Mit Projektmanagement-Tools ins Risikomanagement starten

Know-how to go: ISMS-Automatisierung – Agil. Sicher. Effizient.

HiSolutions AG

Robert Manuel Beck

Robert Manuel Beck

Principal

- Einführung und Auditierung von Informationssicherheitsmanagementsystemen (ISMS) nach ISO 27001 oder ISO 27001 auf Basis IT-Grundschutz
- Erstellung von Sicherheitskonzepten und Koordinierung der Umsetzung
- Erstellung von Richtlinien und Regelungen
- Beratung zum Risikomanagement und Durchführung von Risikoanalysen
- Durchführung von Workshops zu Informationssicherheitsthemen

---

- ISO 27001 Lead Auditor
- ISO 22301 Lead Auditor
- Auditor IT-Si.-Kat. nach EnWG 11 Abs. 1a und 1b
- Auditteamleiter für ISO-27001-Audits auf der Basis von IT-Grundschutz
- IS-Revisions- und -Beratungsexperte auf der Basis von IT-Grundschutz
- IT-Grundschutz-Berater
- Prüfverfahrenskompetenz nach § 8a BSIG

Agenda

- Das Dilemma
- Was will Risikomanagement?
- Ein möglicher Lösungsansatz
- Projektmanagement-Tools nutzen
- Jetzt loslegen…

Das Dilemma

Das Dilemma des Risikomanagements…

Zu detaillierte Risikoanalyse

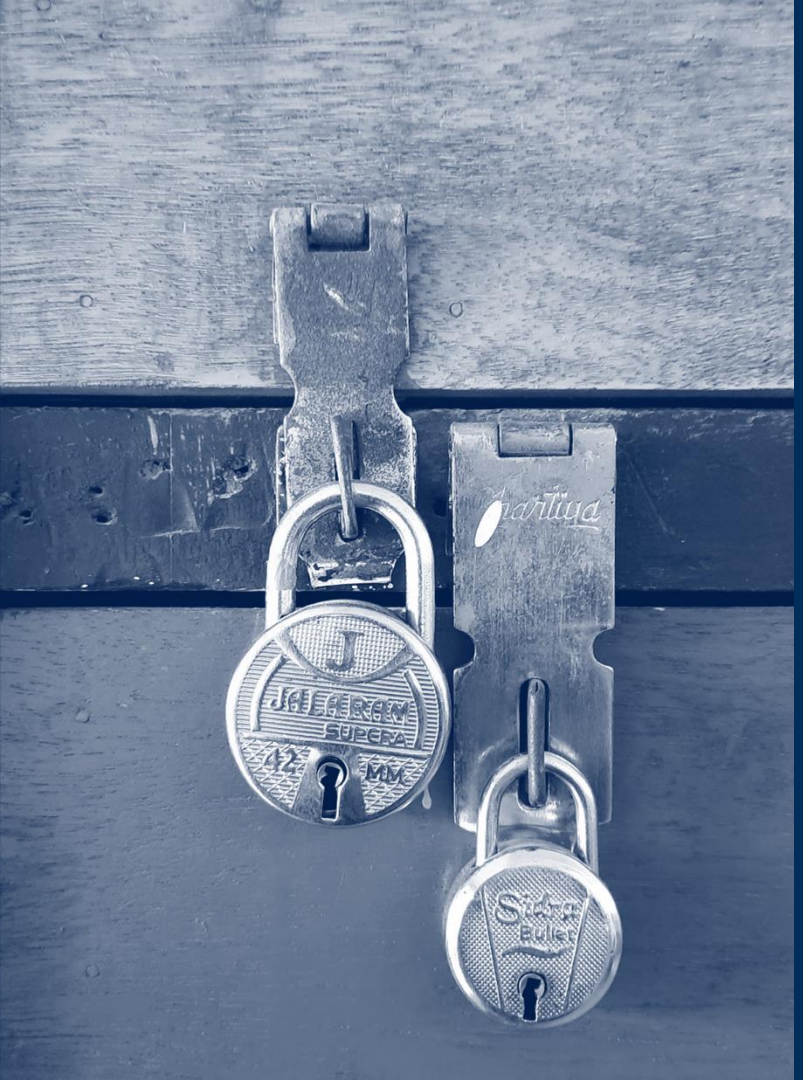
- Hoher Analyseaufwand,
- lange Dauer
- Maßnahmen werden spät wirksam
- Ergebnisse veralten schnell
- Scheingenauigkeit trotz Unsicherheit

Zu abstrakte Risikoanalyse

- Schnelle, aber grobe Bewertung
- Unspezifische, generische Maßnahmen
- Fehlende Priorisierung der Risiken
- Gefahr von Fehlinvestitionen/ Scheinsicherheit

„Analyse-Paralyse“ „Angemessener Detailierungsgrad“ „Blindflug“

Zwischen Gründlichkeit (Detailtiefe) und Pragmatismus (Umsetzbarkeit) muss ein angemessener Detailgrad gefunden werden.



GRC-Tools müssen erst etabliert werden.

- Tool-eigene Vorgehensweise etablieren
- Funktionale Integration
- Technische Integration
- Dauer bis zur Maßnahmenumsetzung

Anfangen und später wechseln.

