



schleupen

creating confidence





Automatisierungsmöglichkeiten im Information Risk Management Prozess

Risk Management Congress, 08. / 09. Mai 2023



Agenda

1. Vorstellung
2. Automatisierungsmöglichkeiten
3. Zusammenfassung
4. Diskussion & Fragen



Referent

Tobias Schöffel

Bereichsleiter Markt

Schleupen SE, Ettlingen

Deutschland





Who we are.

Schleupen SE

Gründung 1970
durch Leo Schleupen



Umsatz 2022
72,5 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 1.000 Kundenprojekte





Unsere Kompetenzen im Überblick

Lösungen aus einer Hand



RISIKO
MANAGEMENT



MELDE- UND
HINWEISGEBER-
SYSTEM



LIEFERKETTEN-
SORGFALTPFLICHTEN
- GESETZ **NEU**



BUSINESS CONTINUITY
MANAGEMENT (BCM)



RICHTLINIEN
MANAGEMENT



TAX
COMPLIANCE



COMPLIANCE
MANAGEMENT



FRAGEBÖGEN



DATENSCHUTZ



INTERNES
KONTROLLSYSTEM



SCHADEN
MANAGEMENT



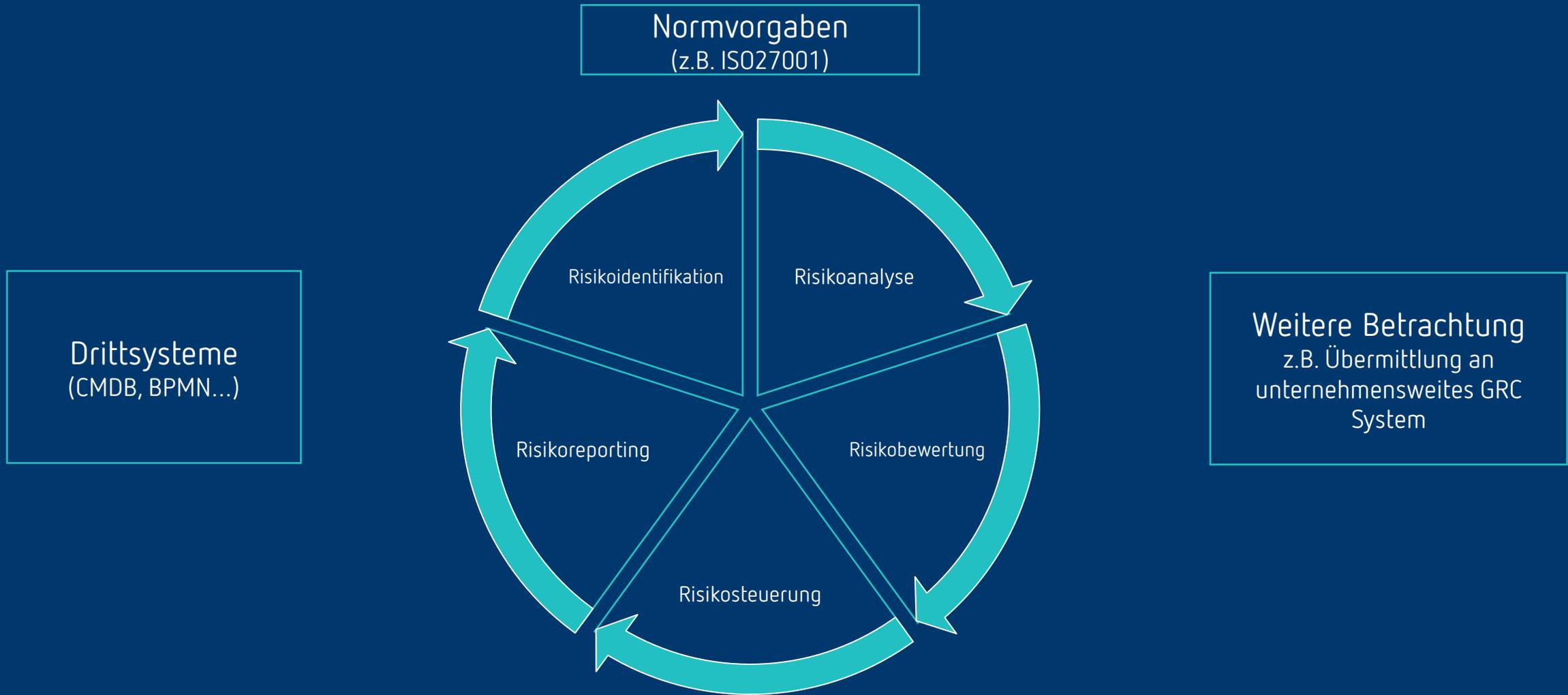
ISMS



Automatisierungsmöglichkeiten im Überblick



Ausgangslage



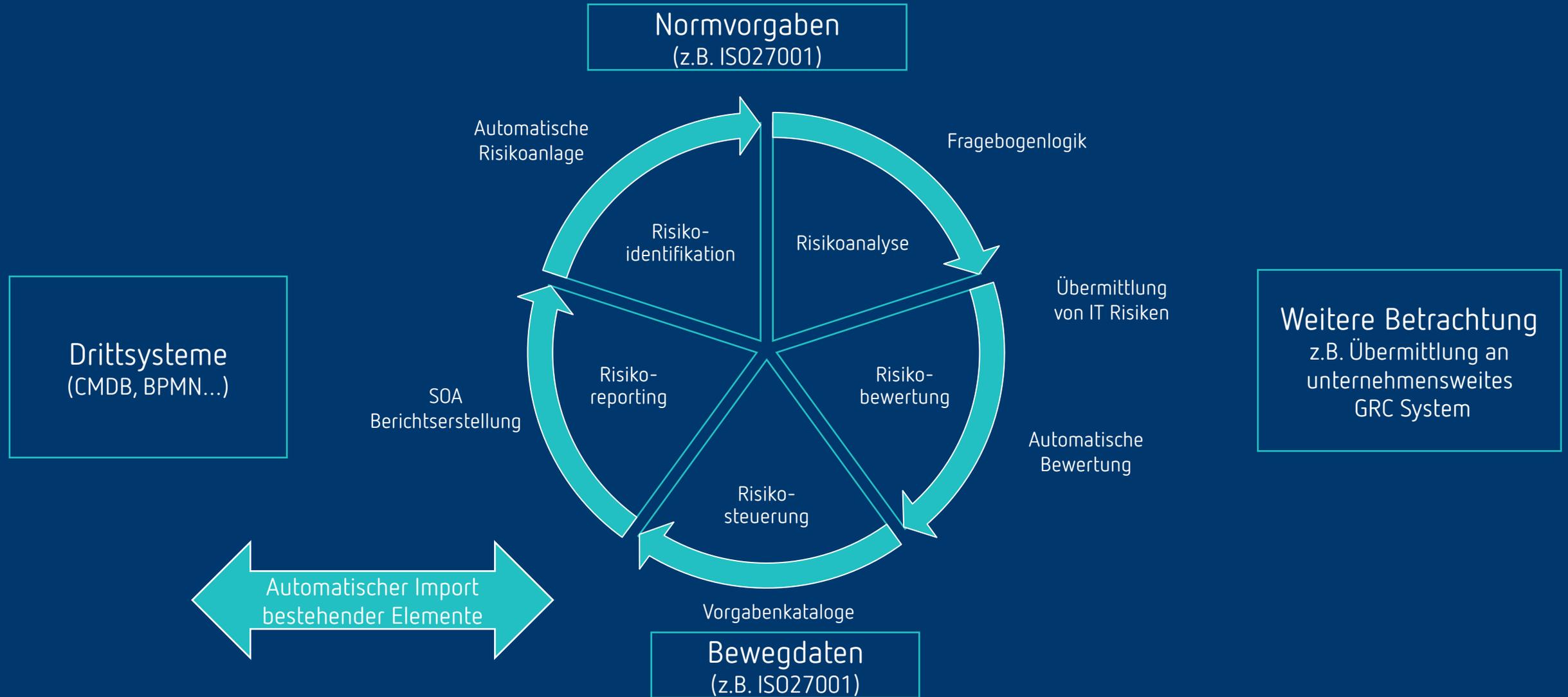


Überblick ausgewählter Automatismen

1. Automatischer Import/Export bestehender Elemente (z.B. Assets)
2. Automatische Risikoanlage über Gefährdungskataloge
3. Automatische Priorisierung von Elementen – Vererbung
4. Vorgabenkataloge – Einhaltung von Normanforderungen
5. Automatische Feldbefüllung mittels Fragebögen
6. SOA Berichtserstellung
7. Übermittlung von IT Risiken in übergreifendes GRC System



