RISIKO-MANAGEMENT FÜR IT-UNTERNEHMEN

Risiken erkennen, bewerten, vermeiden, vernichten und versichern

Präsentation: Wolfram W. Heisen
Heisen Projekt & Prozess Management

Frankfurt, den 28.02.2013

IT- von gestern bis Heute

1973…

Bundesarchiv, B 145 Bild-F038812-0022
Foto: Schaack, Lothar | 28. Januar 1973

40 Jahre

… bis Heute

Bild: (C) Google

Agenda

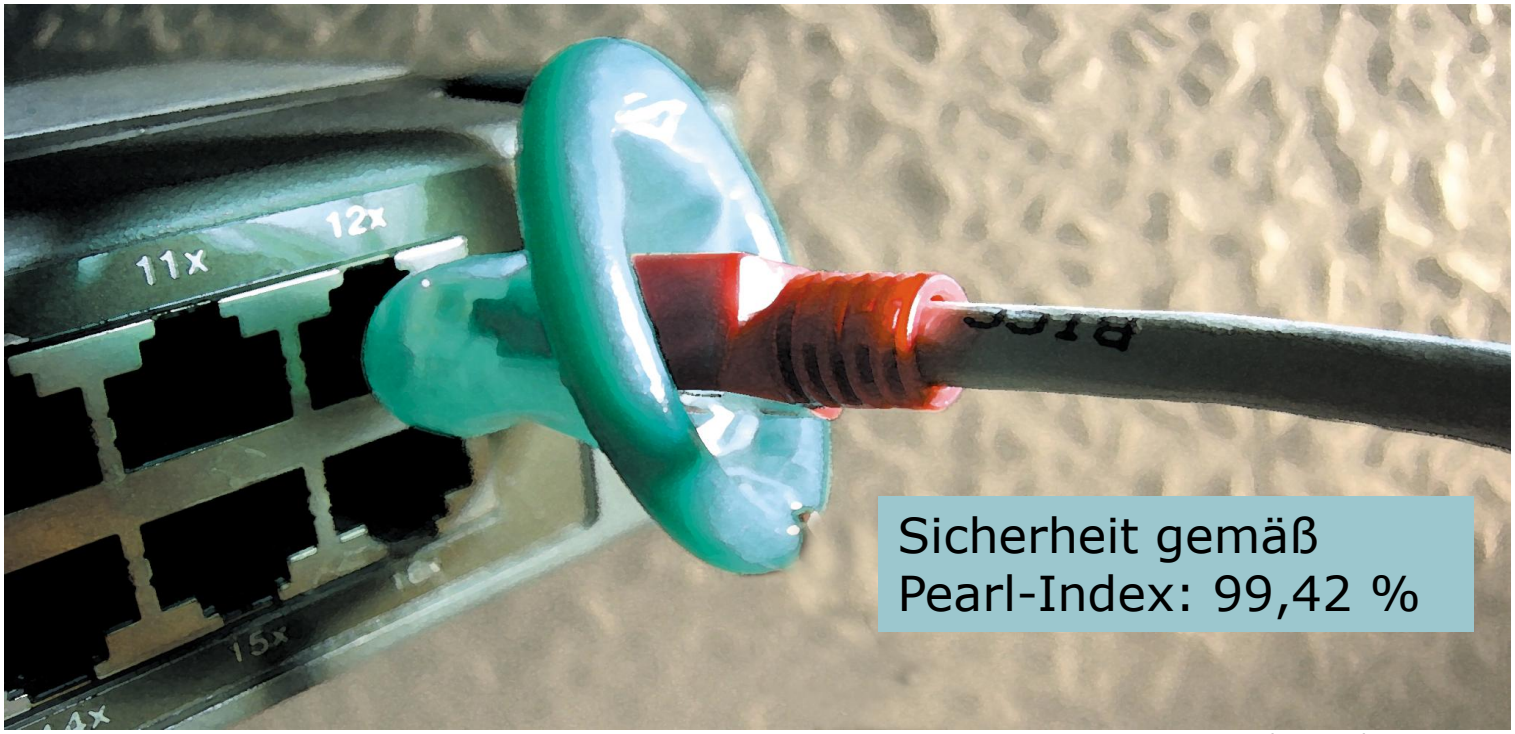
- Einleitung
- Definition
- Vorgehen
- Ergebnis
- Zusammenfassung

„No risk no fun“

Kennen Sie das?