Lösungsansatz: Standardmaßnahmenkatalog + Risikoanalyse

Standardmaßnahmenkatalog (Basis-Schutz)

- Sofort umsetzbar
- Deckt typische Grundrisiken ab
- Einheitlicher Mindeststandard

Risikoanalyse (kontinuierliche Verfeinerung)

- Identifikation besonderer Risiken
- Anpassung und Erweiterung des Katalogs
- Priorisierung der Umsetzung

Realisierung in Projektmanagement-Tools

Was will Risikomanagement?

Definition eines Risikos

Risiko

Auswirkung von Unsicherheit auf Ziele

ISO 31000:2018 – Kap. 3.1

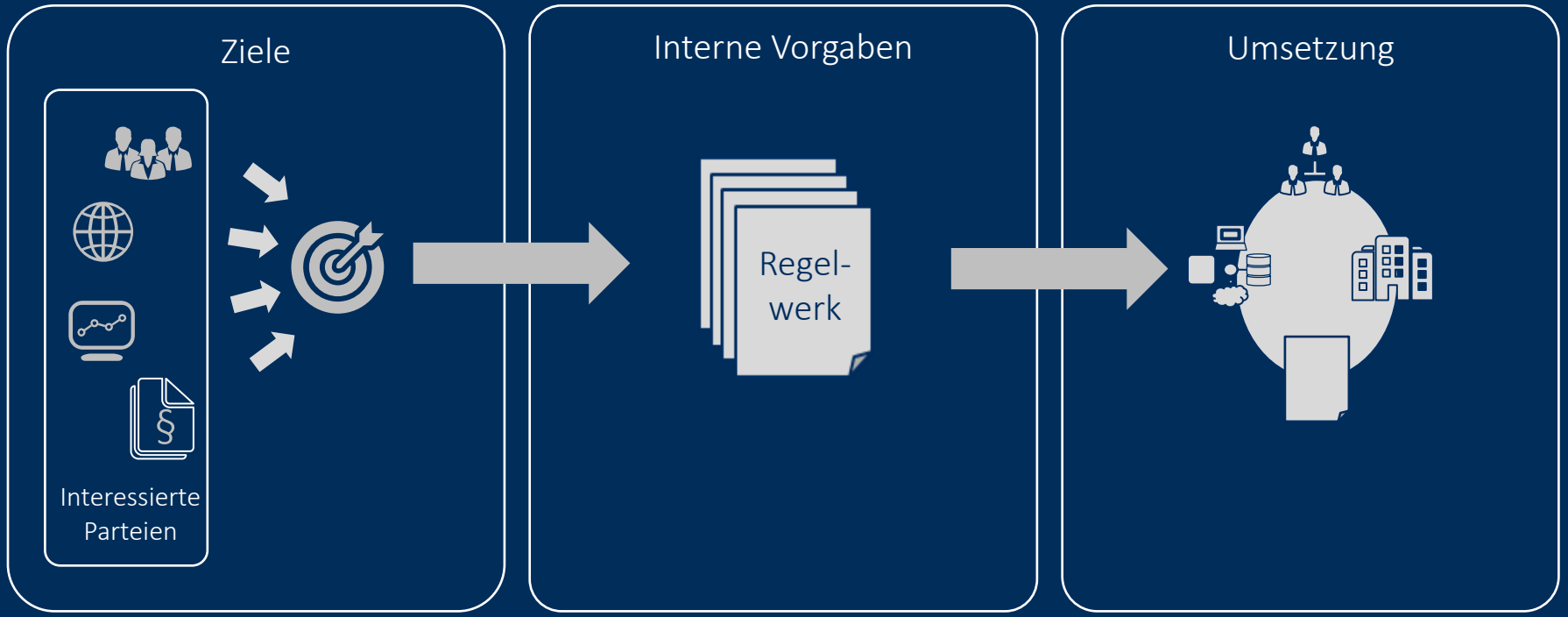
Risikomanagement hat insbesondere zwei Aufgaben

