaltigkeitsaktivitäten und Berichterstattung
- **Skalierbarkeit** stellt sicher, dass neue Vorschriften und Gesetze eingehalten werden

## Organisation

- Eine **klare, vernetzte Struktur** des Nachhaltigkeitsmanagements ist das Fundament des SOM
- Eine **Kultur**, die Nachhaltigkeitsprinzipien einbezieht, fördert **Engagement** und treibt **Innovationen** voran



## Policy, Risk & Governance

- **Nachhaltigkeitsrichtlinien** unterstützen Compliance und Risikomanagement
- **Zuständigkeiten** und **Rollen** sind klar definiert

## Data

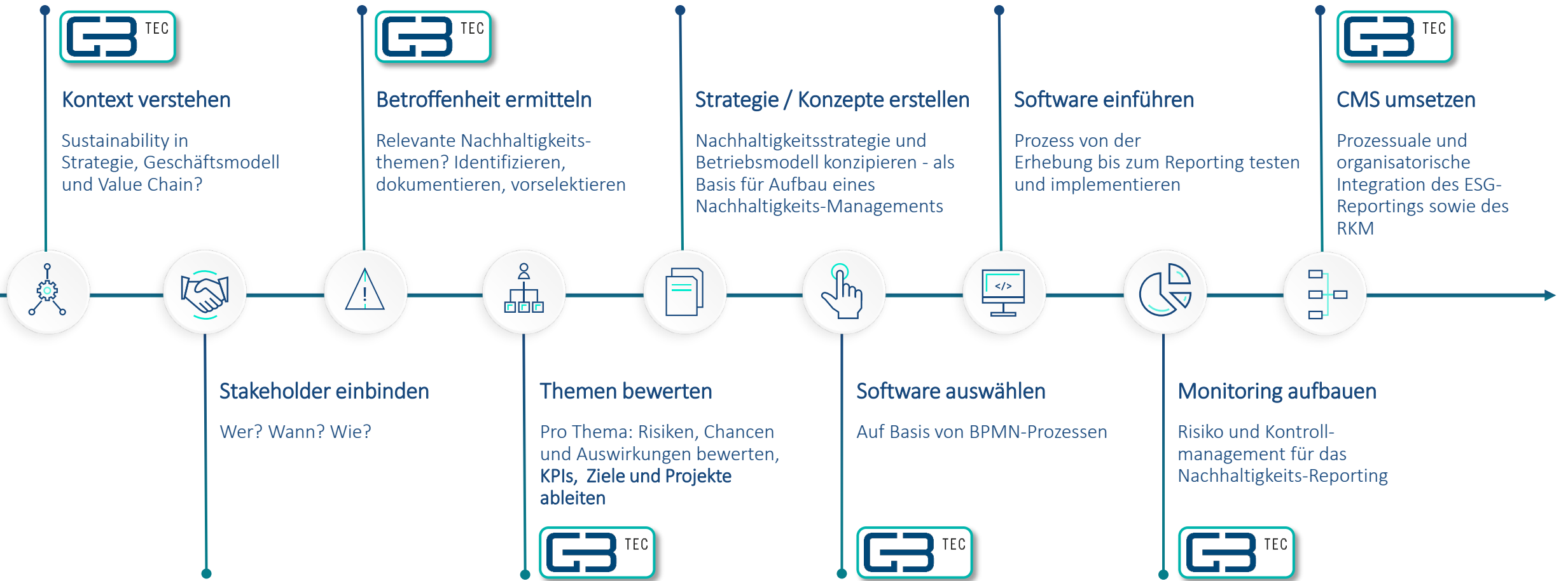
- Eine standardisierte Datenerfassung ermöglicht **aussagefähiges Reporting**
- Datentransparenz unterstützt **fundierte Entscheidungen**

## People

- **Schulungskonzepte** verbessern die Fähigkeiten und das Wissen über Nachhaltigkeit
- **Neue Qualifikationen / Positionen** sind die Voraussetzung für ein integriertes Nachhaltigkeitsmanagement



# Schritte zum Ziel – Beispiel CSRD





---

*greenfield und GBTEC helfen Ihnen enkelfähig zu werden, indem wir durch ESG-Compliance und Digitalisierung Ihr Geschäftsmodell optimieren.*

pragmatisch – professionell – nahbar

---



Vielen Dank!



**Kaspar Kühl**

*Partner,  
greenfield Consulting*



Kaspar.Kuehl@greenfield-group.de



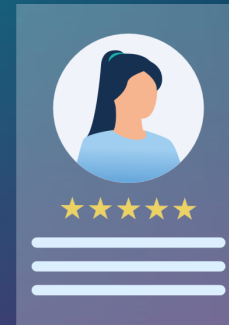
+49 157 857 424 60



[https://www.linkedin.com/in/  
kaspar-k%C3%BChl-5a7111ab/](https://www.linkedin.com/in/kaspar-k%C3%BChl-5a7111ab/)

# Ihre Meinung ist gefragt!

Wir freuen uns über Feedback.





**Sandra Blaha**  
*GRC Solution Architect*



**Ronald Prahs**  
*Head of Presales GRC*



# ESG mit BIC GRC

---

Fachkundige Unterstützung während des gesamten  
Management-Prozesses

**Sandra Blaha & Ronald Prah**

# Agenda

- 01 Doppelte Wesentlichkeit im Fokus
- 02 Von der Long- zur Short-List
- 03 Vernetzung von Nachhaltigkeit und Risikomanagement
- 04 Live-Demo in BIC GRC
- 05 Ihre Fragen

Stimmen Sie jetzt ab!





# Doppelte Wesentlichkeit im Fokus



European Sustainability Reporting Standards  
(ESRS)



Durchführung der doppelten  
Wesentlichkeitsanalyse



Nahtlose Integration des  
Unternehmens-Risikomanagements



Bewertung der Datenpunkte nach ESRS &  
Berichterstattung in XBRL

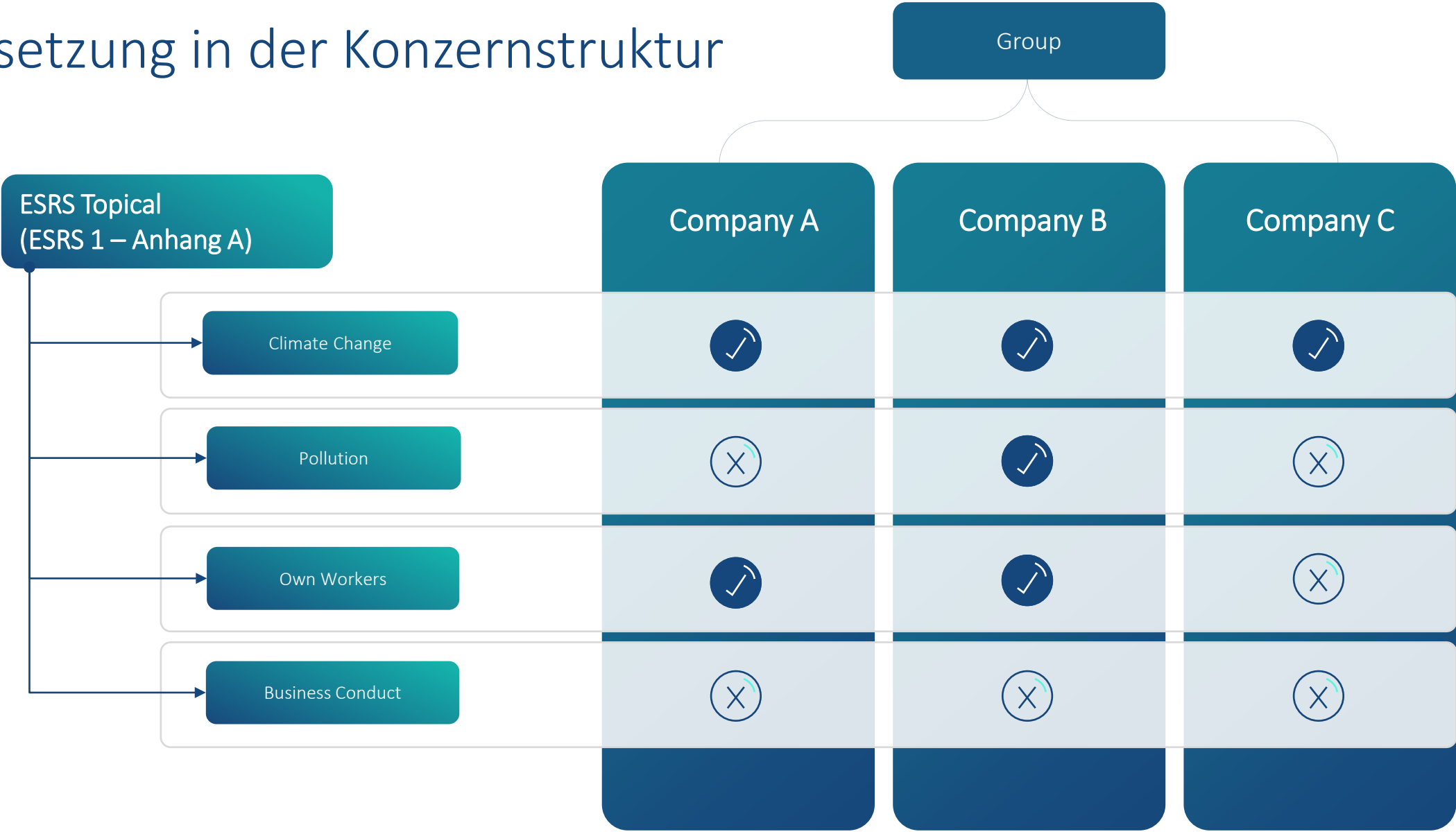
# Durchführung der doppelten Wesentlichkeitsanalyse



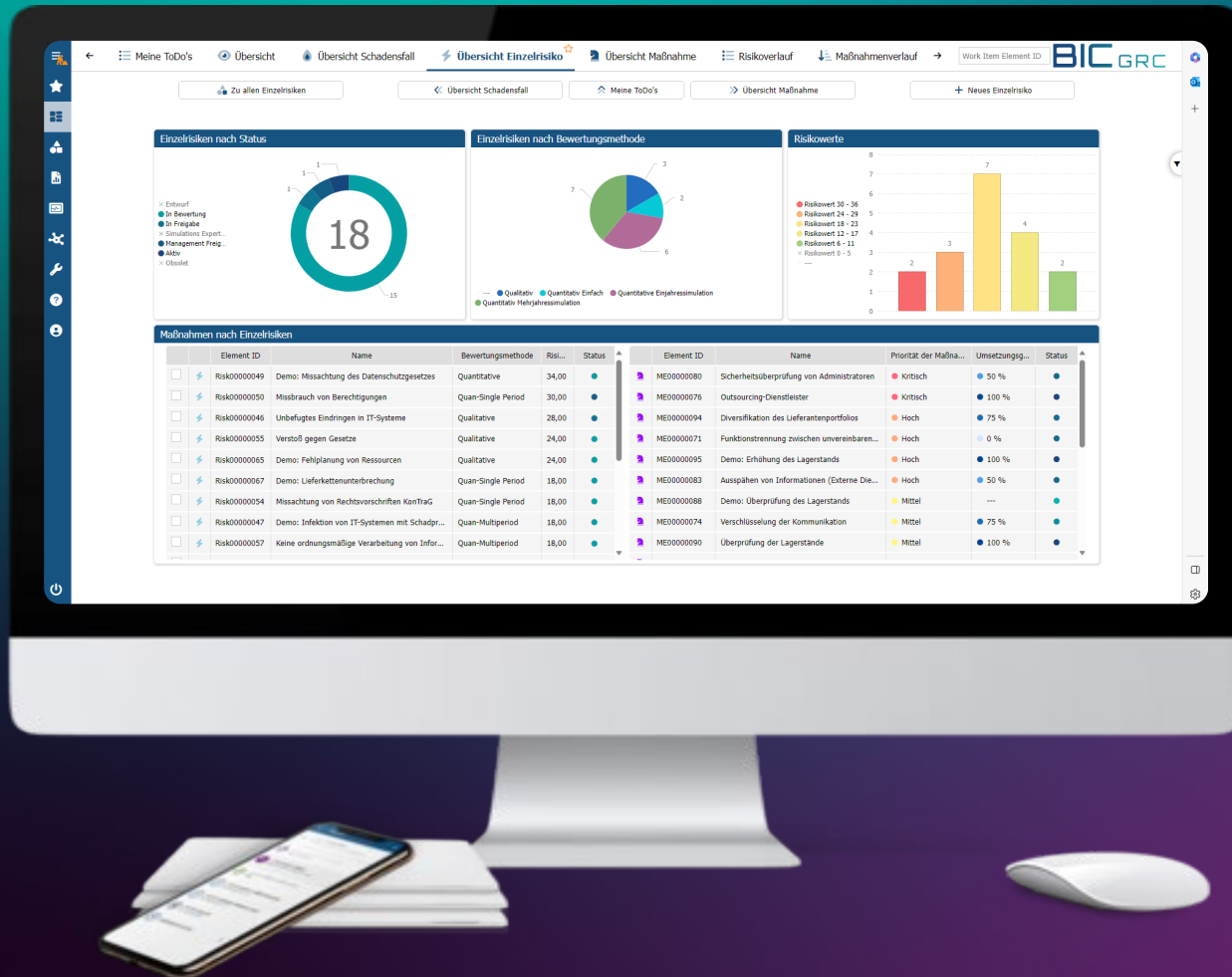
# Prozess zur Erfüllung der Anforderungen



# Umsetzung in der Konzernstruktur



# Live-Demo



# Doppelte Wesentlichkeit mit Risikomanagement



Klare Übersicht erfasster **Nachhaltigkeitsrisiken** bzw. -chancen



Lückenlose **Dokumentation** des Vorgehens und der Ergebnisse



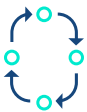
Aufnahme von Risiken und Chancen ins **Non-financial Reporting**



Erweiterung des bestehenden **RMS/IKS** um nachhaltigkeitsbezogene Aspekte



Nahtlose Integration der **Wesentlichkeitsrisiken** in RMS/IKS



Nachvollziehbare Bewertung über **mehrere Perioden**

Stimmen Sie jetzt ab!



