nc3.lu
National Cybersecurity
Competence Center
LUXEMBOURG

Luxembourg House
of Cybersecurity

konzeptacht

Informationssicherheit gestalten.

Risikomanagement mit dem Tool MONARC
(Optimised Risk Analysis Method)

www.konzeptacht.de

Agenda

- Vorstellung
- Was ist MONARC?
- Die MONARC Methodik
- Aufbau und Nutzung des Tools
- Tipps & Tricks

Thomas Kochanek

- 2000 – 2006 Flughafen Köln/Bonn GmbH
- 2006 – 2008 TÜV Rheinland Secure IT GmbH
- 2008 – 2017 TÜV TRUST IT GmbH
- Seit 2017 Geschäftsführer KonzeptAcht GmbH
- Durch akkreditierte Zertifizierungsstellen berufener ISO 27001 Lead-Auditor
- Auditteamleiter für Audits nach ISO 27001 auf der Basis von IT-Grundschutz
- Auditor „Smart Meter Gateway Administrator“ für BSI TR-03109-6
- Auditor gemäß Abschnitt 4 des Konformitätsbewertungsprogramms nach §11 Abs. 1a EnWG
- Auditor gemäß Konformitätsbewertungsprogramm zur Akkreditierung von Zertifizierungsstellen für den IT-Sicherheitskatalog gemäß § 11 Absatz 1b EnWG
- Prüfverfahrenskompetenz für §8a BSIG
- CISA / CRISC, APMG akkreditierter CISA Dozent für die ISACA

Marc Sparwel

- Seit 2017 Security Consultant bei der KonzeptAcht GmbH
- Zertifizierter ISMS-Manager/Auditor nach ISO/IEC 27001:2013
- TISAX® Implementer
- Prüfverfahrenskompetenz nach §8a (3) BSIG
- Wazuh Security Engineer
- Interner sowie Externer Informationssicherheitsbeauftragter
- Tätigkeitsschwerpunkte:
    - Aufbau von ISMS
    - Durchführung interner Audits
    - Durchführung technischer Audits
    - Betrieb von und Beratung zu Systemen zur Angriffserkennung (SzA)

LUXEMBOURG HOUSE OF CYBERSECURITY

Legal Form: G.I.E (Groupement d'Intérêt Economique)

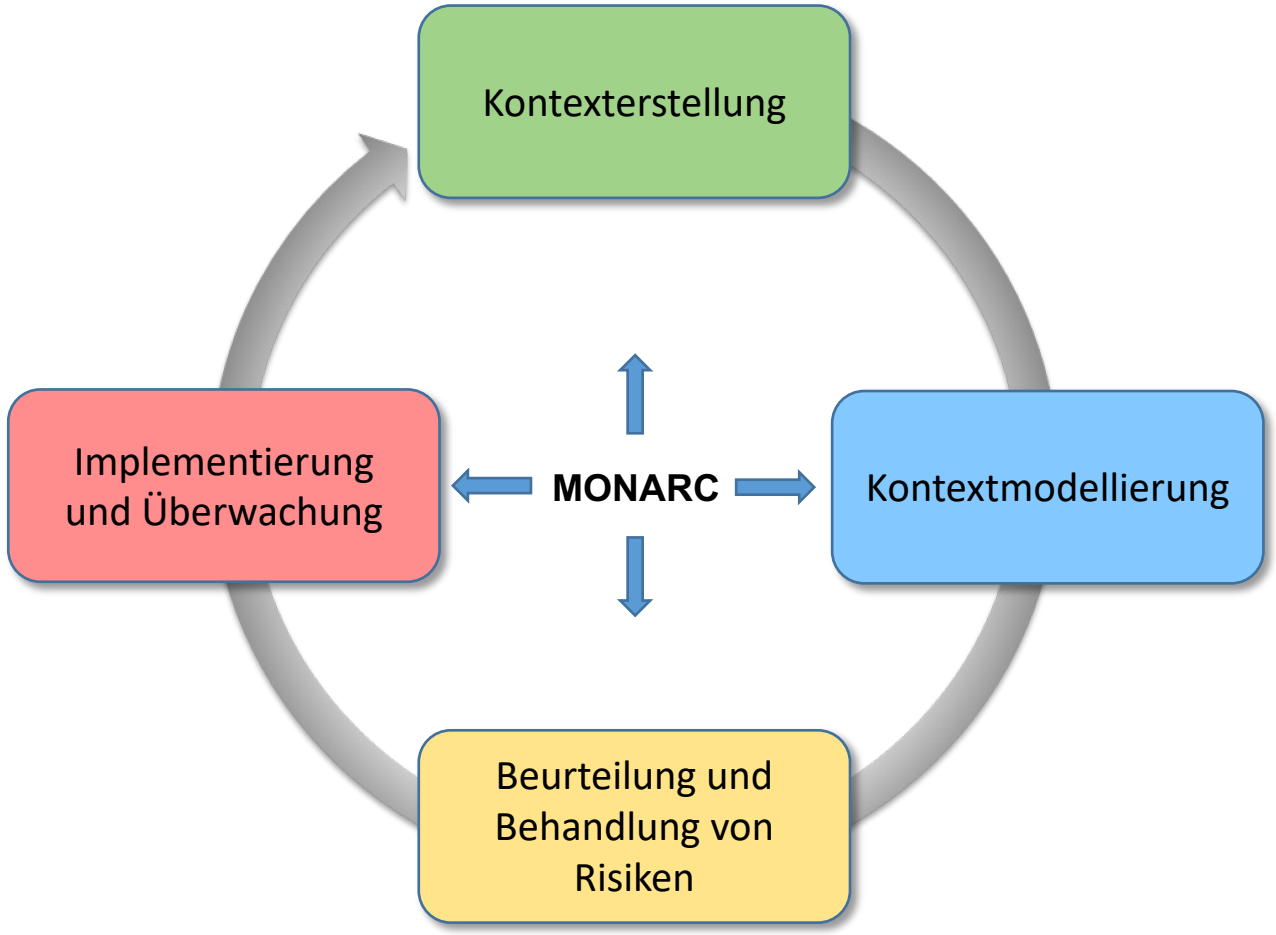
www.lhc.lu
www.nc3.lu

Was ist MONARC?

- Optimised Risk Analysis Method (**M**éthode **O**ptimisée d'A**na**lyse des **R**isques by **C**ASES.lu)
- Open Source Software
- Source Code[3] unter GNU Affero General Public License version 3
- Daten unterliegen CC0 1.0 Universal (CC0 1.0) - Public Domain Dedication
- Web Applikation (SaaS, self-hosted, virtuelle Maschine, hosted by KonzeptAcht GmbH, etc.)
- Oft beginnt alles mit Tabellenkalkulation.
- MONARC ist mittlerweile bei vielen europäischen Unternehmen in unterschiedlichen Branchen im Einsatz.
- In Deutschland nutzen Betreiber kritischer Infrastrukturen, Energieversorger etc. MONARC.

[3] https://github.com/monarc-project

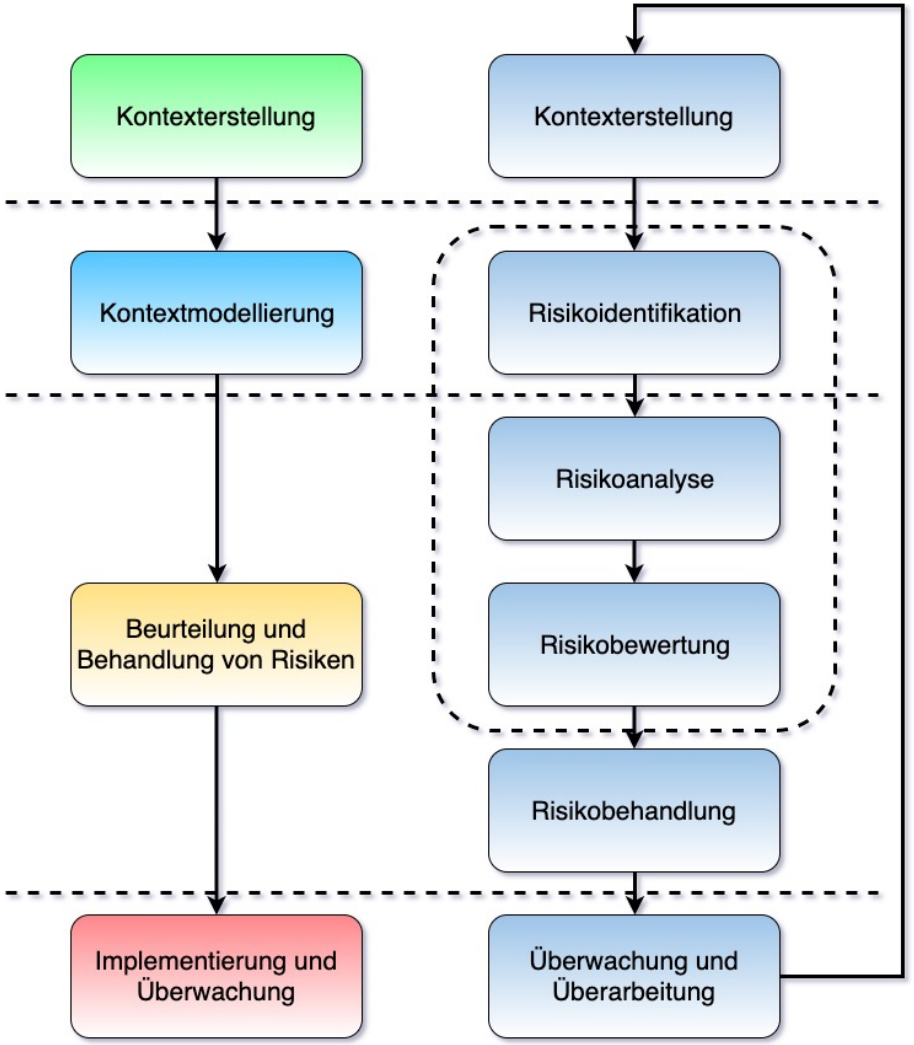
MONARC Methodik



Methodik der Risikoanalyse

- **Strukturiertes Vorgehen**
  1. …
  2. …
  n. …
- **Prozessual**
  - Plan
  - Do
  - Check
  - Act
- **Qualitativ: Werte / Auswirkungen**
  - Reputation, Image
  - Betrieb
  - Legal
  - Finanziell
  - Personen / Menschen
  - …

MONARC Methodik



MONARC Methodik

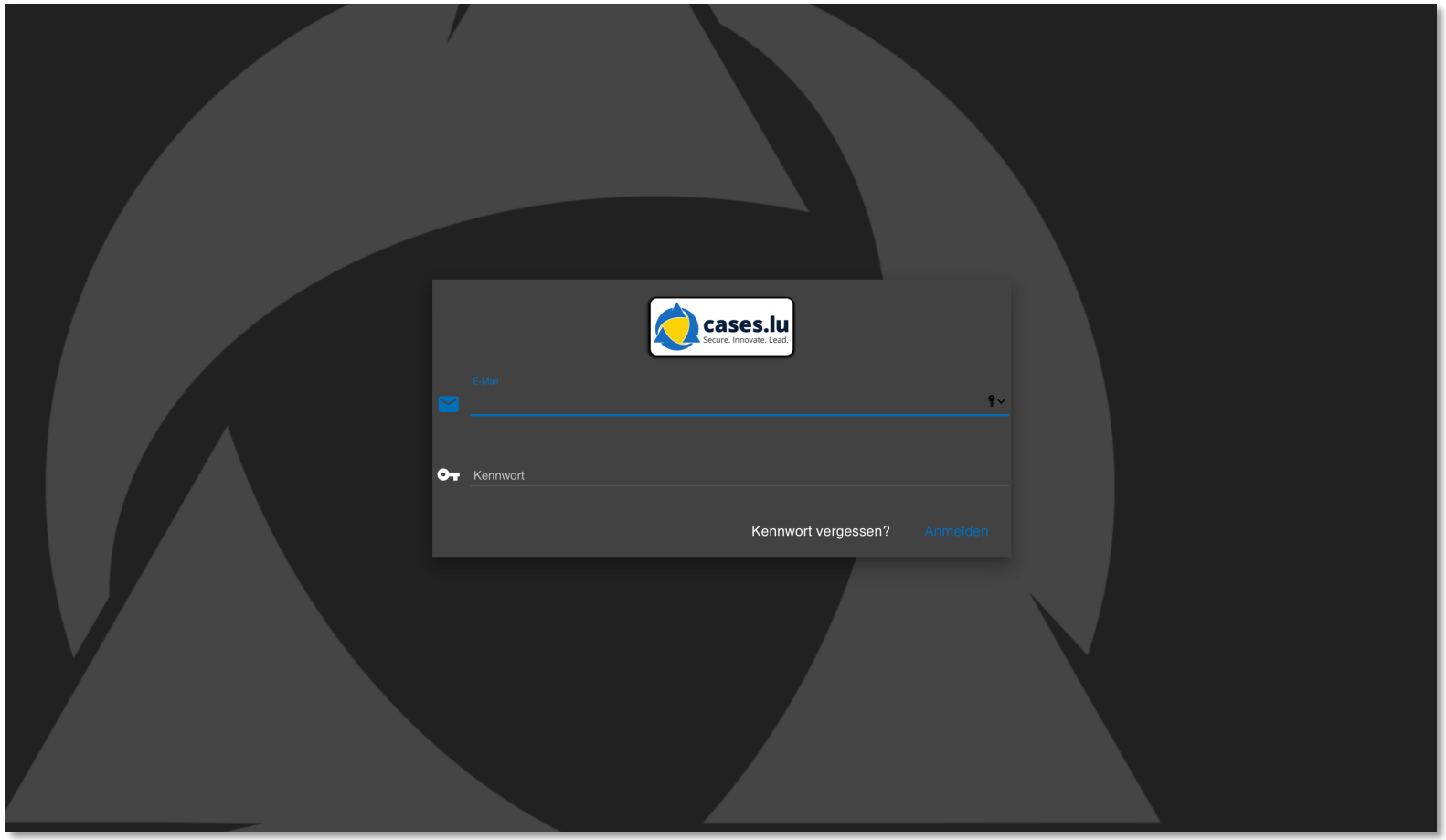
MONARC Methodik

Die folgende Formel wird zur Berechnung des Risikos angewendet:

