# Krisenfest in die Zukunft

**Mit integriertem Risk & Security Management zu nachhaltiger Resilienz**

Ronald Prahs, Martin Tanzer

# Das GBTEC Team

**Ronald Prahs**

*Head of Presales*

**Martin Tanzer**

*GRC Solution Architect*

# Wie ist der Status Quo im Unternehmensalltag?

GRC wird von vielen Unternehmen als Bremse gesehen

# Welche Folgen sind möglich?

- Das Personal im Tower hatte keinen Zugriff auf aktuelle Systeminformationen
- Die Gepäcklogistik kam komplett zum Erliegen
- Die Terminals waren außer Betrieb
- Die Sicherheitskräfte bekamen keine Updates

# Wie konnte es so weit kommen?

# Was sollten Unternehmen daraus lernen?


GRC ist das Betriebssystem moderner Unternehmens-steuerung

# Der Einwand: Die Kosten sind zu hoch

**Welche Kosten entstehen ohne GRC?**

- Reputationsschaden
- Nachrüstungskosten
- Wirschaftlicher Schaden
- Möglicher Schadenersatz

# Gewinn maximieren mit GRC

## Welche Vorteile bringt GRC?

- Stetiger Vertrauensgewinn
- Geringere Kosten
- Stabile Betriebskontinuität
- Planbare Ausgaben

Ein intelligentes, vorausschauendes Steuerungssystem, das sich dann bewährt, wenn es darauf ankommt – nicht wenn es zu spät ist. Denn Resilienz zeigt sich in der Wirkung, nicht in der Wahrscheinlichkeit.