# Q & A





# Vereinbaren Sie ein unverbindliches Gespräch mit uns!

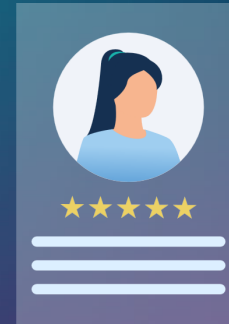
Stellen Sie uns kostenlos Ihre Fragen rund  
um Governance, Risk und Compliance



[https://outlook.office365.com/  
owa/calendar/GRCSales@gbtec.com  
/bookings/](https://outlook.office365.com/owa/calendar/GRCSales@gbtec.com/bookings/)

# Ihre Meinung ist gefragt!

Wir freuen uns über Feedback.





**Sandra Blaha**  
*GRC Solution Architect*



**Ronald Prahs**  
*Head of Presales GRC*



# BIC Enterprise GRC

---

Symbiose zwischen Risikomanagement und  
Internem Kontrollsystem

**Sandra Blaha & Ronald Prah**

# Agenda

- 01 Maximale Synergieeffekte zwischen ERM & IKS
- 02 Umfangreiche Möglichkeiten in der Konfiguration
- 03 Einheitliches Reporting auf neuem Level
- 04 Live-Demo in BIC GRC
- 05 Ihre Fragen

Stimmen Sie jetzt ab!



# Maximale Synergieeffekte



## Direktes Reporting

Gemeinsames Arbeiten in einem System mit direkten Reporting-Möglichkeiten von Prozessrisiken an den Central Risk Manager

## Gemeinsame Verwaltung

Einmaliges Anlegen von Asset-Hierarchie, GRC-Frameworks und Berechtigungen, die in einem System verwaltet werden können

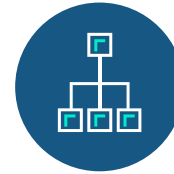
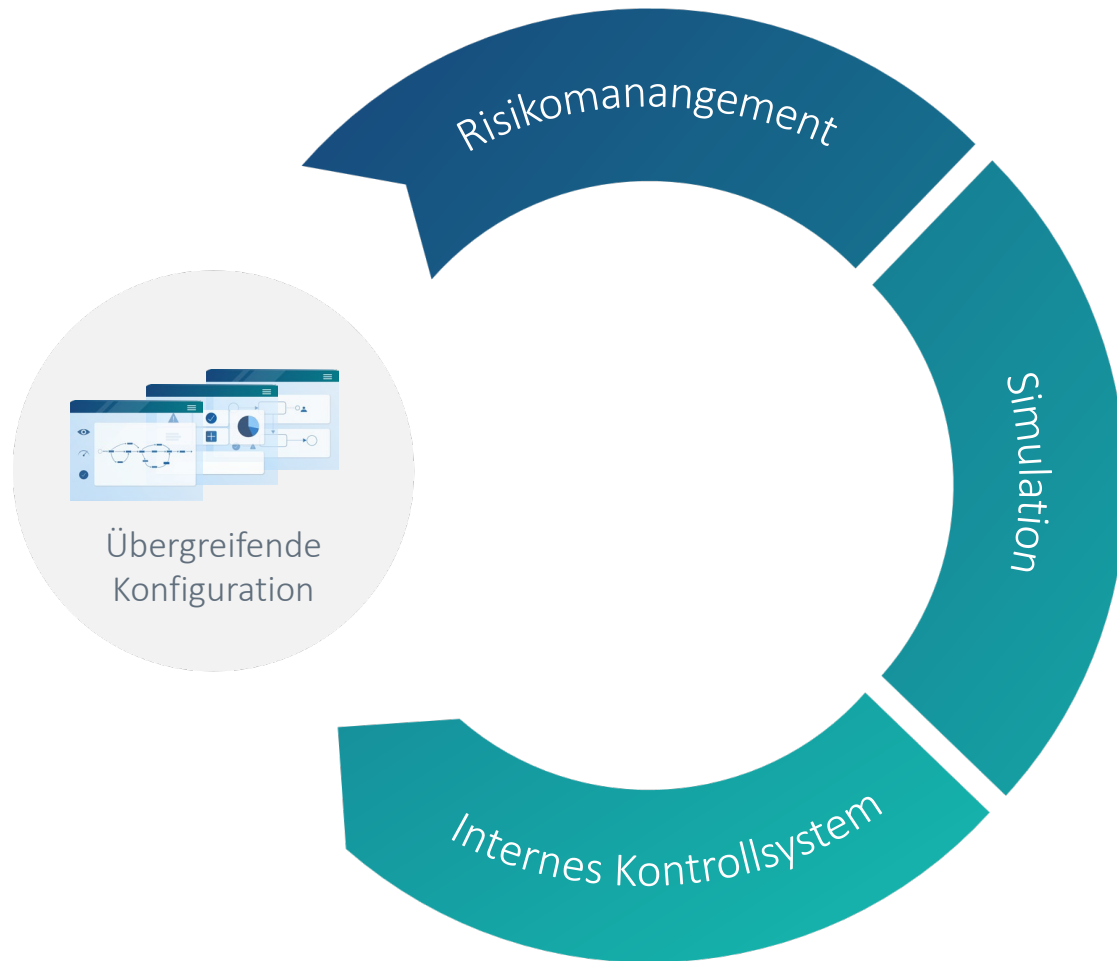
## Getrennte Ansichten & Berechtigungen

Weiterhin getrennte Sichtbarkeiten und eingeschränkte Zugänge zu bestimmten Bereichen für bessere und spezifischere User-Guidance

## Erweiterte Dashboard-Ansichten

Fachspezifische und -übergreifende Dashboards für die bestmögliche Übersicht über alle Daten und Informationen

# Neue Möglichkeiten in der Konfiguration

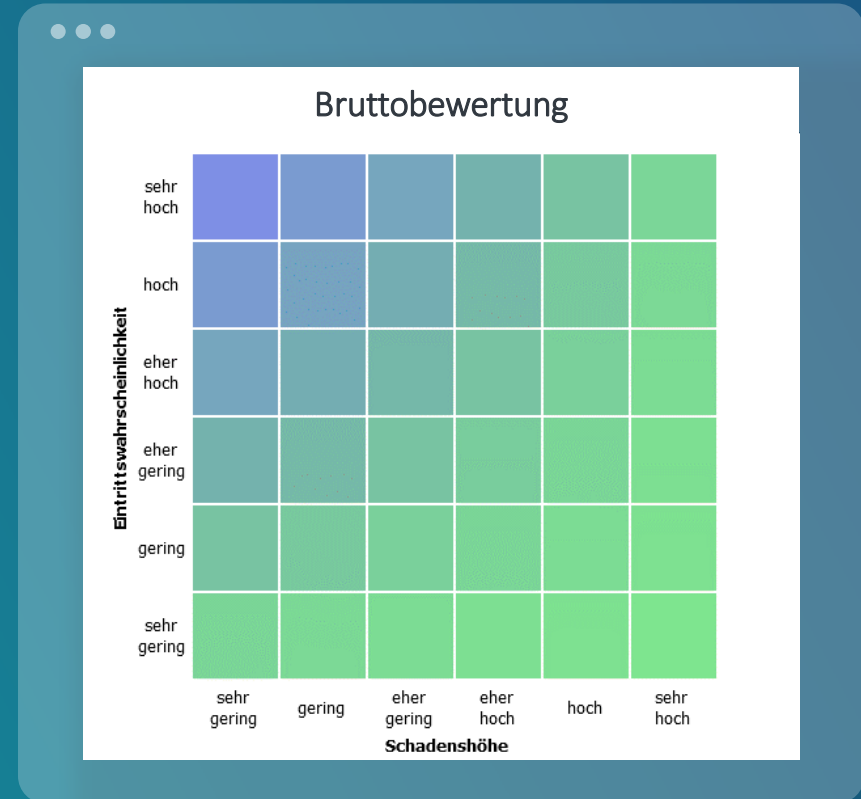
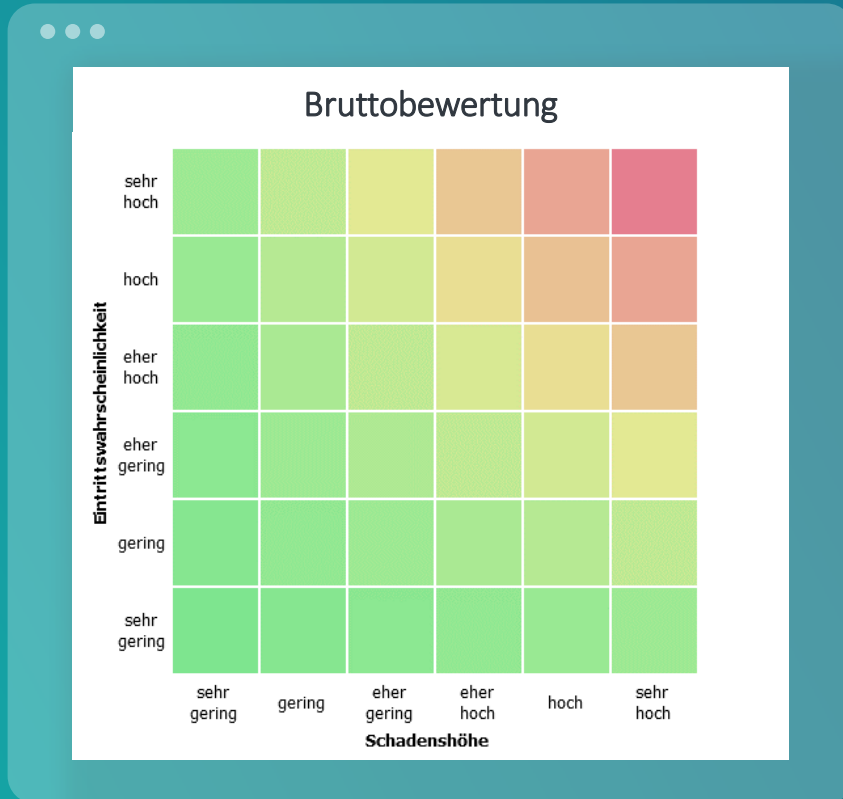