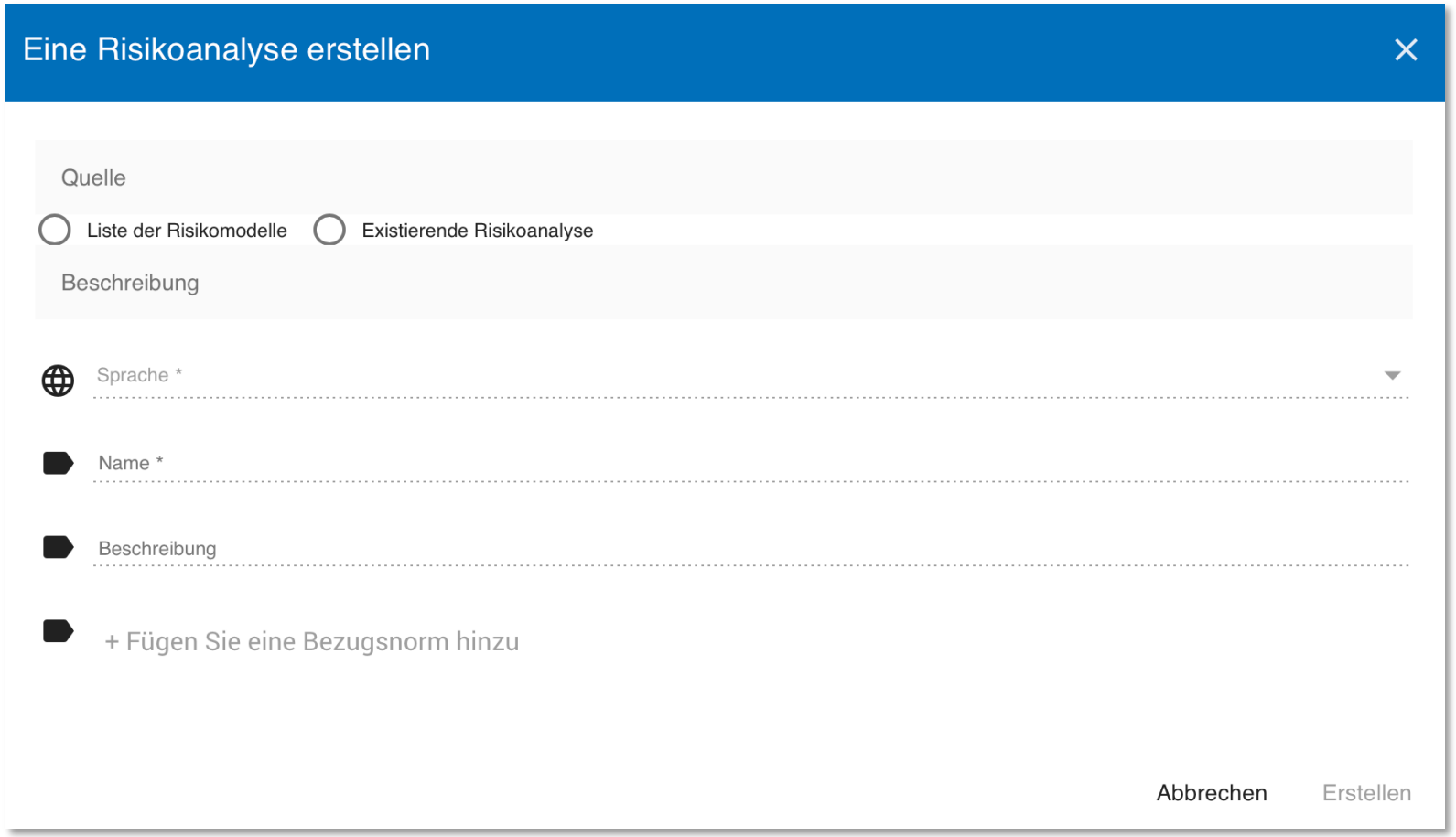
$$R = I \times (T \times V)$$

R: Risiko; **I**: Auswirkung (Impact), **T**: Bedrohung (Threat), **V**: Schwachstelle (Vulnerability)

Erstellung Risikoanalyse in MONARC



Erstellung Risikoanalyse in MONARC

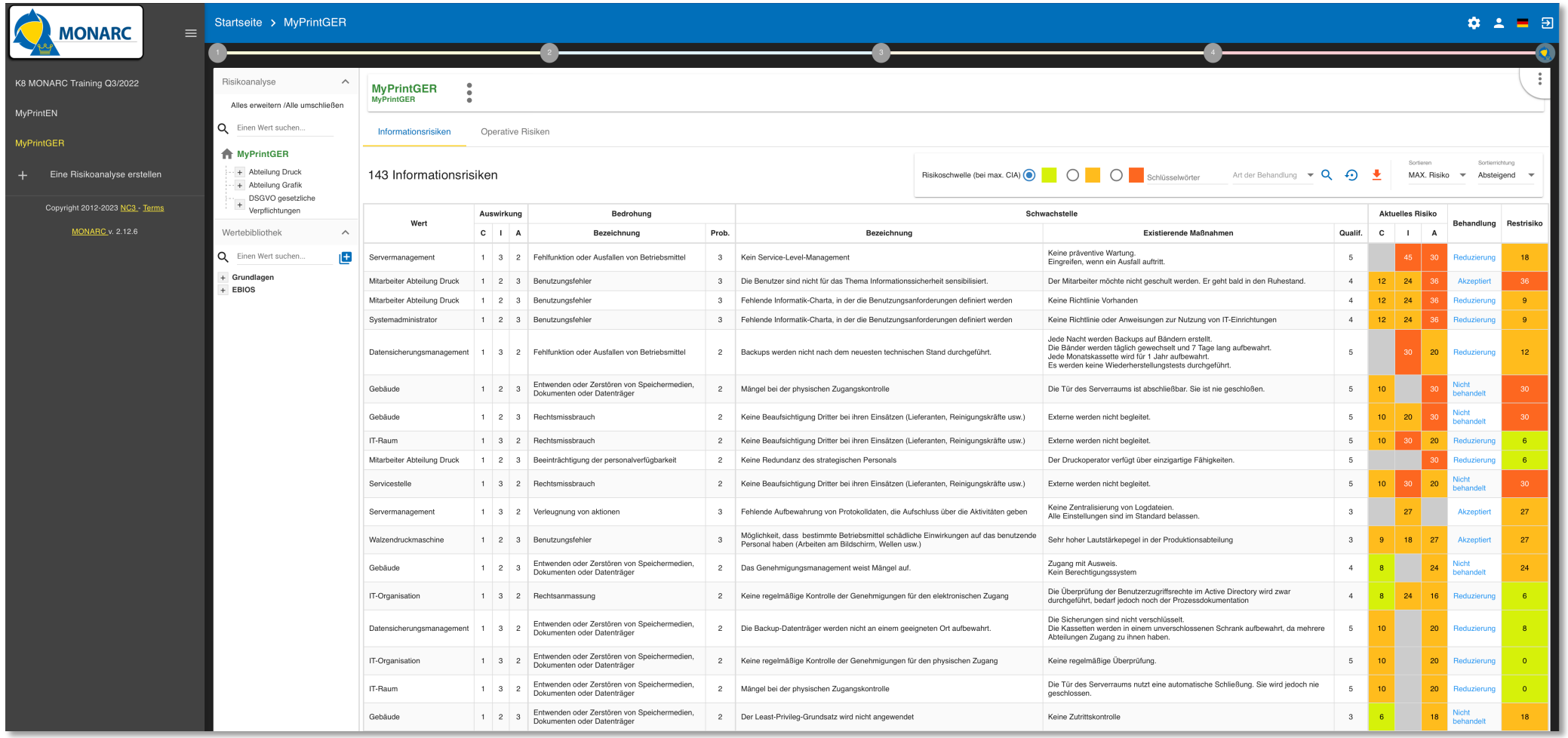


Erstellung Risikoanalyse in MONARC

Übung: Erstellung einer eigenen Risikoanalyse (30 Minuten)

- **Ziel**: Eigene Risikoanalyse erstellen
- **Vorgaben**:
  - Liste der Risikoanalysen: `Leeres Modell`
  - Sprache: `Deutsch`
  - Name: *`<individuell>`*
  - Beschreibung: *`<individuell>`*
  - Bezugsnorm: `ISO 27002`

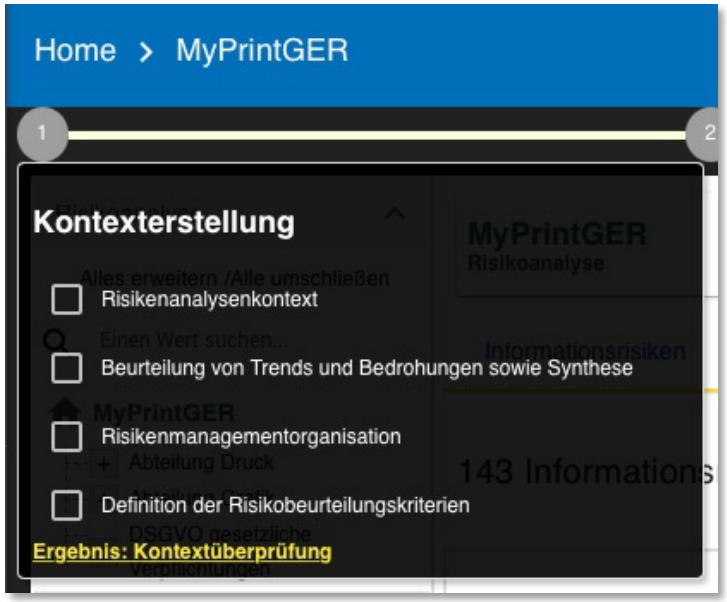
Aufbau und Nutzung des Tools



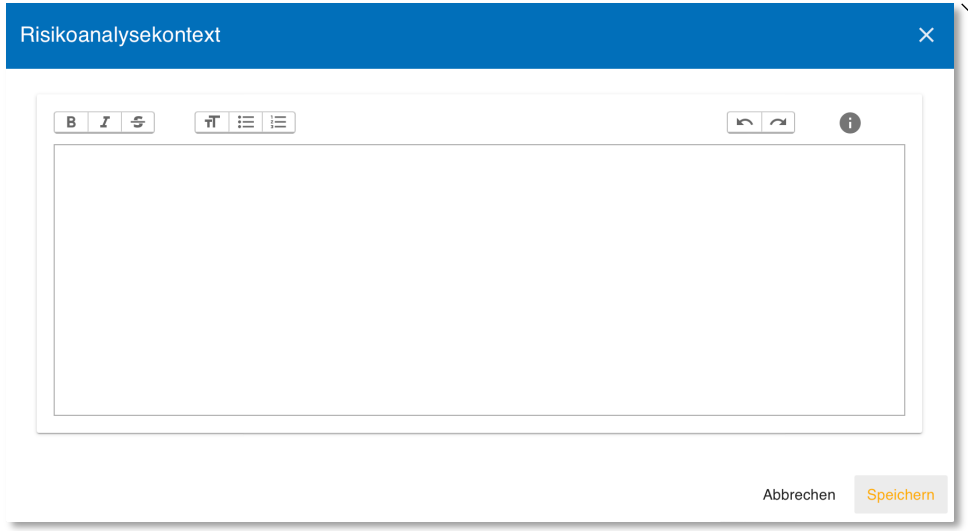
Wert	Auswirkung			Bedrohung		Schwachstelle			Aktuelles Risiko			Behandlung	Restrisiko
	C	I	A	Bezeichnung	Prob.	Bezeichnung	Existierende Maßnahmen	Qualif.	C	I	A		
Servermanagement	1	3	2	Fehlfunktion oder Ausfallen von Betriebsmittel	3	Kein Service-Level-Management	Keine präventive Wartung. Eingreifen, wenn ein Ausfall auftritt.	5		45	30	Reduzierung	18
Mitarbeiter Abteilung Druck	1	2	3	Benutzungsfehler	3	Die Benutzer sind nicht für das Thema Informationssicherheit sensibilisiert.	Der Mitarbeiter möchte nicht geschult werden. Er geht bald in den Ruhestand.	4	12	24	36	Akzeptiert	36
Mitarbeiter Abteilung Druck	1	2	3	Benutzungsfehler	3	Fehlende Informatik-Charta, in der die Benutzungsanforderungen definiert werden	Keine Richtlinie Vorhanden	4	12	24	36	Reduzierung	9
Systemadministrator	1	2	3	Benutzungsfehler	3	Fehlende Informatik-Charta, in der die Benutzungsanforderungen definiert werden	Keine Richtlinie oder Anweisungen zur Nutzung von IT-Einrichtungen	4	12	24	36	Reduzierung	9
Datensicherungsmanagement	1	3	2	Fehlfunktion oder Ausfallen von Betriebsmittel	2	Backups werden nicht nach dem neuesten technischen Stand durchgeführt.	Jede Nacht werden Backups auf Bändern erstellt. Die Bänder werden täglich gewechselt und 7 Tage lang aufbewahrt. Jede Monatskassette wird für 1 Jahr aufbewahrt. Es werden keine Wiederherstellungstests durchgeführt.	5		30	20	Reduzierung	12
Gebäude	1	2	3	Entwenden oder Zerstören von Speichermedien, Dokumenten oder Datenträger	2	Mängel bei der physischen Zugangskontrolle	Die Tür des Serverraums ist abschließbar. Sie ist nie geschloßen.	5	10		30	Nicht behandelt	30
Gebäude	1	2	3	Rechtsmissbrauch	2	Keine Beaufsichtigung Dritter bei ihren Einsätzen (Lieferanten, Reinigungskräfte usw.)	Externe werden nicht begleitet.	5	10	20	30	Nicht behandelt	30
IT-Raum	1	3	2	Rechtsmissbrauch	2	Keine Beaufsichtigung Dritter bei ihren Einsätzen (Lieferanten, Reinigungskräfte usw.)	Externe werden nicht begleitet.	5	10	30	20	Reduzierung	6
Mitarbeiter Abteilung Druck	1	2	3	Beeinträchtigung der personalverfügbarkeit	2	Keine Redundanz des strategischen Personals	Der Druckoperator verfügt über einzigartige Fähigkeiten.	5			30	Reduzierung	6
Servicestelle	1	3	2	Rechtsmissbrauch	2	Keine Beaufsichtigung Dritter bei ihren Einsätzen (Lieferanten, Reinigungskräfte usw.)	Externe werden nicht begleitet.	5	10	30	20	Nicht behandelt	30
Servermanagement	1	3	2	Verleugnung von aktionen	3	Fehlende Aufbewahrung von Protokolldaten, die Aufschluss über die Aktivitäten geben	Keine Zentralisierung von Logdateien. Alle Einstellungen sind im Standard belassen.	3		27		Akzeptiert	27
Walzendruckmaschine	1	2	3	Benutzungsfehler	3	Möglichkeit, dass bestimmte Betriebsmittel schädliche Einwirkungen auf das benutzende Personal haben (Arbeiten am Bildschirm, Wellen usw.)	Sehr hoher Lautstärkepegel in der Produktionsabteilung	3	9	18	27	Akzeptiert	27
Gebäude	1	2	3	Entwenden oder Zerstören von Speichermedien, Dokumenten oder Datenträger	2	Das Genehmigungsmanagement weist Mängel auf.	Zugang mit Ausweis. Kein Berechtigungssystem	4	8		24	Nicht behandelt	24
IT-Organisation	1	3	2	Rechtsanmassung	2	Keine regelmäßige Kontrolle der Genehmigungen für den elektronischen Zugang	Die Überprüfung der Benutzerzugriffsrechte im Active Directory wird zwar durchgeführt, bedarf jedoch noch der Prozessdokumentation	4	8	24	16	Reduzierung	6
Datensicherungsmanagement	1	3	2	Entwenden oder Zerstören von Speichermedien, Dokumenten oder Datenträger	2	Die Backup-Datenträger werden nicht an einem geeigneten Ort aufbewahrt.	Die Sicherungen sind nicht verschlüsselt. Die Kassetten werden in einem unverschlossenen Schrank aufbewahrt, da mehrere Abteilungen Zugang zu ihnen haben.	5	10		20	Reduzierung	8
IT-Organisation	1	3	2	Entwenden oder Zerstören von Speichermedien, Dokumenten oder Datenträger	2	Keine regelmäßige Kontrolle der Genehmigungen für den physischen Zugang	Keine regelmäßige Überprüfung.	5	10		20	Reduzierung	0
IT-Raum	1	3	2	Entwenden oder Zerstören von Speichermedien, Dokumenten oder Datenträger	2	Mängel bei der physischen Zugangskontrolle	Die Tür des Serverraums nutzt eine automatische Schließung. Sie wird jedoch nie geschlossen.	5	10		20	Reduzierung	0
Gebäude	1	2	3	Entwenden oder Zerstören von Speichermedien, Dokumenten oder Datenträger	2	Der Least-Privileg-Grundsatz wird nicht angewendet	Keine Zutrittskontrolle	3	6		18	Nicht behandelt	18

