
# Schluss mit Zettelwirtschaft & Fragebögen

Erfolgsrezepte für effiziente Compliance in Zeiten von NIS-2, DORA, etc.

Daniel Kammerbauer, Controlware GmbH
Team Lead Governance, Risk & Compliance

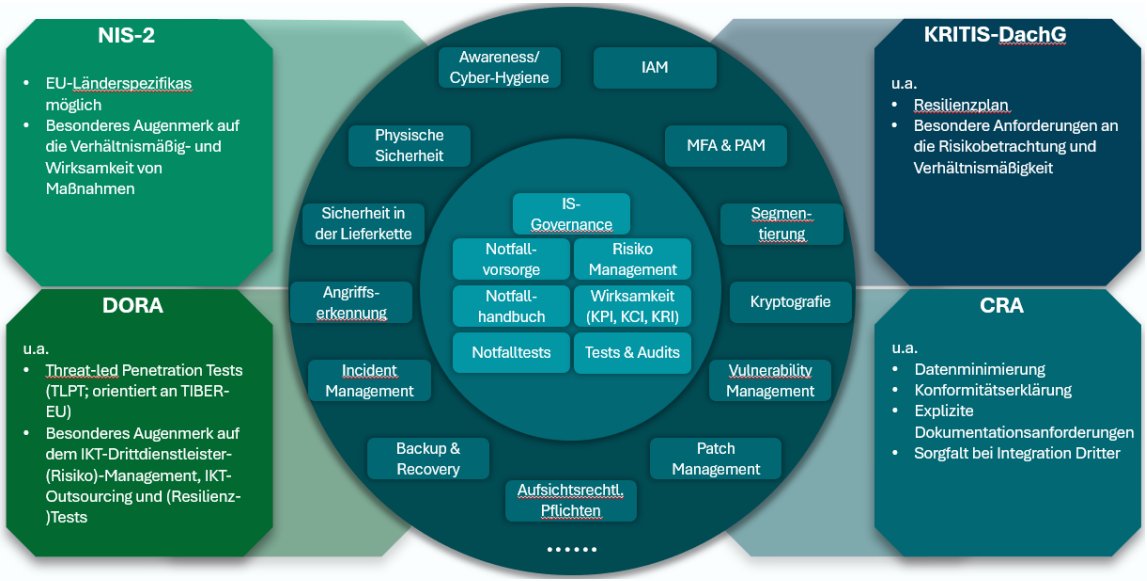
*16.09.2025, Hanau Congress Centrum*


# Immer mehr Standards & Regularien = immer mehr Lösungen?

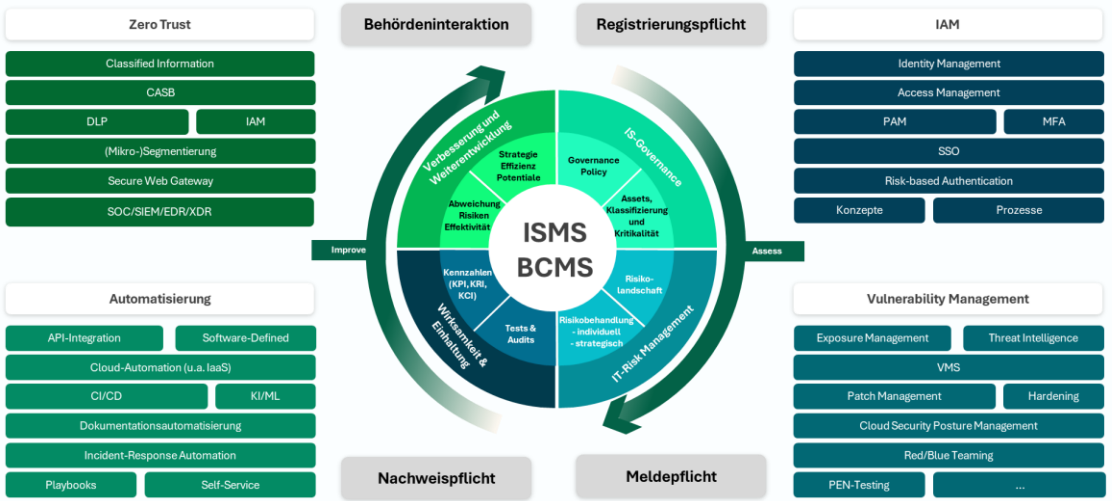
## Ein übergreifender Ansatz

Daniel Kammerbauer, Controlware GmbH, Team Lead – Governance, Risk & Compliance

# Navigation


NIS-2
EU-Länderspezifikas möglich
Besonderes Augenmerk auf die Verhältnismäßig- und Wirksamkeit von Maßnahmen
DORA
u.a.
Threat-led Penetration Tests (TLPT; orientiert an TIBER-EU)
Besonderes Augenmerk auf dem IKT-Drittdienstleister-(Risiko)-Management, IKT-Outsourcing und (Resilienz-)Tests
KRITIS-DachG
u.a.
Resilienzplan
Besondere Anforderungen an die Risikobetrachtung und Verhältnismäßigkeit
CRA
u.a.
Datenminimierung
Konformitätserklärung
Explizite Dokumentationsanforderungen
Sorgfalt bei Integration Dritter
Awareness/ Cyber-Hygiene
IAM
Physische Sicherheit
MFA & PAM
Sicherheit in der Lieferkette
Segmen-tierung
Angriffs-erkennung
Kryptografie
Incident Management
Vulnerability Management
Backup & Recovery
Patch Management
Aufsichtsrechtl. Pflichten
.....
IS-Governance
Notfall-vorsorge
Risiko Management
Notfall-handbuch
Wirksamkeit (KPI, KCI, KRI)
Notfalltests
Tests & Audits

# Ansätze, Lösungen & „Ausrüstung“



# Ansätze, Lösungen & „Ausrüstung“

controlware

Information Security

## Quick Check Informationssicherheit – nach ISO27001

Wir unterstützen Sie bei der zeit- und kosteneffizienten Feststellung Ihrer aktuellen Informationssicherheit gemäß den Anforderungen des internationalen Standards ISO 27001.

**Herausforderung**

Die Implementierung von Maßnahmen zur Informationssicherheit kostet Geld und trägt nicht direkt zum Geschäftserfolg bei. In wirtschaftlich unsicheren Zeiten sind es genau diese Kosten, die Unternehmen zuerst einsparen möchten. Langfristig sind Investitionslücken in der Informationssicherheit jedoch unverhältnismäßig teurer als die Ausgaben für Prävention.