## Risikomanagement

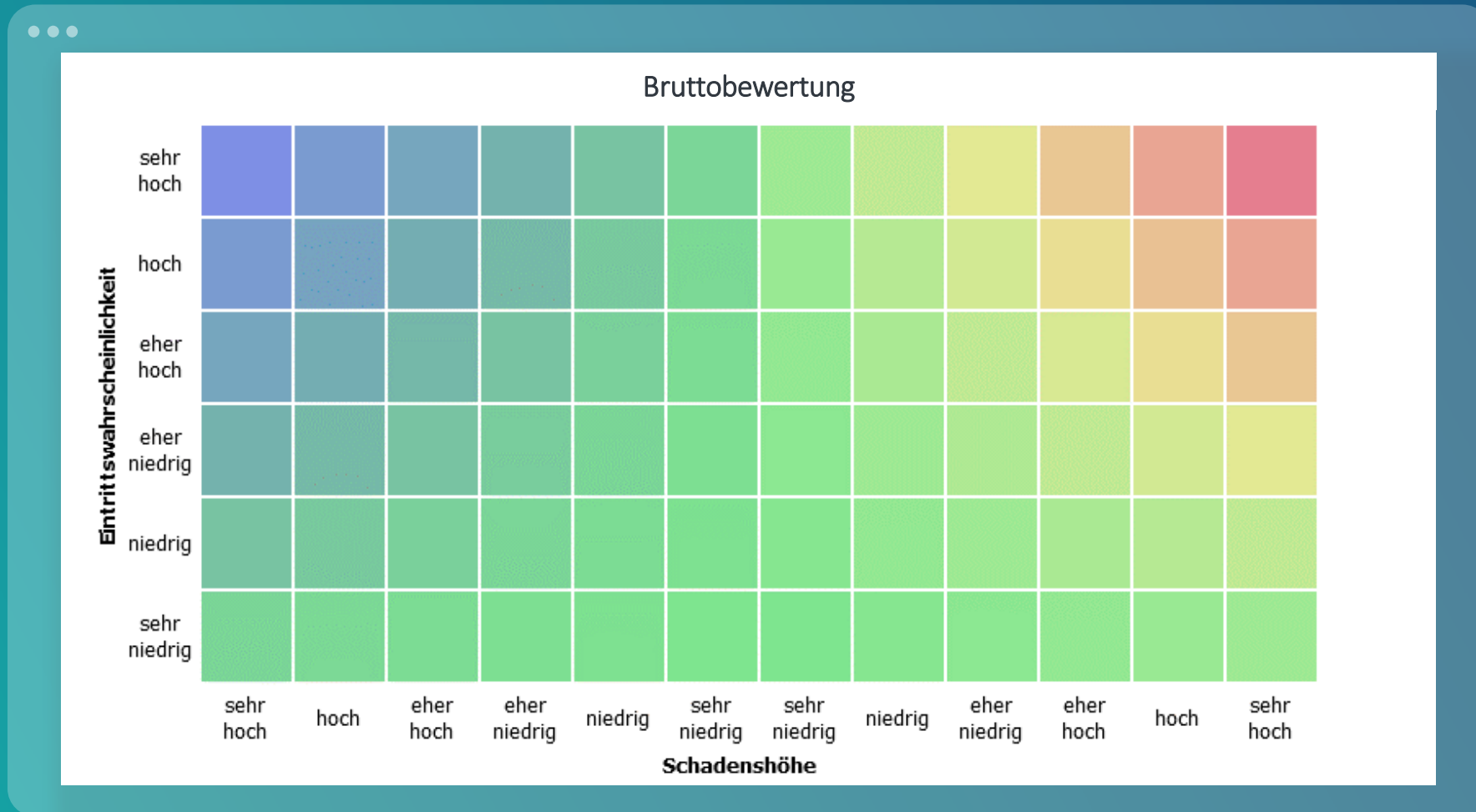
- Reifegrad definieren
- Risikomatrixgröße festlegen



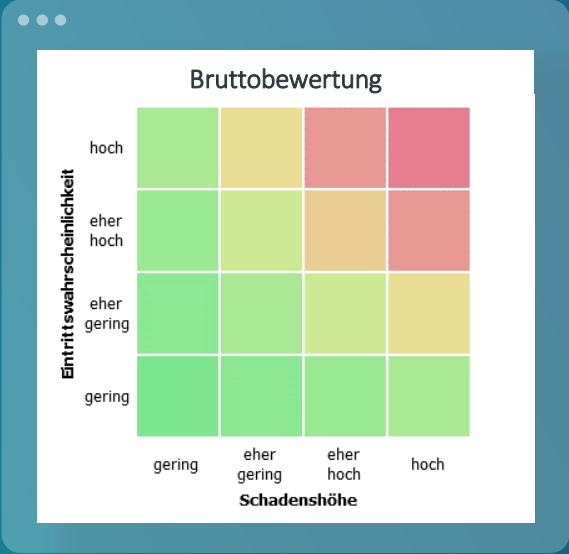
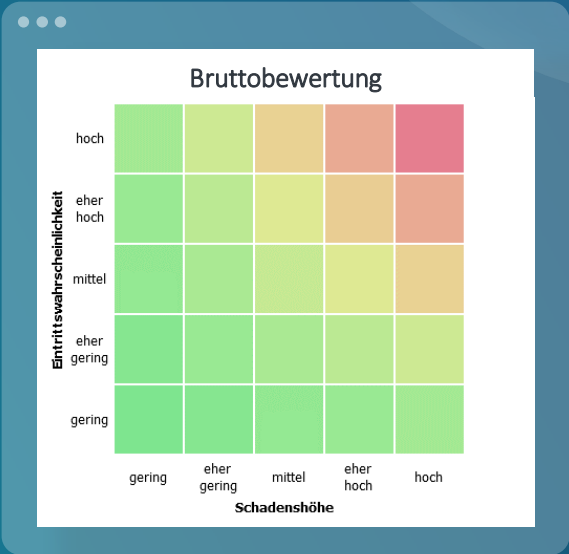
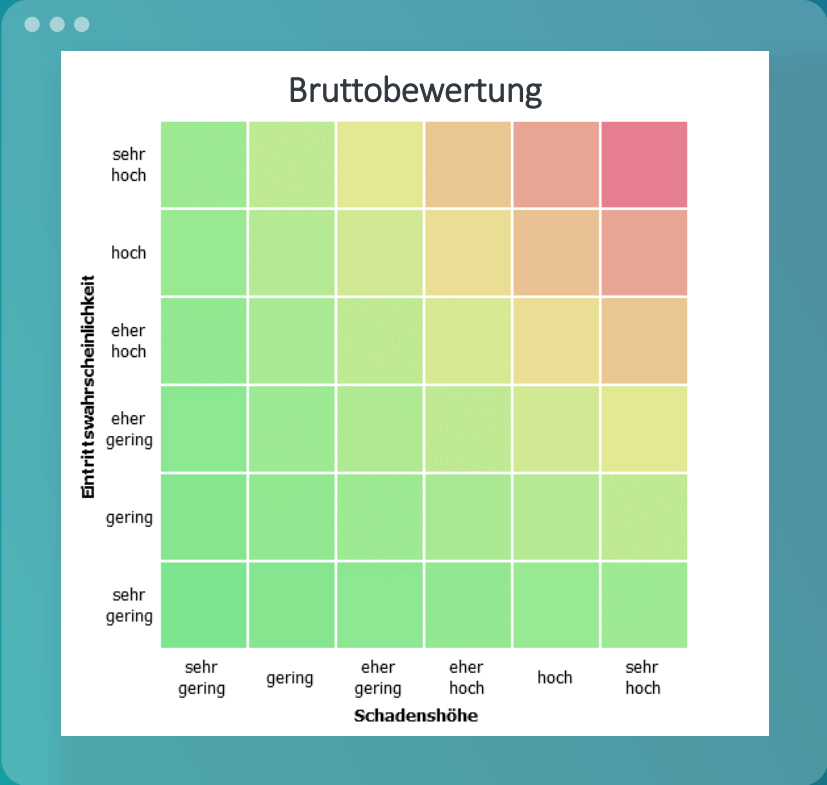
# Bewertung von Risiken und Chancen



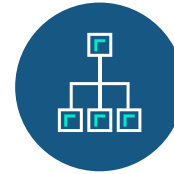
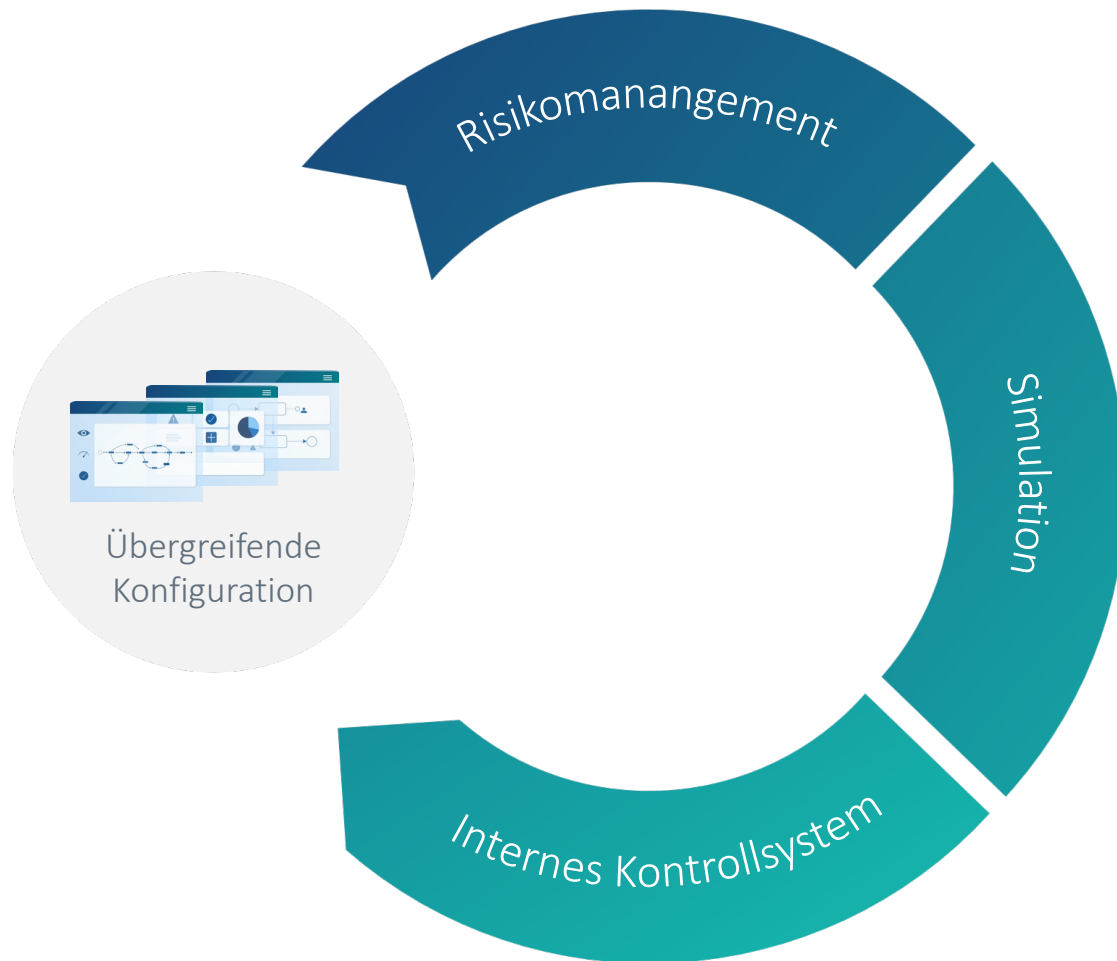
# Risiko- und Chancenmatrix



# Dimension



# Neue Möglichkeiten in der Konfiguration



## Risikomanagement

- Reifegrad definieren
- Risikomatrixgröße festlegen



## Simulation

- Jahre der Mehrjahressimulation bestimmen
- Value-at-Risk und Iterationen harmonisieren



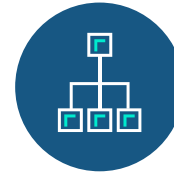
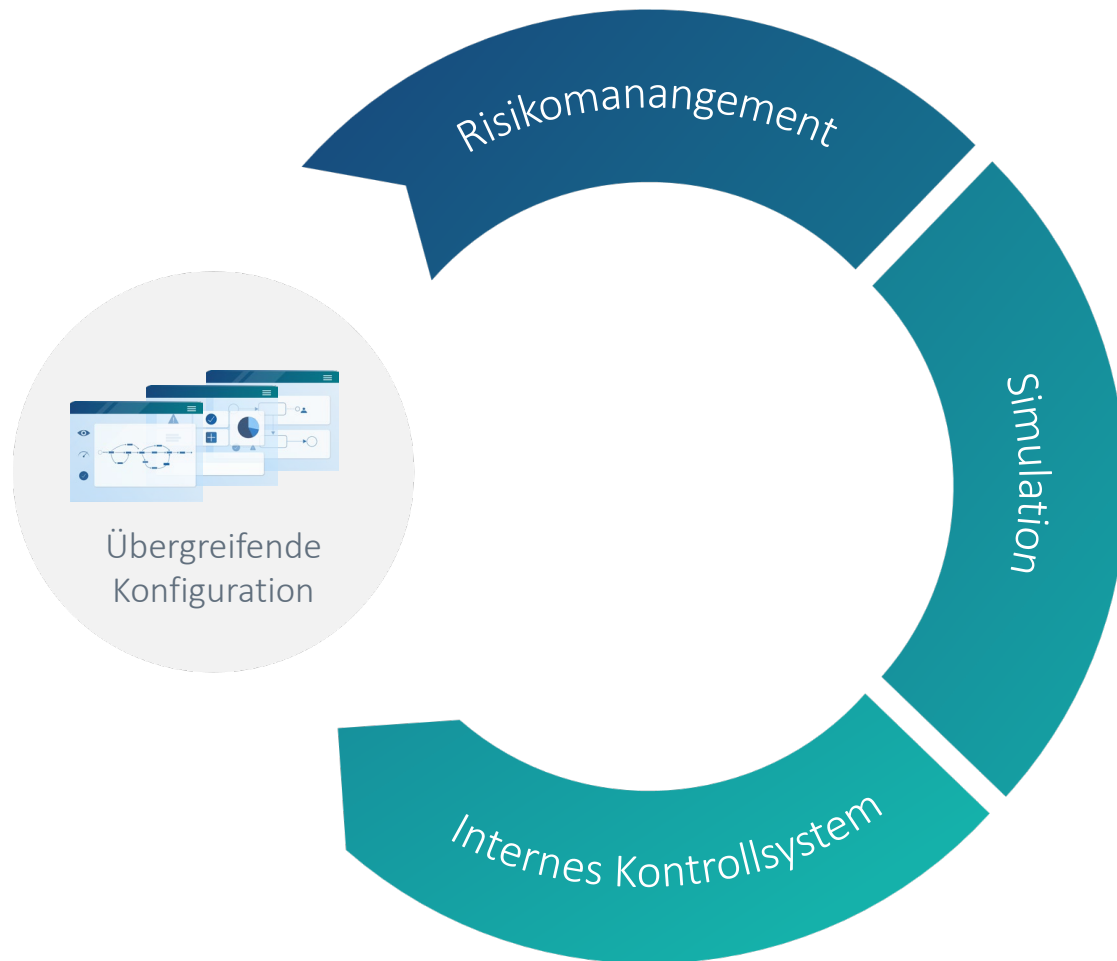
Wie viele Jahre in die Zukunft soll simuliert werden?