Ok, wir kennen Branchen…

Risiko Management
Seit 1855



Vom Prinzip Hoffnung hin zum Risiko Management

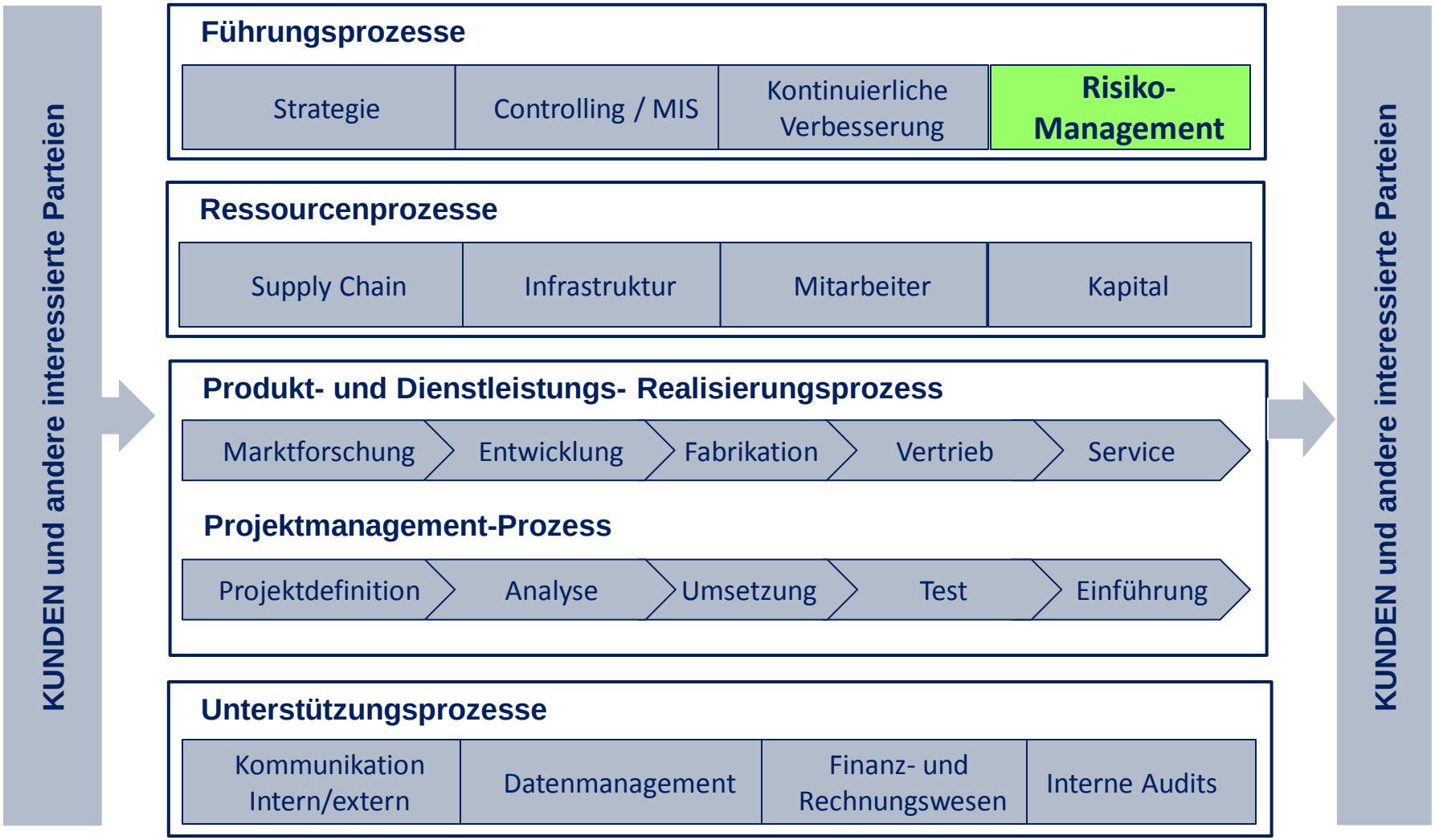
Risiko Begriff
- Ursprung -

Aus dem italienischen Ris(i)co

(unsichtbare) Klippe, die zu umschiffen ist

Prozesslandschaft

In Unternehmen



Definition: Risiko Management

- Systematisches Verfahren
  Identifikation und Vermeidung von Risiken basierend auf Erfahrungen

- Ziel:
  Verhinderung / Verschiebung des zeitlichen Eintritts eines möglichen Schadens (Menschen, Umwelt und Geld), Bildung von Rückstellungen für den Schadensfall

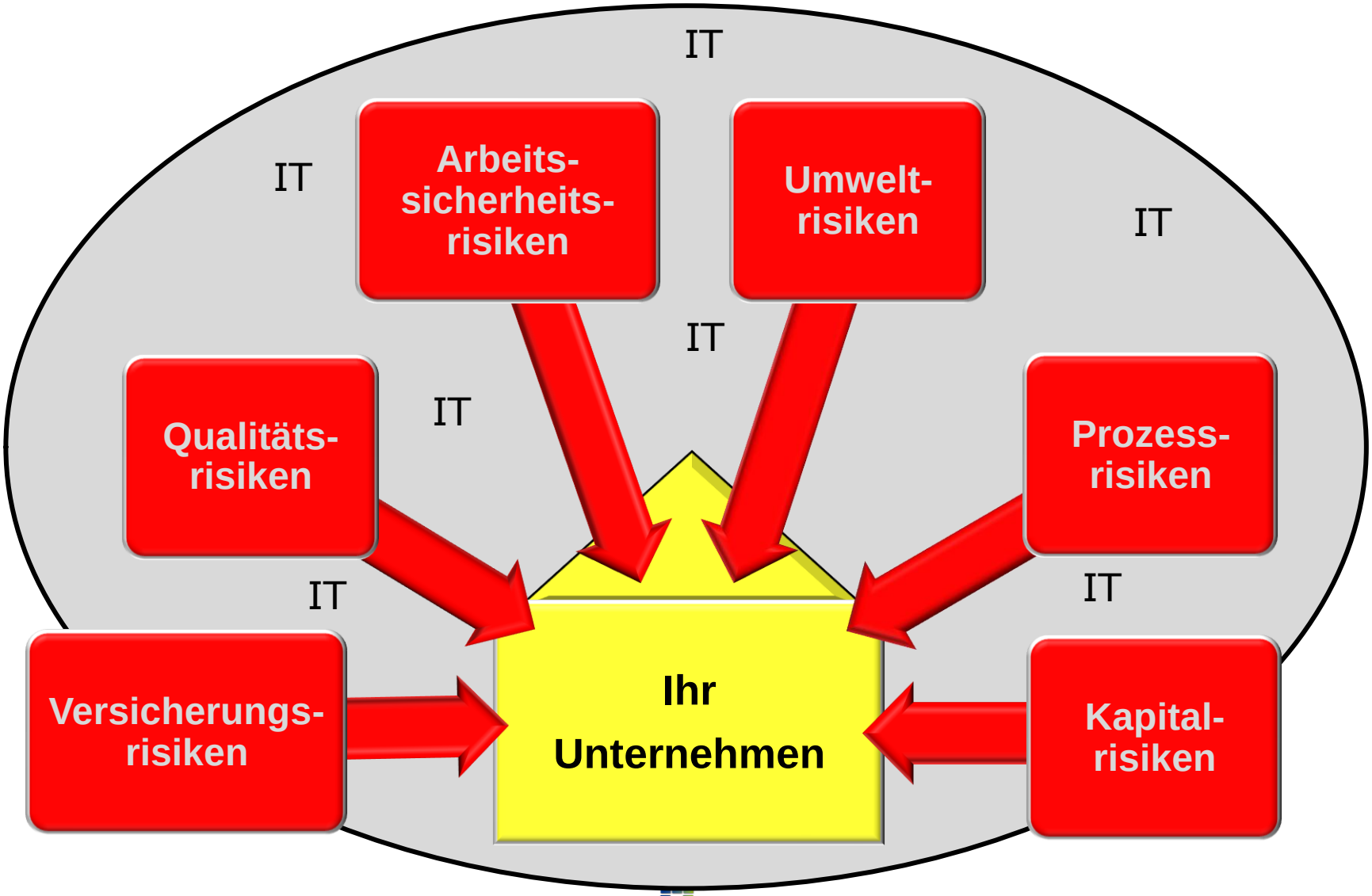
„Agieren statt reagieren“

Wann funktioniert Risiko Management

1. Top-Management gewollt, vom Gechäftsführer gefordert sein
2. Unterstützung aller Führungskräfte
3. Akzeptanz aller Mitarbeiter
4. Ist kein Projekt, sondern eine nicht endende Aufgabe für alle Beteiligten
5. Braucht Zeit… und Nachhaltigkeit

Kurz: Alle machen mit !