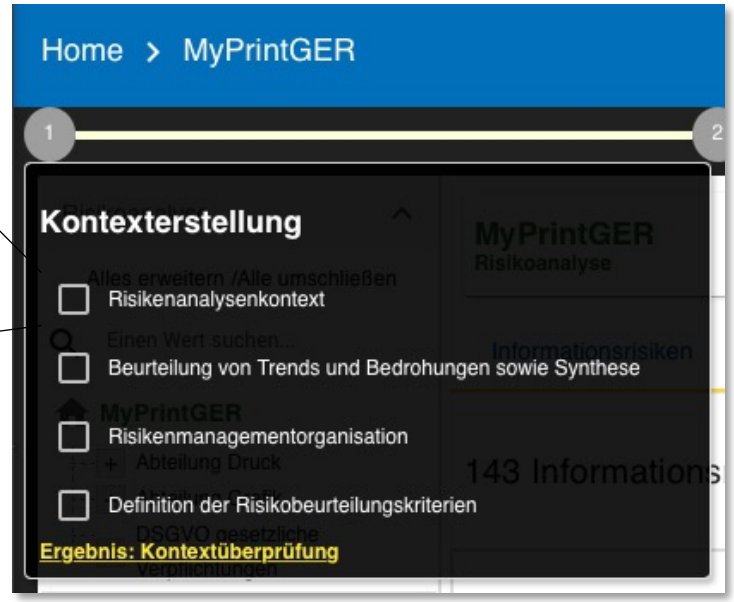
1. Kontexterstellung

- Risikoanalysenkontext
- Beurteilung von Trends und Bedrohungen sowie Synthese
- Risikomanagementorganisation
- Definition der Risikobeurteilungskriterien



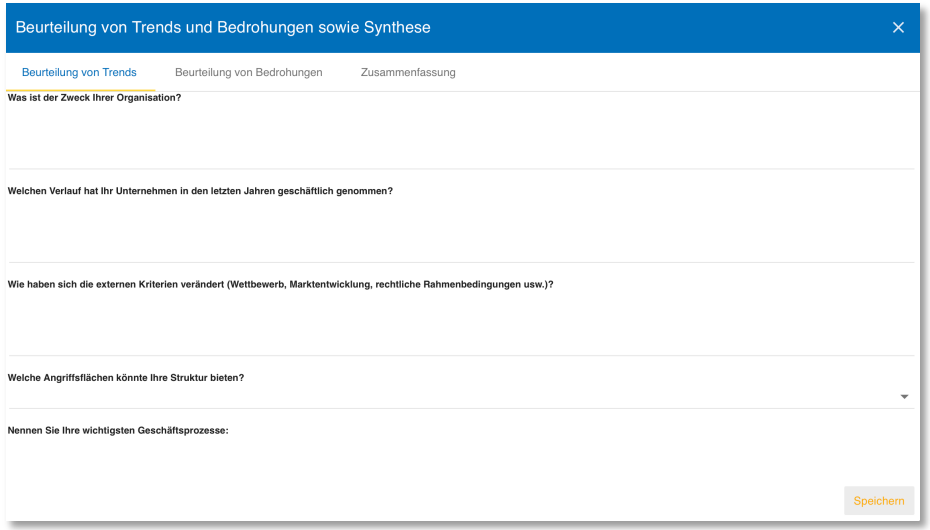
1.1 Risikoanalysekontext

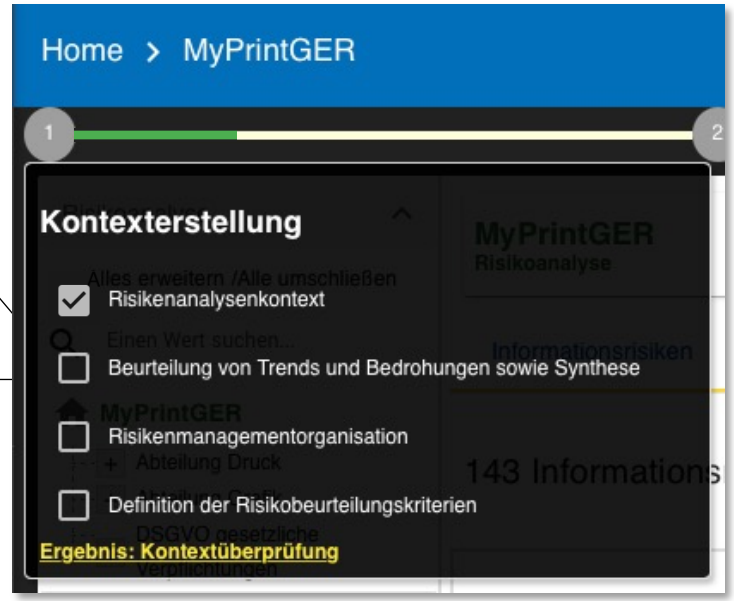




- Definition der Zielorganisation
- Referenz zu ISO 27005:
  - Allgemeine Erwägungen: Kapitel 7.1
  - Risikomanagement-Ansatz: Kapitel 7.2.1
  - Grundlegende Kriterien: Kapitel 7.2.2, 7.2.3, 7.2.4
  - Ziele und Grenzen: Kapitel 7.3, 7.2.3

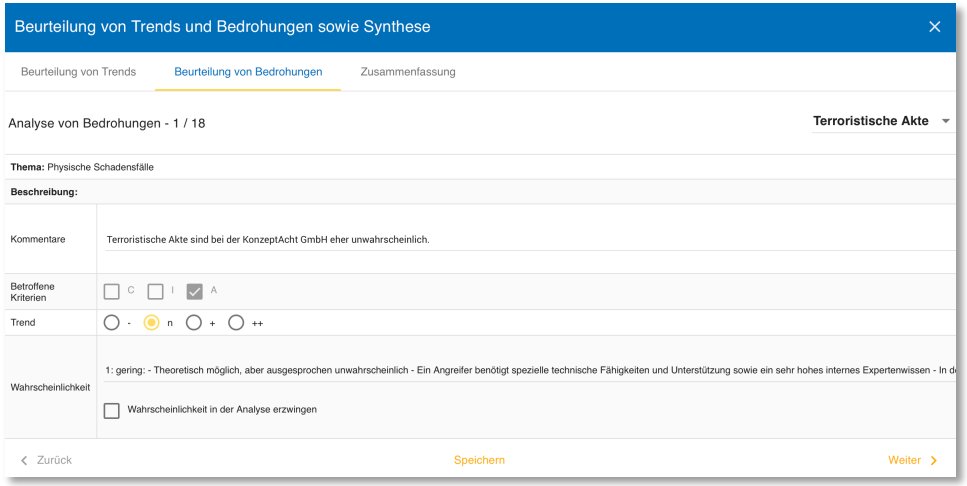
1.2.1 Beurteilung von Trends

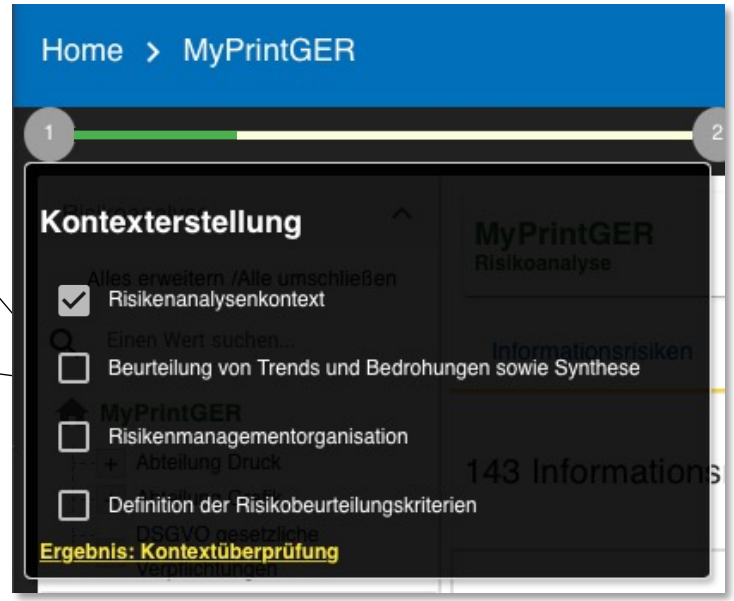




- Allgemeine Fragen zur Ermittlung des Kontexts
- Definieren Sie den Umfang und den Schwerpunkt der Analyse
- Sammlung von Informationen

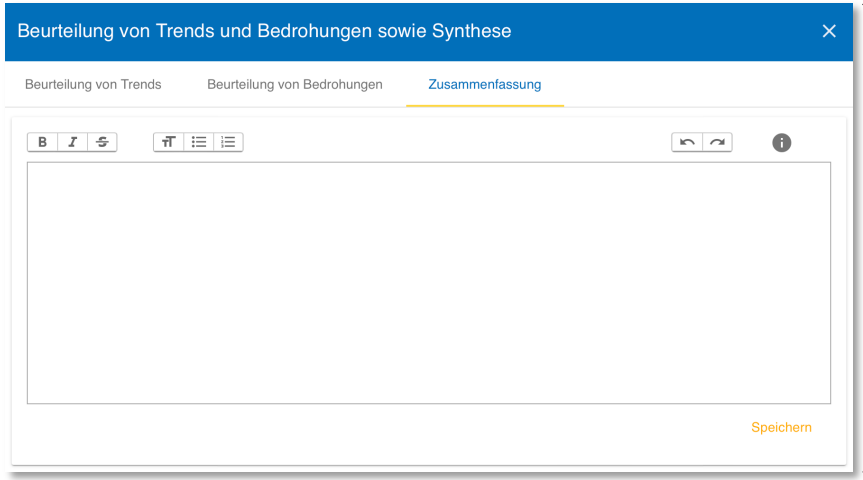
1.2.2 Beurteilung von Bedrohungen

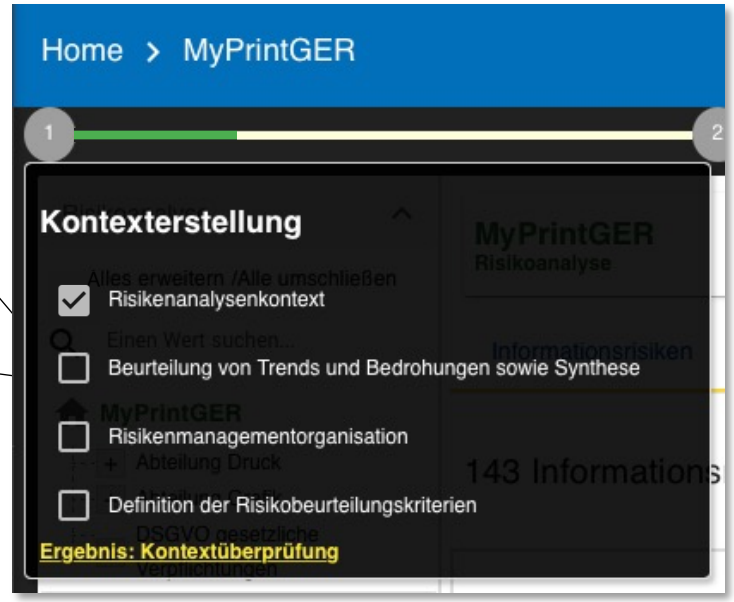




- Bewertung von Bedrohungen vor dem eigenen Kontext
- Sammeln von Informationen aller Beteiligten

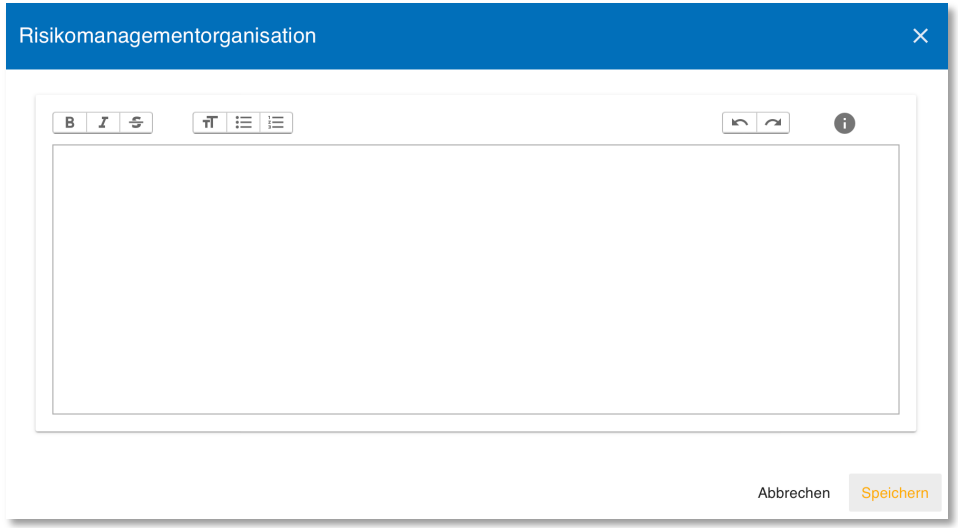
1.2.3 Zusammenfassung

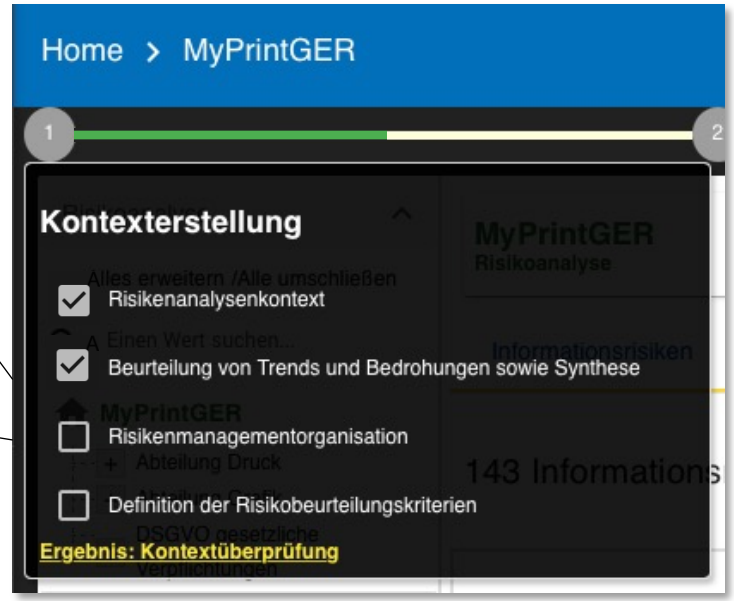




- Zusammenfassung der Ergebnisse von Trends und Bedrohungen
- Abschluss des ersten Arbeitsergebnisses