	2024	2025	2026	2027	2028
<b>Tritt mehrfach auf</b> i	Nein ▼	Nein ▼	Nein ▼	Nein ▼	Nein ▼
<b>Häufigkeit</b> i	Alle 10 Jahre ▼	Alle 15 Jahre ▼	Tritt nicht auf ▼	Tritt nicht auf ▼	Tritt nicht auf ▼
<b>Bester Fall</b> i	342 € ▲▼	32.432 € ▲▼	0 € ▲▼	0 € ▲▼	0 € ▲▼
<b>Wahrscheinlichster Fall</b> i	23.432 € ▲▼	343.242 € ▲▼	0 € ▲▼	0 € ▲▼	0 € ▲▼
<b>Schlechtester Fall</b> i	32.432.423 € ▲▼	234.324.324.32 ... ▲▼	0 € ▲▼	0 € ▲▼	0 € ▲▼

	2024	2025	2026	2027
<b>Tritt mehrfach auf</b> i	Nein ▼	Nein ▼	Nein ▼	Nein ▼
<b>Häufigkeit</b> i	Alle 10 Jahre ▼	Alle 15 Jahre ▼	Tritt nicht auf ▼	Tritt nicht auf ▼
<b>Bester Fall</b> i	342 € ▲▼	32.432 € ▲▼	0 € ▲▼	0 € ▲▼
<b>Wahrscheinlichster Fall</b> i	23.432 € ▲▼	343.242 € ▲▼	0 € ▲▼	0 € ▲▼
<b>Schlechtester Fall</b> i	32.432.423 € ▲▼	234.324.324.32 ... ▲▼	0 € ▲▼	0 € ▲▼

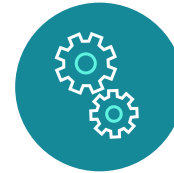
	2024	2025	2026
<b>Tritt mehrfach auf</b> i	Nein ▼	Nein ▼	Nein ▼
<b>Häufigkeit</b> i	Alle 10 Jahre ▼	Alle 15 Jahre ▼	Tritt nicht auf ▼
<b>Bester Fall</b> i	342 € ▲▼	32.432 € ▲▼	0 € ▲▼
<b>Wahrscheinlichster Fall</b> i	23.432 € ▲▼	343.242 € ▲▼	0 € ▲▼
<b>Schlechtester Fall</b> i	32.432.423 € ▲▼	234.324.324.32 ... ▲▼	0 € ▲▼

# Neue Möglichkeiten in der Konfiguration



## Risikomanagement

- Reifegrad definieren
- Risikomatrixgröße festlegen



## Simulation

- Jahre der Mehrjahressimulation bestimmen
- Value-at-Risk und Iterationen harmonisieren



## Internes Kontrollsystem

- Kontrolldurchführung dokumentieren
- Schnittstelle zu BIC Process Design verwenden

# Management-Berichte



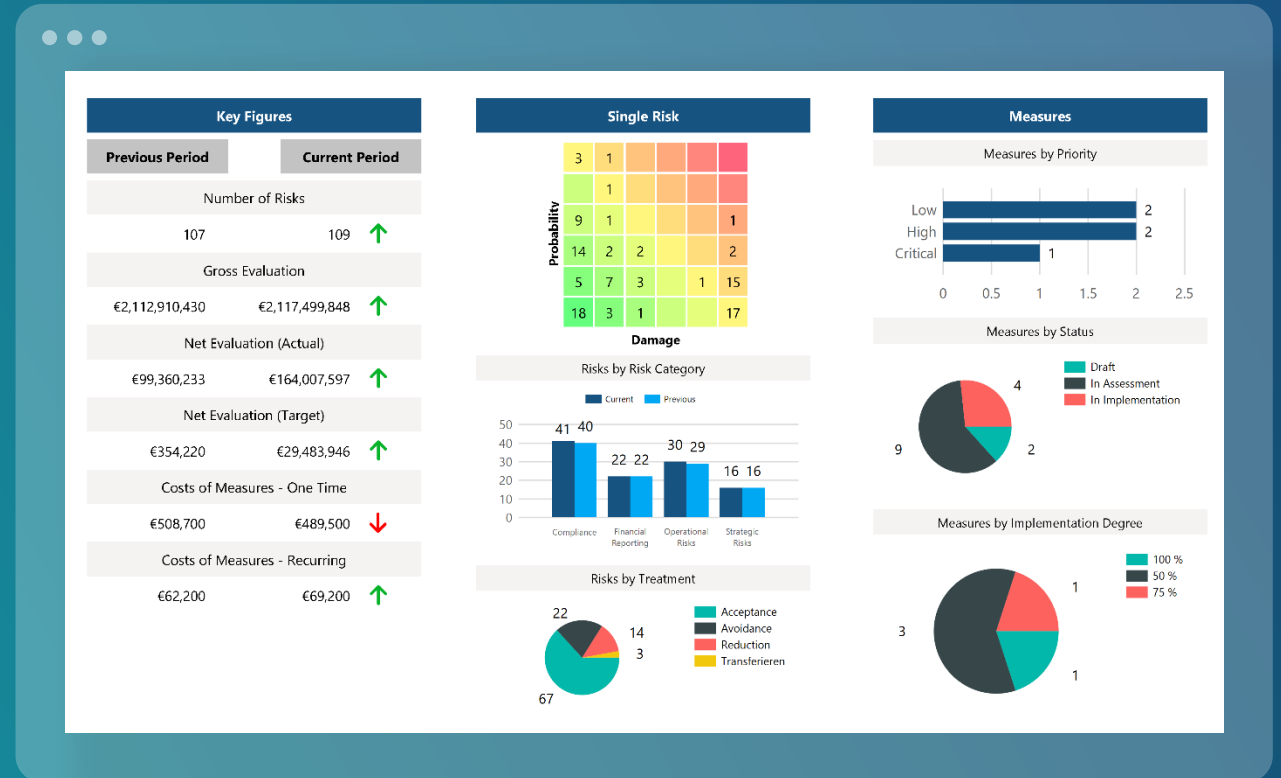
Einheitliches Design



Aufbau im PDF-Format



Zugriff nur für Management-Board



# Live-Demo

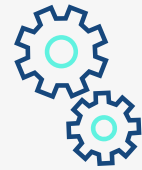




Stimmen Sie jetzt ab!



# BIC GRC & BIC Process Design



Das Beste aus  
beiden Welten



Standardisierte Vorlagen für Prozesse, Prozessrisiken und Kontrollübernahme stehen zur Verfügung.



Alle Konfigurationen sind automatisch hinterlegt und sofort einsatzbereit.



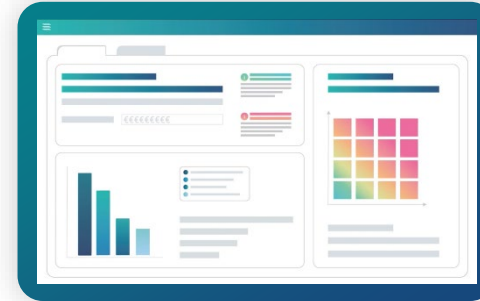
Durch die Einbindung von BIC Process Design ergeben sich zahlreiche Vorteile, aber keinerlei Nachteile.

# Kernfunktionen von BIC Enterprise GRC



## Herausragende Usability

Enduser-Dashboard als zentraler Einstieg  
Übersicht über den gesamten ERM & IKS-Prozess  
Interaktive Nutzerführung in der Risikobewertung



## Flexible Bewertungsmethoden

Automatische Klassifizierung aller Risiken/Chancen  
Qualitative oder quantitative Bewertung  
Vergleich zwischen Brutto- und Nettorisiko

## Aussagekräftige Auswertungen

Dynamische Dashboards und Reports  
Vordefinierte Management-Berichte  
Modul-spezifische Dashboards



## Effektive Zusammenarbeit

Workflow-gestützter ERM & IKS-Prozess  
Kommentierung und Diskussion im Tool  
Automatisierte Freigabe-Prozesse



## Zeitsparende Administration

Excel Import- und Exportfunktion  
Einfache Massendatenbearbeitung  
Automatisierung wiederkehrender Aufgaben



## Integration von ERM und IKS

Eindeutige Trennung durch Berechtigung  
Gemeinsame Verwendung derselben Stammdaten  
Zielführende Integration

Q & A



# Vereinbaren Sie ein unverbindliches Gespräch mit uns!

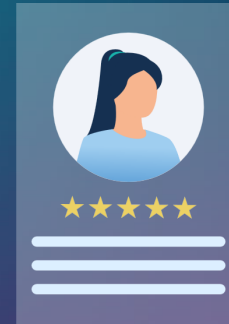
Stellen Sie uns kostenlos Ihre Fragen rund  
um Governance, Risk und Compliance



[https://outlook.office365.com/  
owa/calendar/GRCSales@gbtec.com  
/bookings/](https://outlook.office365.com/owa/calendar/GRCSales@gbtec.com/bookings/)

# Ihre Meinung ist gefragt!

Wir freuen uns über Feedback.





**Marcin Fijałkowski**  
*GRC Solution Architect*



**Florian Korosec**  
*Sales Specialist & Account Manager*



# Monte Carlo Simulation

---

Key Benefits of Quantitative Risk Assessment

Marcin Fijałkowski & Florian Korosec



# Agenda

- 01 Why Choose GBTEC for Your GRC Project
- 02 Questions to Ask Yourself
- 03 Monte Carlo Simulation - Your Benefits
- 04 Key Insights for Management
- 05 Live-Demo in BIC GRC
- 06 Your Questions

# Why Choose GBTEC for Your GRC Project

## Market Leadership

GBTEC is one of the market leaders for digital transformation, BPM and GRC

## Investment Safety

Sustainable business model & continuous development of new innovations

## Attractive Conditions

Unbeatable price-performance ratio: strong functions at the best prices



## Most Modern Design

Greatest possible acceptance & usability through attractive user interface

## Technological Pioneer

Cutting-edge technologies and large development teams

## All-in one Solution

Holistic platform for your BPM and GRC management

# Questions to Ask Yourself



How does **risk exposure** change with new measures?



How does my **risk portfolio** fluctuate over multiple years?



Which **risks** are most dangerous to my company?



How do I consider **dependencies** between risks?



What is my risk exposure if the „**worst case scenario**“ realizes?



How shall I choose my **measures** most efficiently?





There is  
*this*  
option ...