**Ausgangslage**

Sie haben den Wunsch oder die konkrete Anforderung, sich hinsichtlich Informationssicherheit gut und belastbar aufzustellen. Dabei sind zunächst eine klare Vorstellung und ein ausreichendes Verständnis des angestrebten Ziels notwendig.

Will man sich hierbei an dem international anerkannten

controlware

Information Security

## Aufbau eines Managementsystems für Informationssicherheit (ISMS)

Systematisch – Zielgerichtet – Risikobasiert – Effizient – Verbessernd

**Herausforderung / Ausgangslage:**

Die Sicherheitslage ist branchenübergreifend angespannt. Die **Gefährdungslage** ist **hoch** und die Anzahl möglicher Bedrohungen nimmt weiter zu.

Ebenso wächst das Volumen und die Qualität der An-

**Beispiele für regulatorische Rahmen, Gesetze und Anforderungen:**

- DSGVO
- NIS2
- IT-Sicherheitsgesetz (UBI)

controlware

Information Security

## Quick-Check zur Feststellung der NIS2-Readiness

Wir unterstützen Sie bei der kompakten Feststellung des aktuellen Standes Ihrer Informationssicherheit gegenüber den Anforderungen der europäischen NIS2-Richtlinie und des nationalen NIS2-Umsetzungsgesetzes

**Herausforderung in der sich verändernden, Bedrohungs- und regulatorischen Landschaft**

Die Sicherheitslage ist branchenübergreifend angespannt. Die **Gefährdungslage** ist hoch, das Volumen und die Qualität der Angriffe, auf die Informationssicherheit von Unternehmen, nehmen stetig zu.

Ergänzend dazu kommt die Heterogenität des Informationssicherheitsniveaus über Sektoren und Staaten. Aufgrund dieser Situation hat die EU auf die NIS-Direktiven (2016) die **NIS2-Direktiven** (2022) veröffentlicht. EU-Direktiven greifen nicht unmittelbar in den Rechtsverkehr

eine Rechtsberatung erfolgen. Nach finaler Beantwortung der Frage „Bin ich von dem NIS2-Umsetzungsgesetz betroffen?“ ist der eigene Standort hinsichtlich der NIS2-Anforderungen zu bestimmen.

Hierbei stellen sich sofort zahlreiche Fragen:

- Gibt es einen machbaren und nachhaltigen Ansatz um mit den unzähligen regulatorischen, vertraglichen und weiteren Anforderungen an die Informationssicherheit umzugehen?
- Welche Konsequenzen drohen und welche Durchgriffsmöglichkeiten haben Behörden im Falle eines Verstoßes?

controlware

Information Security

## Externer Informationssicherheitsbeauftragter (eISB)

Unsere Berater für Informationssicherheit stehen Ihnen als externe Informationssicherheitsbeauftragte zur Verfügung und managen professionell und systematisch Ihre Informationssicherheit im Unternehmen. Dabei berücksichtigen wir die internen und externen Anforderungen Ihres Unternehmens zur Informationssicherheit sowie weitere Themen im Bereich Governance, Risikomanagement und Compliance.

**Welche Leistungen bieten wir?**

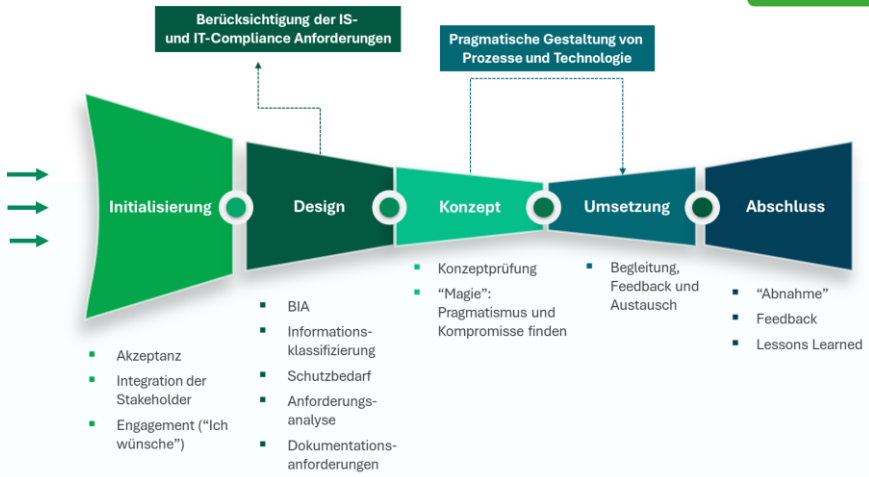
Mit der Einführung von **NIS2** und anderen **regulatorischen Vorgaben** rückt die Frage nach einem **Informationssicherheitsbeauftragten (ISB)** oder einem Verantwortlichen für die Informationssicherheit immer stär-

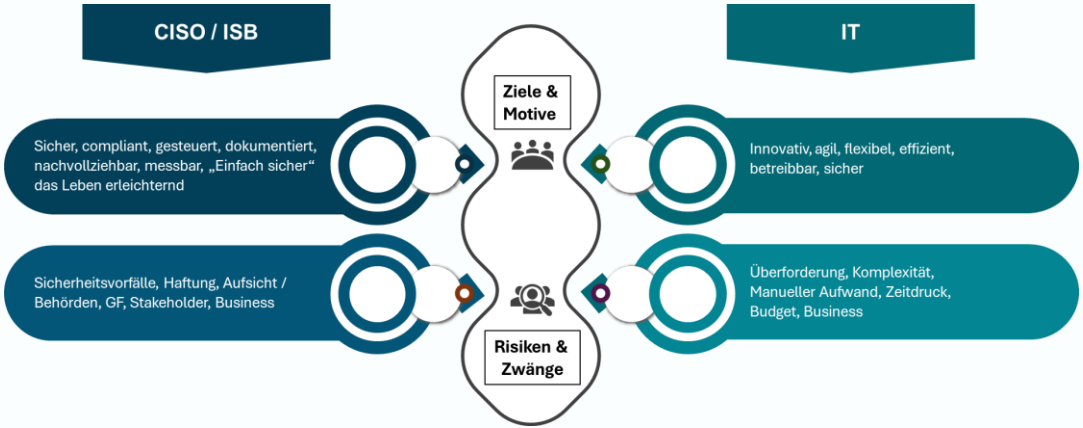
**Welche Vorteile bieten wir?**

Folgende Vorteile bietet ein externer ISB der Controlware:

- **Expertise und Erfahrung**

# Faktor „Mensch“




controlware

# Schluss mit Zettelwirtschaft & Fragebögen

Erfolgsrezepte für effiziente Compliance in Zeiten von NIS-2, DORA, etc.