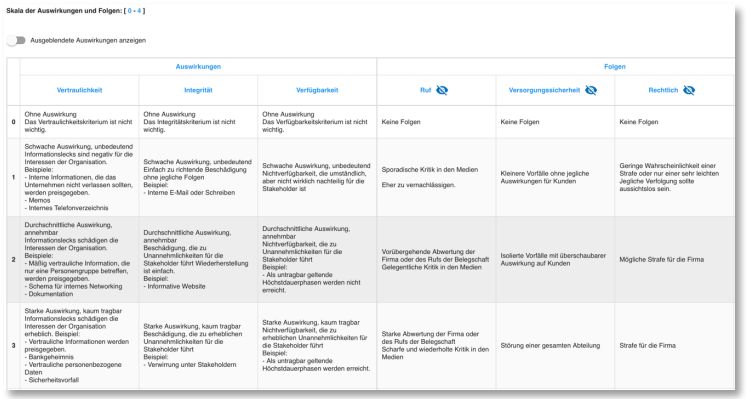
1.3 Risikomanagementorganisation





- Zusätzliche Informationen zur Risikomanagementorganisation
- Referenz zu ISO 27005:
  - Allgemeine Erwägungen: Kapitel 7.4

1.4 Definition der Risikobeurteilungskriterien

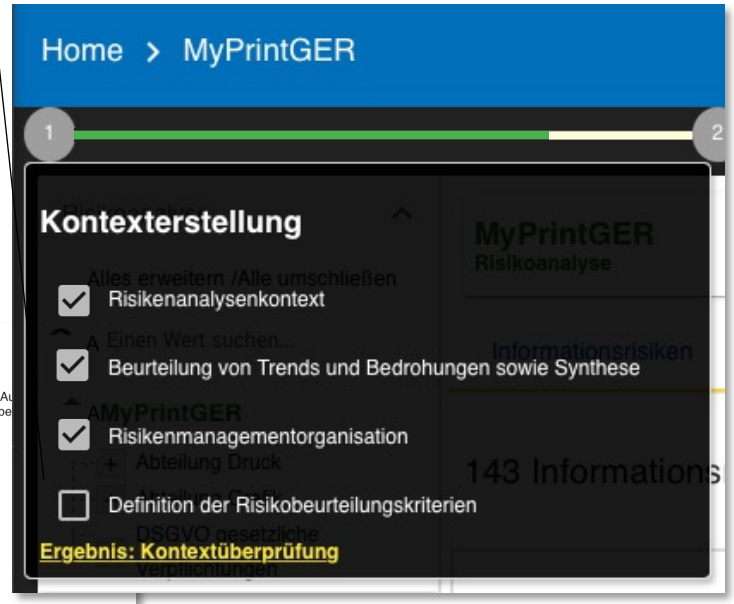


Wahrscheinlichkeitsskala: [0 - 4]

0. Unmöglich
1. Sehr unwahrscheinlich: Bei KonzeptAcht nie aufgetreten, erfordert ein hohes Niveau an Fachwissen oder ist kostspielig bei der Au
2. Unwahrscheinlich: hätte auftreten können, seltenes Phänomen, das ein gutes Niveau an Fachwissen erfordert oder kostspielig be
3. Könnte gelegentlich auftreten, vermutlich einmal in 5 Jahren
4. Sehr wahrscheinlich: einfach auszuführen, keine nennenswerte Investitionen oder Kenntnisse erforderlich

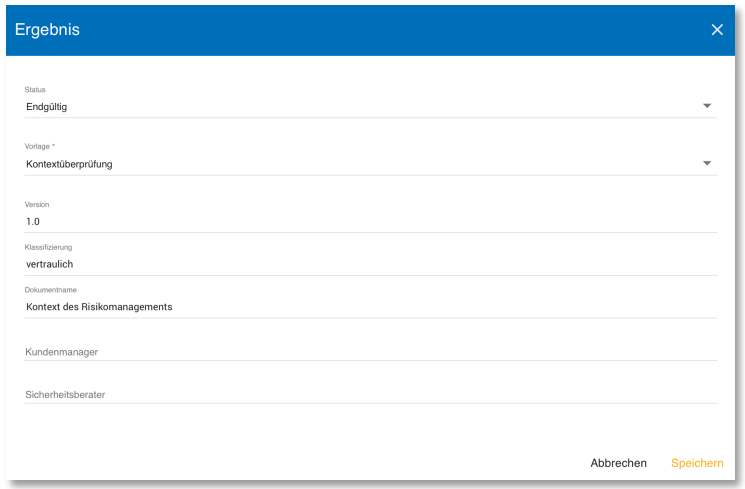
Qualifizierungsskala: [0 - 5]

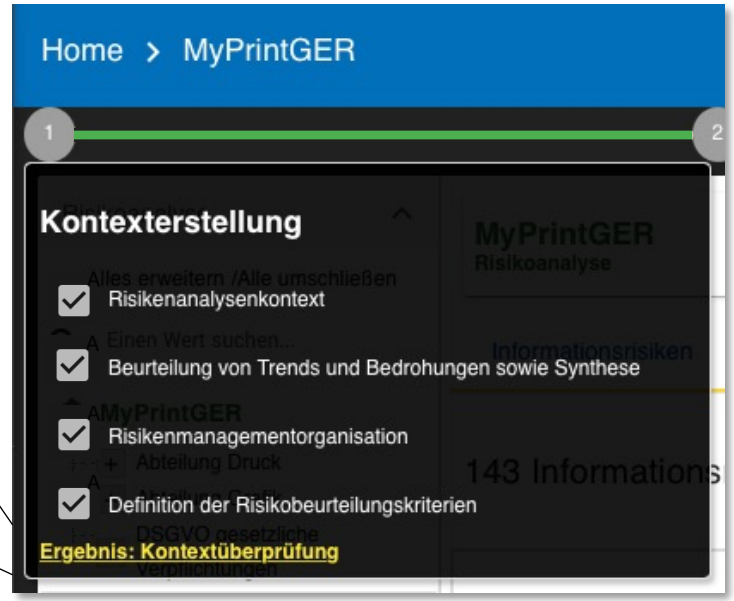
0. Keine Sicherheitsrisiken
1. Sehr geringes Sicherheitsrisiko: Einige effiziente Maßnahmen wurden bereits getroffen und ihre Effizienz wird kontrolliert.
Sehr hoher Reifegrad: Bewährte Verfahrensweisen sind implementiert und werden häufig überprüft.
2. Geringes Sicherheitsrisiko: Einige effiziente Maßnahmen wurden bereits getroffen.
Hoher Reifegrad: Bewährte Verfahrensweisen sind implementiert.
3. Durchschnittliches Sicherheitsrisiko: Einige Maßnahmen wurden bereits ergriffen, könnten jedoch besser sein.
Durchschnittlicher Reifegrad: Bewährte Verfahrensweisen sind implementiert ohne Suche nach einem besseren Weg.
4. Hohes Sicherheitsrisiko: Einige Maßnahmen wurden bereits ergriffen, sind jedoch ineffizient oder ungeeignet.
Niedriger Reifegrad: Bewährte Verfahrensweisen sind nicht implementiert, aber es gibt einige positive unüberlegt Reaktionen.
5. Sehr hohes Sicherheitsrisiko: Maßnahmen wurden nicht implementiert.
Sehr niedriger Reifegrad oder völlig fehlender Reifegrad



- Referenz zu ISO 27005:
  - Organisation of risk management: Kapitel 7.2,2, 7.2.3, 7.2.4

1.5 Ergebnis: Kontextüberprüfung





- Sammlung aller Informationen aus der Kontexterstellung
- Ziel: Validierung des Kontextes vor der Risikoidentifikation beginnt
- Format: MS Word

1. Kontexterstellung - Übung

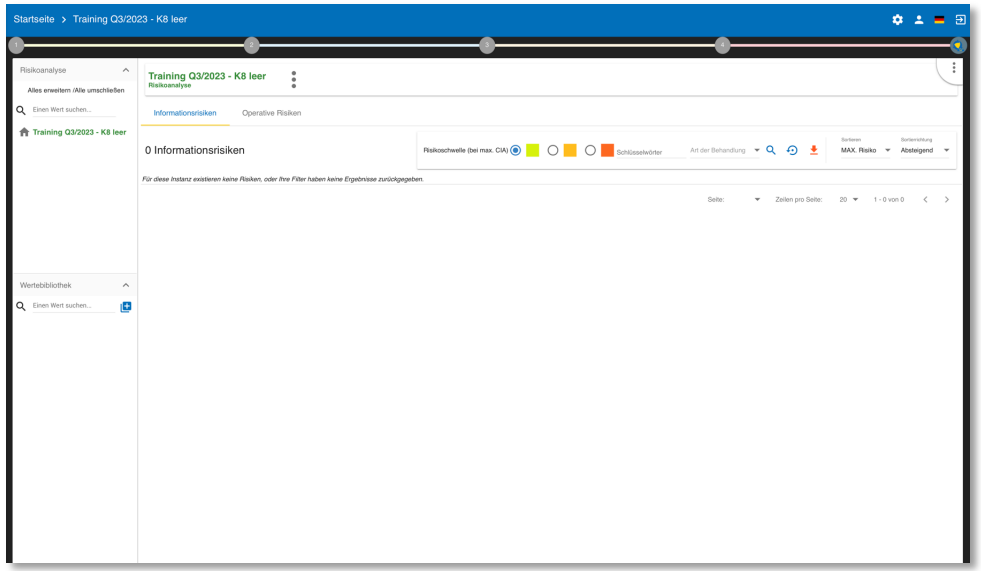
Übung: Durchführen der Kontexterstellung (30 Minuten)

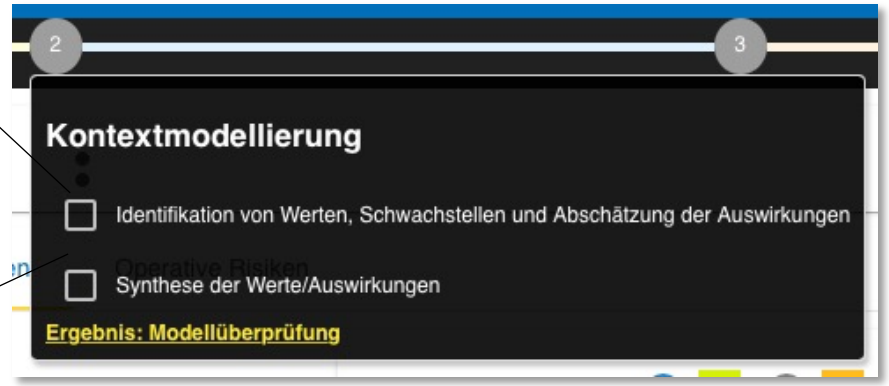
- **Ziel**: Definition des eigenen Kontext
- **Vorgaben**:
  - Risikoanalysekontext: *<individuell>*
  - Beurteilung von Trends: *<individuell>*
  - Beurteilung von Bedrohungen: *<individuell>*
  - Zusammenfassung: *<individuell>*
  - Risikomanagementorganisation: *<individuell>*
  - Definition der Risikobeurteilungskriterien: *<individuell>*
  - Erstellung eines eigenen Reports

2. Kontextmodellierung

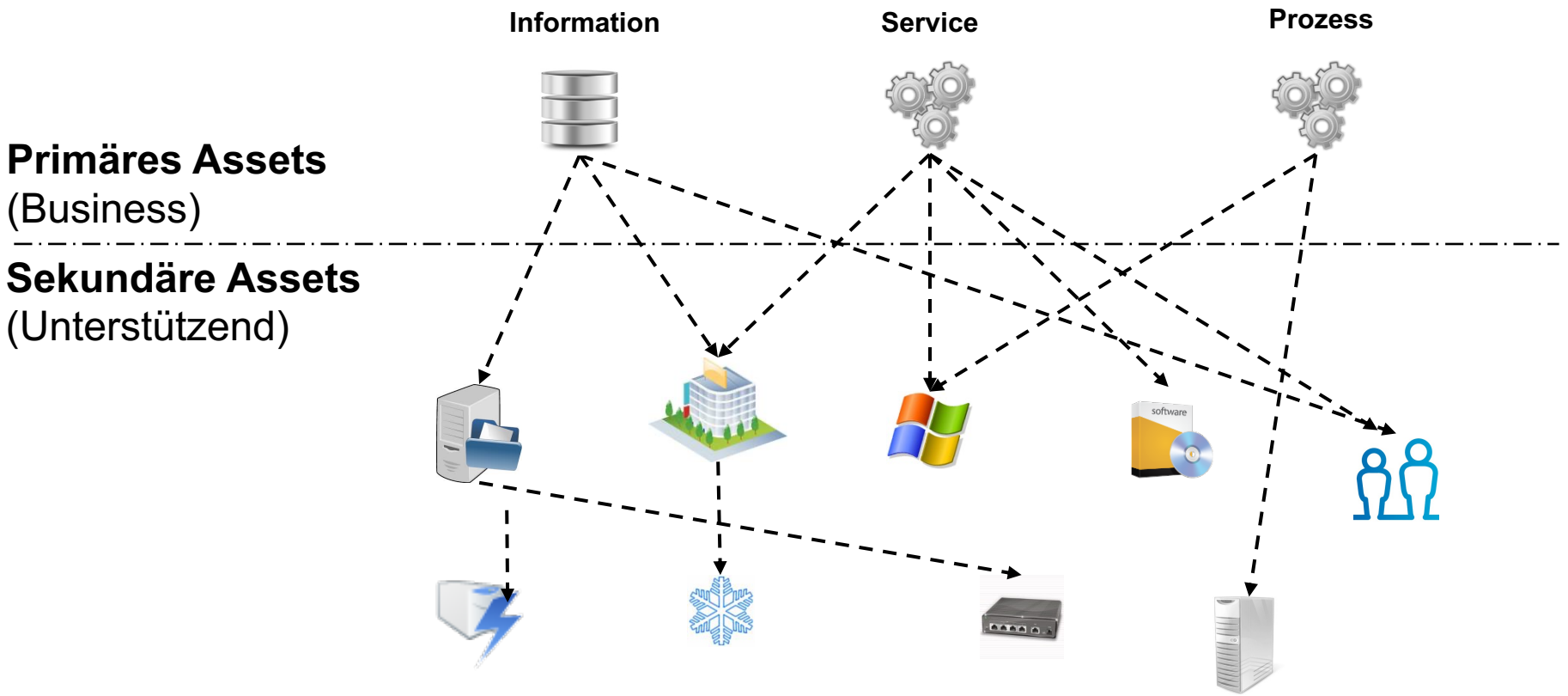
- Identifikation von Werten, Schwachstellen und Abschätzung der Auswirkungen
- Synthese der Werte/Auswirkungen

2.1 Identifikation von Werten, Schwachstellen und Abschätzung der Auswirkungen





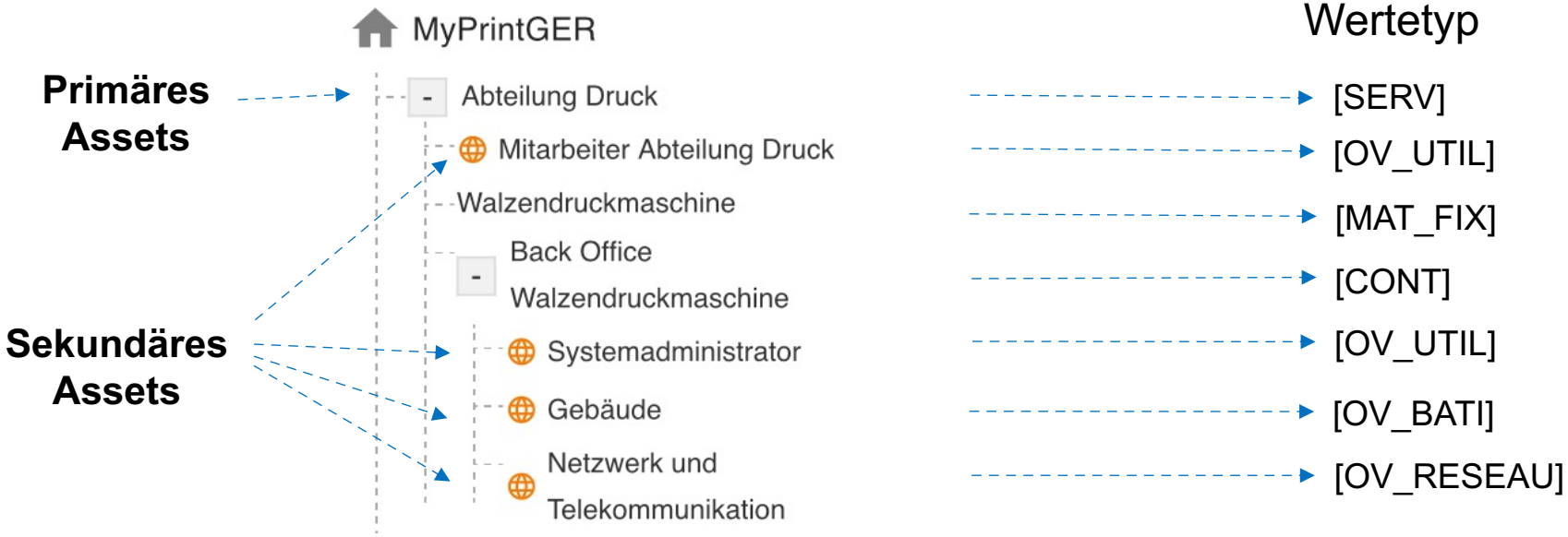
2.1 Identifikation von Werten, Schwachstellen und Abschätzung der Auswirkungen



Die Bewertung der Vertraulichkeit, Integrität und Verfügbarkeit wird von den primären Assets auf die sekundären Assets vererbt.