# Out of the Box

## Was eine integrierte GRC-Lösung leisten kann

# What is GRC?

**G** **GOVERNANCE**
... achieve objectives

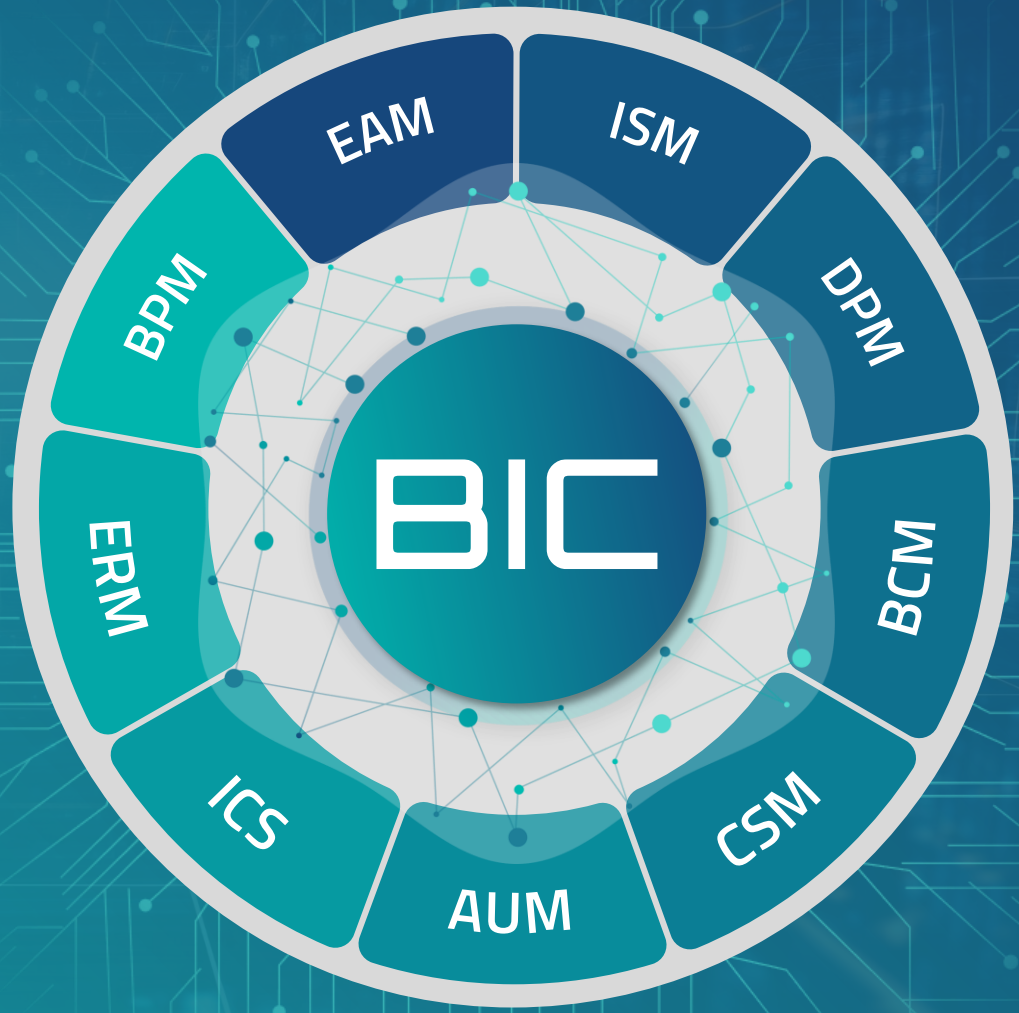
**R** **RISK**
... address uncertainty

**C** **COMPLIANCE**
... act with integrity

# GRC is …

… looking **together** at the same **objectives**, but from different **perspectives**!

… an **integrated** collection of capabilities to reliably achieve **objectives**, address **uncertainty**, and act with **integrity**.



# Gestatten, 4WHEELS Automotive AG!


- 40.000 Mitarbeiter
- 2.300 User
- 2 Tochterunternehmen

Die 4WHEELS Automotive AG* ist ein international tätiger Konzern mit Fokus auf die Herstellung, den Vertrieb und die Finanzierung von PKWs. Die zunehmenden regulatorischen Anforderungen, Lieferkettenrisiken, Nachhaltigkeitsziele, sowie eine komplexe Prozess- und IT-Landschaft zwingen das Unternehmen, GRC holistisch und integriert zu denken.

*fiktives Unternehmen

## 4WHEELS Automotive Production GmbH

Produktion in drei Werken in Europa

## 4WHEELS Automotive Finance GmbH

Fahrzeugfinanzierung, Restwertmanagement

# Beispiel-Szenario: 4WHEELS Automotive AG*

## Anlass
Die neue E-Plattform ist „connected by design“ – Fahrzeuge erhalten regelmäßige Softwareupdates

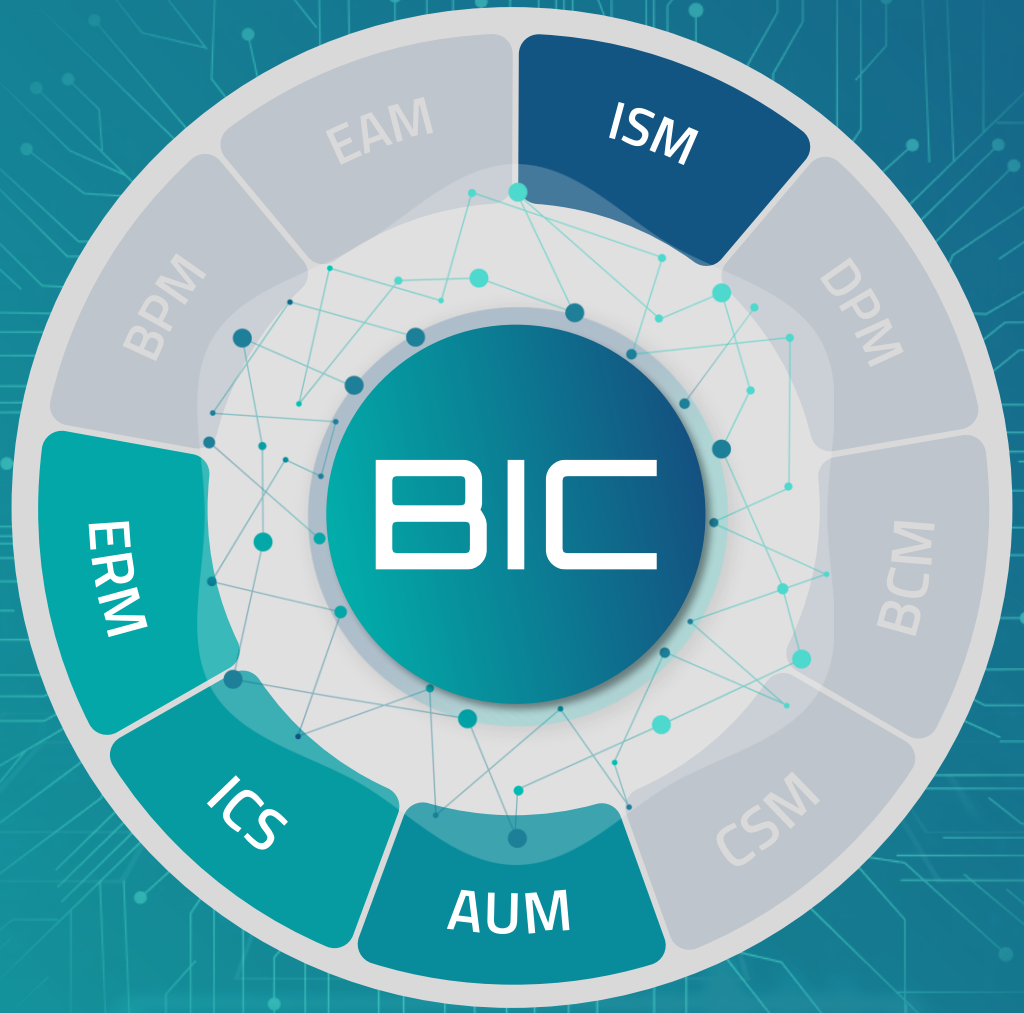
## Auswirkung
neue Angriffsfläche für Angriffe von außen, etwa durch unautorisierte Zugriffe auf Fahrzeugdaten oder Manipulationen der Software