Wichtigsten Unternehmensrisiken



Risikobeispiele im Unternehmen

- Daten (-sicherung), Kundendaten
- Datenvernichtung
- Datenschutz, Datensicherheit
- Zutritts-, Zugangs-, Zugriffsrechte
- Hacker
- Cyberkriminelle
- Mitarbeiter (Wirtschaftskriminalität, Fluktuation, Krankheit, Arbeitszeit …)
- Arbeitssicherheit (Gefährdungsanalysen, Schutzausrüstung, Schulungsnachweise)
- Umwelt (Umgang m. Gefahrstoffen, Sicherheitsdatenblätter)

Risikobeispiele im Unternehmen

- Qualität (Gewährleistung, Reklamationen, Qualifikation …)
- Zahlungsausfall, Zahlungsverzug
- Insolvenz (Kunden, Lieferanten, eigene)
- Mitbewerber
- Juristische Risiken (Arbeits-, Vertragsrecht, Steuerrecht …)
- Lagerbestände
- Das Management

Unternehmensrisiken

Bei allen Punkten geht es nur um:

- Ertragsrisiken (Geld)
- Fortführungsrisiken (Zeit)
- Reputationsrisiken (Kunden, Presse, Shit-Storm)
  - Social-Media, Facebook, Xing, LinkedIn, Twitter, etc.

Normen für Risiko Managementsysteme

Welche Normen gibt es – Auszug -

- ISO 31000 Risk Management - Guidelines for principles and implementation of risk management
- IDW PS 340 Deutschland (Institut der Wirtschaftsprüfer)
- AS / NZS 4360 Australien / Neuseeland
- COSO Standard USA
- **ONR 49000 ff.** Österreich

Risiko Management nach einer Norm

Integriertes Management-System

(ON = Österreichisches Normungsinstitut)

Die Norm unterteilt

Risikobereiche im Überblick

Die Unternehmensrisiken

Risikobereich I

Risiken „Höherer Gewalt“

Erdbeben, Überschwemmungen, Sturm, Hagel etc.

Nicht beeinflussbar

Risikobereich II

Politische und / oder ökonomische Risiken

Veränderungen im ökonomischen und gesellschaftlichen Umfeld

Kaum beeinflussbar

Risikobereich III

Geschäftsrisiken

Unternehmensziele (Strategie)
Organisation
Beschaffung
Produkte
Absatz/Vertrieb
Forschung und Entwicklung

Finanzrisiken

Liquiditäts- und Finanzplanung
Zins- und Währungsabhängigkeiten
Verlustrisiken in Finanzpositionen

Betriebsrisiken

Unternehmensstruktur
Ablaufprozesse
IT/ IT-Sicherheit,
Personal

beeinflussbar

Cyberkriminalität in Deutschland

Zur Erinnerung: Angriffszielgruppe

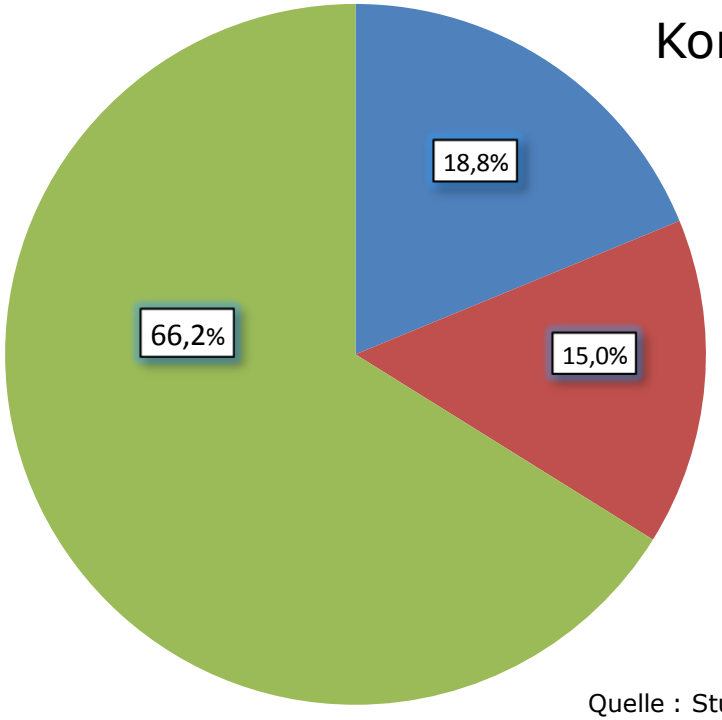
Angegriffene Unternehmen

<u>Mittelstand</u>

99,7 % aller Unternehmen

1,9 Billionen € Umsatz pro Jahr

Anteil am Gesamtumsatz 38,3 %



Konzerne

Kleinunter-nehmen

Quelle: Statistisches Bundesamt

Quelle : Studie "Industriespionage 2012 Aktuelle Risiken für die deutsche Wirtschaft durch Cyberwar