Daniel Kammerbauer, Controlware GmbH
Team Lead Governance, Risk & Compliance

*16.09.2025, Hanau Congress Centrum*

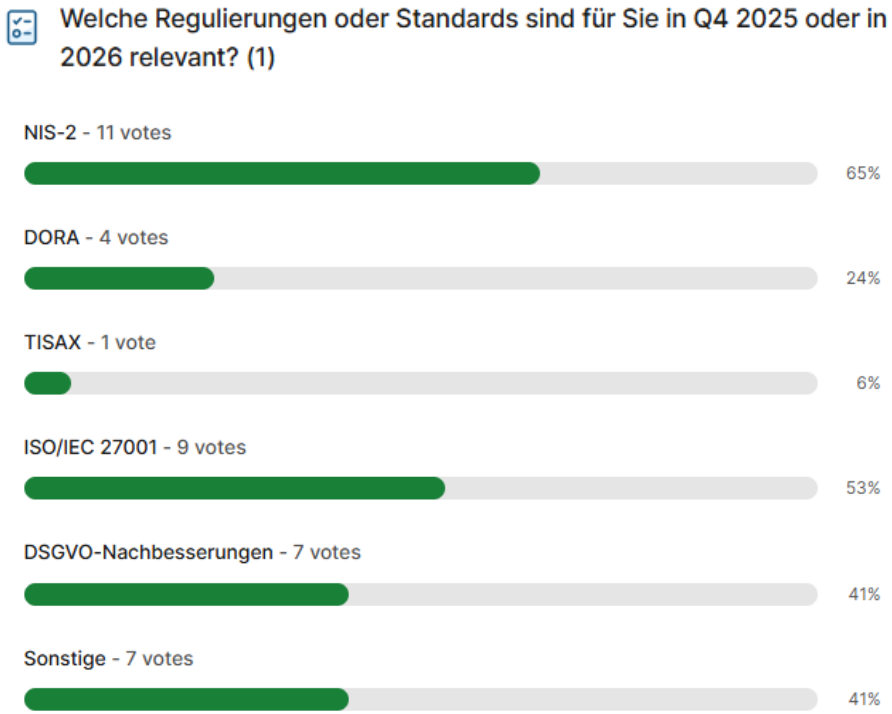
**Finden Sie sich wieder**
**oder**
**haben Sie das schon erlebt?**


**Ihre Stimme und Ihr Bild aus der Praxis**
**In 5 Minuten zu besserer Einschätzung und Antworten**

**Reality-Check:**
Wer von Ihnen hat sich gerade
ein wenig
in Martin wiedergefunden?

slido

# Welche Regulierungen oder Standards sind für Sie in Q4 2025 oder in 2026 relevant? (1)



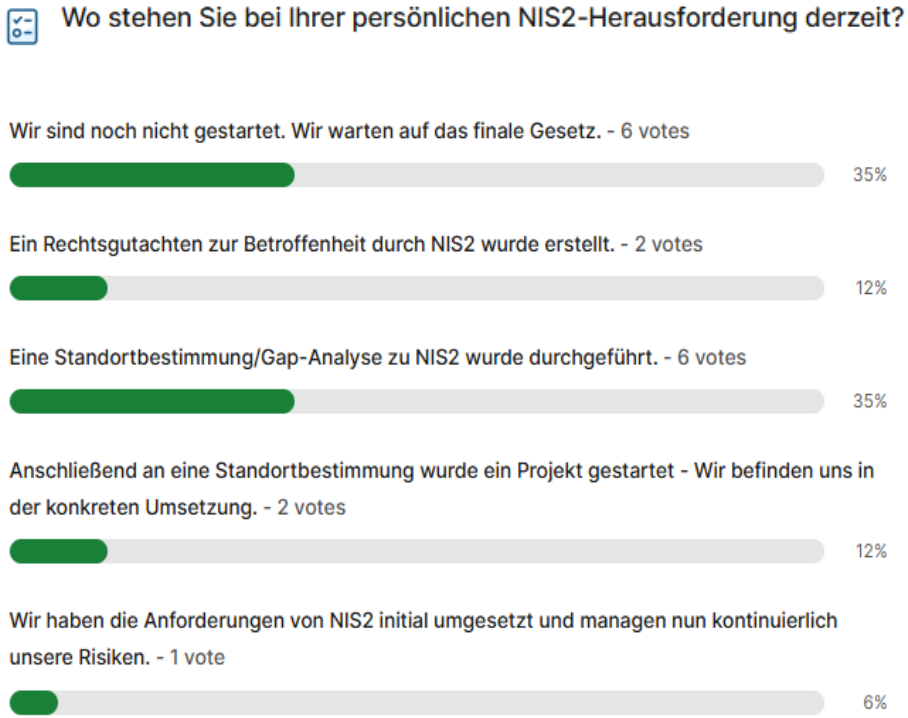
slido

# Welches Wort beschreibt Ihre NIS-2-Situation am treffendsten?

Welches Wort beschreibt Ihre NIS-2-Situation am treffendsten? (Tippen Sie das erste Wort ein, das Ihnen in den Kopf kommt - wir wollen ehrlich sein) (2)