## Risiko
Schwachstellen in der IT-Sicherheitsarchitektur könnten dazu führen, dass Insassen und Fahrzeuge gefährdet werden

## Ziel
Sicherstellung einer robusten IT-Sicherheitsarchitektur, die Cybersicherheit und Kontrollsysteme der Fahrzeuge umfassend schützt

*fiktives Unternehmen

# Fokus auf die Domänen …



# Relevante GRC-Managementsysteme

## Information Security Management (ISM)

Aufbau eines Informationssicherheitsmanagementsystems nach ISO 27001, inklusive Threat Intelligence und Penetration Testing

## Enterprise Risk Management (ERM)

Risikoanalyse für Cyber-Angriffe → Bewertung anhand des Schadensausmaßes und der Eintrittswahrscheinlichkeit

## Internal Control System (ICS)

Implementierung interner Kontrollen für sichere Update-Prozesse, Protokollierung und Zugriffsbeschränkungen

## Audit Management (AUM)

Regelmäßige Prüfung der Sicherheitsmaßnahmen durch interne Revision (Audit-Trails, Schwachstellenmanagement, Korrekturmaßnahmen, …)

# Effizienz durch verzahnte GRC-Systeme

**Beteiligte GRC-Systeme**

| ISM | ERM | ICS | AUM |
|---|---|---|---|
| Vertraulichkeit, Integrität und Verfügbarkeit von Daten werden abgesichert | Bedrohungen durch OTA-Schnittstellen werden frühzeitig erkannt | Zuverlässigkeit von Kontrollen wird durch regelmäßige Überprüfung gewährleistet | Laufende Prüfung und Optimierung der Prozesse werden sichergestellt |

**BIC GRC als Single Point of Truth**

- Integrierte Betrachtung führt zu einem belastbaren, kontinuierlich lernenden Sicherheits- und Kontrollsystem
- Sicherheitsvorfälle werden nicht nur reaktiv gemeldet, sondern führen direkt zu Verbesserungen im System
- Geschlossener Regelkreis von der Bedrohungserkennung bis zur risikobasierten Optimierung, zentral gesteuert im GRC-Framework

# Vorteile durch verzahnte GRC-Systeme

## Transparenz

Zentrale Erfassung aller Risiken, Kontrollen und Anforderungen für ganzheitliche Steuerung

## Effizienz

Vermeidung von Redundanzen senkt Dokumentations- und Prüfaufwand

## Synergien

Wechselwirkungen zwischen Risiken werden sichtbar und gezielt adressiert

## Resilienz

Integration von BCM, ISMS, Datenschutz und IKS stärkt Krisenfestigkeit

## Compliance

Einheitliche Umsetzung und Nachweis regulatorischer Anforderungen

## Steuerung

Fundierte, informierte Entscheidungen auf Basis konsolidierter Informationen

# Sehen Sie hier weitere konkrete integrierte GRC Use Cases!

Einfache und zeitsparende Integration von:

BCM, CSM, BPM

BCM, ERM, BPM

ISM, ERM, IKS, AUM