2.1 Die Modellierung in MONARC

Hierarchie der Assets



OV_BATI

Bedrohung	Sicherheitsrisiko
Entwenden oder Zerstören von Speichermedien, Dokumenten oder Datenträger	Mängel bei der physischen Zugangskontrolle
Entwenden oder Zerstören von Speichermedien, Dokumenten oder Datenträger	Der Least-Privileg-Grundsatz wird nicht angewendet
Entwenden oder Zerstören von Speichermedien, Dokumenten oder Datenträger	Das Genehmigungsmanagement weist Mängel auf.
Rechtsmissbrauch	Keine Beaufsichtigung Dritter bei ihren Einsätzen (Lieferanten, Reinigungskräfte usw.)
Umweltkatastrophe (Feuer, Überschwemmung, Staub, Smutz, etc.)	Die Räumlichkeiten sind nicht gesichert bzw. können von fremden Personen betreten werden.

2.1 „Lokale“ und „Globale“ Assets

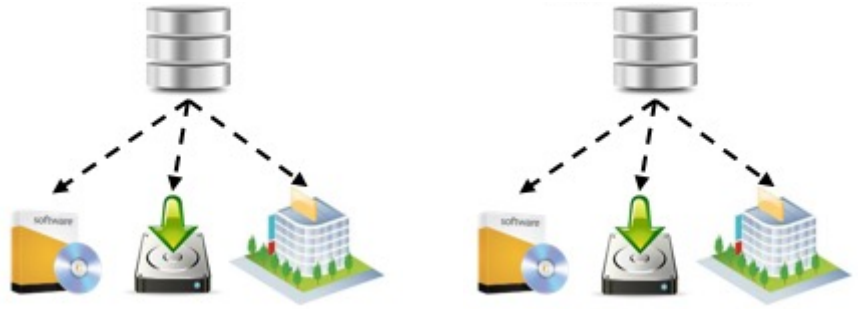
“Lokal”

Meine Risikoanalyse

- Datenbank #1
  - Software
  - Backup NAS
  - Serverraum
- Datenbank #2
  - Software
  - Backup NAS
  - Serverraum

30 Risiken

Datenbank #1 Datenbank #2



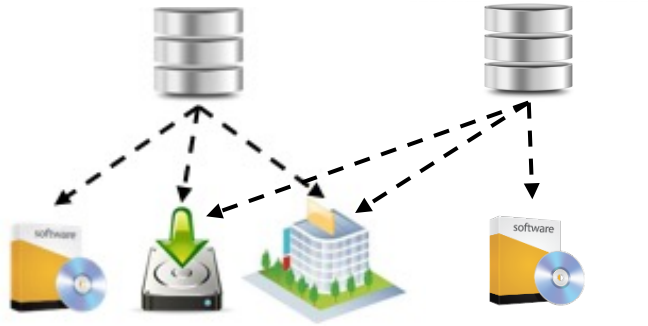
“Global”

Meine Risikoanalyse

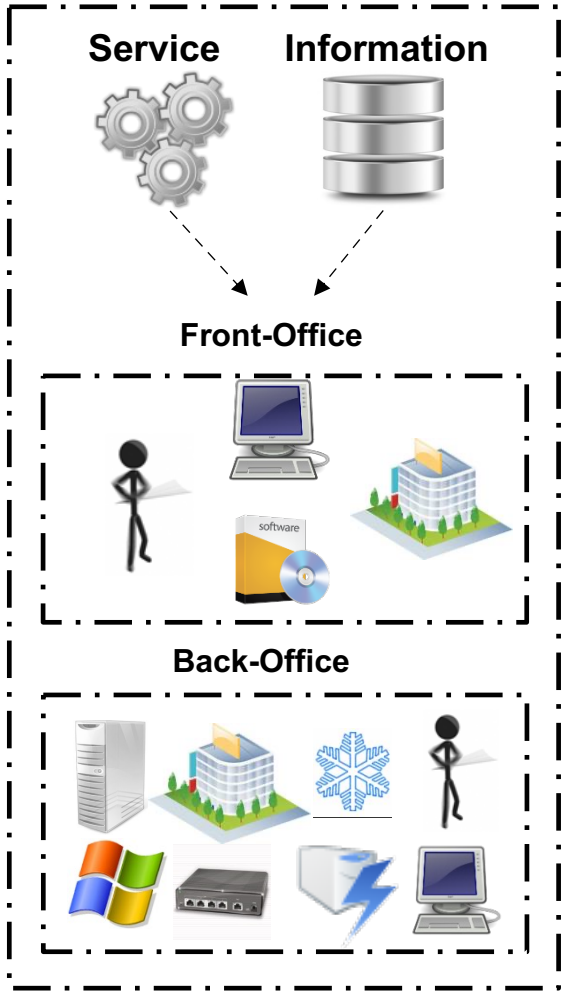
- Datenbank #1
  - Software
  - Backup NAS
  - Serverraum
- Datenbank #2
  - Software
  - Backup NAS
  - Serverraum

21 Risiken

Datenbank #1 Datenbank #2

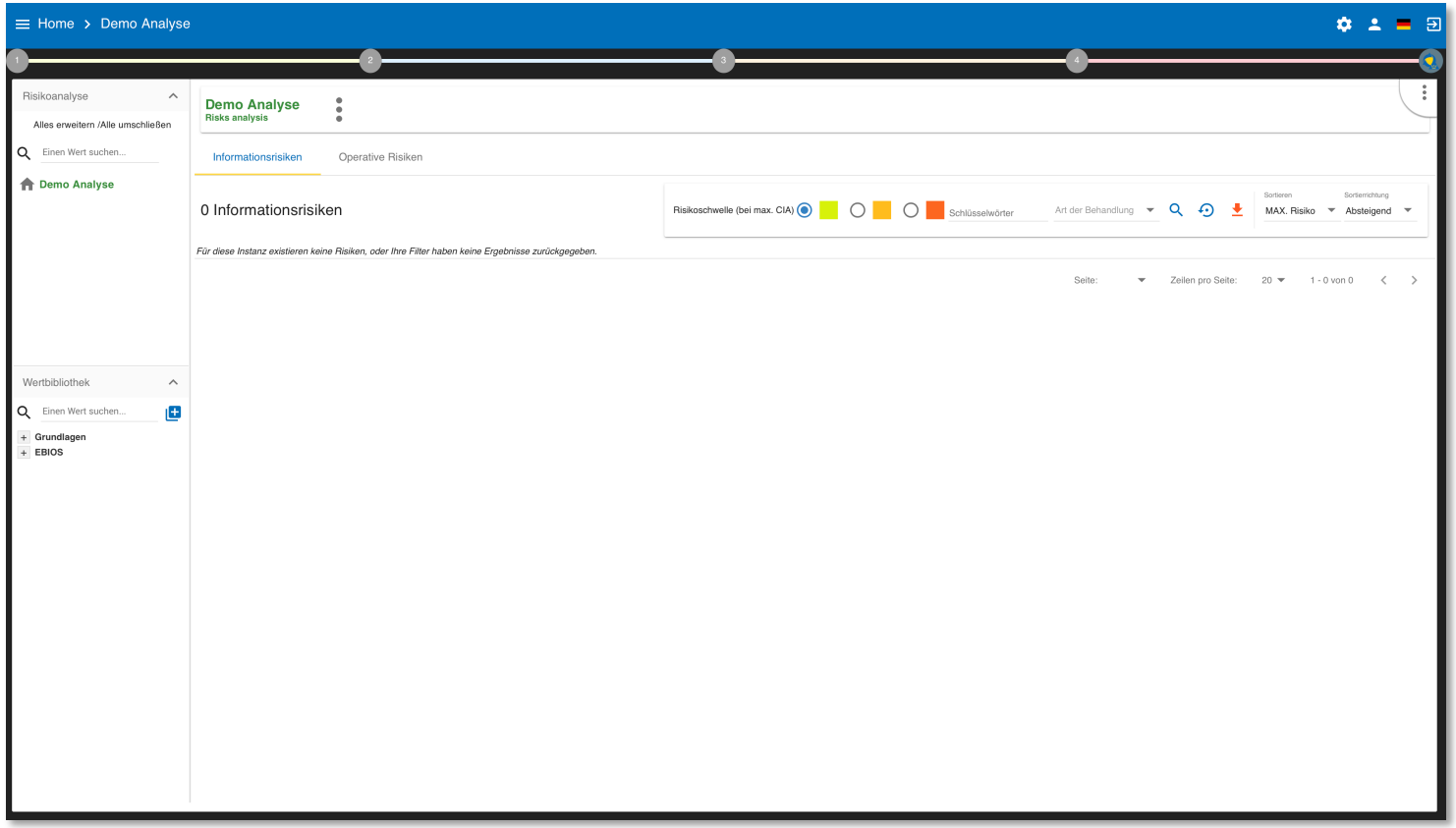


2.1 CASES Modellierung



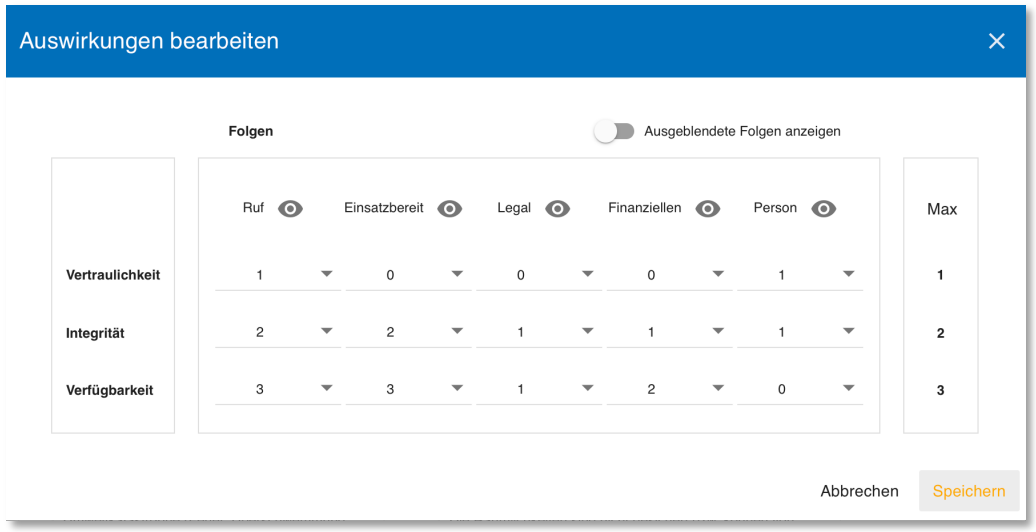
- MyPrintGER
  - Abteilung Druck
    - Mitarbeiter Abteilung Druck
    - Walzendruckmaschine
    - Back Office Walzendruckmaschine
      - Systemadministrator
      - Gebäude
      - Netzwerk und Telekommunikation
  - Abteilung Grafik
    - Frontoffice
      - Servicestelle
      - Mitarbeiter
      - Benutzer-Arbeitsstationen
      - Spezifische Software
    - Backoffice
      - Gebäude
      - IT-Raum
      - Systemadministrator
      - Administrator-Arbeitsstationen
      - Servermanagement
      - Datensicherungsmanagement
      - Netzwerk und Telekommunikation
      - IT-Organisation
      - Softwareentwicklung

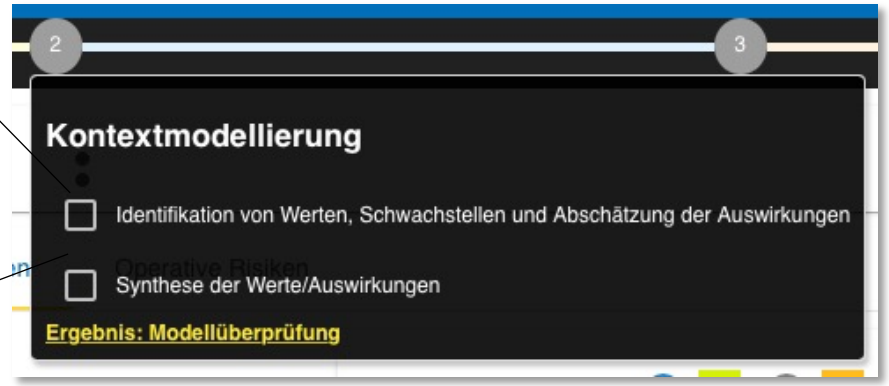
2.1 Identifikation von Werten, Schwachstellen und Abschätzung der Auswirkungen



- Hauptansicht von MONARC
- Erstellung eines Risikomodells
- Referenz zu ISO 27005:
  - Identification of assets: Kapitel 8.2.2
  - Identification of vulnerabilities: Kapitel 8.2.5

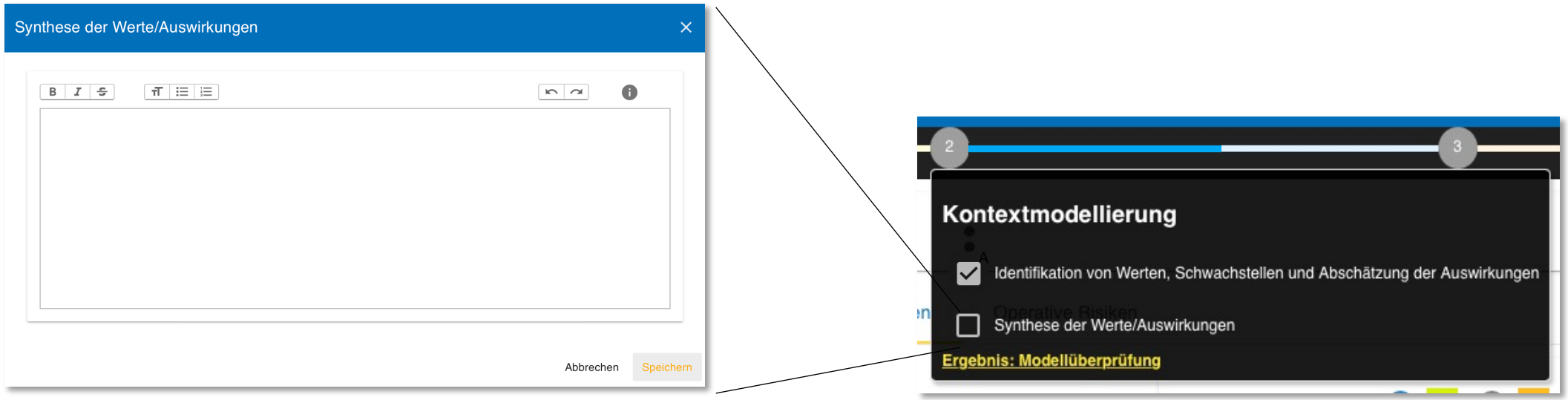
2.1 Identifikation von Werten, Schwachstellen und Abschätzung der Auswirkungen