Übersicht der Zielgefährdungen

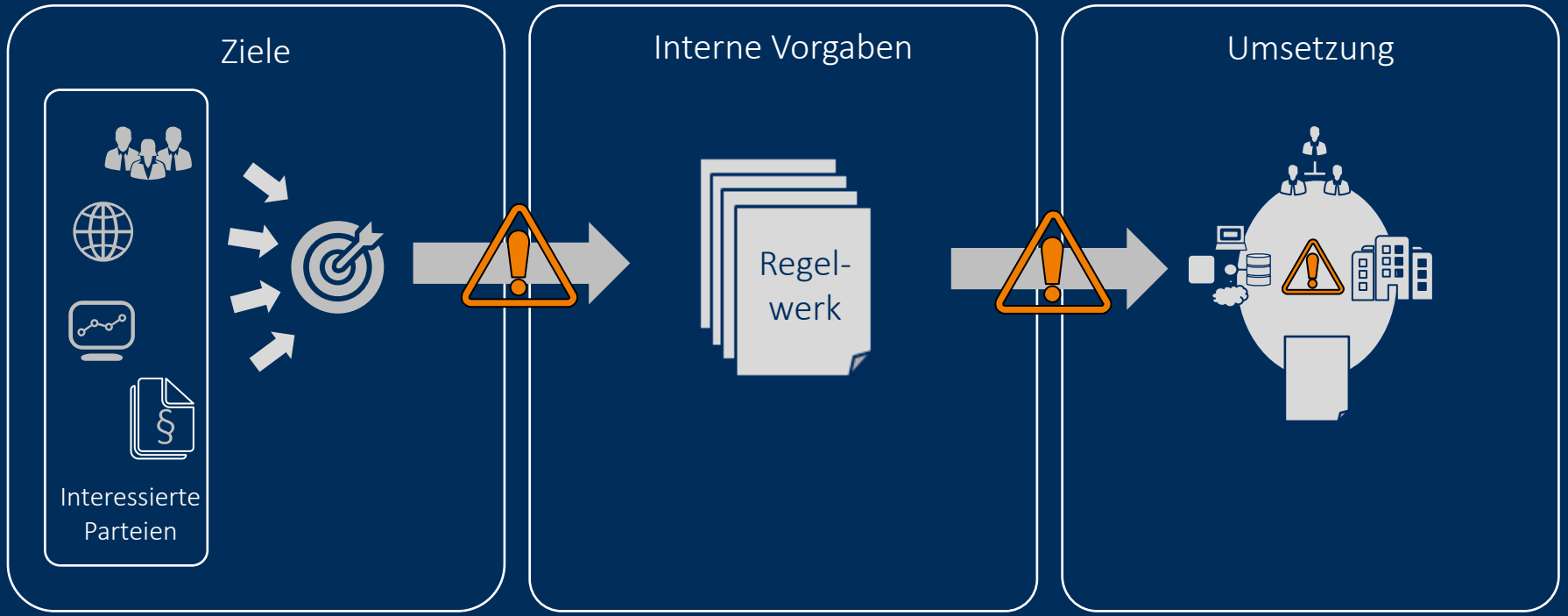
Priorisierung der Risikobehandlung

Ein möglicher Lösungsansatz

Ziele werden über interne Vorgaben umgesetzt.



Risiken entstehen am Pfad vom Ziel bis zur Umsetzung.



Ein mögliches Vorgehen…

Ein mögliches Vorgehen…

Regelwerk aufstellen... „Baselining“

ISO/IEC 27002:2022

CIS Controls

BSI IT-Grundschutzkompendium

CIS Benchmarks

OWASP ASVS

PCI DSS

OWASP Top 10

TISAX

BSI Grundschutz++-Kompendium

NIST SP 800-53

Das eigene Regelwerk sollte passen.

- Vollständigkeit
- Konsistenz
- Aktualität
- Angemessenheit
- Zielgruppenorientierung

Dann werden die Risiken identifiziert.

Drohende Zielabweichungen können anhand unterschiedlicher Quellen identifiziert werden.