Übersicht – Unterstützung durch Automatismen im IT RM





Umfrage I - Mentimeter

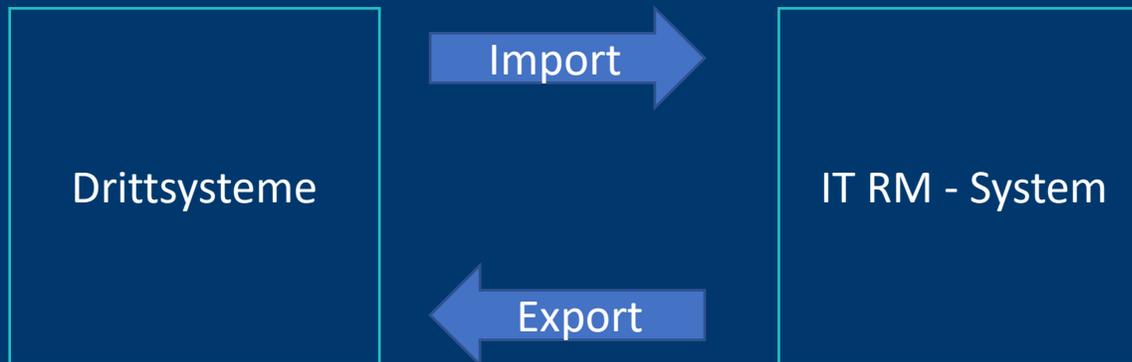
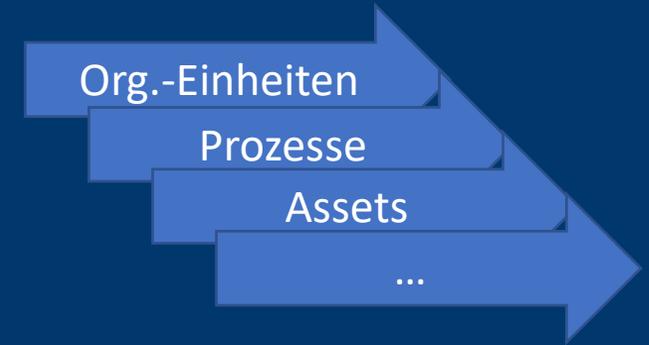
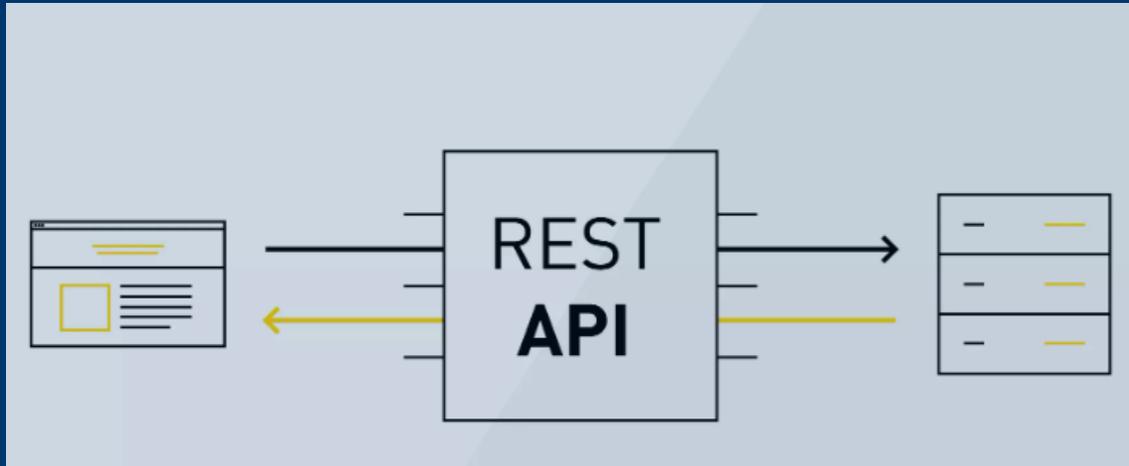
- Nutzen Sie bereits Automatisierungsmechanismen?
- Code: 2860 1797



Überblick ausgewählter Automatismen

1. Automatischer Import/Export bestehender Elemente (z.B. Assets)
2. Automatische Risikoanlage über Gefährdungskataloge
3. Automatische Priorisierung von Elementen – Vererbung
4. Vorgabenkataloge – Einhaltung von Normanforderungen
5. Automatische Feldbefüllung mittels Fragebögen
6. SOA Berichtserstellung
7. Übermittlung von IT Risiken in übergreifendes GRC System

Automatisierter Import von Prozessen / Assets etc.