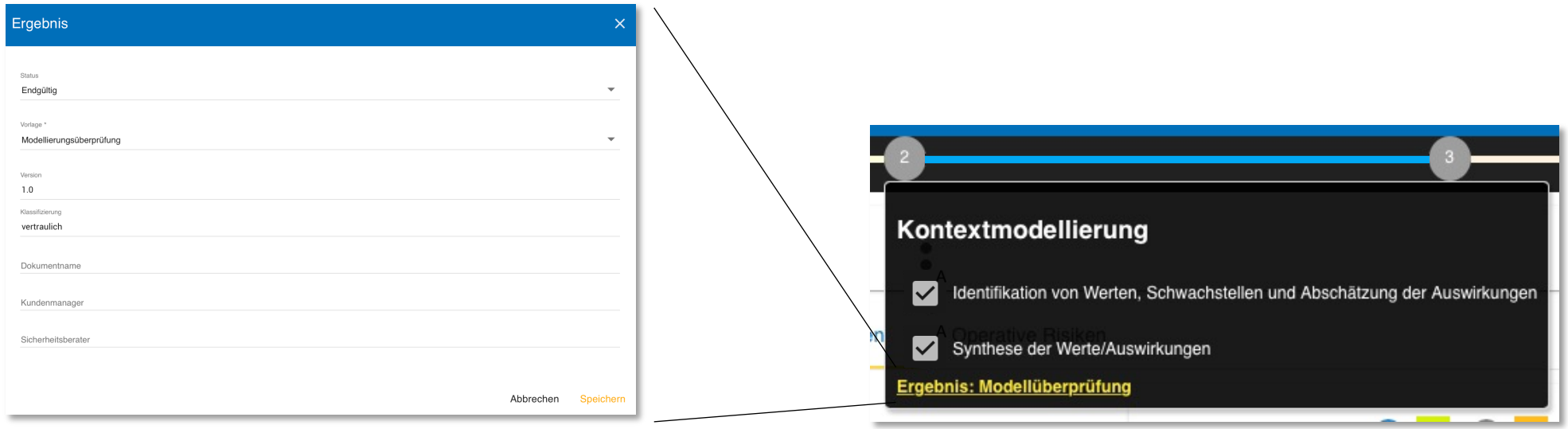
- Hauptansicht von MONARC
- Auswirkungen bearbeiten
- Referenz zu ISO 27005:
  - Identification of assets: Kapitel 8.3.2

2.2 Synthese der Werte/Auswirkungen



- Eigene Zusammenfassung der Identifikation von Werten, Schwachstellen und Auswirkungen
- Zur Vervollständigung der Ergebnisse gedacht.

2.3 Ergebnis: Kontextüberprüfung



- Enthält:
  - Wichtige, primären Assets des Modells
  - Die Synthese von Vermögenswerten und Auswirkungen
- Ziel: Überprüfung der Modellierung
- Format: MS Word

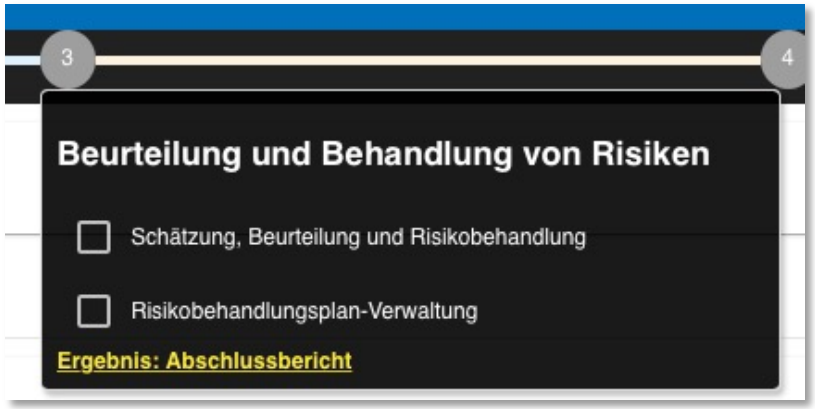
2. Kontextmodellierung - Übung

Übung: Durchführen der Kontextmodellierung (30 Minuten)

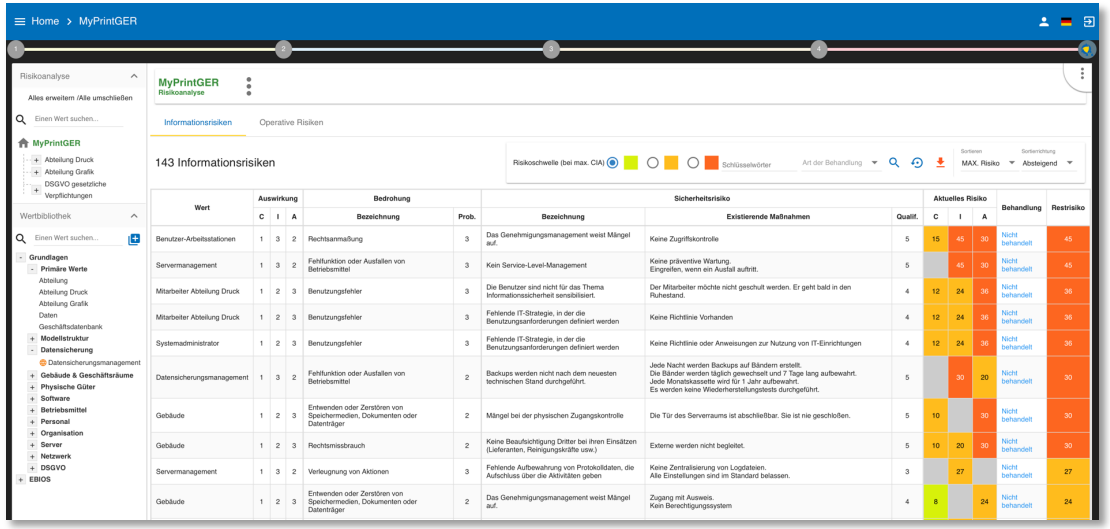
- **Ziel**: Definition des eigenen Kontext
- **Vorgaben**:
  - Anlagen eigener
    - Lokaler und globaler Assets: *<individuell>*
    - Clonen von Assets: *<individuell>*
    - Asset-Kategorien: *<individuell>*
  - Modellierung von Abhängigkeiten: *<individuell>*
  - Erstellen der Risikoanalyse per Drag & Drop: *<individuell>*
  - Bewertung von Auswirkungen: *<individuell>*
  - Erstellung eines eigenen Reports

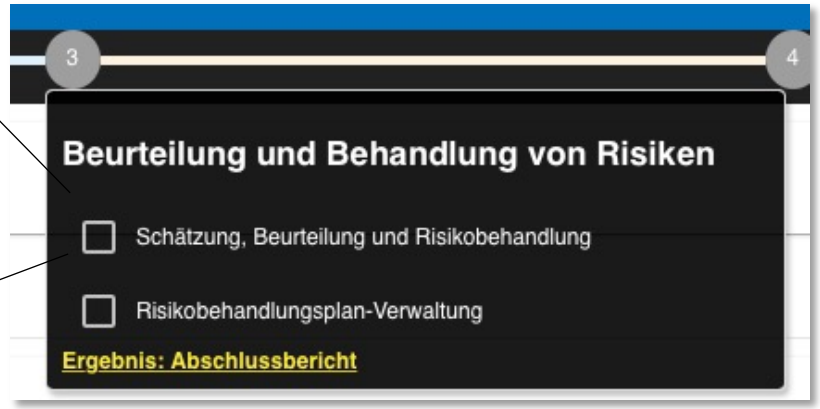
3. Beurteilung und Behandlung von Risiken

- Schätzung, Beurteilung und Risikobehandlung
- Risikobehandlungsplan-Verwaltung



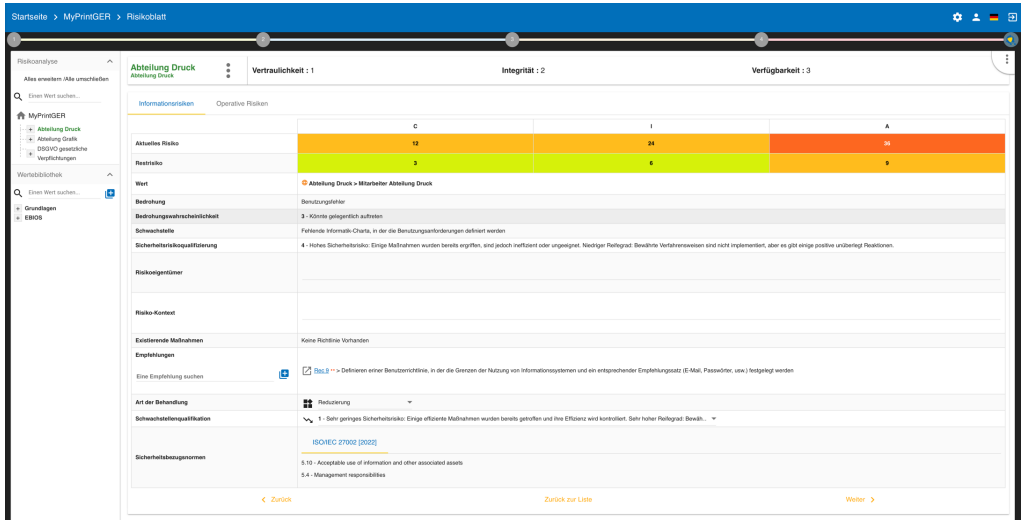
3.1 Schätzung, Beurteilung und Risikobehandlung

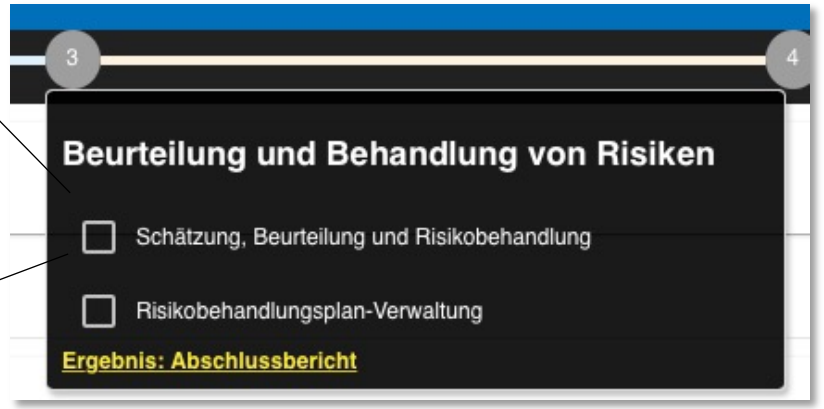




- Hauptansicht von MONARC
- Alle Risiken bewerten

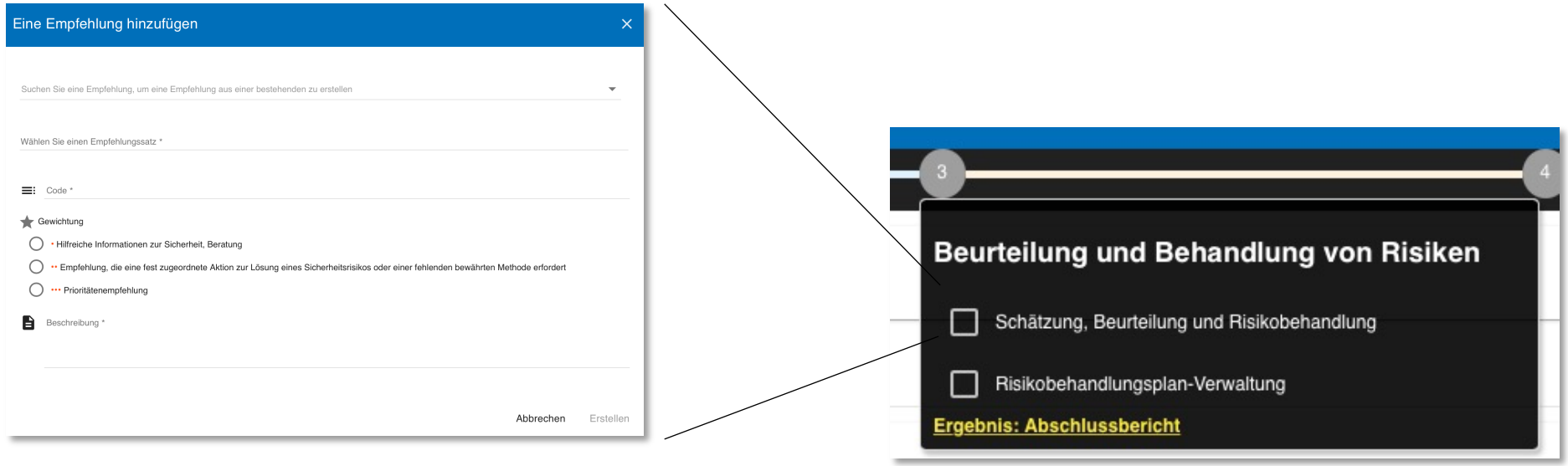
3.1 Schätzung, Beurteilung und Risikobehandlung





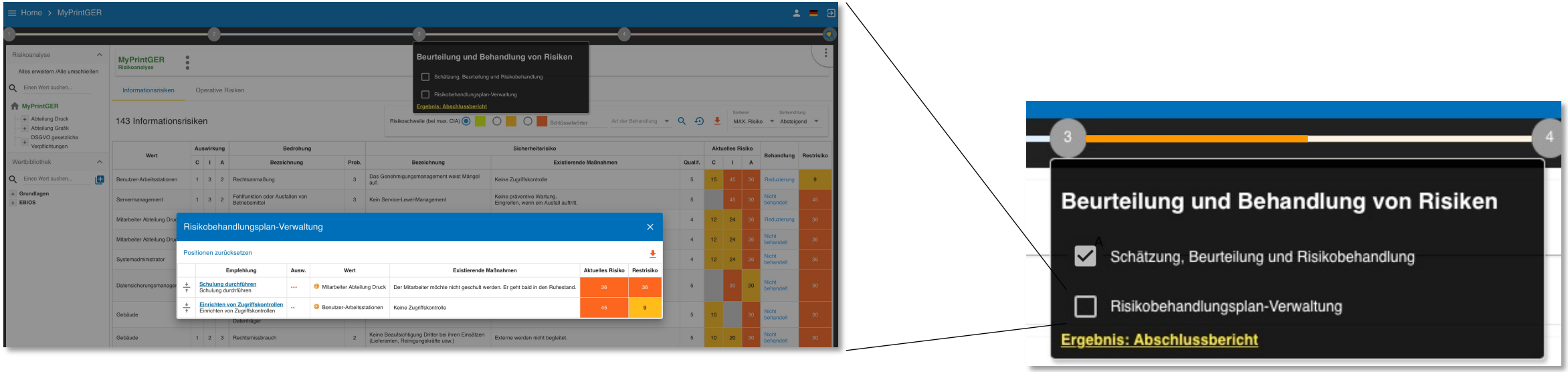
- Aktuelles Risiko und Restrisiko
- Risikobehandlung