Risiken in IT-Abteilungen

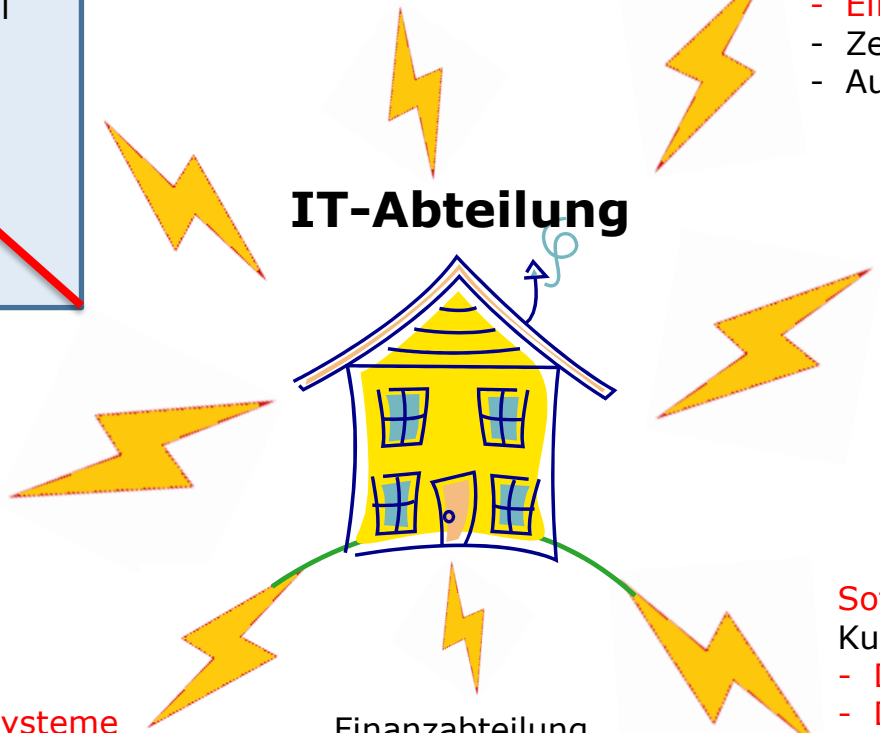
~~Risikobereich I + II~~

~~Umwelt, Erdbeben, Hochwasser, Sturm, Hagel~~
- ~~Ausfall~~
- ~~Beeinträchtigung~~

~~Politische und / oder ökonomische Risiken~~
- ~~Gesetze~~
- ~~Auflagen…~~

Externe Dienstleister, Lieferanten
- Datenvernichtung
- Leasing-Gesellschaften
- Outsourcing

Stromversorgung, IT-Anbindung nach Außen
- Klimatisierung
- USV
- Löschsysteme
- Einbruchmelde-Anlage
- Zerstörung
- Ausfall



Kunden, Mitarbeiter, Auszubildende, Interne Kunden, Hacker
- Sabotage
- Datendiebstahl
- BYOD, Handys
- Datenverlust
- Manipulation
- Ma Fluktuation
- Korruption

Hardware, Server, Telefonanlagen
- VOIP
- Versagen
- Performance
- Disaster Recovery

Software, CRM, ERP, Kundendaten, Mitarbeiterdaten
- Datendiebstahl
- Datenverlust
- Manipulation
- Datenschutz
- Datensicherung
- Firewall, SSL-Zertifikate…

Gebäude, Zugangssysteme Überwachung
- Einbruch
- Sicherheitsdienste
- Reinigungsfirmen!

Finanzabteilung
- Budget
- Wartung
- Versicherungen

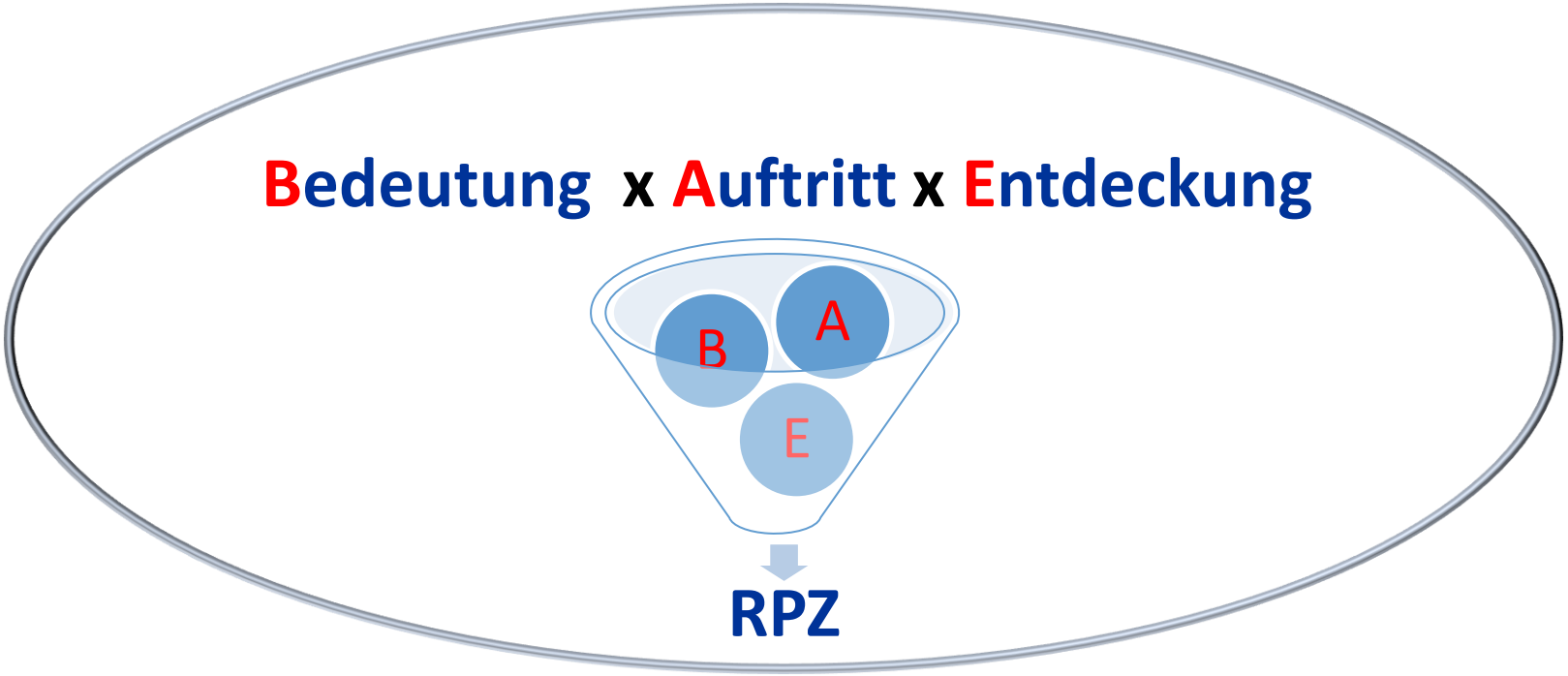
Klassifizierung der Risiken

Bedeutung	**Gewich-tung B**	**A**uftritts-wahrscheinlichkeit	**Gewich-tung A**	**E**ntdeckungs-wahrscheinlichkeit	**Gewich-tung E**
unbedeutend	1 - 2	unwahrscheinlich	1 - 2	hoch	1 - 2
gering	3 - 4	sehr selten	3 - 4	mäßig	3 - 4
spürbar	5 - 6	selten	5 - 6	gering	5 - 6
kritisch	7 - 8	möglich	7 - 8	sehr gering	7 - 8
katastrophal	9 - 10	häufig	9 - 10	unwahrscheinlich	9 - 10