Überblick ausgewählter Automatismen

1. Automatischer Import/Export bestehender Elemente (z.B. Assets)
2. **Automatische Risikoanlage über Gefährdungskataloge**
3. Automatische Priorisierung von Elementen – Vererbung
4. Vorgabenkataloge – Einhaltung von Normanforderungen
5. Automatische Feldbefüllung mittels Fragebögen
6. SOA Berichtserstellung
7. Übermittlung von IT Risiken in übergreifendes GRC System



Automatische Risikoanlage über Gefährdungskataloge

1. Ausgangslage

- Bei vielen Assets treffen immer dieselben (Standard-) Gefährdungen zu
- Aus diesen Gefährdungen werden dann jeweils immer dieselben Risiken angelegt

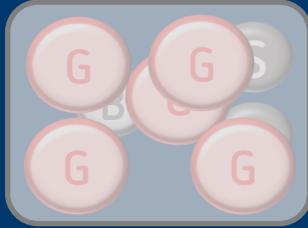
2. Idee

- Die Standardgefährdungen werden systematisch erfasst
- Bei neuen Assets werden die entsprechenden Standardrisiken automatisch angelegt



Automatische Risikoanlage über Gefährdungskataloge

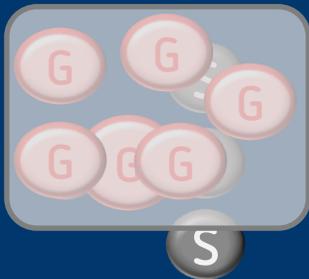
GK Serverraum



GK Server



GK Client



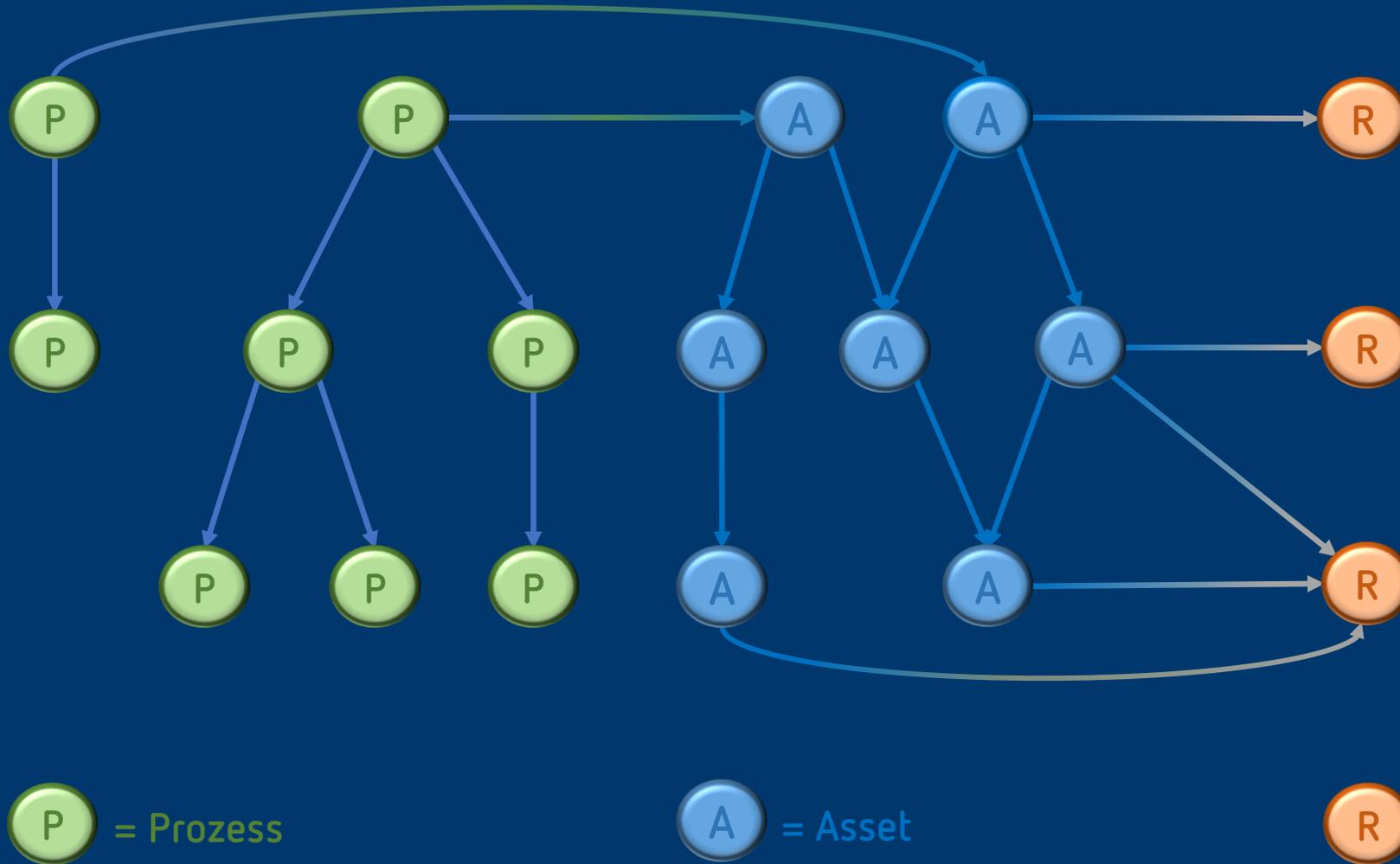


Überblick ausgewählter Automatismen

1. Automatischer Import/Export bestehender Elemente (z.B. Assets)
2. Automatische Risikoanlage über Gefährdungskataloge
3. **Automatische Priorisierung von Elementen – Vererbung**
4. Vorgabenkataloge – Einhaltung von Normanforderungen
5. Automatische Feldbefüllung mittels Fragebögen
6. SOA Berichtserstellung
7. Übermittlung von IT Risiken in übergreifendes GRC System