But what if  
there is a  
**better way?**





## Introducing the Monte Carlo Simulation!



# Monte Carlo Simulation – Your Benefits



Widely used tool in risk management



Accounts for the complexity of the real world



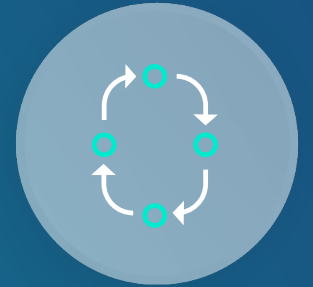
Helps optimize risk management strategies



Incorporates a wide range of inputs

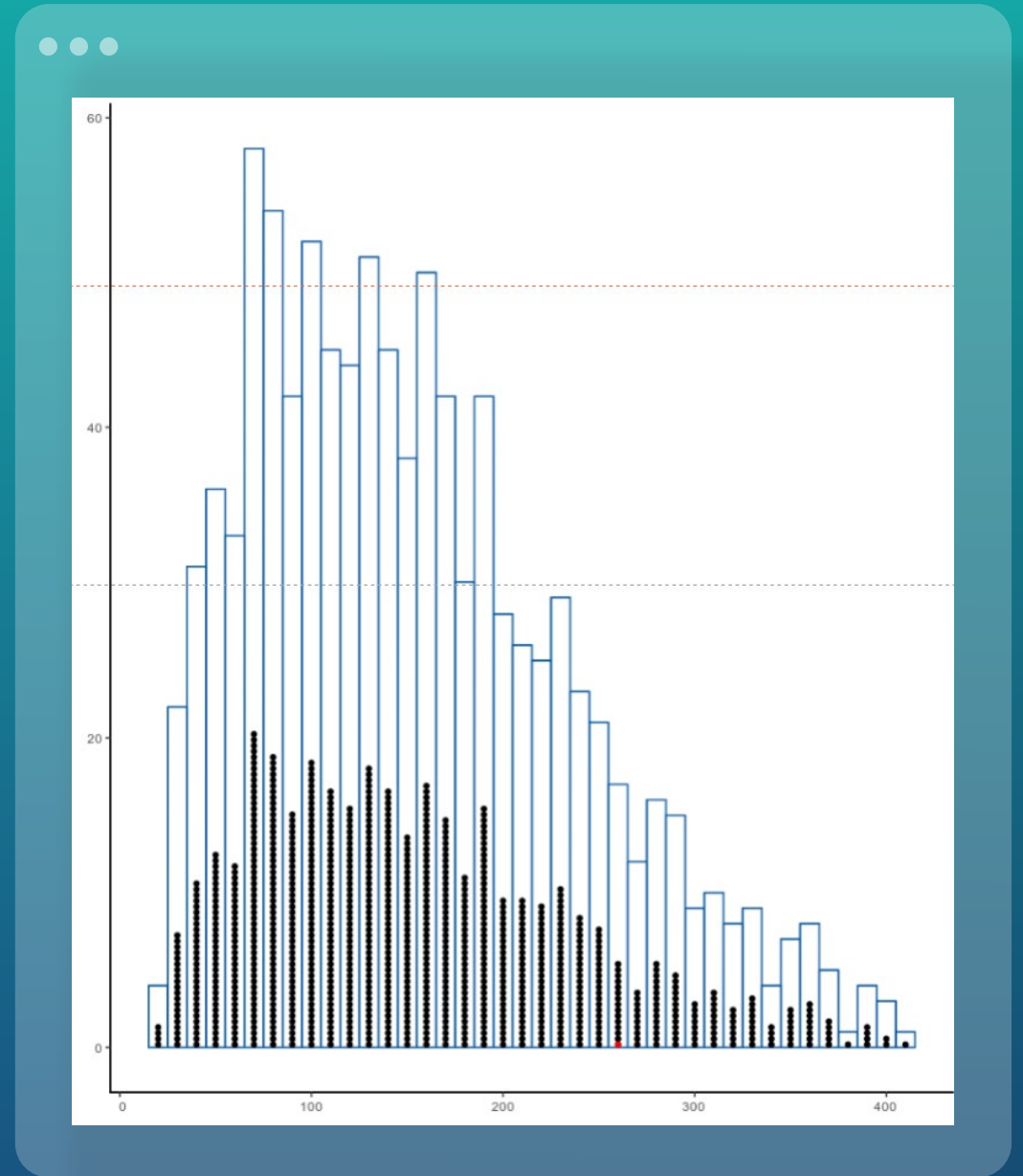
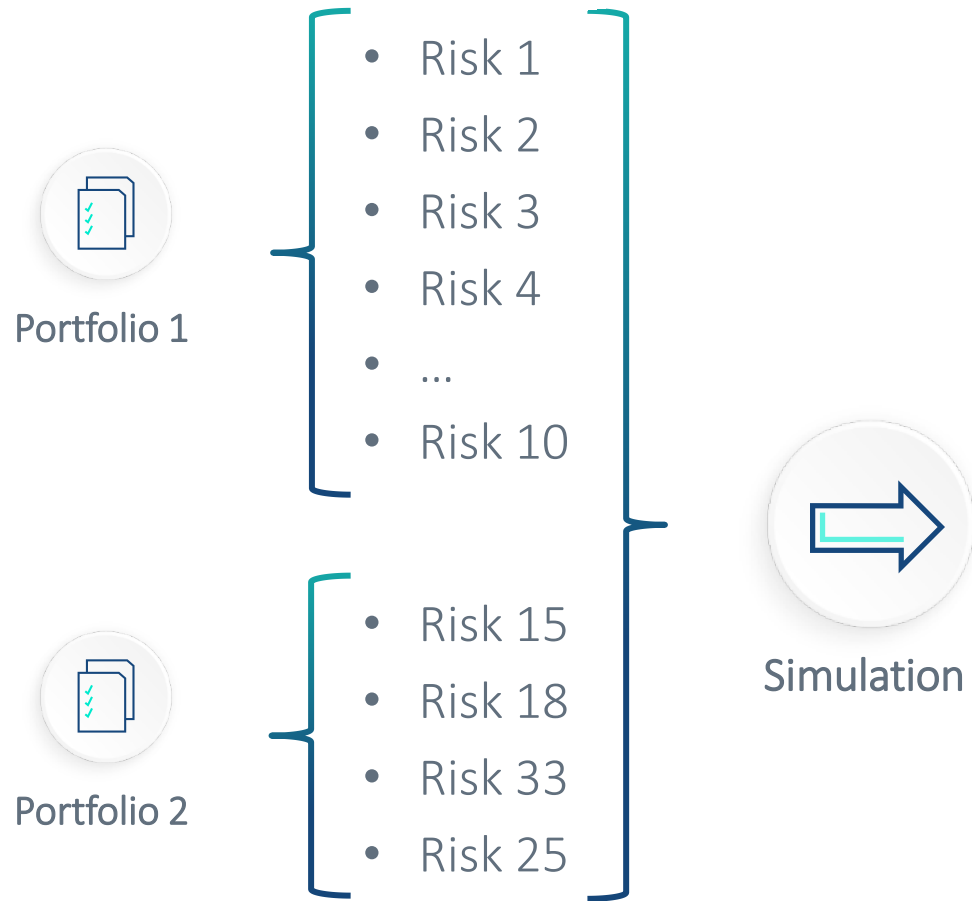


Provides intuitive visualizations



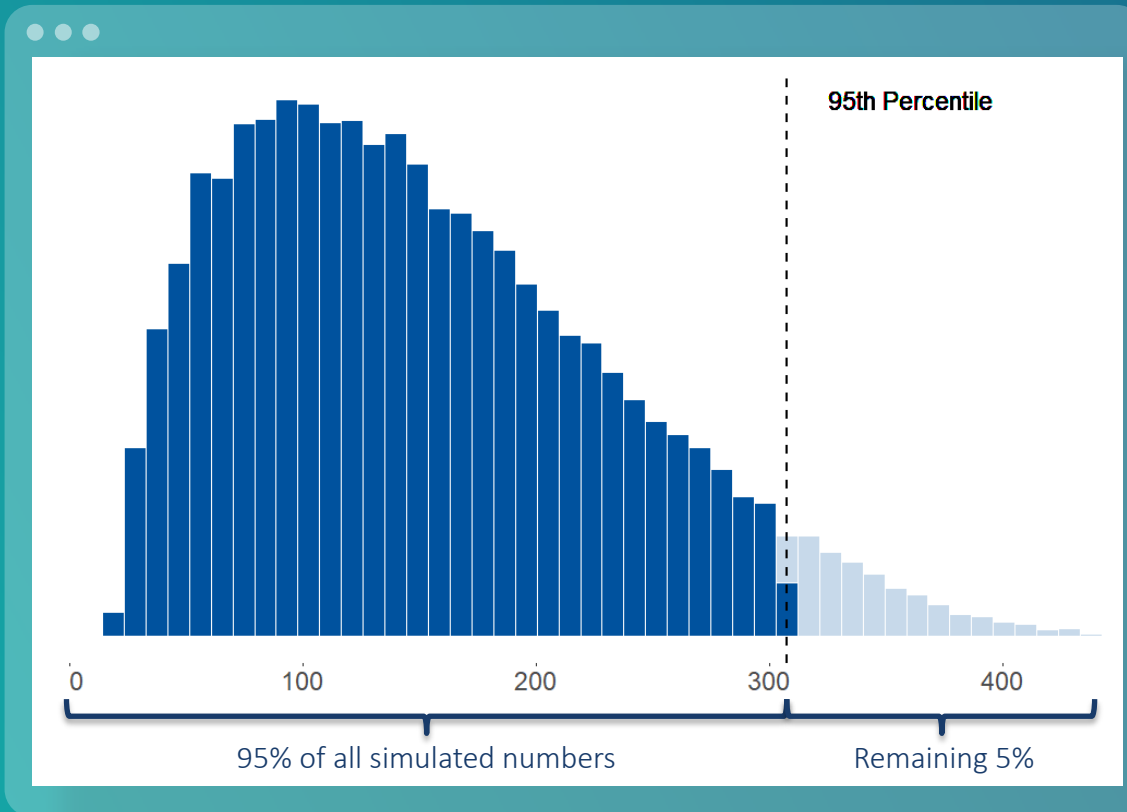
Helps understand the relationships between risk factors

# What Makes the Monte Carlo Simulation So Special?



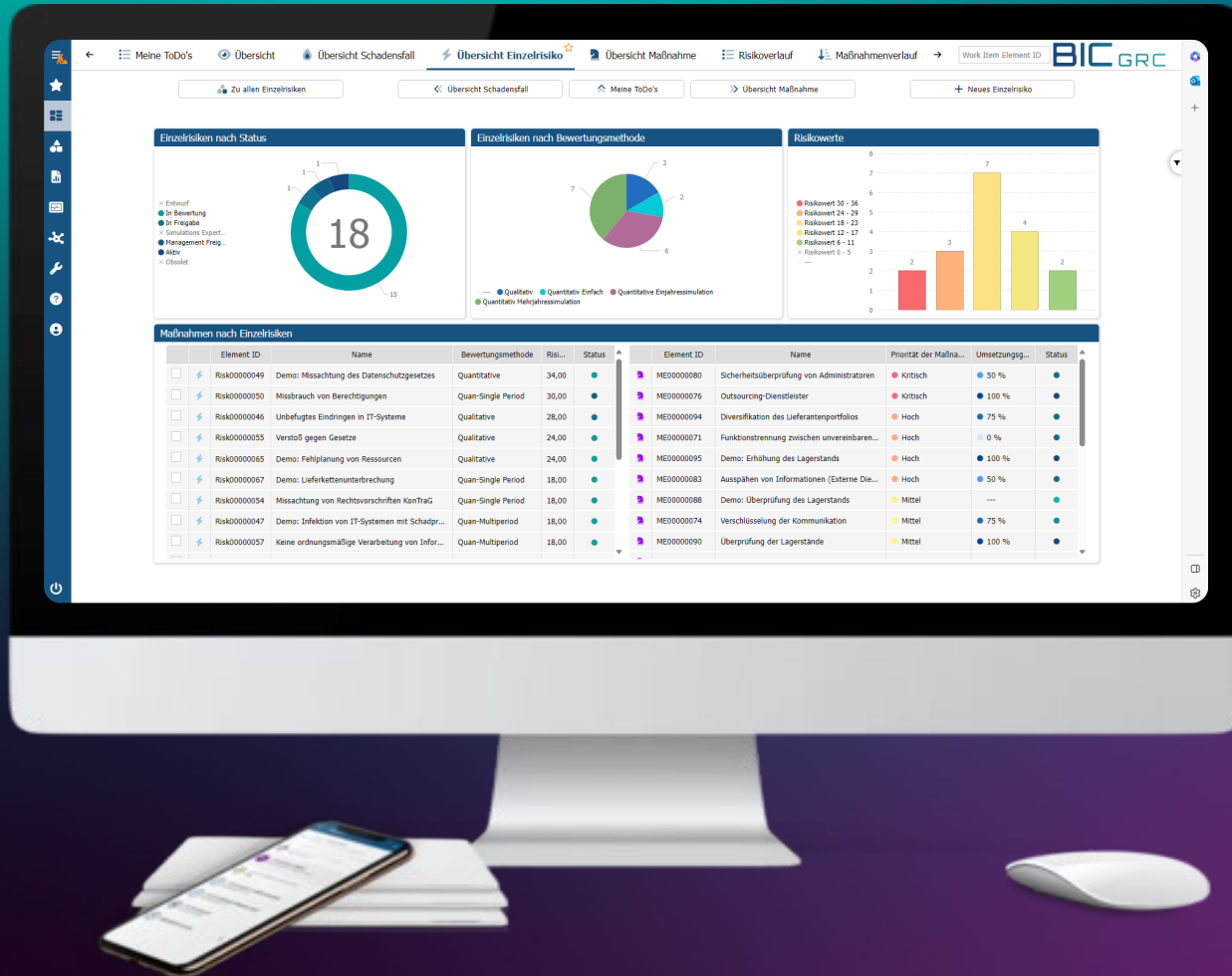


# Interpretation – Key Insights for Management



- **n**-th percentile says:  
„in n% of all simulated results, numbers were lower than XYZ.“
- Example: **95**-th Percentile  
In **95%** of all simulated results, numbers were lower than **307**.
- In other words:  
Only **5%** of all simulated numbers are higher than **307**.

# Live-Demo



# Simulation Use Cases in BIC Enterprise Risk

## SIMULATION



### Risk Simulation

- What is the possible damage the specific risk could cause?
- How does it change based on the measures currently selected?



### Measure Simulation

- What is the commercial effect of a specific measure on the risk it mitigates?
- How does this effect compare to the measure cost?

## PORTFOLIO AGGREGATION



### Portfolio Simulation (Aggregation)

- What is the aggregated financial impact to be expected from a portfolio of risks?
- A portfolio can be selected by entity, by org-unit, by risk-type or individually.