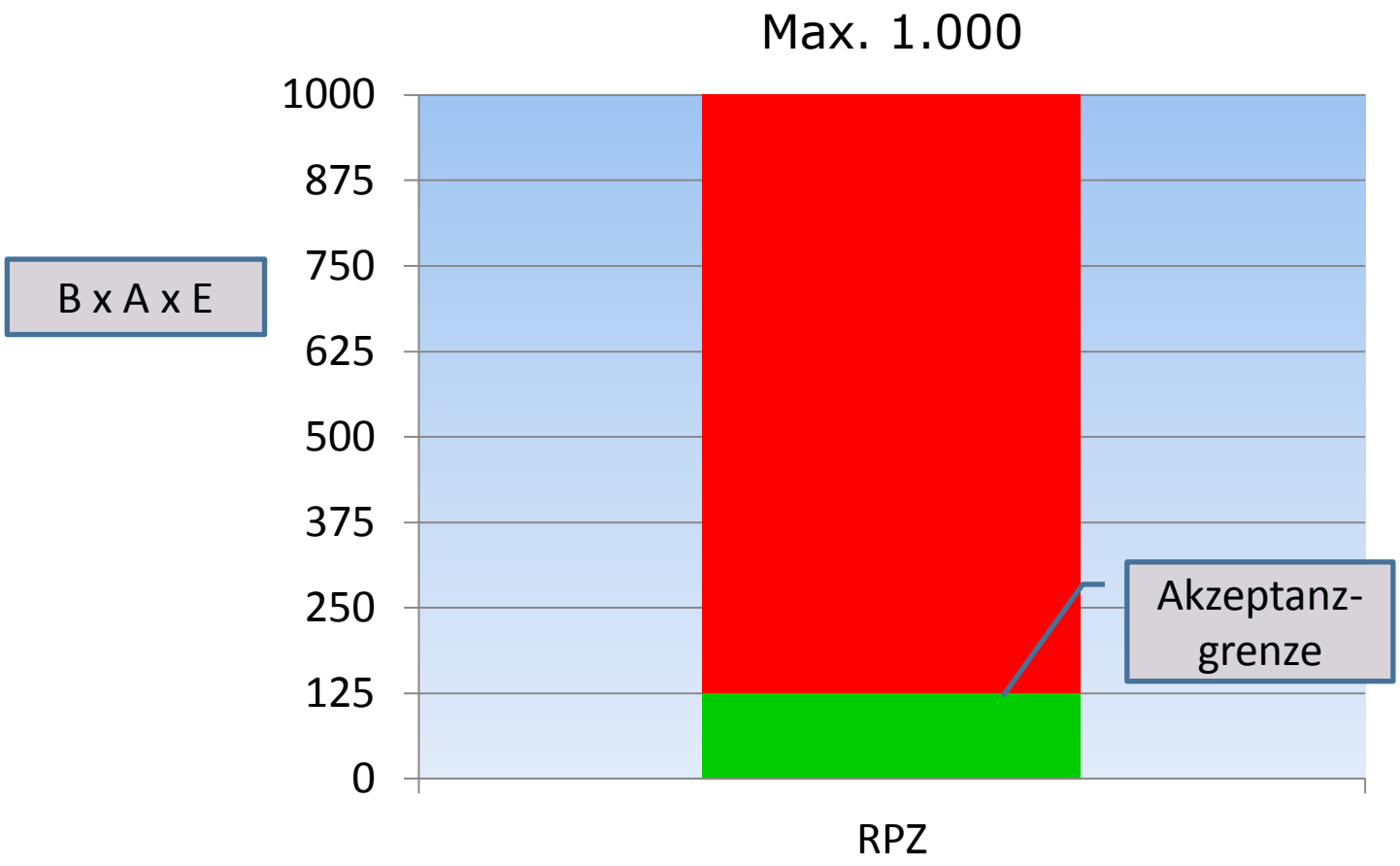
Messgröße: Risiko-Prioritäts-Zahl (RPZ)