Automatische Vererbung der Bewertungen



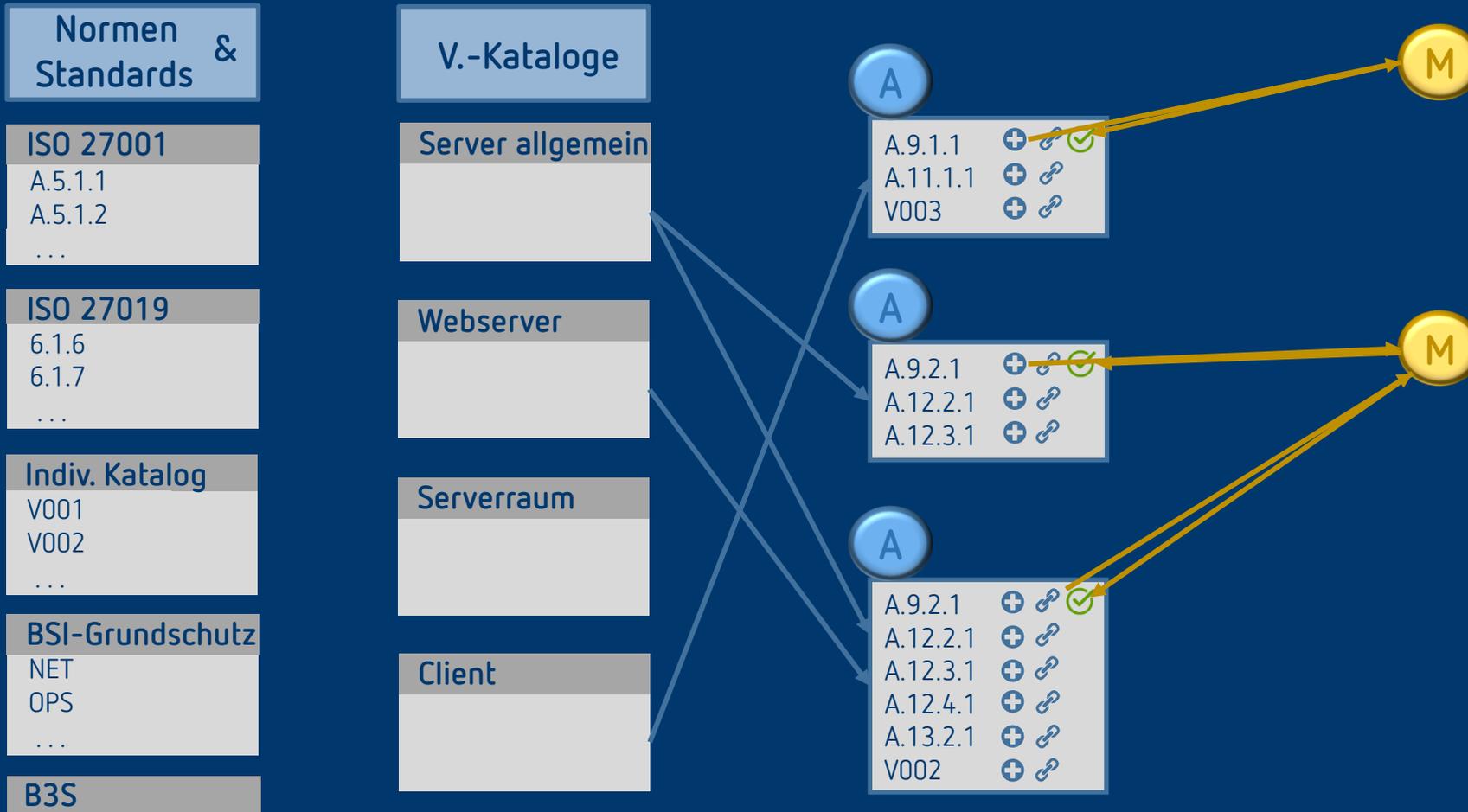


Überblick ausgewählter Automatismen

1. Automatischer Import/Export bestehender Elemente (z.B. Assets)
2. Automatische Risikoanlage über Gefährdungskataloge
3. Automatische Priorisierung von Elementen – Vererbung
4. **Vorgabekataloge – Einhaltung von Normanforderungen**
5. Automatische Feldbefüllung mittels Fragebögen
6. SOA Berichtserstellung
7. Übermittlung von IT Risiken in übergreifendes GRC System



Vorgabekataloge





Überblick ausgewählter Automatismen

1. Automatischer Import/Export bestehender Elemente (z.B. Assets)
2. Automatische Risikoanlage über Gefährdungskataloge
3. Automatische Priorisierung von Elementen – Vererbung
4. Vorgabenkataloge – Einhaltung von Normanforderungen
5. **Automatische Feldbefüllung mittels Fragebögen**
6. SOA Berichtserstellung
7. Übermittlung von IT Risiken in übergreifendes GRC System



Fragebogenlogik

- Möglichkeit zur Konfiguration beliebiger Fragebögen
 - Viele unterschiedliche Frage- / Antworttypen (Auswahllisten, Text, Checkboxen, Datum, Währungsbeträge uvm.)