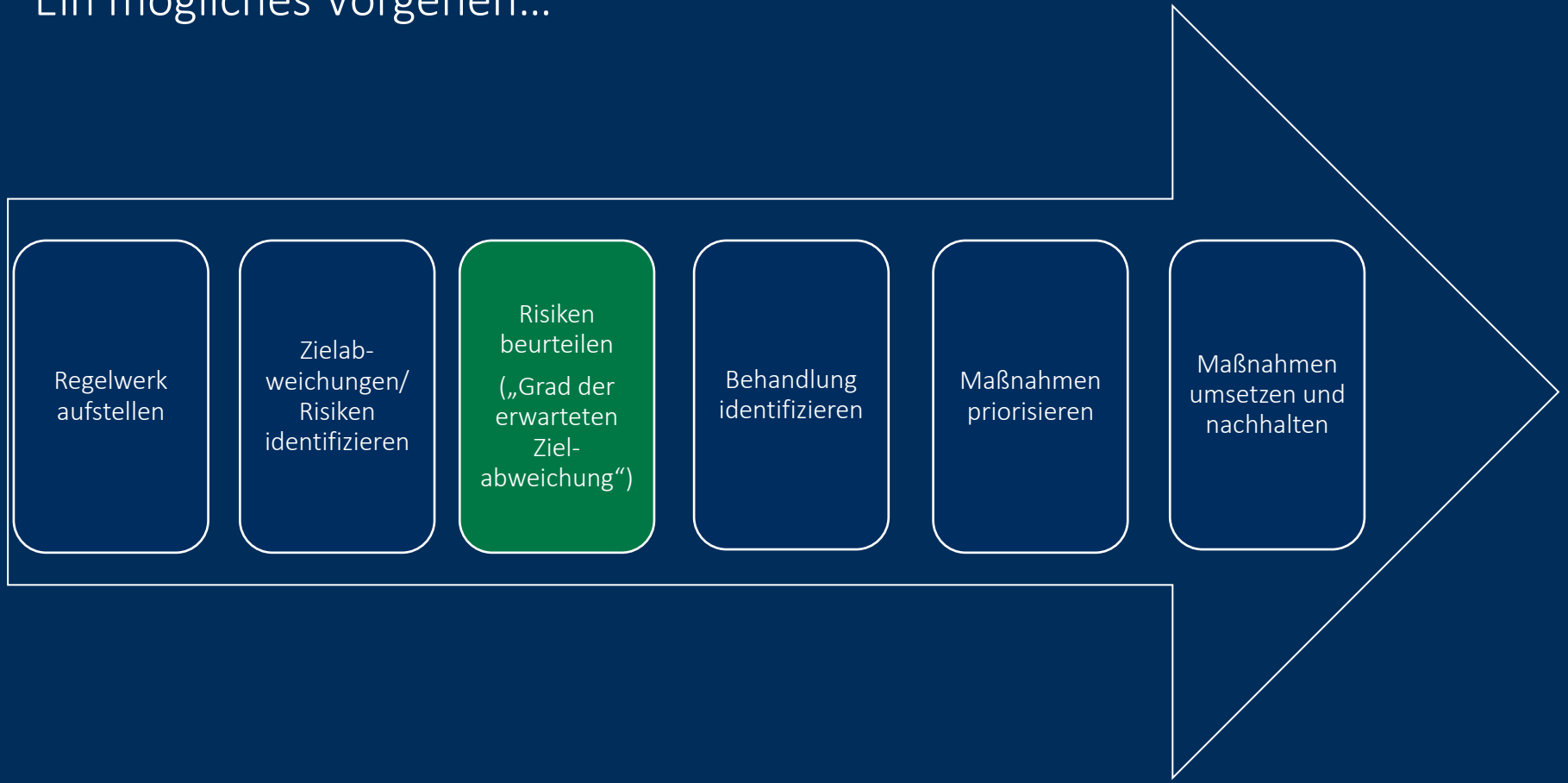
Externe Meldungen

Ergebnisse aus Ereignissen

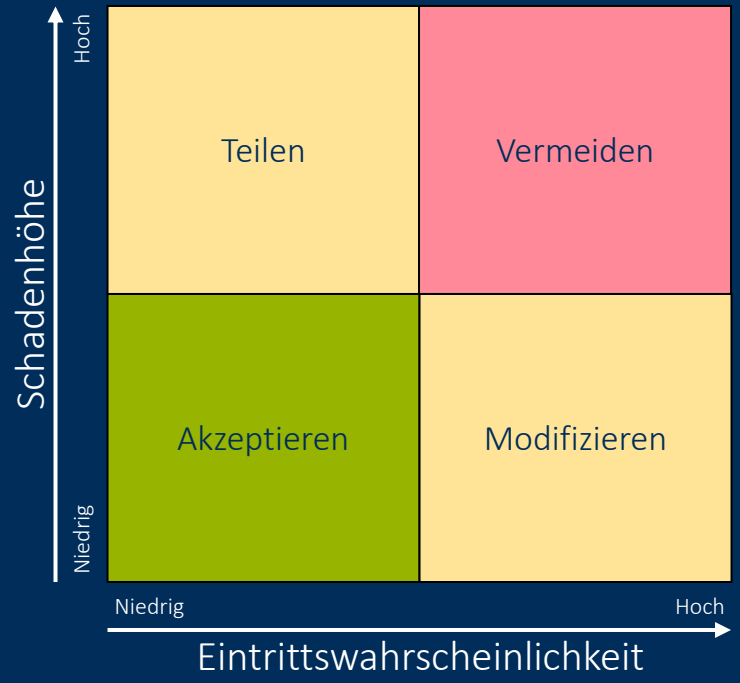
Interne Meldungen

Ergebnisse aus Audits & Tests

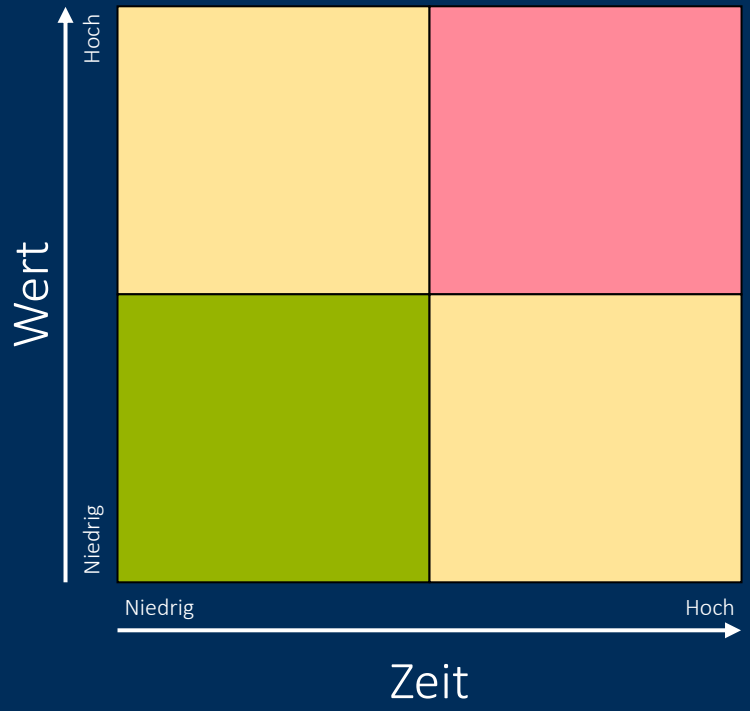
Ein mögliches Vorgehen…