### Multi-Period Simulation

- How does a risk portfolio evolve over multiple time periods?
- This is used to simulate the risk portfolio impact on the financial planning.



### High-Attention-Risks (Top10)

- Which single risks are the biggest damage-contributors to a risk portfolio?
- Which single risks should therefore be treated with high management-attention?



### Stress Testing

- How does a risk portfolio change when probability or impact are stressed for certain risks?
- Does the risk bearing capacity still sufficiently cover the financial impact with stressed risks?



### Risk Dependencies

- What is the aggregated Value-at-Risk for the given portfolio, taking dependencies between risks within the portfolio into account?

## OPTIMIZATION



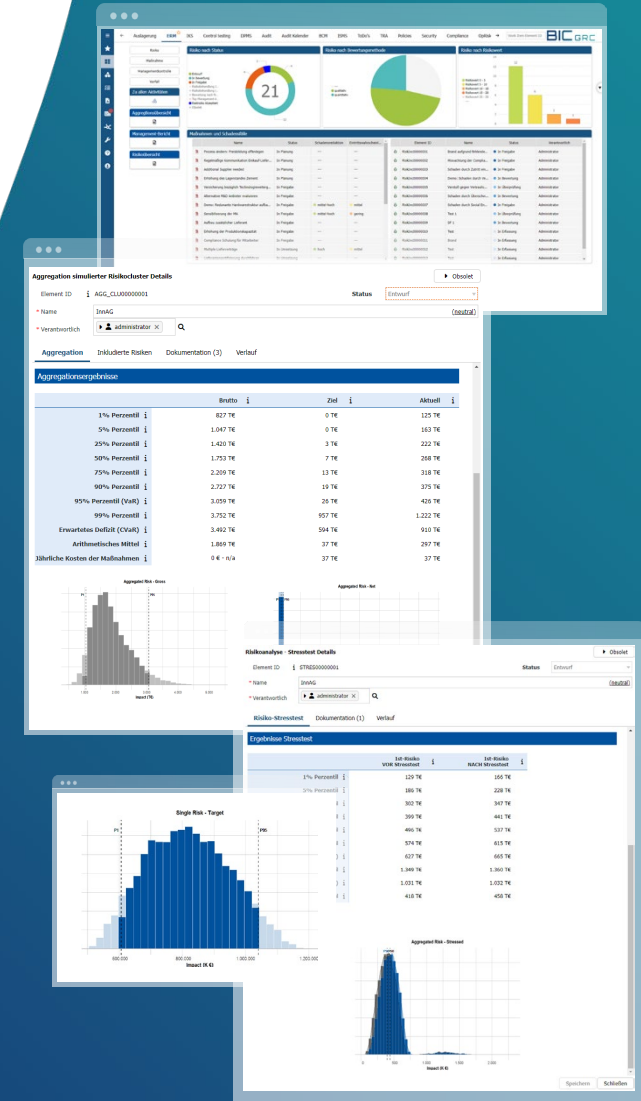
### Budget Optimization

- Which set of measures is recommended for optimal mitigation effect within the given budget constraints?



### Risk-Appetite Optimization

- Which set of measures should be taken to reduce the simulated Value-at-Risk to fit the agreed-on risk-appetite and/or risk-bearing-capacity?



# Q&A



# Vereinbaren Sie ein unverbindliches Gespräch mit uns!

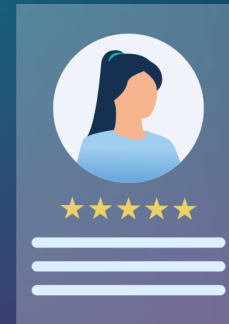
Stellen Sie uns kostenlos Ihre Fragen rund  
um Governance, Risk und Compliance



[https://outlook.office365.com/  
owa/calendar/GRCSales@gbtec.com  
/bookings/](https://outlook.office365.com/owa/calendar/GRCSales@gbtec.com/bookings/)

# Ihre Meinung ist gefragt!

Wir freuen uns über Feedback.





**Martin Tanzer**  
*GRC Solution Architect*



**Matthias Singer**  
*Account Manager*



# BIC Security GRC

---

Umfassender Schutz Ihrer gesamten  
Unternehmenswerte

**Martin Tanzer & Matthias Singer**



# Agenda

- 01 Die Herausforderungen
- 02 Gemeinsam stärker
- 03 Das Sicherheits-Betriebssystem
- 04 Live-Demo in BIC GRC
- 05 Ihre Fragen

# Die Herausforderungen

Druck zur Einhaltung internationaler Standards

Bewertung und Priorisierung von Geschäftsprozessen

Schwierigkeiten bei Risikoidentifikation und -priorisierung

Identifizierung potenzieller Geschäftsunterbrechungen

Identifizierung und Verwaltung von personenbezogenen Daten & Datenverfälschung

Sicherstellung von Ressourcen für den Notfallbetrieb



# Und was bereitet Ihnen Kopfschmerzen?



Es gibt viele Möglichkeiten...

**Excel-Werkzeuge**

**Checklisten-Tools**

**Statische Anwendungen**

**Silo-Lösungen**

**Insel-Software**

Es gibt viele Möglichkeiten...



Werkzeuge  
Checklisten-Tools  
S  
Lösungen  
Silo-Lösungen  
Insel-Software

Es gibt viele Möglichkeiten...



# Gemeinsam stärker!

## BIC Internal Audit

Intern/Kunden/Lieferanten/Zertifizierung

## BIC Data Protection

ISO 27701:2019 & DSGVO



## BIC Information Security

ISO 27001:2022 & BSI Grundschutz

## BIC Business Continuity

ISO 22301:2019 & BSI 200-4

# BIC Security GRC – Ihr Sicherheits-Betriebssystem



Zentrale Asset-Verwaltung für alle Domänen



Navigation & Datensichten via Dashboards



Fachliche Verschränkung durch  
gemeinsam genutzte Datenobjekte



Reports jederzeit per Knopfdruck



Systemimmanenter PDCA-Zyklus



Skalierbarkeit durch Konfigurierbarkeit



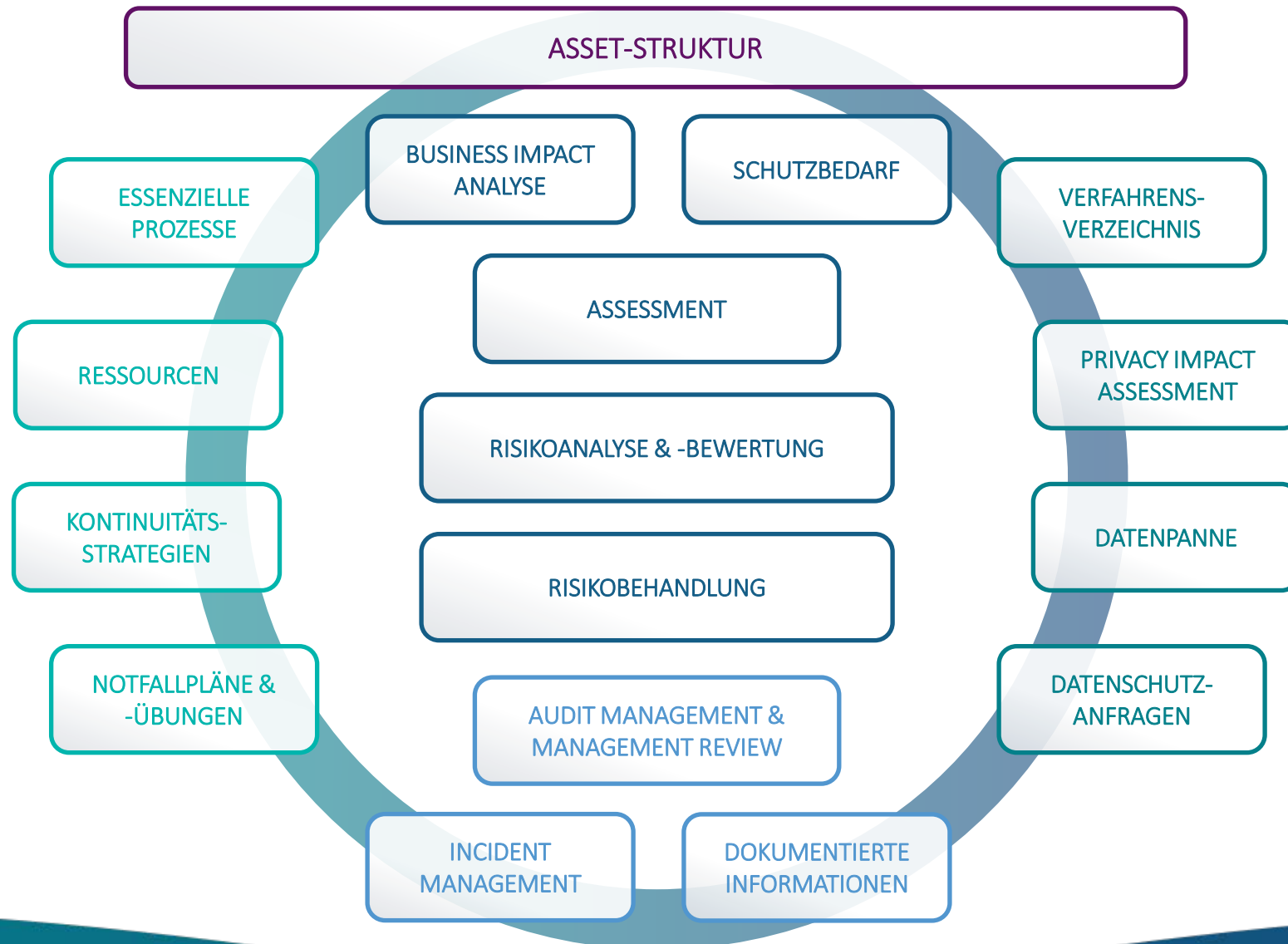
Vordefiniertes Rollenkonzept & Workflows



Bei Bedarf erweiterbar & adaptierbar



# Nahtlose Integration



# Auf alle Eventualitäten top vorbereitet!



Bewirtschaften Sie Ihre Security-Managementsysteme **zentral in einem Tool**.



**Steigern Sie die Qualität** Ihrer Daten durch unseren holistischen Ansatz.



Vermeiden Sie Redundanzen und sparen Sie **Zeit und Geld**.



Profitieren Sie von **Synergien** durch kollaboratives Arbeiten.



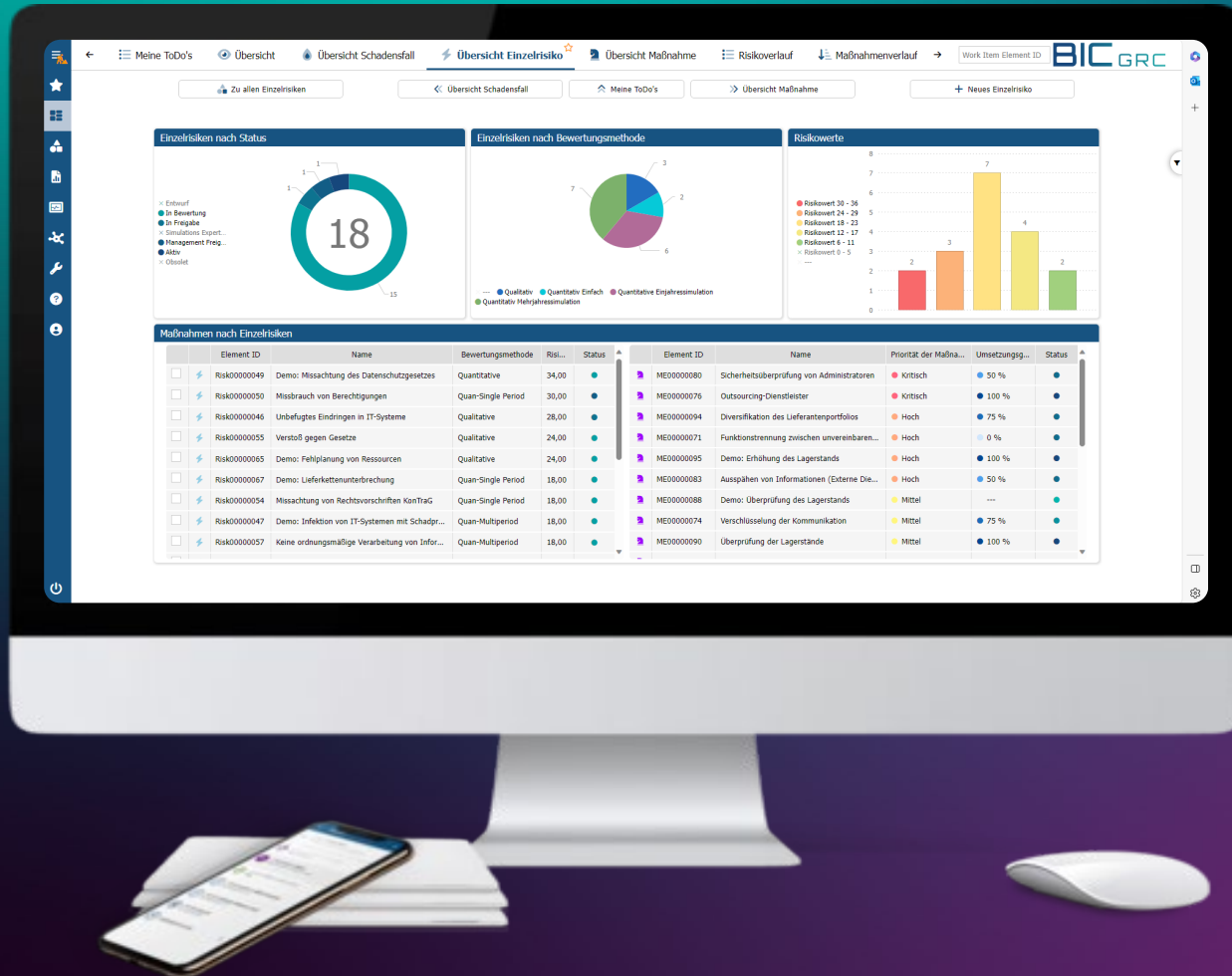
Nutzen Sie die **richtigen Informationen zur richtigen Zeit** in der richtigen Form.