 - Frage- / Antwort-Logiken zum antwortabhängigen Überspringen von Fragen
- Optionale Berechnung von Feldwerten, z.B. Eintrittswahrscheinlichkeiten, Auswirkungen, Auswahllisten u.a.
- Versendung von Umfragen an interne User und automatisch erstellte Gastkonten
- Automatische E-Mail-Workflows

Fragebogenlogik

Eingabedialog Risiko

Risiko
R-00000180, Gezielte IT-Angriffe

Bewertung **DS-Bewertung**

Automatisch aus VIVA-Bewertung

Bestimmung der Eintrittswahrscheinlichkeit  

Brutto-Eintrittswahrscheinlichkeit

Brutto-Auswirkung

Brutto-Risikokennzahl

Bewertung

Fragebogen

Ist das Risiko in den letzten drei Jahren eingetreten? ● Ja

Was war die Ursache? ● Vorsätzliche Handlung

Wurden nach Risikoeintritt konkrete Maßnahmen zur Risikominderung geplant? ● Ja

Wurden die Maßnahmen vollständig umgesetzt und die konkrete Umsetzung dokumentiert? ● Ja

Wurden die umgesetzten Maßnahmen auf Wirksamkeit überprüft? ● Nein

Könnten Sie sich vorstellen, dass dasselbe Risiko in den nächsten drei Jahren erneut eintritt? ● Ja

Hinweis ✕

 Für den ermittelten Wert ist das Ergebnis: Wahrscheinlich

✓ OK

Fragebogen

Ist das Risiko in den letzten drei Jahren eingetreten?