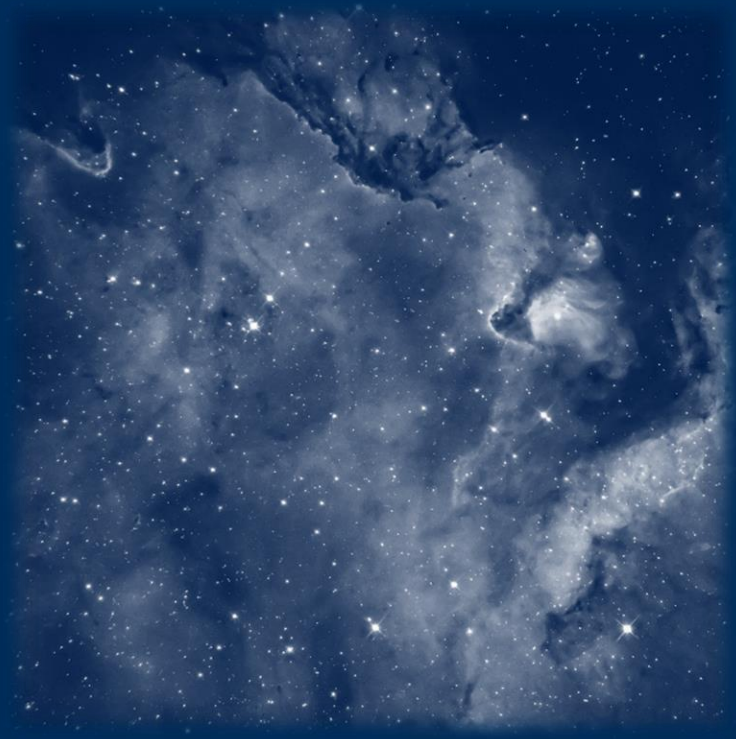


Risikobeurteilungen erfolgen meist nach Eintrittswahrscheinlichkeit und Schadenshöhe.

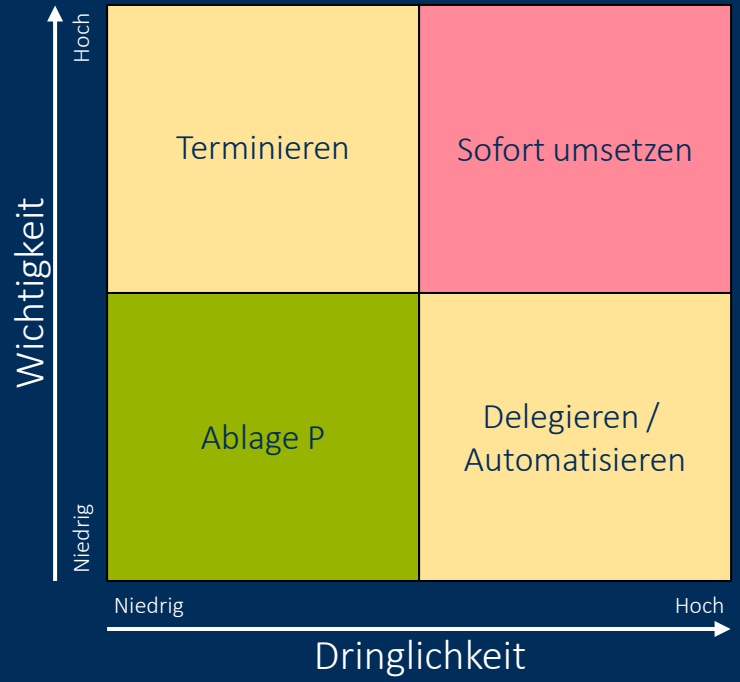


Es gibt eine zeit- und eine wertorientierte Dimension.