slido

# Wo stehen Sie bei Ihrer persönlichen NIS2-Herausforderung derzeit?

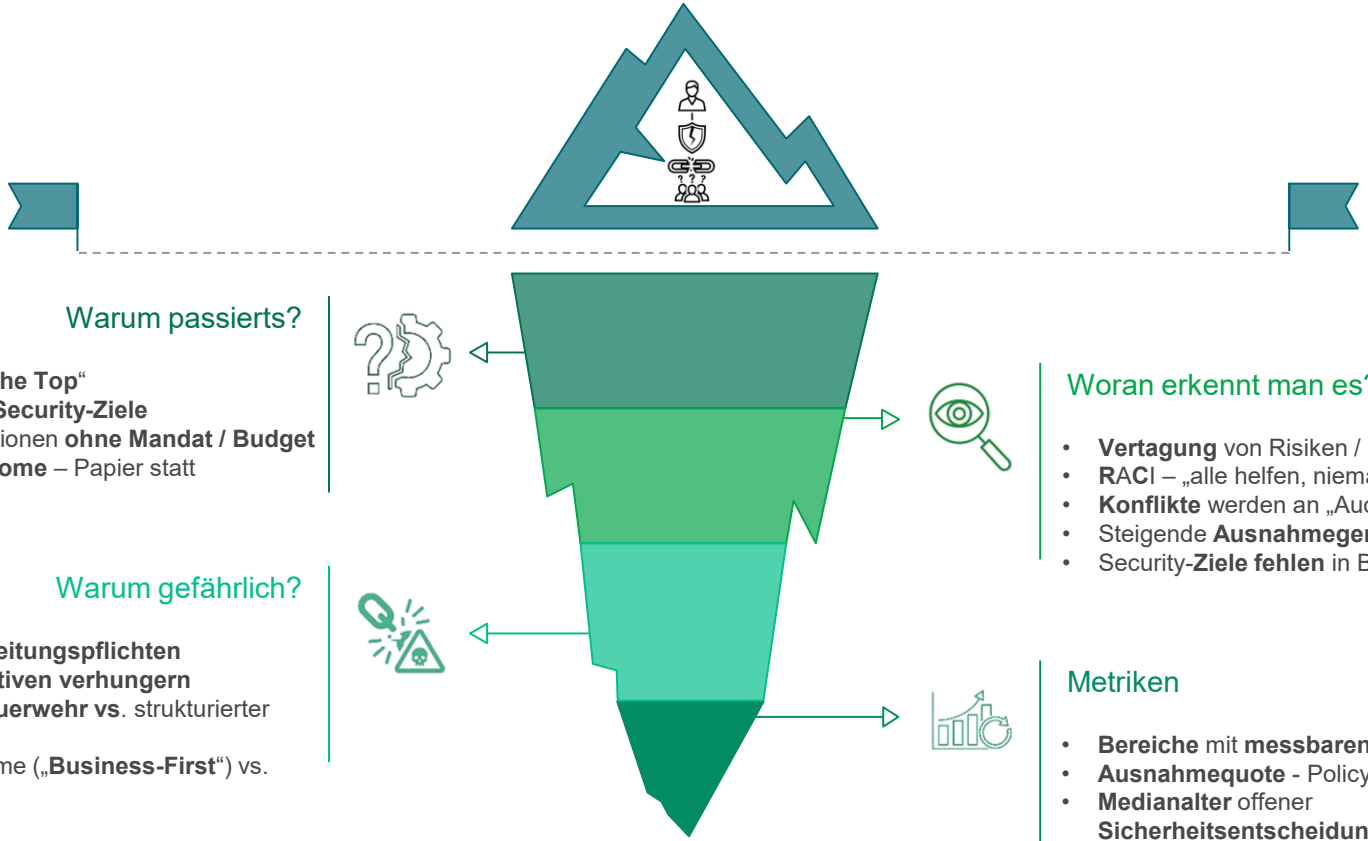


slido

# Was frisst bei Ihnen derzeit in der Umsetzung und Aufrechterhaltung von Anforderungen (z.B. TISAX, ISO, NIS-2) am meisten Zeit? (3)

# Typische Pain Point-Cluster aus der Praxis

# Fehlendes Management-Mandat & RACI-Diffusions-Dings



## Warum passierts?

- **Kein „Tone from the Top“**
- **Keine** etablierten **Security-Ziele**
- CISO/Risiko-Funktionen **ohne Mandat / Budget**
- **Output statt Outcome** – Papier statt Wirksamkeit

## Warum gefährlich?

- NIS-2 verschärft **Leitungspflichten**
- Strategische **Initiativen verhungern**
- Projekt- / Audit-**Feuerwehr vs**. strukturierter **Aufbau**
- Kultur der Ausnahme („**Business-First**“) vs. Kontrolldisziplin

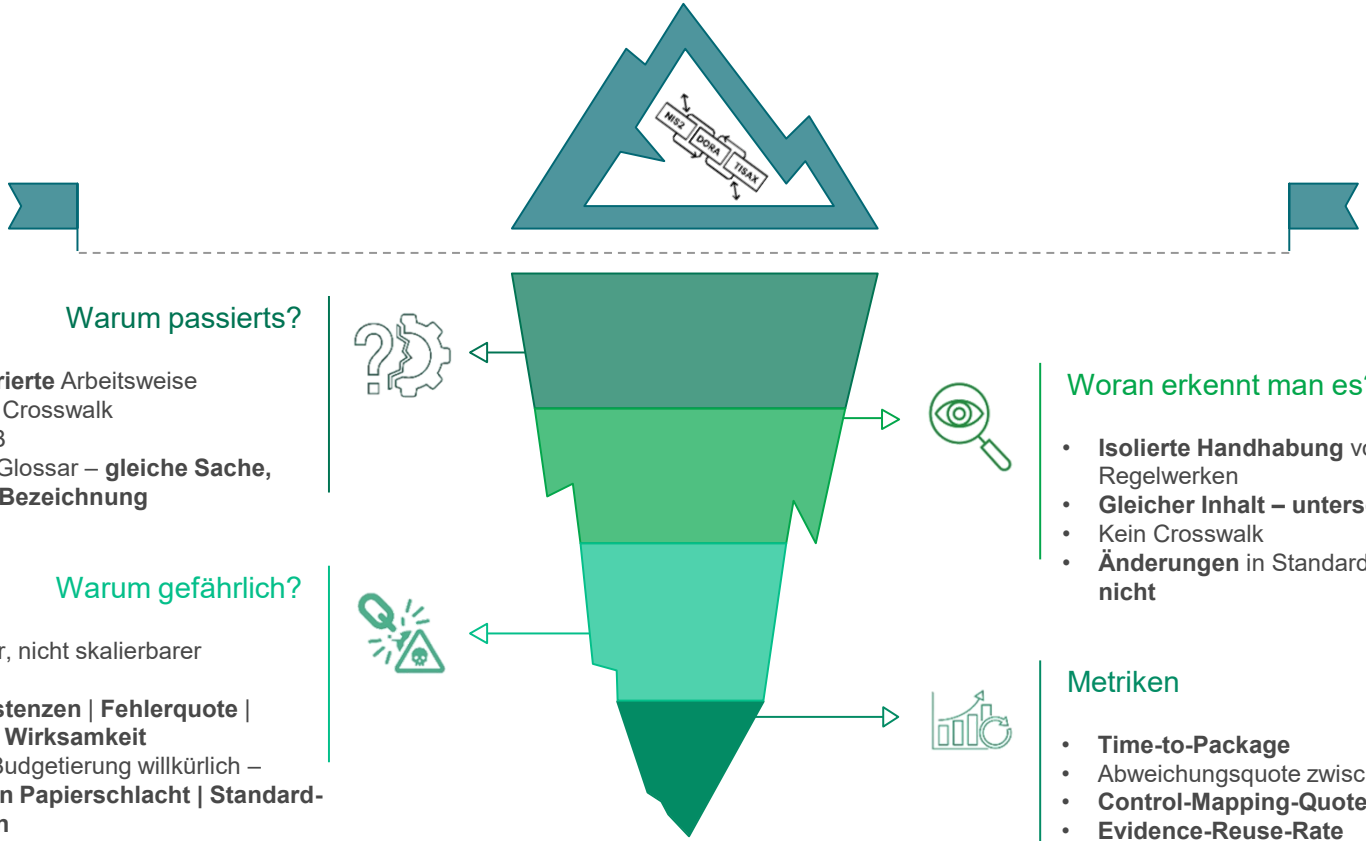
## Woran erkennt man es?