Was war die Ursache?

Wurden nach Risikoeintritt konkrete Maßnahmen zur Risikominderung geplant?

Wurden die Maßnahmen vollständig umgesetzt und die konkrete Umsetzung dokumentiert?

Wurden die umgesetzten Maßnahmen auf Wirksamkeit überprüft?

Könnten Sie sich vorstellen, dass dasselbe Risiko in den nächsten drei Jahren erneut eintritt?

Eingabedialog Risiko

Risiko
R-00000180, Gezielte IT-Angriffe

Bewertung **DS-Bewertung**

Automatisch aus VIVA-Bewertung

Bestimmung der Eintrittswahrscheinlichkeit  

Brutto-Eintrittswahrscheinlichkeit Wahrscheinlich ● Info Netto-Eintrittswahrscheinlichkeit

Brutto-Auswirkung Gravierend ● Info Netto-Auswirkung

Brutto-Risikokennzahl 8,00 Punkte Netto-Risikokennzahl

Bewertung



Überblick ausgewählter Automatismen

1. Automatischer Import/Export bestehender Elemente (z.B. Assets)
2. Automatische Risikoanlage über Gefährdungskataloge
3. Automatische Priorisierung von Elementen – Vererbung
4. Vorgabenkataloge – Einhaltung von Normanforderungen
5. Automatische Feldbefüllung mittels Fragebögen
6. SOA Berichtserstellung
7. Übermittlung von IT Risiken in übergreifendes GRC System



SoA Berichterstellung

- Die SoA ist zentraler Bestandteil eines Informationssicherheits-Management systems (ISMS)
- Die SoA bietet in Verbindung mit dem Geltungsbereich des Informationssicherheits-Management systems (4.3 der ISO 27001) eine Übersicht über Maßnahmen, die vom Unternehmen angewendet werden.



SoA Berichterstellung

Allgemein

Statement of Applicability (SOA)

Erklärung zur Anwendbarkeit im Rahmen des Informationssicherheitsmanagementsystems

21 %

- Statement of Applicability (SOA)
 - SOA-Assistent
 - 1 Basisinformationen
 - 1.1 Angaben des Unternehmens
 - 1.2 Externe Unterstützung
 - 2 Administrative Daten
 - 2.1 Ersteller und Freigabe
 - 2.2 Regelung**
 - 3 Aufbau festlegen
 - 3.1 Einleitung
 - 3.2 Scoping darstellen
 - 3.3 Ausführliche Konformitätserklärung
 - 4 Kontext der Organisation
 - 5 Führung
 - 6 Planung
 - 7 Unterstützung
 - 8 Betrieb
 - 9 Bewertung der Leistung
 - 10 Verbesserung
 - 11 Anforderungen der Referenzmaßnahmenziele
 - 11.1 Verweis auf R2C_SECURITY
 - 11.2 Darstellung der Katalogmaßnahmen
 - 11.3 Darstellung der Geschäftsprozesse
 - 11.4 Darstellung der Assets
 - 11.5 Zusatzverweis auf R2C_SECURITY
 - 12 Abschließen

2.2 Regelung

Geben Sie bitte die Informationen bezüglich der Regelung an.

Wann tritt die Regelung in Kraft?