Berechnung

- Multiplikation der einzelnen Gewichtungen

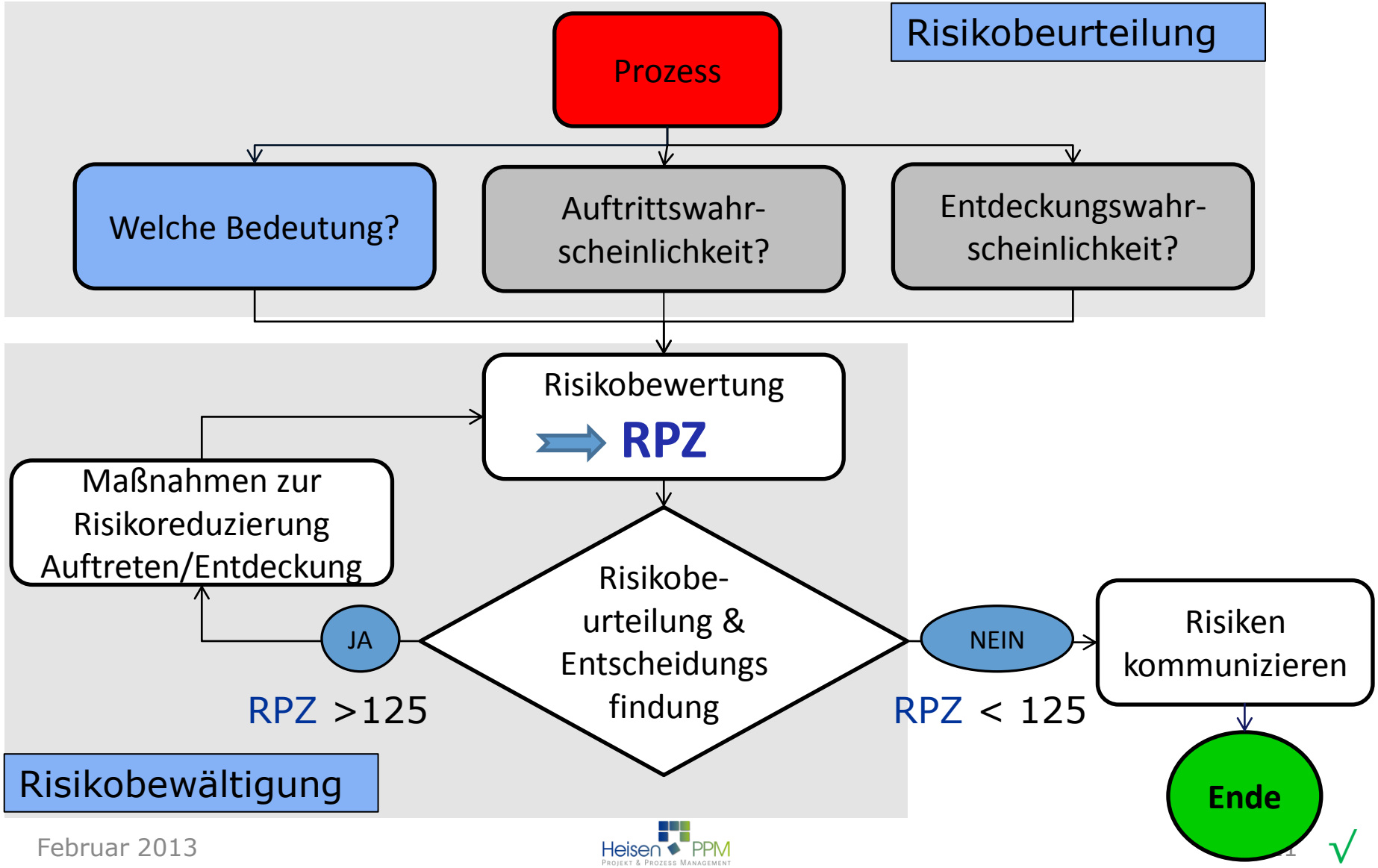


Akzeptanzgrenze RPZ

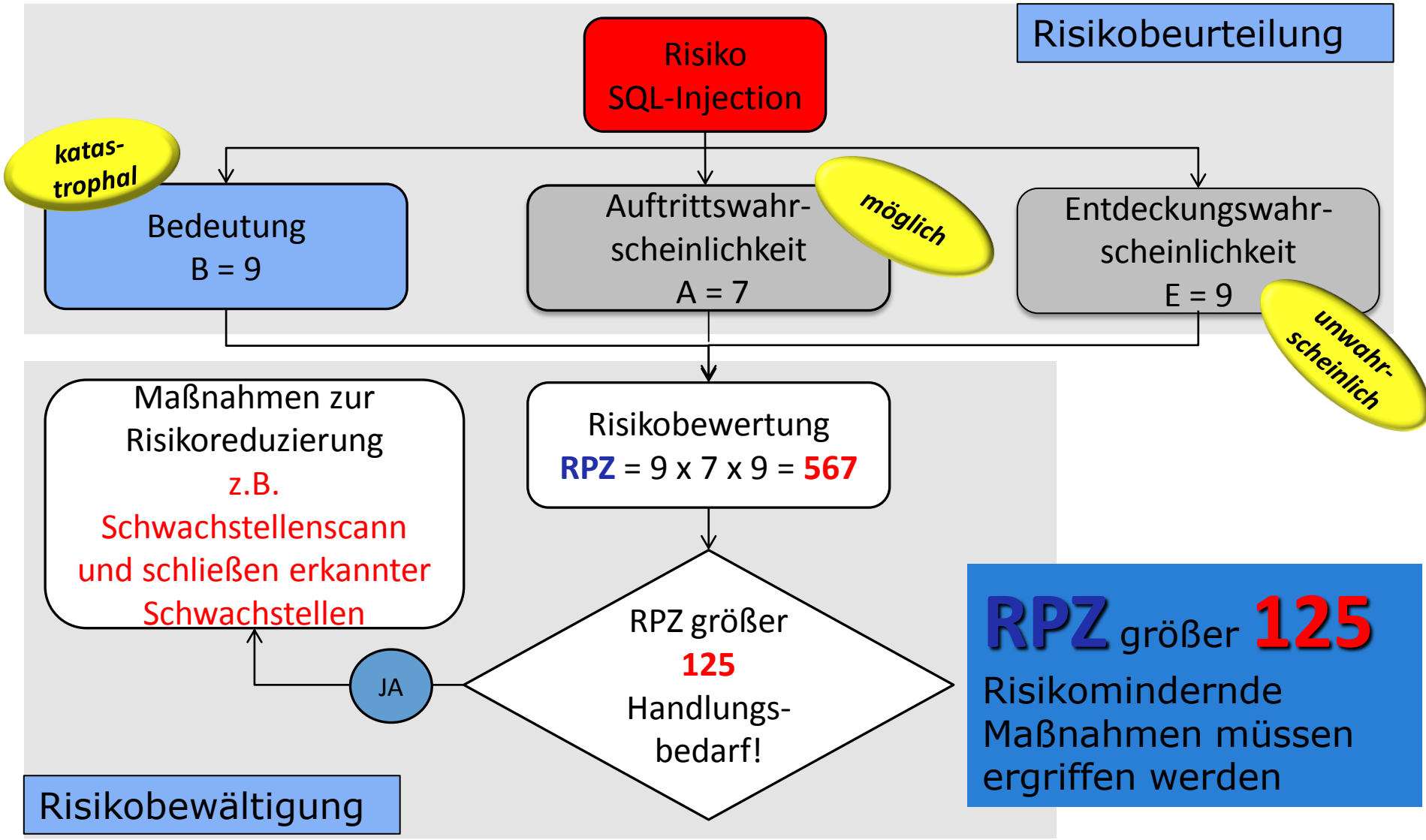


Methodik zur Risikoanalyse