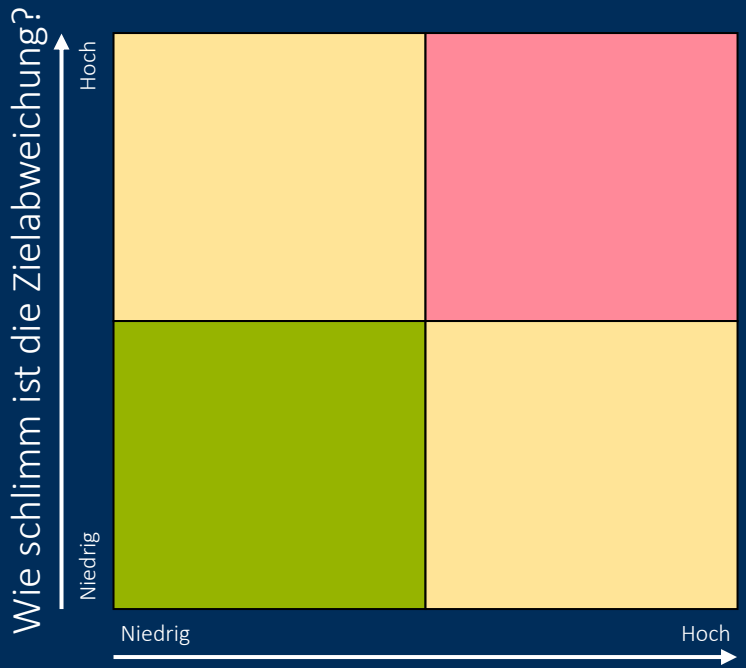




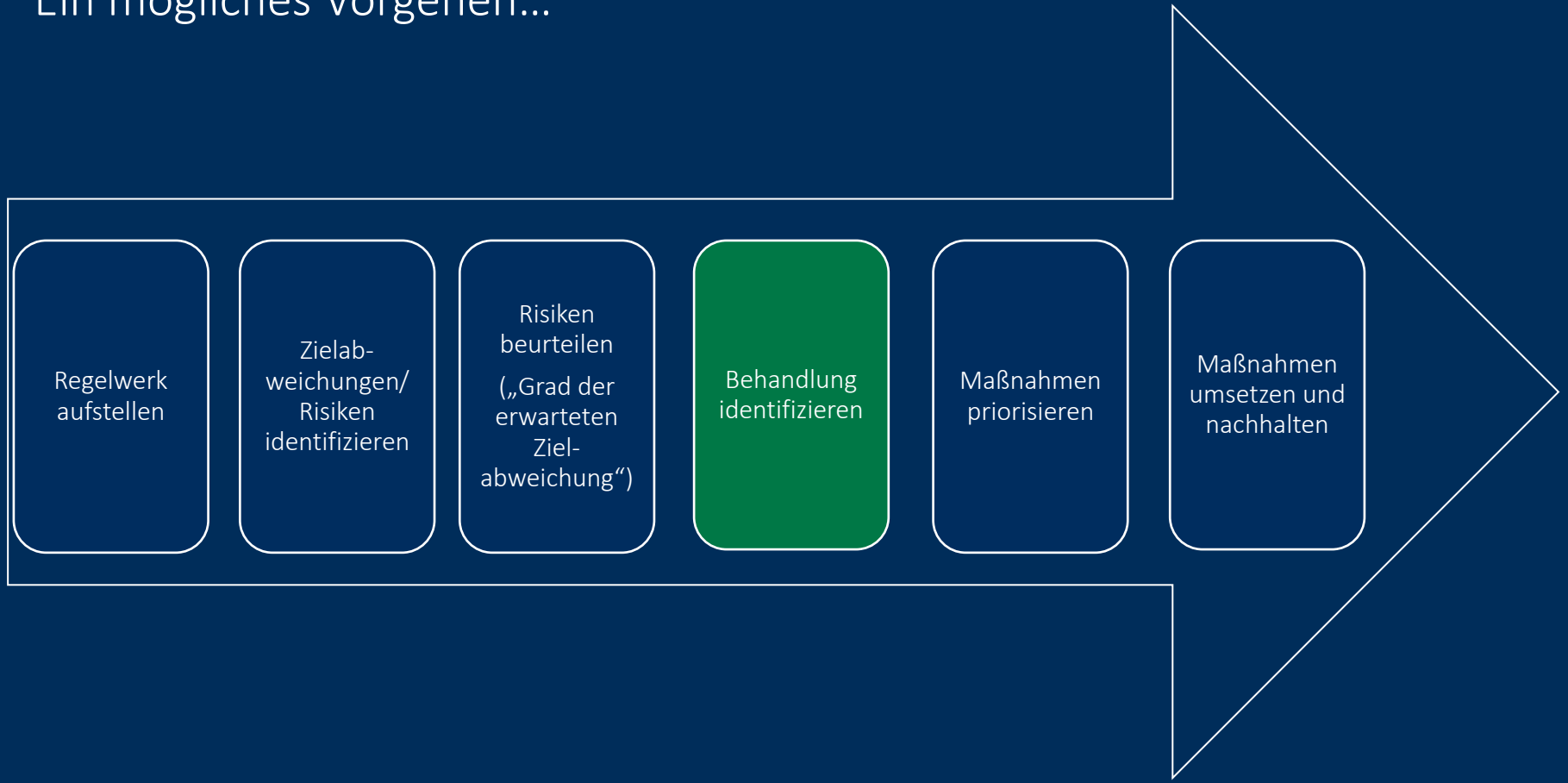
Diese Kombination wird auch in der Eisenhower-Matrix genutzt.



Die Eisenhower-Matrix könnte also adaptiert werden…



Ein mögliches Vorgehen…



Bei der Identifikation von Sicherheitsmaßnahmen darf man kreativ sein.