3.1 Schätzung, Beurteilung und Risikobehandlung



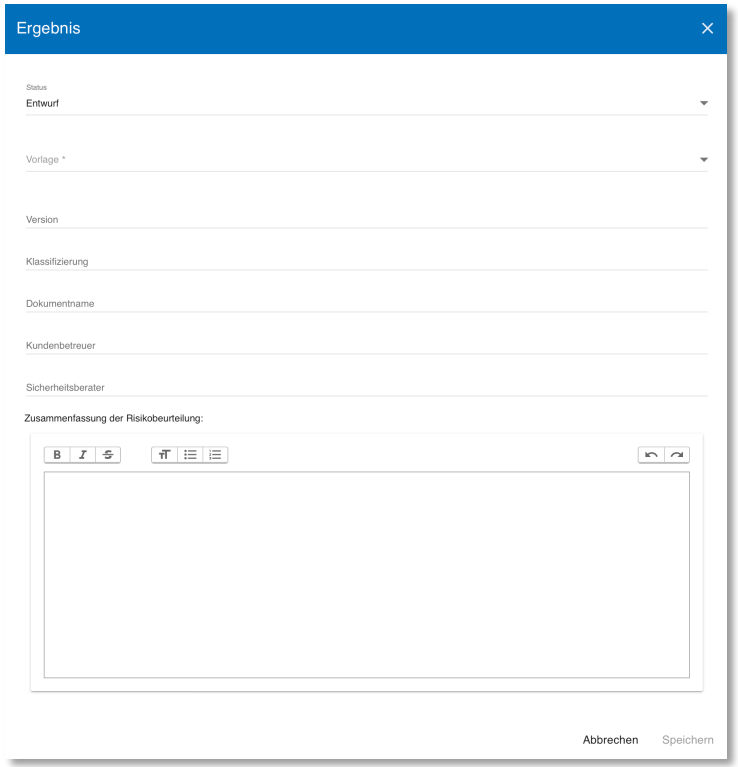
- Anlegen einer Maßnahme

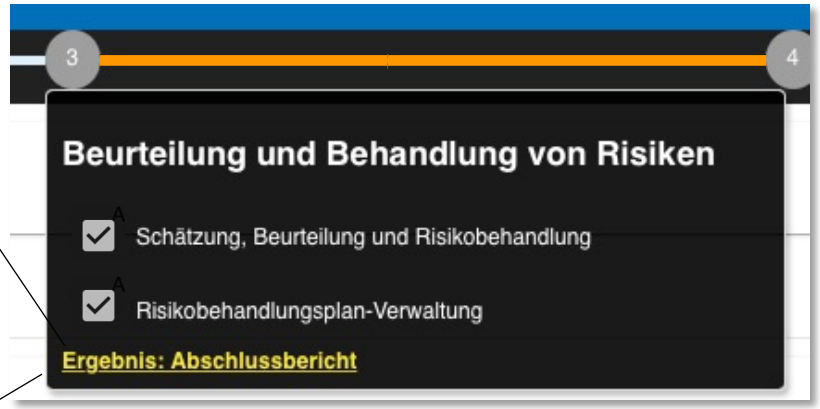
3.2 Risikobehandlungsplan-Verwaltung



- Liste aller Risiken, für die bereits eine Maßnahmen definiert wurde

3.3 Ergebnis: Abschlussbericht





- Zusammenfassung aller Risiken und bisherigen Informationen inkl. eigener Zusammenfassung
- Ziel: Abschlussbericht der Phasen 1 - 3
- Format: MS Word

3. Beurteilung und Behandlung von Risiken - Übung

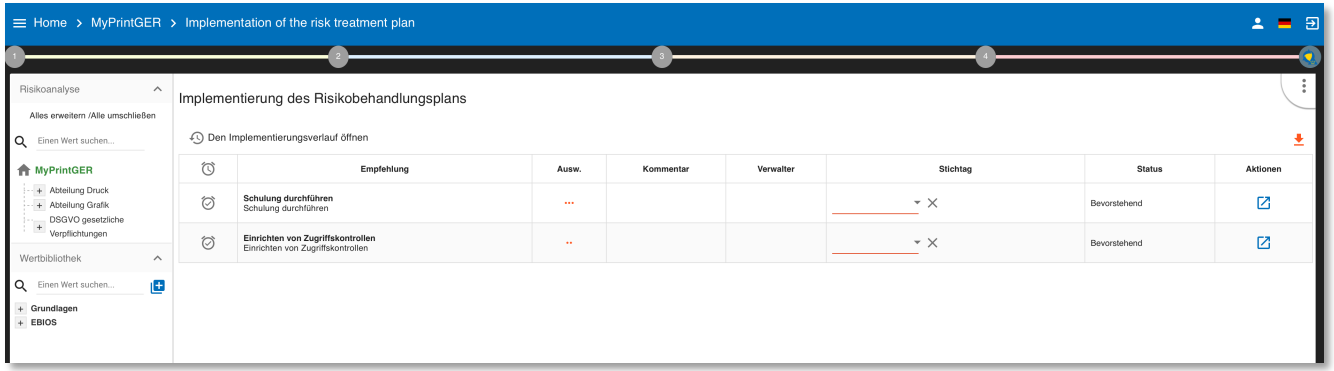
Übung: Durchführen der Beurteilung und Behandlung von Risiken (30 Minuten)

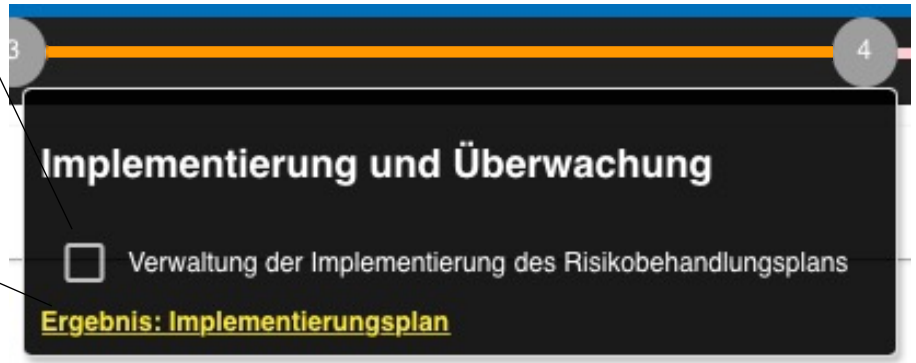
- **Ziel**: Durchführen einer eigenen Risikobeurteilung mit Behandlungsmaßnahmen
- **Vorgaben**:
  - Nennung existierender Maßnahmen: *<individuell>*
  - Beurteilung des Reifegrads existierender Maßnahmen: *<individuell>*
  - Auswahl der Risikobehandlung: *<individuell>*
  - Anlegen von Maßnahmen / Empfehlungen: *<individuell>*
  - Bestimmen des Restrisikos: *<individuell>*
  - Erstellung eines eigenen Reports

4. Implementierung und Überwachung

- Verwaltung der Implementierung des Risikobehandlungsplans

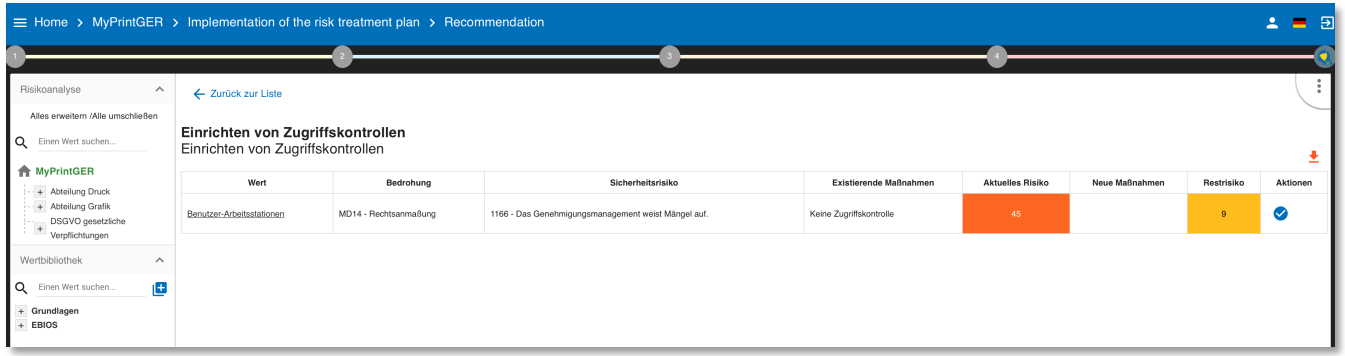
4.1 Verwaltung der Implementierung des Risikobehandlungsplans

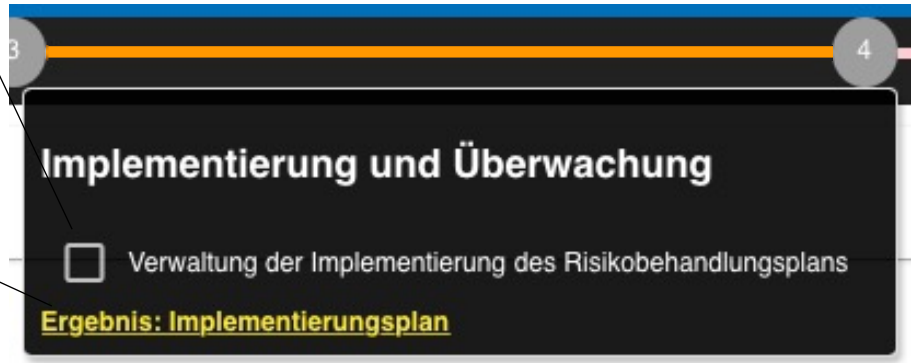




- Festlegen eines Verantwortlichen
- Hinterlegen von Kommentaren
- Definition eines Stichtages
- Verifikation des Umsetzungsstatus

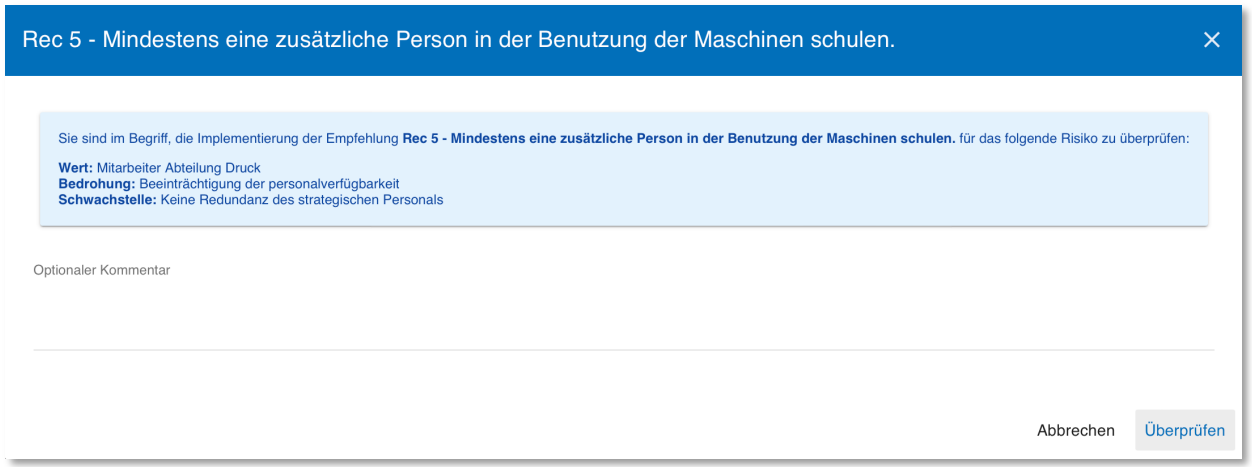
4.1 Verwaltung der Implementierung des Risikobehandlungsplans

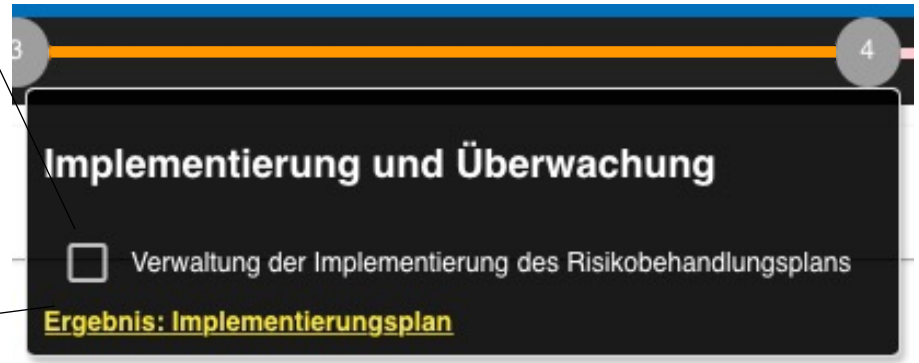




- Änderung des Risikos:
  Das „Restrisiko“ wird zum „aktuellen Risiko“
- Die „neue Maßnahme“ wird zur „existierenden Maßnahme“

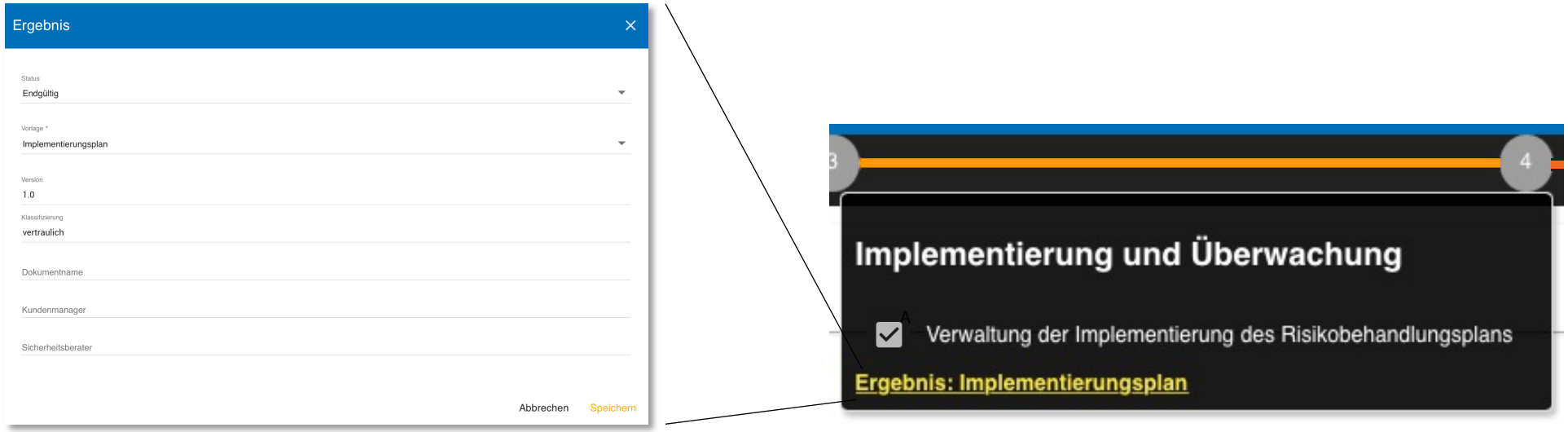
4.1 Verwaltung der Implementierung des Risikobehandlungsplans