Flussdiagramm



Risikoanalyse: SQL-Injection

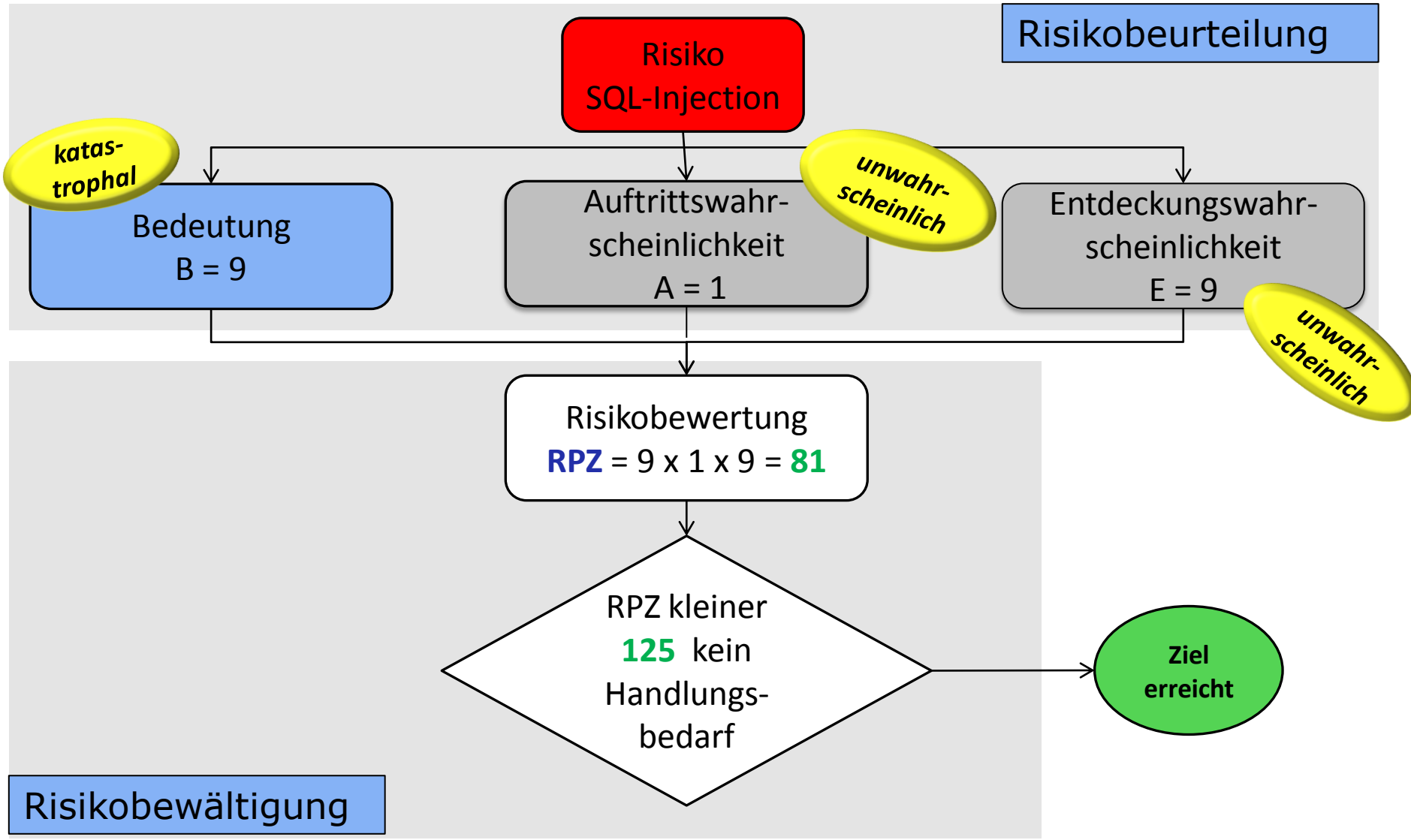


RPZ größer **125**

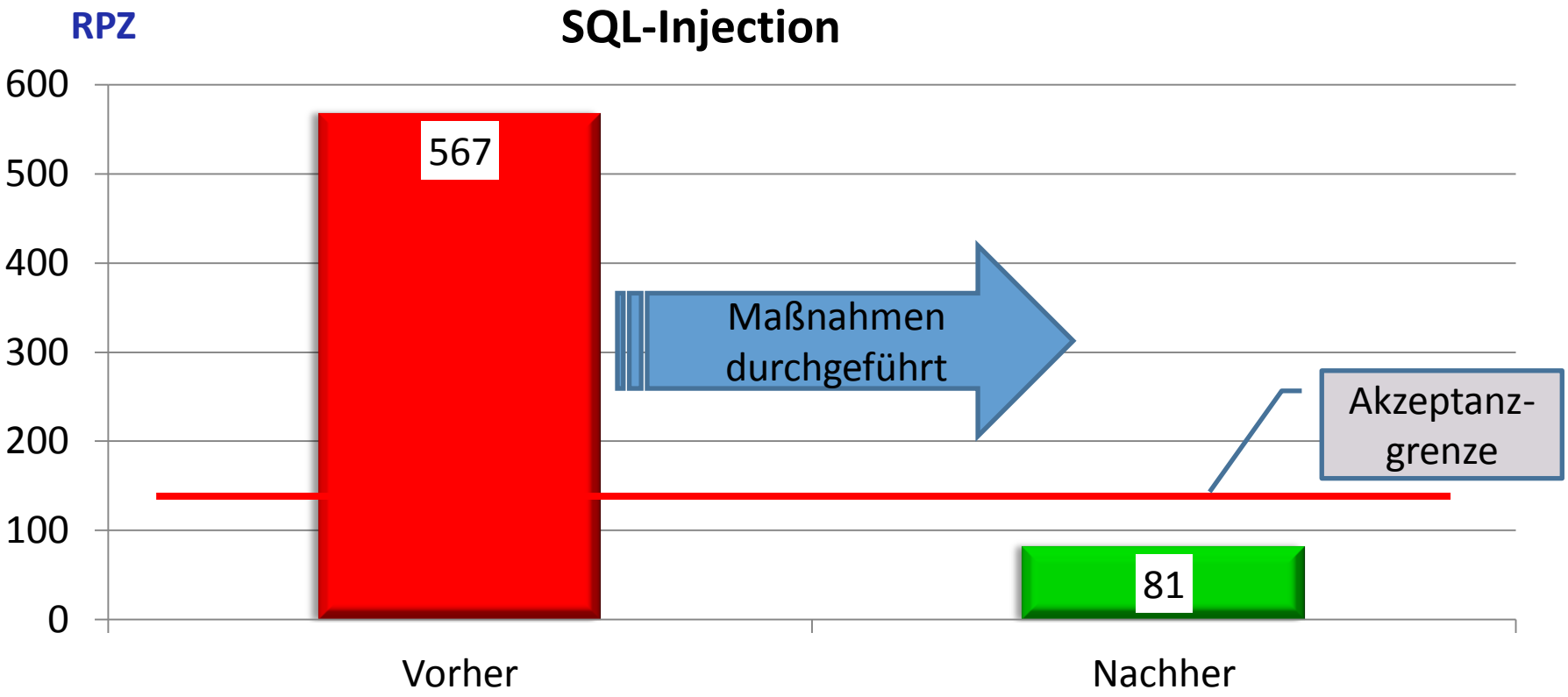
Risikomindernde Maßnahmen müssen ergriffen werden