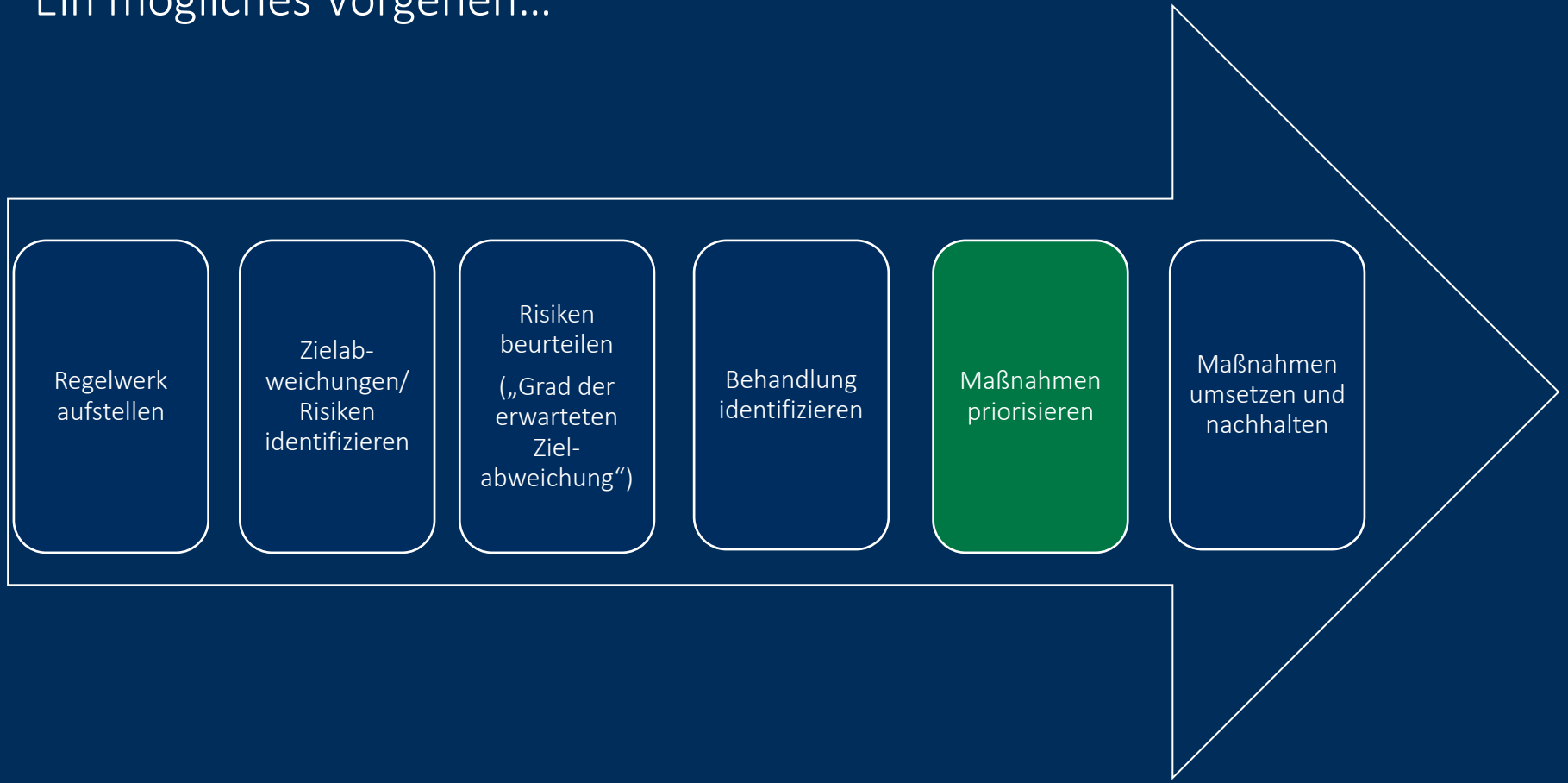
Ursachen analysieren

Best Practices nutzen

Brainstorming durchführen

o o o

Ein mögliches Vorgehen…



Für die Priorisierung gibt es unterschiedliche Herangehensweisen.

Die kritischste Lücke zuerst

Die leichteste Behandlung zuerst

Die Maßnahmen mit dem größten Effekt zuerst

Ein mögliches Vorgehen…

Die entstanden Aufgaben müssen umgesetzt und nachverfolgt werden.

Projektmanagement-Tools nutzen

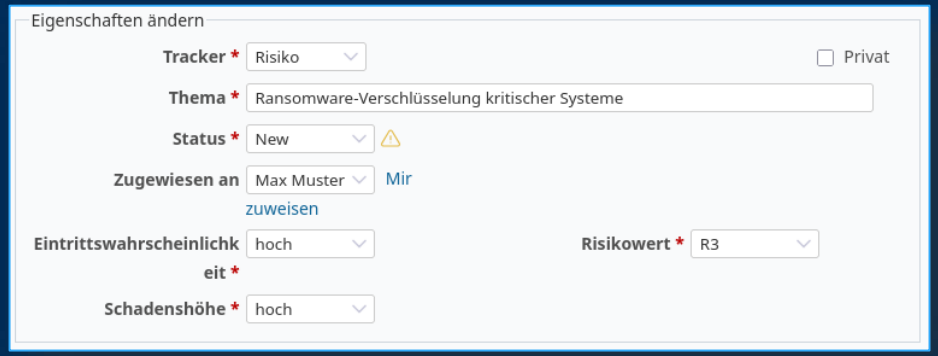
Projektmanagement-Tools können für das Risikomanagement verwendet werden.

- Alles an einem Ort
- Hohe Nutzerakzeptanz
- Automatisierte Workflows & Erinnerungen
- Schnelle & aussagefähige Reports
- Geringer Aufwand

Jedes Risiko wird ein Ticket.

1. Risikobeschreibung
2. Risikostufe (Priorität)
3. Eintrittswahrscheinlichkeit
4. Schadenhöhe
5. Maßnahmen (ggf. als Sub-Tickets)
6. Risikoeigentümer (Verantwortlicher)
7. Status
8. Fälligkeitsdatum
9. …

Beispiel „Redmine“:



Aus den Tools können aussagekräftige Risikoberichte erstellt werden.