- **Vertagung** von Risiken / Invests
- **RACI** – „alle helfen, niemand verantwortlich“
- **Konflikte** werden an „Audit-Termine“ delegiert
- Steigende **Ausnahmegenehmigung**
- Security-**Ziele fehlen** in Bereichs-OKRs

## Metriken

- **Bereiche** mit **messbaren** Security-**Zielen** (OKR)
- **Ausnahmequote** - Policy-Ausnahmen / Anträge
- **Medianalter** offener **Sicherheitsentscheidungen**

# Orchestrierungsdefizit: Multi-Compliance-Hölle & Fragebögen-Drift




## Warum passierts?

- **Dokumentenzentrierte** Arbeitsweise
- **Kein SSOT** – kein Crosswalk
- Keine „Answer"-DB
- Kein kanonisches Glossar – **gleiche Sache, unterschiedliche Bezeichnung**

## Warum gefährlich?

- **Ineffizienz** – hoher, nicht skalierbarer Handarbeitsanteil
- Risiko für **Inkonsistenzen** | **Fehlerquote** | **Auditfragen nach Wirksamkeit**
- Priorisierung und Budgetierung willkürlich – **wahrgenommenen Papierschlacht | Standard-/Control-getrieben**

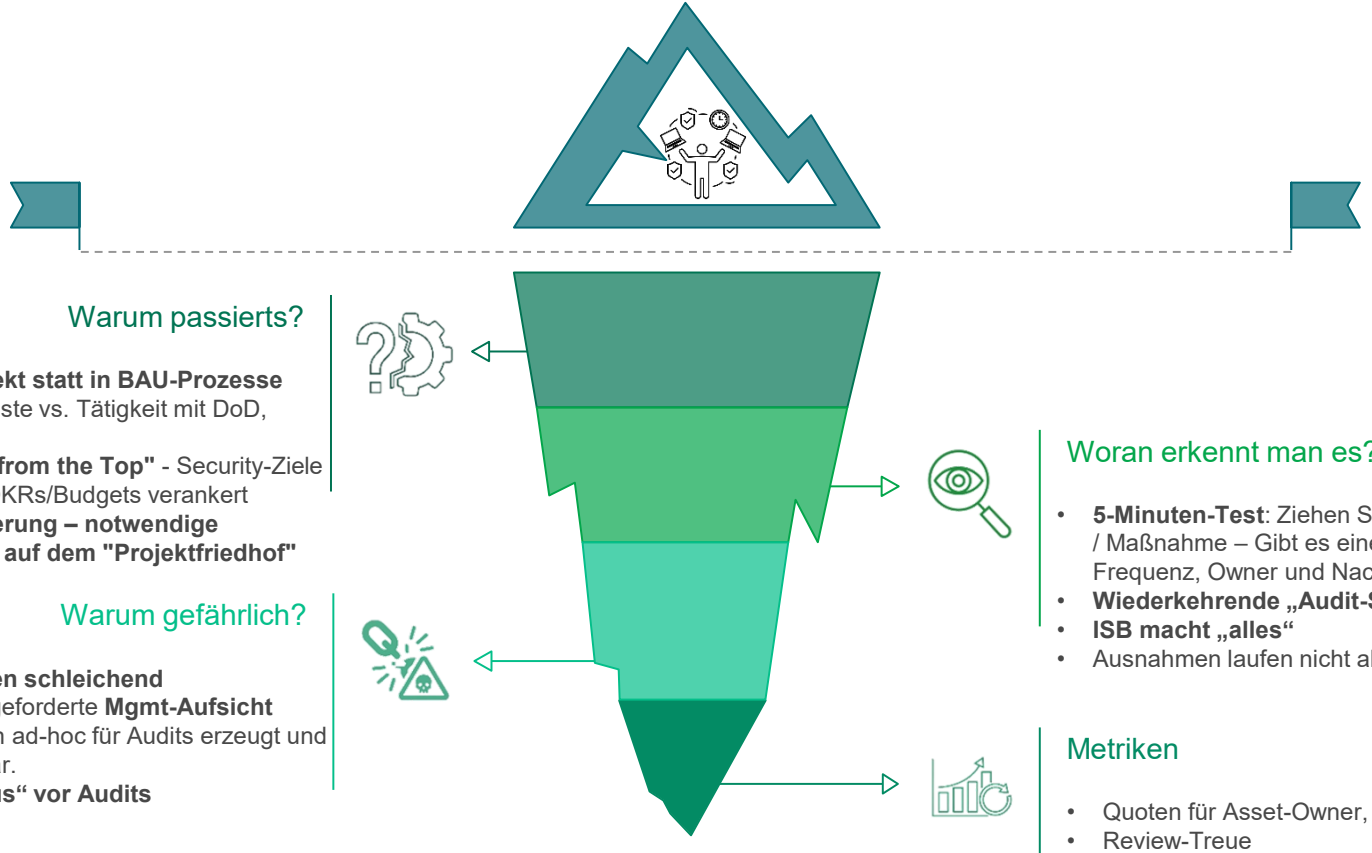
## Woran erkennt man es?

- **Isolierte Handhabung** von Standards & Regelwerken
- **Gleicher Inhalt – unterschiedliche Bezeichnung**
- Kein Crosswalk
- **Änderungen** in Standards oder Scope **skalieren nicht**

## Metriken

- **Time-to-Package**
- Abweichungsquote zwischen Antworten (je Std)
- **Control-Mapping-Quote**
- **Evidence-Reuse-Rate**

# Tagesgeschäft vs. Informationssicherheit – (undefined) Operating Model



## Warum passierts?

- **Security als Projekt statt in BAU-Prozesse integriert** (Checkliste vs. Tätigkeit mit DoD, Owner etc.)
- Kein klarer "**Tone from the Top**" - Security-Ziele sind nicht in den OKRs/Budgets verankert
- **fehlende Priorisierung – notwendige Vorhaben landen auf dem "Projektfriedhof"**