Passen Sie BIC Security GRC an Ihre **individuellen Anforderungen** an.



# Live-Demo



# Q & A



# Vereinbaren Sie ein unverbindliches Gespräch mit uns!

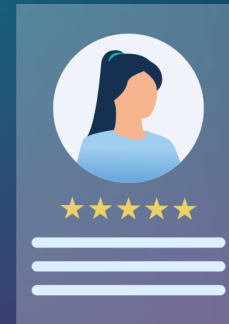
Stellen Sie uns kostenlos Ihre Fragen rund  
um Governance, Risk und Compliance



[https://outlook.office365.com/  
owa/calendar/GRCSales@gbtec.com  
/bookings/](https://outlook.office365.com/owa/calendar/GRCSales@gbtec.com/bookings/)

# Ihre Meinung ist gefragt!

Wir freuen uns über Feedback.





**Jens Feistel**

*Informationssicherheits-  
Beauftragter, DEW21*



# Success Story

---

Umfassende Integration von ISMS & BCM bei DEW21,  
dem Energie- und Wasserversorger der Stadt Dortmund

Jens Feistel



# Agenda

- 01 Managementsysteme
- 02 Mountain Journey: Zugspitze
- 03 Und dann kam Corona!
- 04 Mountain Journey: Mont Blanc
- 05 GBTEC Plattform
- 06 Mountain Journey: Die Achttausender
- 07 Ihre Fragen

# Managementsystem



Aus Sicht der Normen setzt sich der Begriff aus zwei Anteilen zusammen: „**Management**“ besteht aus „**aufeinander abgestimmten Tätigkeiten zum Führen und Steuern einer Organisation**“ und kann nach Anmerkung 1 „**das Festlegen von Politik, Zielen und Prozessen zum Erreichen dieser Ziele**“ umfassen (ISO 9000:2015, 3.3.3).

Ein „**System**“ ist dabei ein „**Satz zusammenhängender und sich gegenseitig beeinflussender Elemente**“ (ISO 9000:2015, 3.5.1). Ein „**Managementsystem**“ ist demnach ein solcher Satz Elemente einer Organisation, um Ziele zu erreichen (ISO 9000:2015, 3.5.3; ISO 14001:2015, 3.1.1).

Es **bündelt Tätigkeiten, Instrumente und Methoden**, um das Unternehmen bezüglich konkreter **Zielsetzungen** eines spezifischen Arbeitsfelds (z. B. Qualität) zu führen und zu steuern.



Susanne Petersen, *Führung und Zusammenarbeit in Managementsystemen*, 2016, S. 130.



Steuerung von **Geschäftsprozessen** und **Unternehmungen**



Festlegen und Messen von KPIs zur **Performance** und **Qualitätssicherung**

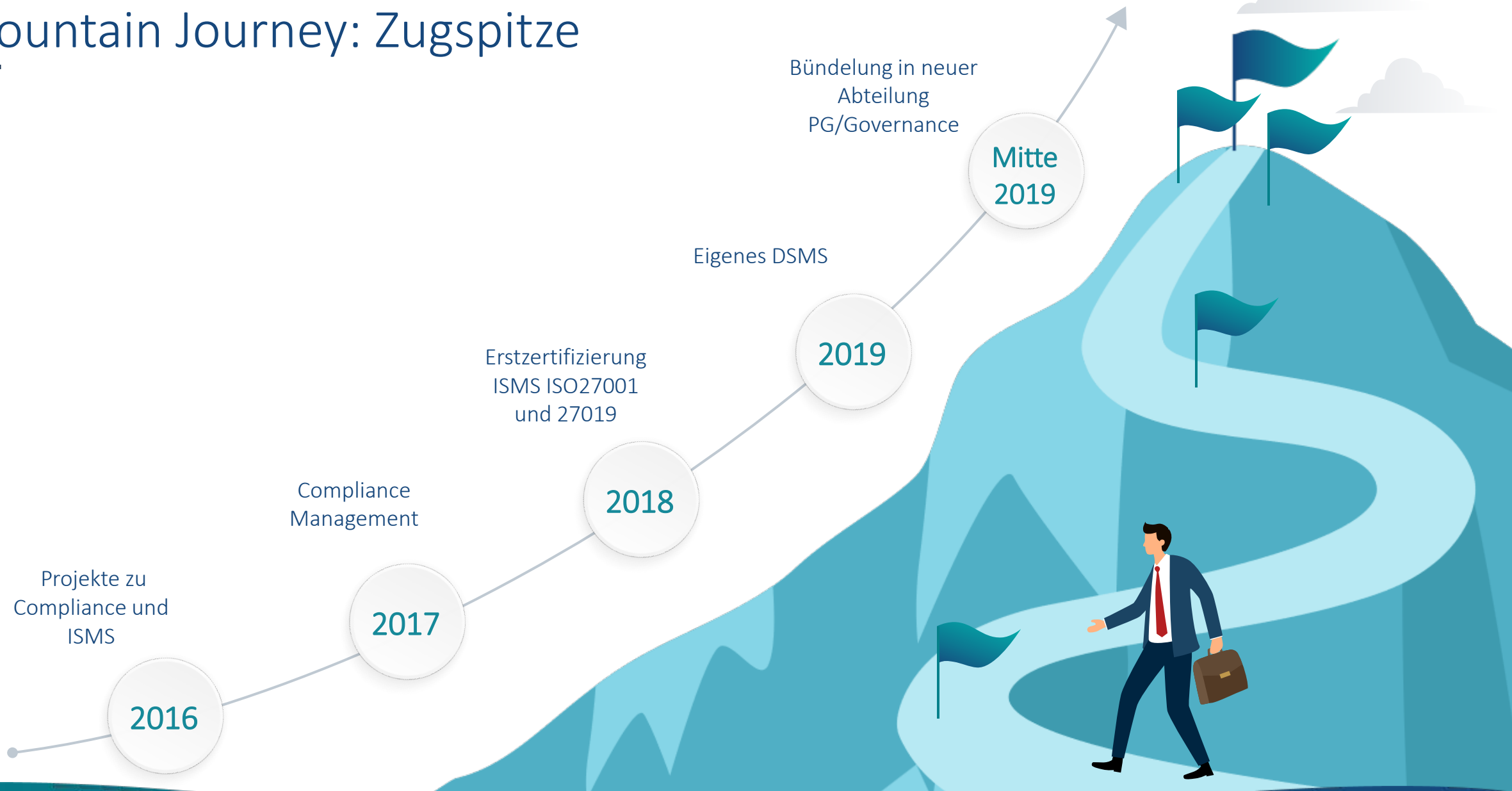


Management von **Chancen** und **Risiken**

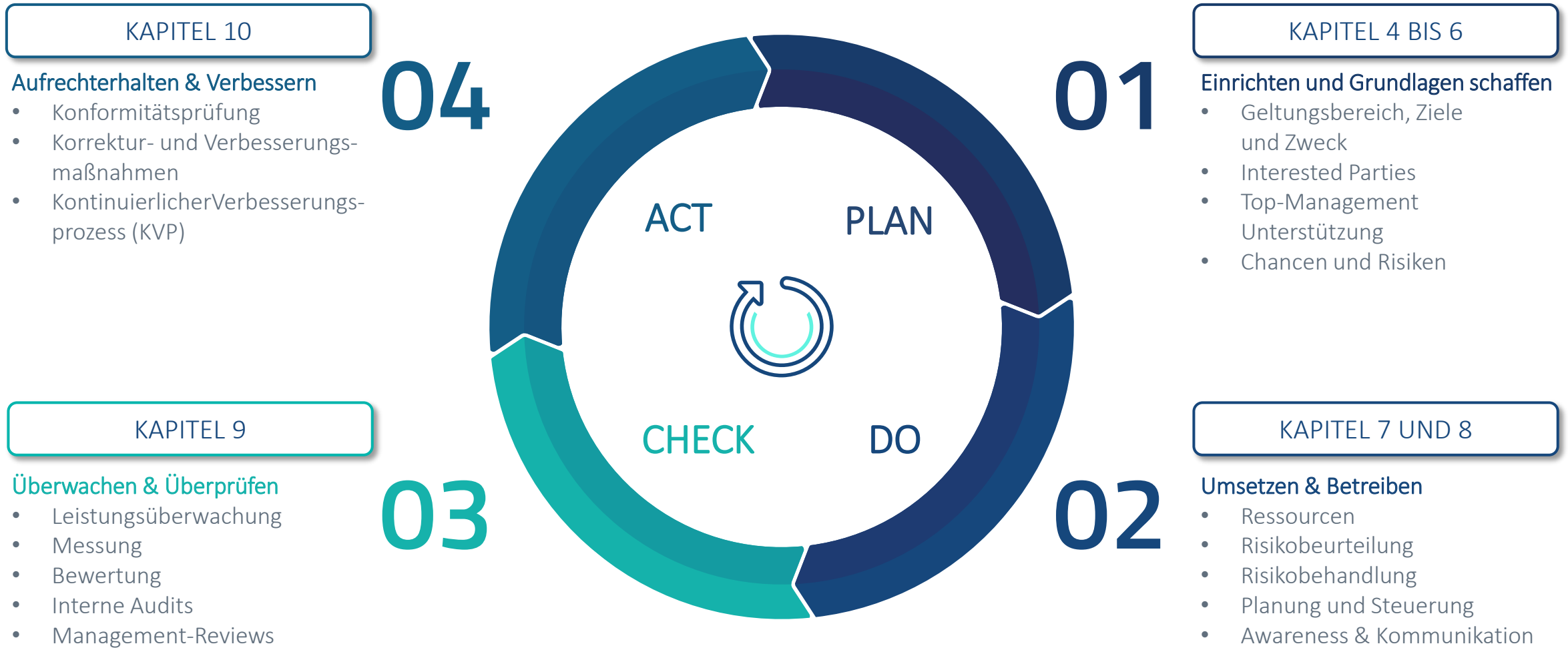


**Prozessbasierter Ansatz** ist empfehlenswert

# Mountain Journey: Zugspitze



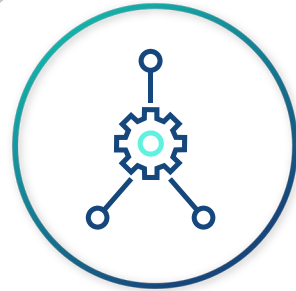
# PDCA Cycle nach ISO-Normen



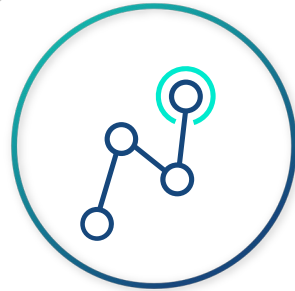
# Zusammenfassung



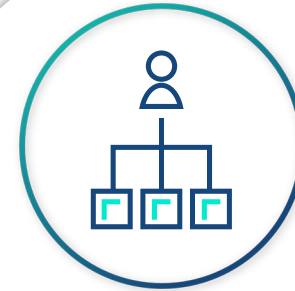
Vielfalt an **Normen** und **Regularien** sind zu berücksichtigen



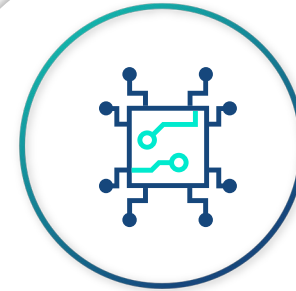
Uneinheitliches **Risikomanagement**



**Risikobehandlung** und **Maßnahmen** sind häufig unabgestimmt



Jedes **MMS** auditiert und berichtet (mehr oder weniger) ausführlich und eigenständig



**Synergien** bleiben vielfach unausgeschöpft

# Informationssicherheits-Managementsystem



Leitlinie, Stakeholder-Management,  
Dokumentenlenkung, Programmplanung & KVP



## Vorfallsbearbeitung

- Sicherheitsereignisse
- Schwachstellen/Meldungen



## Auditierungen, Nachweise und Zertifizierungen, weitere Entwicklungen

- IT-Sicherheitsgesetz, EU NIS-2, EU-CER
- Hoher Zeitaufwand



## Berichterstattung, Reporting und Management-Review

- Unterschiedliche Formate, keine Standardisierung
- Kennzahlen in verschiedenen Reports verteilt



## Unterschiedliche Tools zur Risikoanalyse und Prozessunterstützung

- Von XLSX über DOCX und über PPTX
- Hin zu Ticketsystemen & Einzellösungen

# BIC GRC ISO Solution



Nun endlich zu professionellen, workflowbasierten und integrierten Lösungs-Plattformen.