Bitte geben Sie das Datum ein *

01.04.2023

Ersetzt die Regelung eine Vorgängerversion? *

Ja Nein

Ist die Vorgängerversion in der Software enthalten? *

Ja Nein

SOA-00000005

Wer soll diesen Bericht erhalten? *

Schmitt, Dieter; Bit, Harry

Soll der Verteilerkreis um nicht aufgeführt sein? *

Ja Nein

< Zurück

DIN_ISO27001_A.6 Organisation der Informationssicherheit

DIN_ISO27001_A.6.1 Interne Organisation

Normenverbindliche Maßnahmen	Gelebte Schutzmaßnahmen				
	Bezeichnung	Status	Vollständigkeit/Erfüllung	Wirksamkeit	Angemessenheit
DIN_ISO27001_A.6.1.1 Informationssicherheitsrollen und -verantwortlichkeiten	Relevant -				
M-00000005 Hochverfügbarkeit physikalischer Systeme	<input checked="" type="checkbox"/> In Betrieb	<input type="checkbox"/> Unvollständig	<input type="checkbox"/> Mittel	<input type="checkbox"/> Nicht angemessen	
Berücksichtigte Assets <ul style="list-style-type: none">- A-00000073 Firewall- A-00000024 Datenbankserver- A-00000058 Webserver		Berücksichtigte Geschäftsprozesse <ul style="list-style-type: none">- P-00000037 Administration- P-00000002 IT-Support			
M-00000017 Stromversorgung wird sichergestellt	<input checked="" type="checkbox"/> In Betrieb	<input type="checkbox"/> Unvollständig	<input type="checkbox"/> Mittel	<input checked="" type="checkbox"/> Angemessen	
Berücksichtigte Assets <ul style="list-style-type: none">- A-00000034 Hauptgebäude (Ettlingen)- A-00000036 Rechenzentrum (Ettlingen)		Berücksichtigte Geschäftsprozesse <ul style="list-style-type: none">- P-00000037 Administration			
DIN_ISO27001_A.6.1.2 Aufgabentrennung	Relevant -				
M-00000005 Hochverfügbarkeit physikalischer Systeme	<input checked="" type="checkbox"/> In Betrieb	<input type="checkbox"/> Unvollständig	<input type="checkbox"/> Mittel	<input type="checkbox"/> Nicht angemessen	



Überblick ausgewählter Automatismen

1. Automatischer Import/Export bestehender Elemente (z.B. Assets)
2. Automatische Risikoanlage über Gefährdungskataloge
3. Automatische Priorisierung von Elementen – Vererbung
4. Vorgabenkataloge – Einhaltung von Normanforderungen
5. Automatische Feldbefüllung mittels Fragebögen
6. SOA Berichtserstellung
7. Übermittlung von IT Risiken in übergreifendes GRC System



Schnittstelle und Darstellung im übergreifenden GRC-System

- Vollautomatischer, zeitgesteuerter Übertrag von Risiken, Maßnahmen, Kontrollen uvm. zwischen R2C-Systemen sowie von / zu Drittsystemen (z.B. ERP, BPM, etc.)
- Freie Definition der Transformation der Elemente, d.h. konfigurierbare Übersetzungslogik
- Darstellung als eigenständiger Risikotyp möglich → „IT / Cyber risk“
 - Wenn gewünscht mit eigener (abweichender) Bewertungslogik
 - Separat zuweisbare Berechtigungen



Umfrage II - Mentimeter

- Sehen Sie Bedarf in Ihrem Unternehmen verstärkt Automatisierungsmechanismen im IT RM Prozess zu nutzen?
- Code: 1883 1314



Zusammenfassung

Vorteile:

- Automatismen reduzieren Aufwände für Routinetätigkeiten
- Vermeidung von „Doppeltätigkeiten“
- Fehler Reduzierung, z.B. falsche Risikoeinschätzung
- Reduktion von „Human Errors“
- Optimale Umsetzung von „Top Down“ Ansätzen



Zusammenfassung

Nachteile:

- Vorbereitungsdauer / Aufwand für Automatismen
- Delegieren von Verantwortung an die Anwendung(?)
- Risiko der Erzeugung von Massendaten(?)



Vielen Dank!



Disclaimer

Die vorliegende Präsentation ist unverbindlich. Sie dient ausschließlich Informationszwecken und nicht als Grundlage eines späteren Vertrags. Änderungen, Ergänzungen, Streichungen und sonstige Bearbeitungen dieser Präsentation können jederzeit durch die Schleppen SE nach freiem Ermessen und ohne vorherige Ankündigung vorgenommen werden.

Obschon die in dieser Präsentation enthaltenen Informationen von der Schleppen SE mit größtmöglicher Sorgfalt erstellt wurden, wird aufgrund des reinen Informationscharakters für die Richtigkeit, Vollständigkeit, Aktualität und Angemessenheit der Inhalte keinerlei Gewähr übernommen und jegliche Haftung im gesetzlich zulässigen Umfang ausgeschlossen. Verbindliche Aussagen können stets nur im Rahmen eines konkreten Auftrags getroffen werden.

Die Inhalte dieser Präsentation sind urheberrechtlich geschützt. Sie dürfen nur nach vorheriger Genehmigung durch die Schleppen SE verwendet werden. Dies gilt insbesondere für die Vervielfältigung von Informationen oder Daten, insbesondere die Verwendung von Texten, Textteilen oder Bildmaterial.