## Warum gefährlich?

- **Controls erodieren schleichend**
- Regulatorisch eingeforderte **Mgmt-Aufsicht**
- Nachweise werden ad-hoc für Audits erzeugt und sind nicht belastbar.
- **„Feuerwehrmodus“ vor Audits**
- Wissensinseln

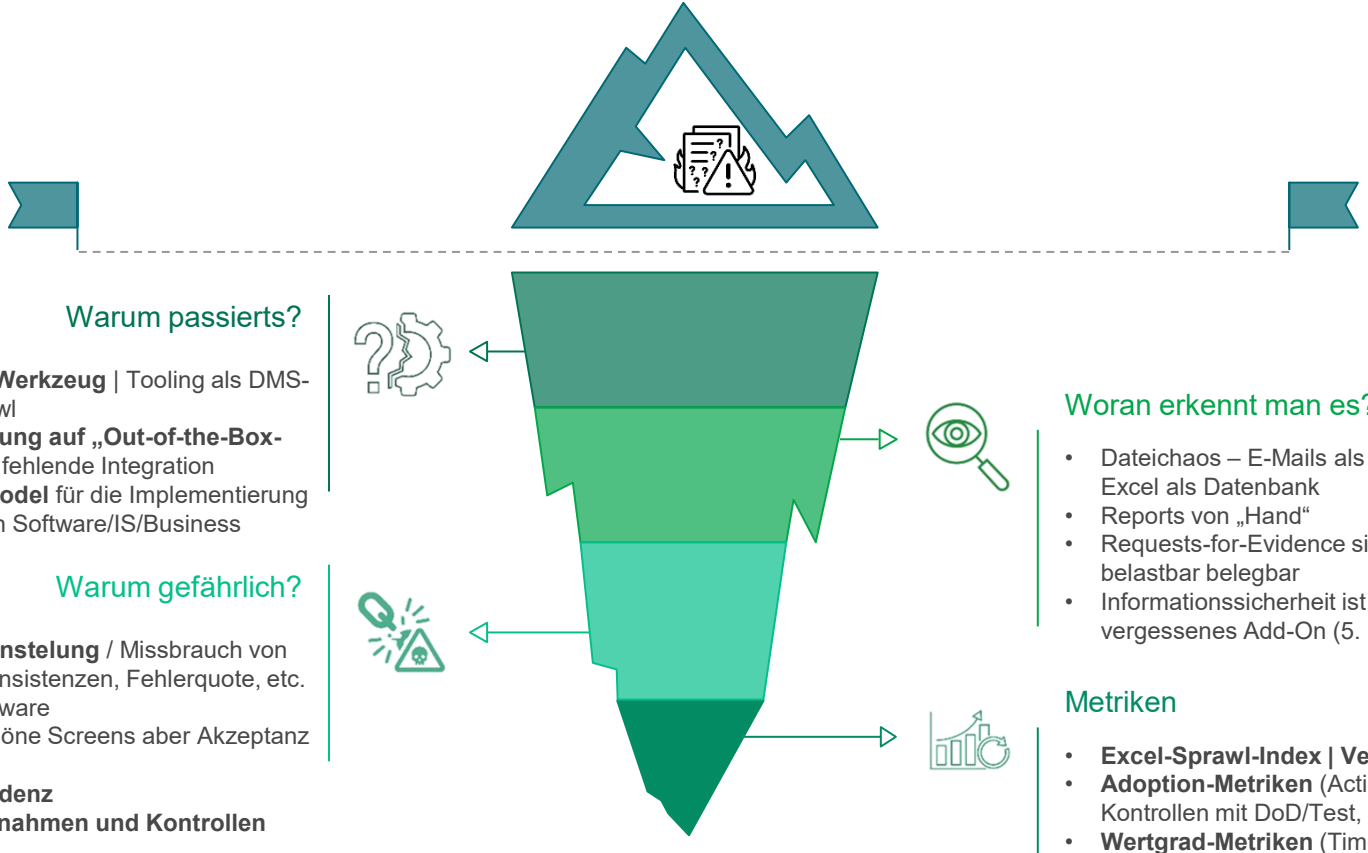
## Woran erkennt man es?

- **5-Minuten-Test**: Ziehen Sie eine zufällige Kontrolle / Maßnahme – Gibt es eine DoD mit Testmethode, Frequenz, Owner und Nachweis-Ort?
- **Wiederkehrende „Audit-Sprints“**
- **ISB macht „alles“**
- Ausnahmen laufen nicht ab und versanden

## Metriken

- Quoten für Asset-Owner, Control-Owner,
- Review-Treue
- **Quote für Kontrollen mit DoD**, Review, etc.
- **Anteil Ausnahmen mit Ablauf**

# (Null)Tooling als Selbstzweck



## Warum passierts?

- **Unzureichendes Werkzeug** | Tooling als DMS-Ersatz | Tool-Sprawl
- Kaufdruck – **Hoffnung auf „Out-of-the-Box-Compliance“** und fehlende Integration
- **Kein Operation Model** für die Implementierung und Integration von Software/IS/Business

## Warum gefährlich?

- **Ineffiziente Verkünstelung** / Missbrauch von Excel führt zu Inkonsistenzen, Fehlerquote, etc.
- **Neues Silo** | Shelfware
- **Bullshit-in…** - schöne Screens aber Akzeptanz bröckelt
- **Hohe Time-to-Evidenz**
- **Unwirksame Maßnahmen und Kontrollen**

## Woran erkennt man es?

- Dateichaos – E-Mails als Workflow-Engine – Excel als Datenbank
- Reports von „Hand“
- Requests-for-Evidence sind nicht kurzfristig und belastbar belegbar
- Informationssicherheit ist immer ein gern vergessenes Add-On (5. Rad am Wagen)

## Metriken

- **Excel-Sprawl-Index | Versionproliferation**
- **Adoption-Metriken** (Active-User-Rate, Kontrollen mit DoD/Test, gültige Evidenzen)
- **Wertgrad-Metriken** (Time-to-Evidence, Evidence-Reuse, Zeit für Auditvorbereitung, First-Pass)

# Rezepte, die sich bewährt haben (1)

## … und notwendig sind …

# Governance-Charter & Mandat

Von „Mach mal“ zur verankerten Unternehmensaufgabe:

Executive, Sponsorship, Rollen & Budget

Informationssicherheit wird als Geschäftsprozess geführt.