Risikoanalyse

Bewertung nach Schwachstellenscann

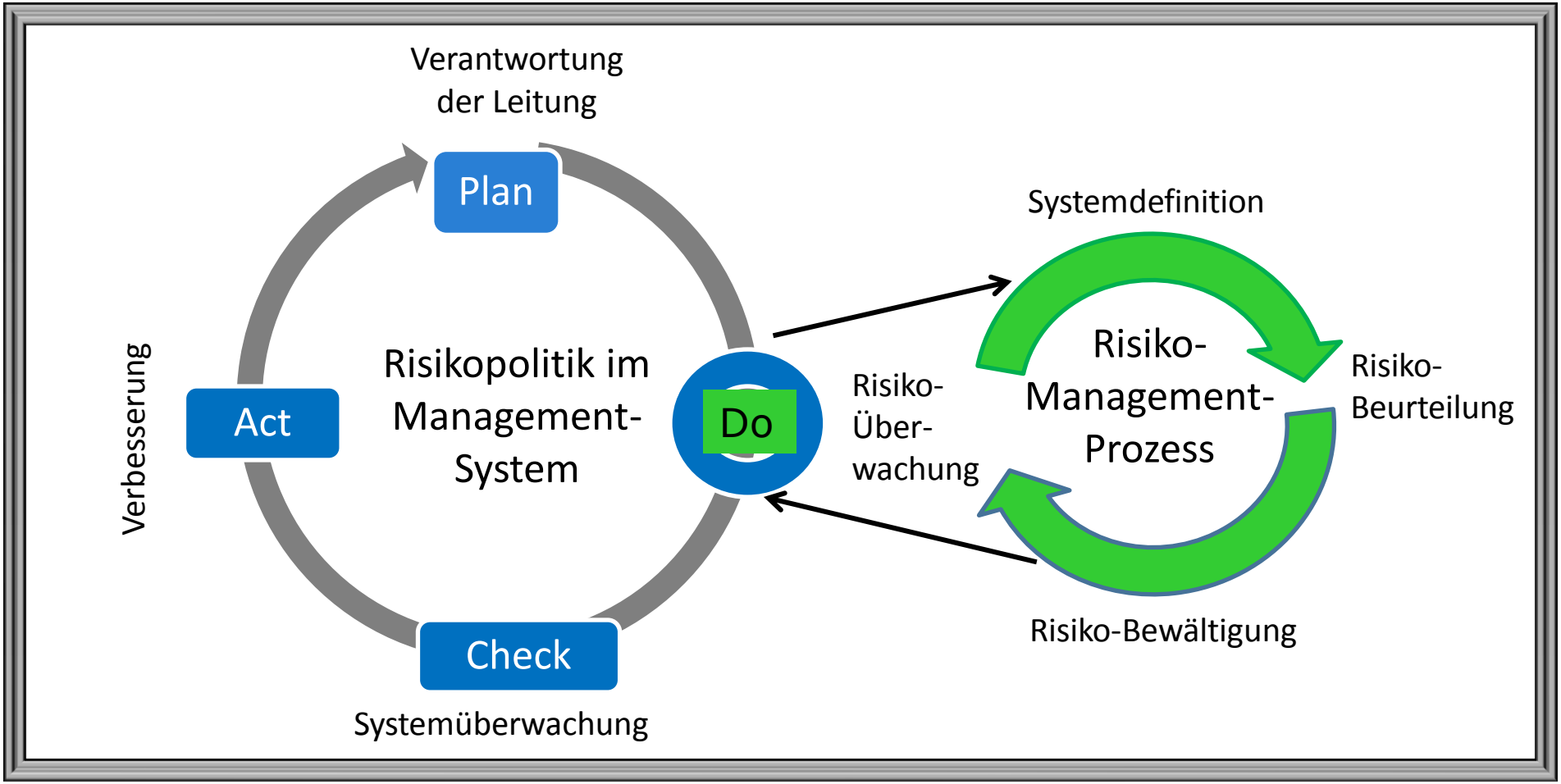


Risikodiagramm aus RPZ



Risiko Management

Dynamischer Zustand – PDCA-Zyklus



Risiko Management ONR 49000 ff.

- Risiken methodisch analysieren & bewerten
  - Vergl. BSI-Standard 100-4
- Szenarien für den Risikoeintritt erstellen
- Risikodiagramm erstellen
- Maßnahmenplanung
- Bewertung der Ergebnisse
- Risk Review durchführen

Risikoanalyse in 3 Schritten

Risiko Management

Zusammenfassung

- Es gibt viele Ansätze
- Unterschiedlichste Werkzeuge
- Unterschiedlichste Softwarelösungen
- Teamarbeit ist immer erforderlich!
- Entscheidend ist immer die schriftliche Dokumentation!
- Mehr Rechtssicherheit im Schadensfall

Historische Ansätze 1921

„Wenn wir nicht sicher wissen, was passieren wird, aber die Auftrittswahrscheinlichkeit kennen, ist das RISIKO."

„Wenn wir aber noch nicht einmal diese Wahrscheinlichkeit kennen, ist es UNGEWISSHEIT."

Frank Knight (USA, 1921)
In seinem Buch *„Risk, uncertainty and profit"*

Heisen PPM
Projekt & Prozess Management

Vielen Dank für Ihre Aufmerksamkeit, vermeiden Sie Ungewissheit !

Wolfram W. Heisen
Zertifizierter Risikomanager
gem. ONR 49000 ff

www.heisen-ppm.de
info@heisen-ppm.de