Offene Tasks

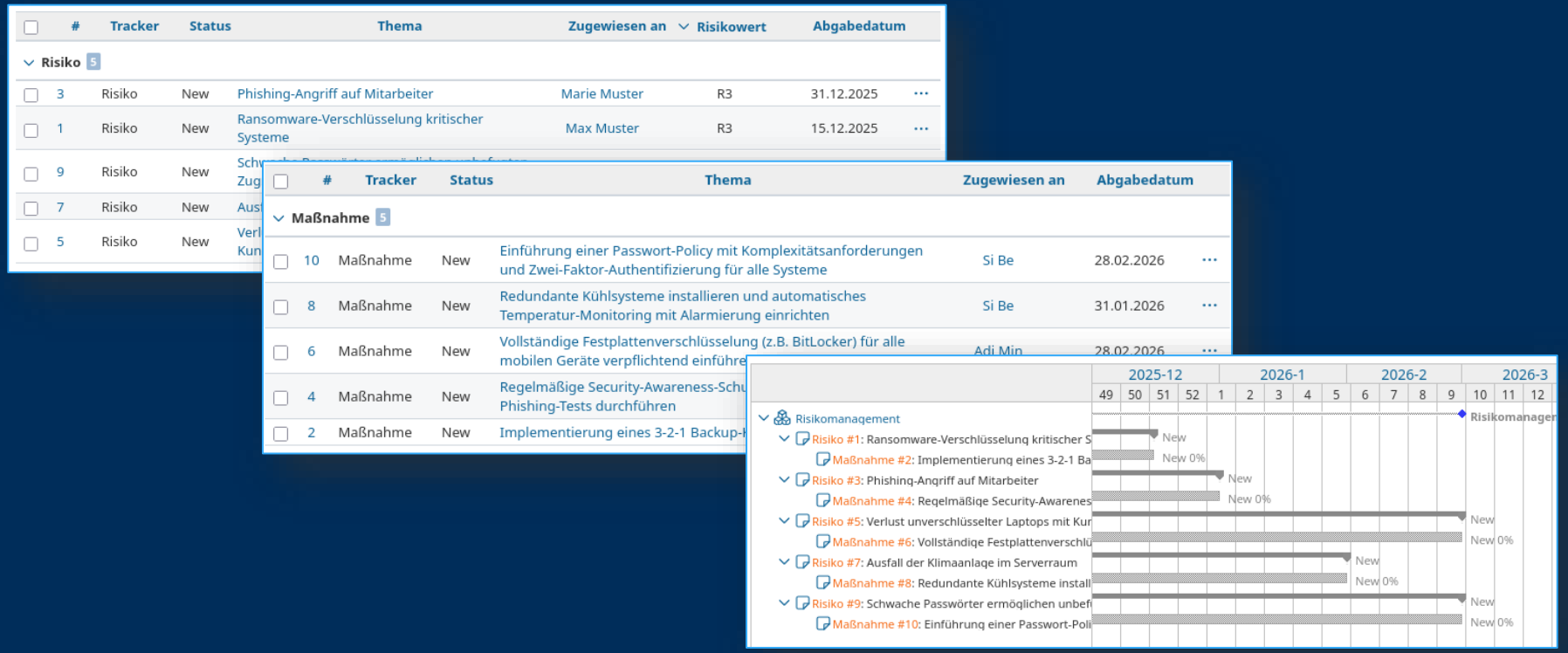
Geschlossene Tasks

Burn-Down-Charts

Prioritäten

Zeithorizonte

Im Beispiel „Redmine“ gibt es entsprechende Auswertungen.



#	Tracker	Status	Thema	Zugewiesen an	Risikowert	Abgabedatum
Risiko 5						
3	Risiko	New	Phishing-Angriff auf Mitarbeiter	Marie Muster	R3	31.12.2025
1	Risiko	New	Ransomware-Verschlüsselung kritischer Systeme	Max Muster	R3	15.12.2025
9	Risiko	New	Schwache Passwörter ermöglichen unbefugten Zug			
7	Risiko	New	Aust			
5	Risiko	New	Verl Kun			

#	Tracker	Status	Thema	Zugewiesen an	Abgabedatum
Maßnahme 5					
10	Maßnahme	New	Einführung einer Passwort-Policy mit Komplexitätsanforderungen und Zwei-Faktor-Authentifizierung für alle Systeme	Si Be	28.02.2026
8	Maßnahme	New	Redundante Kühlsysteme installieren und automatisches Temperatur-Monitoring mit Alarmierung einrichten	Si Be	31.01.2026
6	Maßnahme	New	Vollständige Festplattenverschlüsselung (z.B. BitLocker) für alle mobilen Geräte verpflichtend einführe	Adi Min	28.02.2026
4	Maßnahme	New	Regelmäßige Security-Awareness-Schu Phishing-Tests durchführen		
2	Maßnahme	New	Implementierung eines 3-2-1 Backup-K		

Jetzt loslegen…

Erstmal nutzen, was bereits da ist.

Risikomanagement kann schnell…

- …integriert werden.
- …wirksam werden.

Projektmanagement-Tools sind oft schon da:

- Schnell nutzbar
- Eigene Methoden = mehr Awareness

Migration zu einem „echten“ GRC-Tool später möglich.

HISOLUTIONS

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com