## Schritte

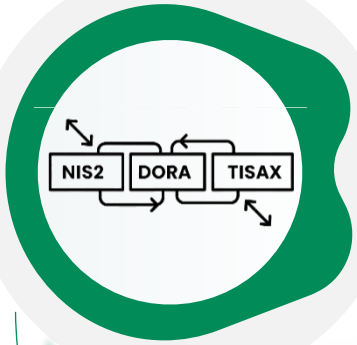
- ISMS-/NIS2-Governance-Charter erstellen
- Sponsor aus der Geschäftsführung bestellen
- Rollenprofile auf allen Ebenen schärfen
- RACI für Kernprozesse schärfen
- Kommunikationspaket veröffentlichen

## Was brauchts?

- Mgmt-Entscheidungsvorlage + Charter
- RAC-Matrix & Rollenprofile
- Schulungspaket

## KPIs

- Signed Charter
- 100% Kernfunktionen mit Zielen und Accountable
- Ausnahmequote




# Single Source of Truth & Multi-Compliance-Orchestrierung

Von der Zettelwirtschaft zur zentralen Steuerungsumgebung.

Ein System-of-Record statt Datei-Sprawl und Standards, Normen sowie Regularien als Overlay.

## Schritte

- Tool-Set auswählen & Operation Model definieren
- Kern-Control-Library definieren und Standards, Normen sowie Regularien anbinden/mappen
- Multi-Views
- Control-Design
- Top-25-Evidenzen priorisieren & designen
- Dashboards & KPIs aufsetzen

## Was brauchts?

- bestenfalls GRC-Plattform als SSOT
- Crosswalk-Matrix
- Control-Steckbriefe
- Workflows

## KPIs

- Control-Duplikate
- Time-to-Package für Standards
- Evidence-Reuse & Time-To-Evidence
- Evidence Freshness im Zielkorridor (z. B. Patch-Report < 30 Tage).

# Asset-To-Process Backbone & Risk Factory

Transparenz & Business-Fokus: kritische Prozesse sind mit Assets, Schutzbedarf, Risiken und Controls verknüpft – Risikoarbeit wird planbar, wiederholbar und auditfest

## Schritte

- Kritische Geschäftsprozesse bestimmen
- Prozess-Owner bestimmen
- Asset-Inventory konsolidieren, Prozessen zuordnen, Schutzbedarf/Owner definieren
- Einheitliche Risikomethodik
- “Risk-Factory”-Takt

## Was brauchts?

- Asset-Register
- Prozesslandkarte
- Risikomethodik
- Tooling-Unterstützung

## KPIs

- Assets mit Owner & Schutzbedarf
- Assets mit Risikobetrachtung
- Risiken mit Behandlungsplan
- Risk Acceptances mit Enddatum

# Lean Governance – RACI, Heartbeat, Exceptions

„Just enough – but always enforced“

Von Ad-Hoc zur fixen Kadenz: - von der Bremse zum Enabler. Feste Reviews, klare Zuständigkeiten, sauberes Ausnahme-Management, mehr Verbindlichkeit im Tagesgeschäft.

## Schritte

- Monatlicher 30-minütiger “Compliance-Heartbeat”
- ITSM/CAB: Security-Folgeabschätzung integriert in Prozessen
- Embedded Governance identifizieren und implementieren
- Exception-Workflow
- Playbooks für wiederkehrende Nachweise

## Was brauchts?

- Heartbeat-Agenda
- CAB-Integration & Exception-WF
- Pattern-Library
- Playbook-Vorlagen

## KPIs

- Review-On-Time-Rate
- Exceptions mit Enddatum
- Kritische Changes ohne Security-Abschätzung
- Risiko-Quote / Integrationsgrad Gov.


# KPI-Stack & Audit-Readiness-Factory

Von Fleißarbeit zu Outcome-Steuerung: managementtaugliche KPIs und planbare Audits. Keine Überraschungen, sondern Dry-Runs mit Evidenzpaketen aus der SSOT.

## Schritte

- KPI-Stack definieren (u.a. Coverage, Freshness, Remediation-SLAs, Exception-Burn-Down, Evidence-Automation)
- Pre-Audit-Check, Stichprobenliste, Interviewleitfäden, Evidenzpakete.
- Findings-Backlog mit Owner/Frist
- Management-Dashboards aufsetzen

## Was brauchts?

- KPI-Katalog
- Dashboards
- Audit-Playbooks
- Findings-Register

## KPIs

- >90% On-time-Reviews
- Time-to-Close (Major) < 30 Tage
- Zielerreichung > 80%.

# Nachweis-Automatisierung und Telemetrie

Wiederkehrende Evidenzen kommen automatisch, gestempelt und überwacht. Freshness und Abdeckung sind sichtbar. Ausreißer werden gejagt, nicht gesucht.

## Schritte

- Top-10 automatisierbare Evidenzen wählen
- Schnittstellen u. Intervalle definieren
- Evidenz-Metadaten pflegen
- Dashboards entwickeln (u.a. Coverage, Freshness) und monatlich im Heartbeat reviewen

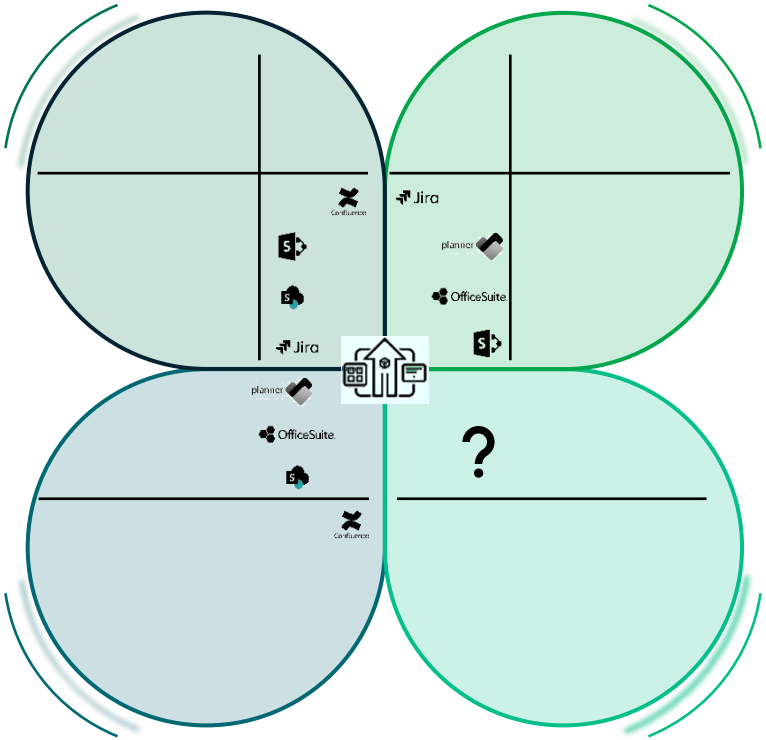
## Was brauchts?