The screenshot displays the BIC GRC software interface. The top navigation bar includes 'Meine ToDo's', 'Übersicht Assessment', 'Übersicht Risikoanalyse', 'Übersicht Maßnahme', 'Übersicht Vorfall', and 'Übersicht Schutzbedi'. The main content area features three dashboards: 'Maßnahmen nach Status' (Measures by Status) with a donut chart showing 68 measures; 'Maßnahmen nach Priorität' (Measures by Priority) with a pie chart showing 32 measures; and 'Maßnahmen nach Umsetzungsgrad' (Measures by Implementation Degree) with a pie chart showing 44 measures. Below these is a table titled 'Wirksamkeitsnachweis nach Maßnahmen' (Effectiveness proof by measures).

Name	Status	Schadensreduktion	Extritzwahrsch...	Element ID	Name	Status	Test Verantwortlicher
Whiskly Gold	In Planung	---	---	TsE00000034	Prüfung der Chancen & RL...	In Planung	Festl Jans
Projekt Objektschutz KRITIS	In Planung	---	---	TsF00000035	SMCWA Softwareschulung...	In Planung	Mittendorf Lars
Duozentrale USV für FWT	In Planung	mittel-hoch	mittel-hoch				
Einführung neuer Antivirus-Software	In Planung	---	---				
Technisches Sicherheitsmanagement	In Planung	---	---				
Offizielle Bereitschaft schaffen (Intern PRG)	In Planung	---	---				
Betriebsanbuch SMCWA DEW21	In Planung	---	---				
Zweiter FW-Hersteller in der PDV	In Planung	---	---				
Zweiter Internet-Service-Provider für das...	In Planung	---	---				

# Und dann kam Corona!



Was sind unsere  
wichtigsten  
Geschäftsprozesse?



Welches Personal  
brauchen wir dafür?



Welche IT-Ausstattung  
wird mindestens  
benötigt?



...und plötzlich arbeiten  
(fast) ALLE mobil!

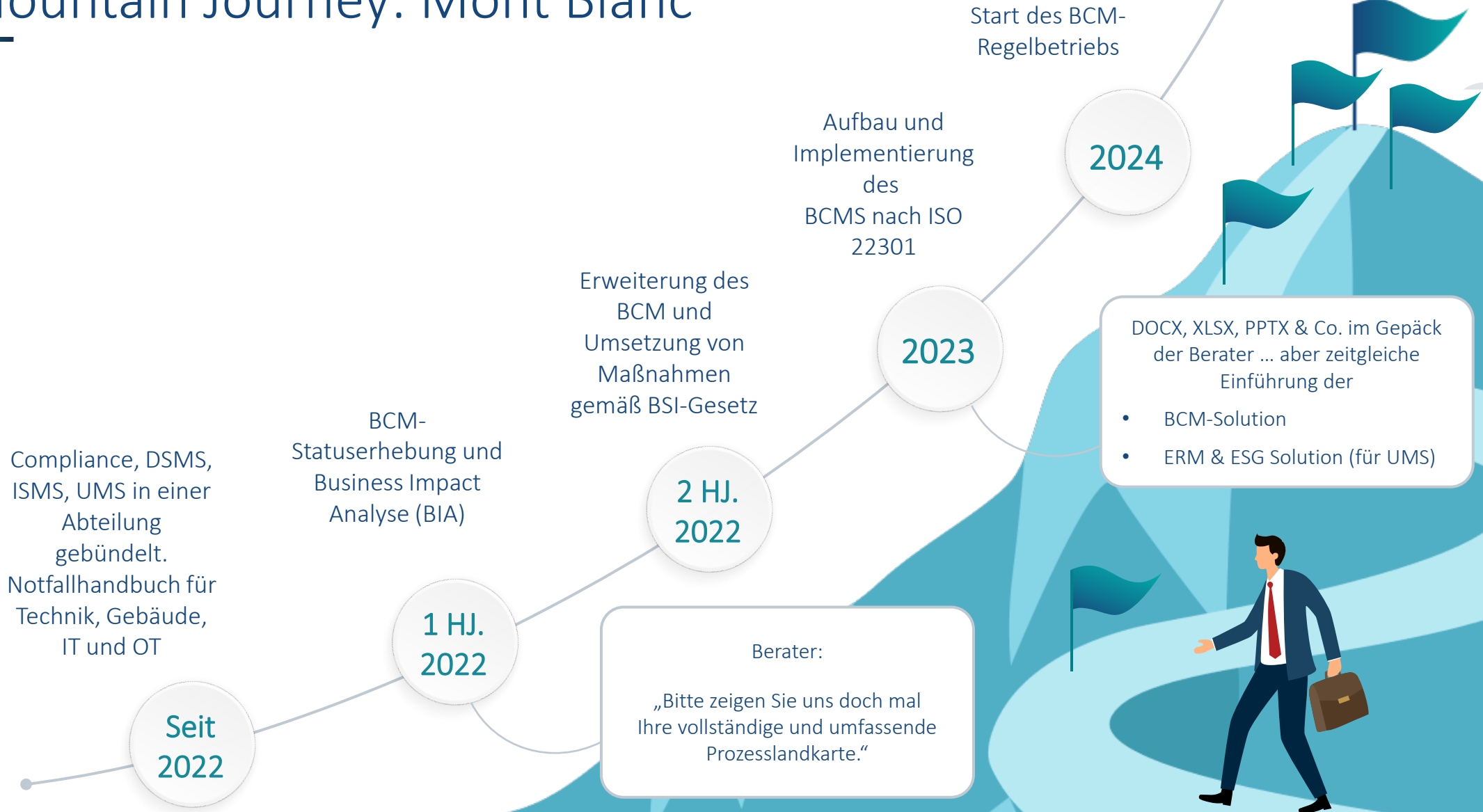


## Zentrale Frage:

Wie steht es eigentlich um unser  
**Business Continuity Management**  
und die  
**unternehmerische Resilienz?**



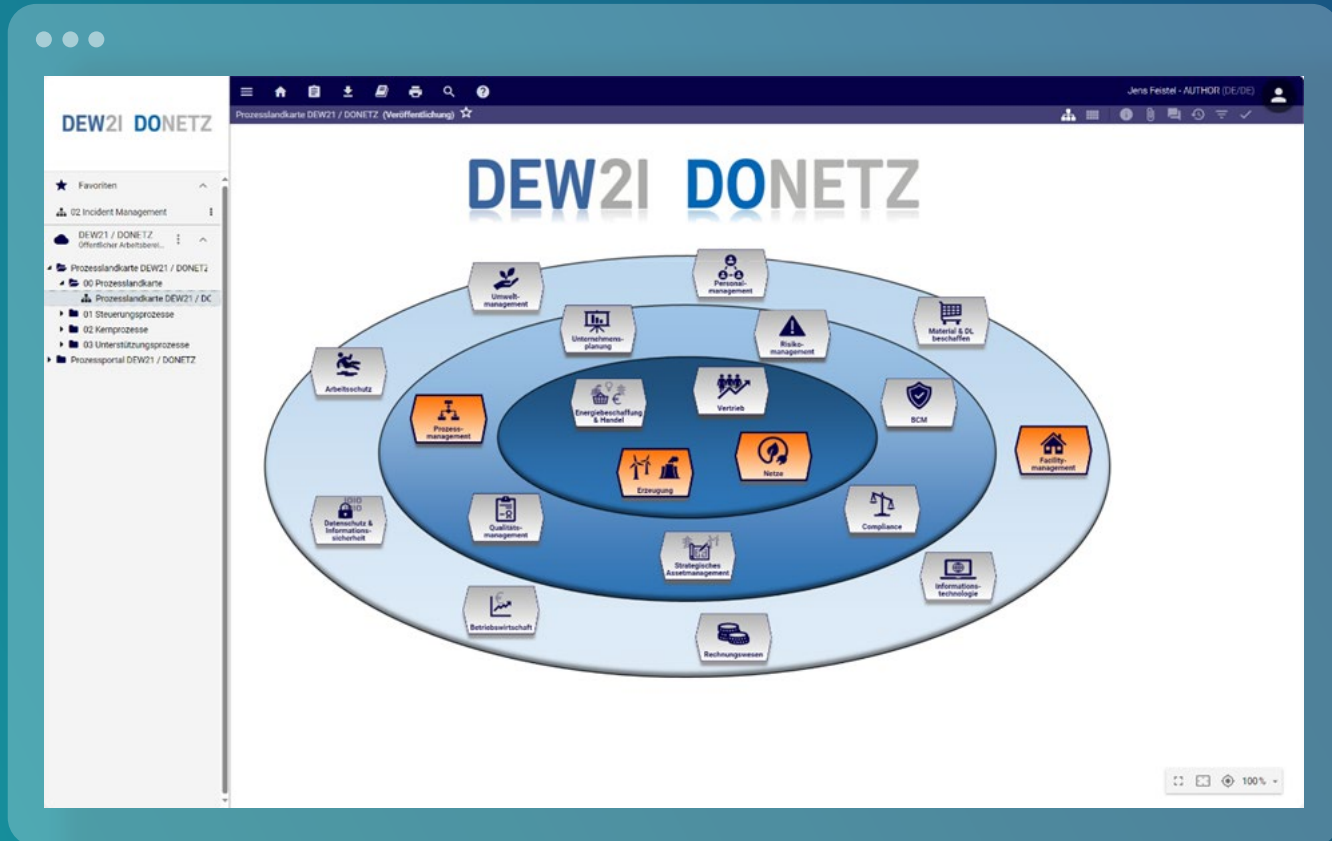
# Mountain Journey: Mont Blanc



# Exkurs Prozessmanagement



Seit Juli 2023 ist das Prozessmanagement auf Basis von BIC Process Design ebenfalls in unsere Abteilung integriert.



# GBTEC Plattform

## Software as a Service

- Alles vom Anbieter, kaum Aufwand für die eigene IT
- Consulting, Patches und Updates aus einer Hand
- Aus Anwendersicht nur ein Ansprechpartner
- Schnelle Bereitstellung und Reaktionszeiten

## BIC Plattform

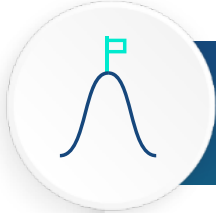
- Motivierte und kompetente Solution Consultants und Projektmanager:innen
- Innovative und erprobte (Kunden-) Lösungen
- Customizing und Kundenausrichtung

“

Mit der BIC Plattform werden Sie zu MacGyver, der mit Kaugummipapier und einem Taschenmesser alle Herausforderungen meistert!

”

# Mountain Journey: Die Achttausender



## Vision:

Integrierte Managementsysteme

### Ganzheitliche Betrachtung der ...

- ... Geschäftsprozesse (End-to-End),
- ... Key Performance Indicators (KPIs),
- ... Umfeldfaktoren,
- ... Chancen und Risiken,
- ... Stakeholder,
- ... Dashboards und Reports,
  
- ... um **maximale Synergie** in Steuerungs- und Kontrollmechanismen sowie **unternehmerische Resilienz** zu erreichen.



# Q & A



Vielen Dank!



**Jens Feistel**

Informationssicherheits-  
Beauftragter, DEW21



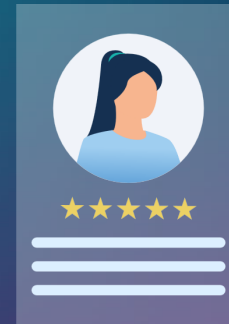
Jens.Feistel@dew21.de



+49 231 544 20 53

# Ihre Meinung ist gefragt!

Wir freuen uns über Feedback.





**Kaspar Kühl**  
*Partner,  
greenfield Consulting*



**Samuel Brandstätter**  
*Head of Product Line GRC  
& Managing Director  
GBTEC Austria*



**Christian Buechler**  
*GRC Consulting & Training*



**Philipp Strokosch**  
*Head of Sales GRC*



# Expert Talk

---

Verschiedene Aspekte einer gelungenen  
Unternehmensstrategie

**Kaspar Kühl, Samuel Brandstätter,  
Philipp Strokosch & Christian Buechler**

# Vereinbaren Sie ein unverbindliches Gespräch mit uns!

Stellen Sie uns kostenlos Ihre Fragen rund  
um Governance, Risk und Compliance



[https://outlook.office365.com/  
owa/calendar/GRCSales@gbtec.com  
/bookings/](https://outlook.office365.com/owa/calendar/GRCSales@gbtec.com/bookings/)

Save the Date!



---

7.11.2024