- Evidence Data Dictionary
- Collector/Scheduler-Plan inkl. Template
- Dashboard für GRC

## KPIs

- >70% wiederkehrender Evidenzen automatisiert
- Freshness < 30 Tage für technische Controls

# “Nicht ganz unwesentlich” – die unterstützende Tool-Landschaft



**Schnell startklar, aber manuell und fragil**

**–**

**Gut für den Einstieg und im operativen Doing**

**–**

**Schwächen bei SSOT und Multi-Compliance**

# M365-Setup

- Zentrale Evidenzablage (Ordner/Bibliotheken)
- Nutzen von Metadaten (Quelle, Datum, Owner, Gültig bis)
- Multi-Compliance-Tagging
- Ordner je Themenbereich

- Wiki für Policies, Prozesse, Control-Steckbriefe sowie statische Inhalte
- Answer-Bank-Seiten/Abschnitte mit Evidenz-Links und Labels für Standards

- Heartbeat-Plan
- Buckets vgl. Boards in JIRA
- Fällige Evidenzen, Ausnahmen

planner

Abbildung mithilfe von Excel

- Statement of Applicability
- Crosswalk ISO–TISAX–NIS2 &
- KPI-Tracking

Abbildung mithilfe von Word

- Berichte, Protokolle, Policies

OfficeSuite

**Einheitlich in M365 und einfach in der Nutzung**

**–**

**Handarbeit und Schwächen im Tagesgeschäft**

**–**

**Schwächen bei SSOT und Multi-Compliance**


**Ein Control-Backbone, eine Evidenz, mehrere Sichten**

**–**

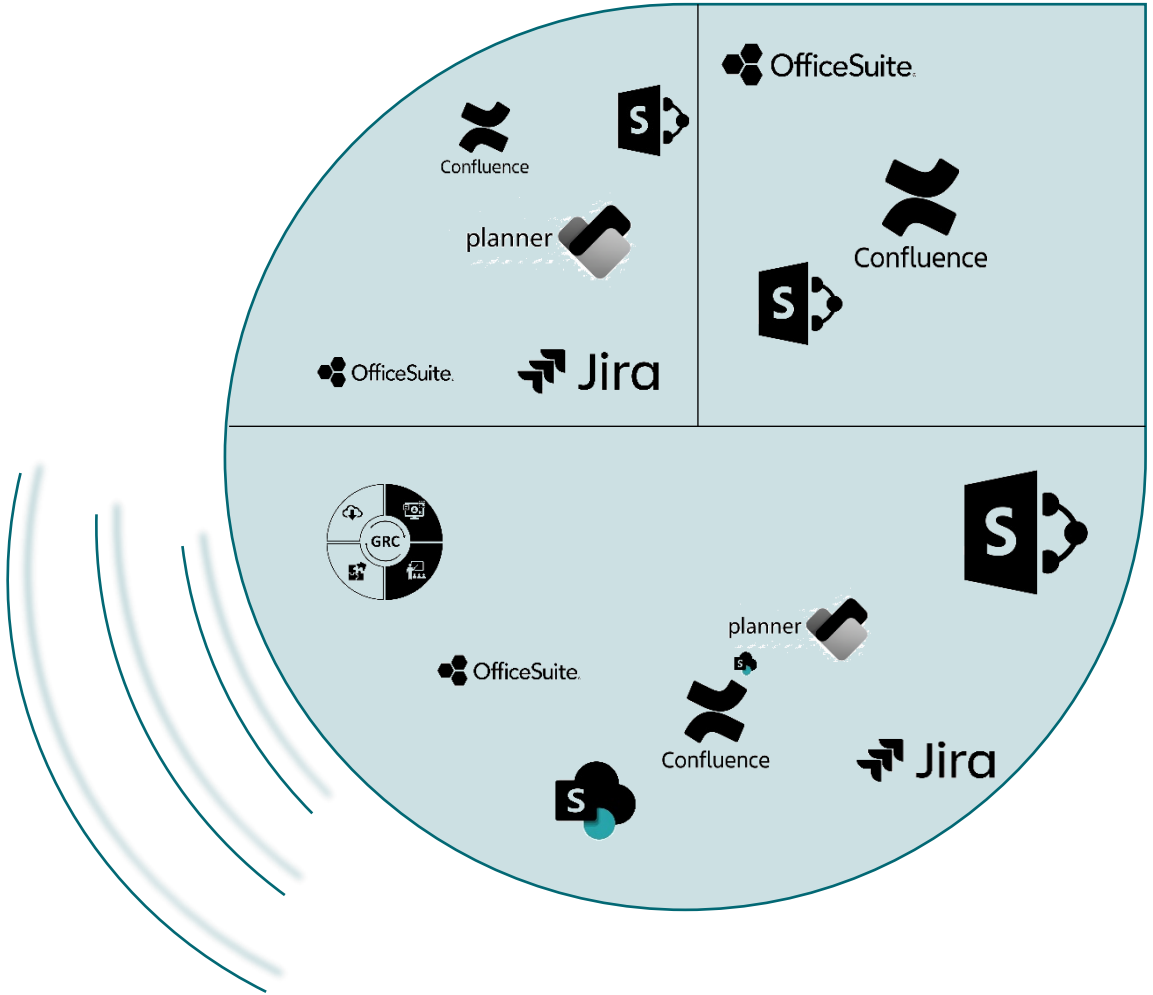
**effiziente Multi-Compliance**

**–**

**mit messbaren KPIs**

**und ‚auf Knopfdruck‘-Pakete**

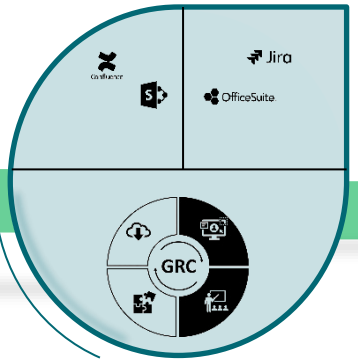
## Was ist ihr Operating Model und Ihre Tool-Landschaft?



# Martin 2.0

- Dokumentenchaos
- Fragebogen-Hölle
- Tagesgeschäft vs. IS-Sicherheit
- Multi-Framework-Drift

**Single Source of Truth für Controls & Evidencen**




„Let‘s make it simple and right!“

**Controlware**

**Governance, Risk & Compliance**

Starten Sie Ihren Weg aus dem Zettelchaos
Noch Fragen?
**Zögern Sie nicht, sprechen Sie uns an!**


Controlware
Security Day
2025
Danke für Ihre Aufmerksamkeit.
Wir freuen uns über Ihr Feedback!