- Hinweis: Nach Abschluss einer Maßnahme erhält das Risiko den Status „Nicht behandelt“

4.2 Ergebnis: Implementierungsplan



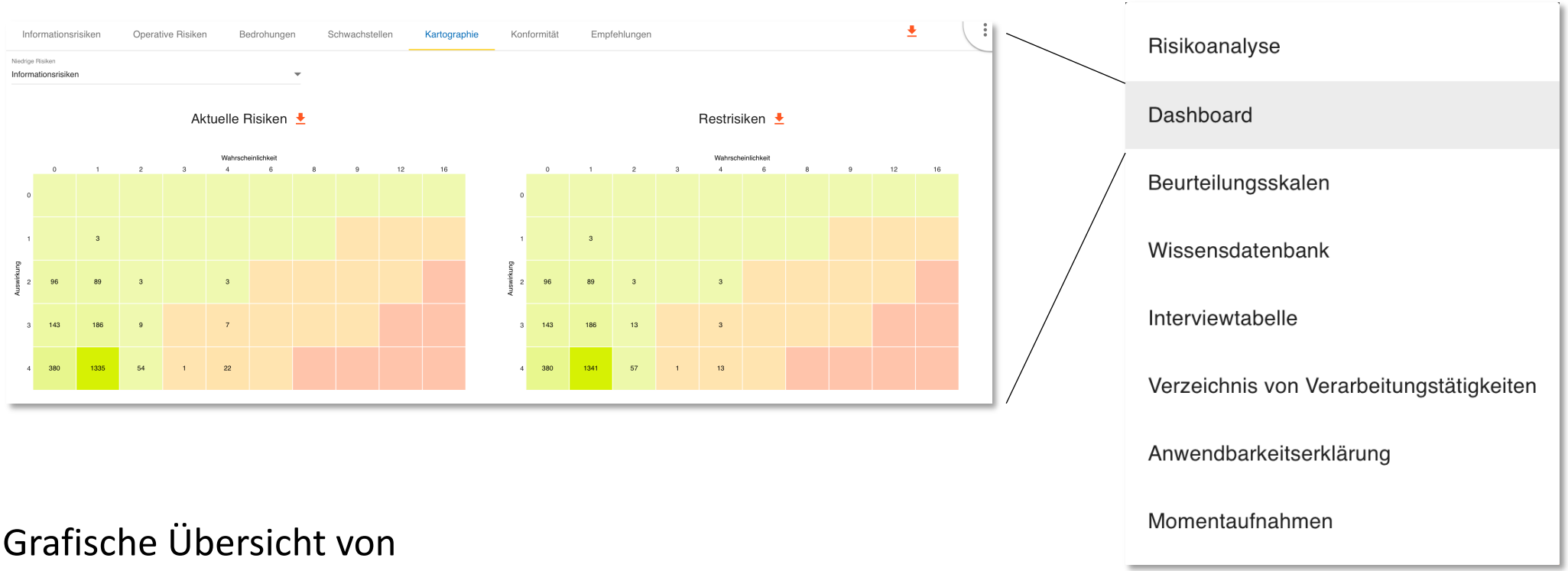
- Zusammenfassung des Risikobehandlungsplanes
- Aufstellung der bereits umgesetzten Maßnahmen
- Ziel: Offizieller Bericht zur Risikobehandlung
- Format: MS Word

4. Implementierung und Überwachung - Übung

Übung: Implementierung und Überwachung von Maßnahmen (30 Minuten)

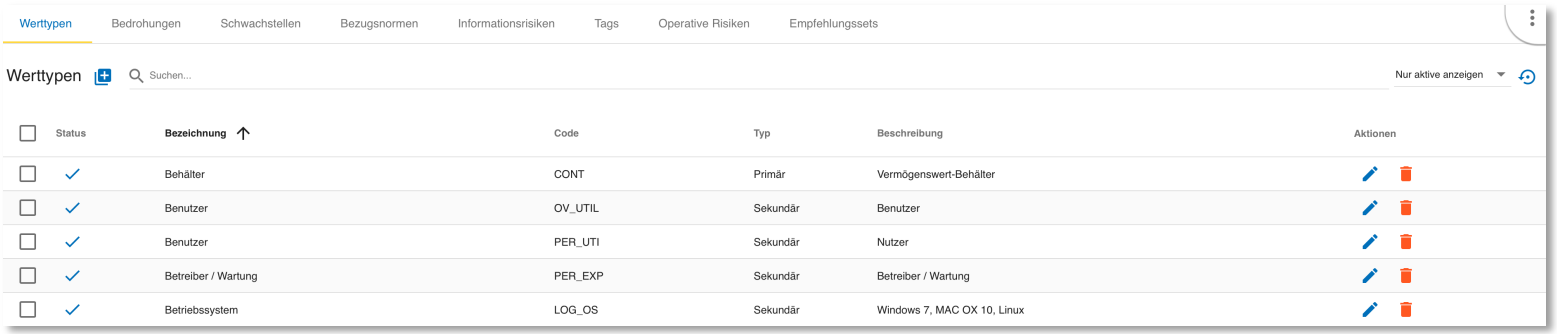
- **Ziel**: Durchführen einer eigenen Maßnahmenplanung und Umsetzung
- **Vorgaben**:
  - Import der einheitlichen Testumgebung: `MyPrintGER.json`
  - Bestimmung eigener Maßnahmenplanungen: *<individuell>*
  - Umsetzung von Maßnahmen dokumentieren: *<individuell>*
  - Erstellung eines eigenen Reports

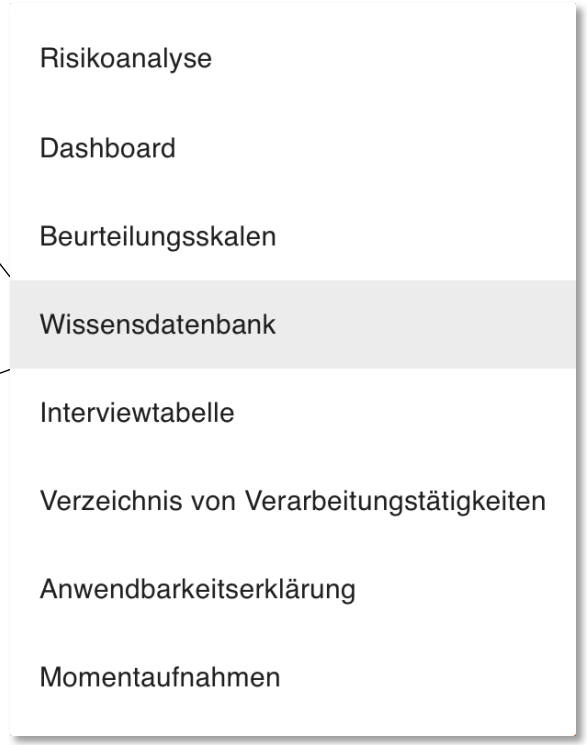
MONARC - Dashboard



- Grafische Übersicht von
  - Informationsrisiken, Operative Risiken, Bedrohungen, Schwachstellen, Kartographie, Konformität, Empfehlungen

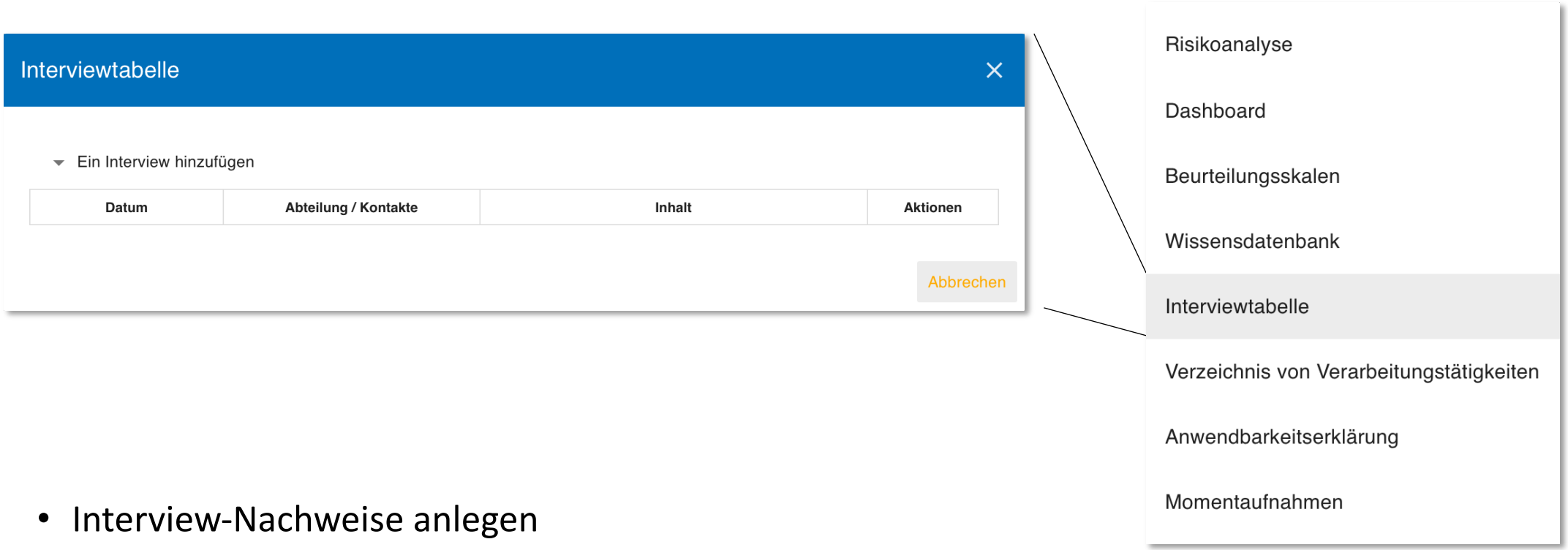
MONARC - Wissensdatenbank





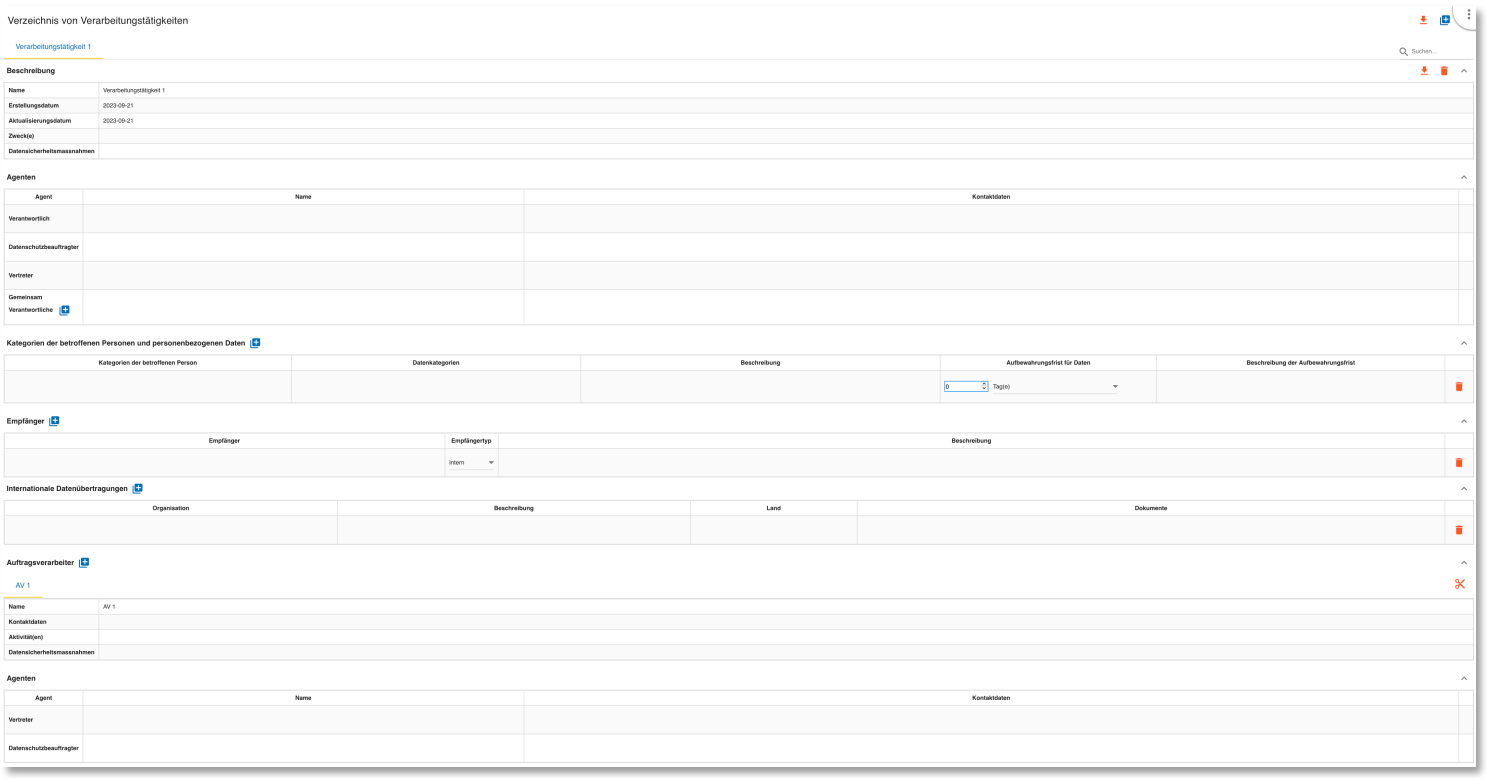
- Wissensdatenbank mit
  - Wertetypen, Bedrohungen, Schwachstellen, Bezugsnormen, Informationsrisiken, Tags, Operative Risiken, Empfehlungssets

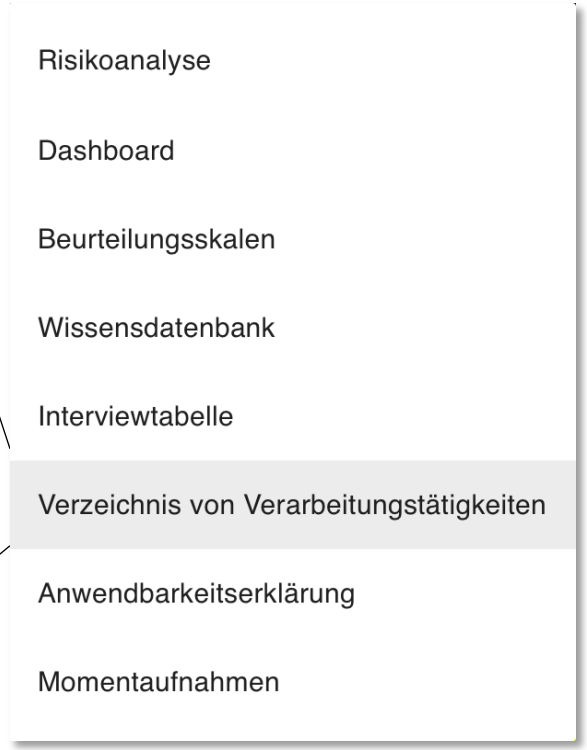
MONARC - Interviewtabelle



- Interview-Nachweise anlegen
- Nachweis für die Erhebung von Informationen

MONARC - Verzeichnis Verarbeitungstätigkeiten

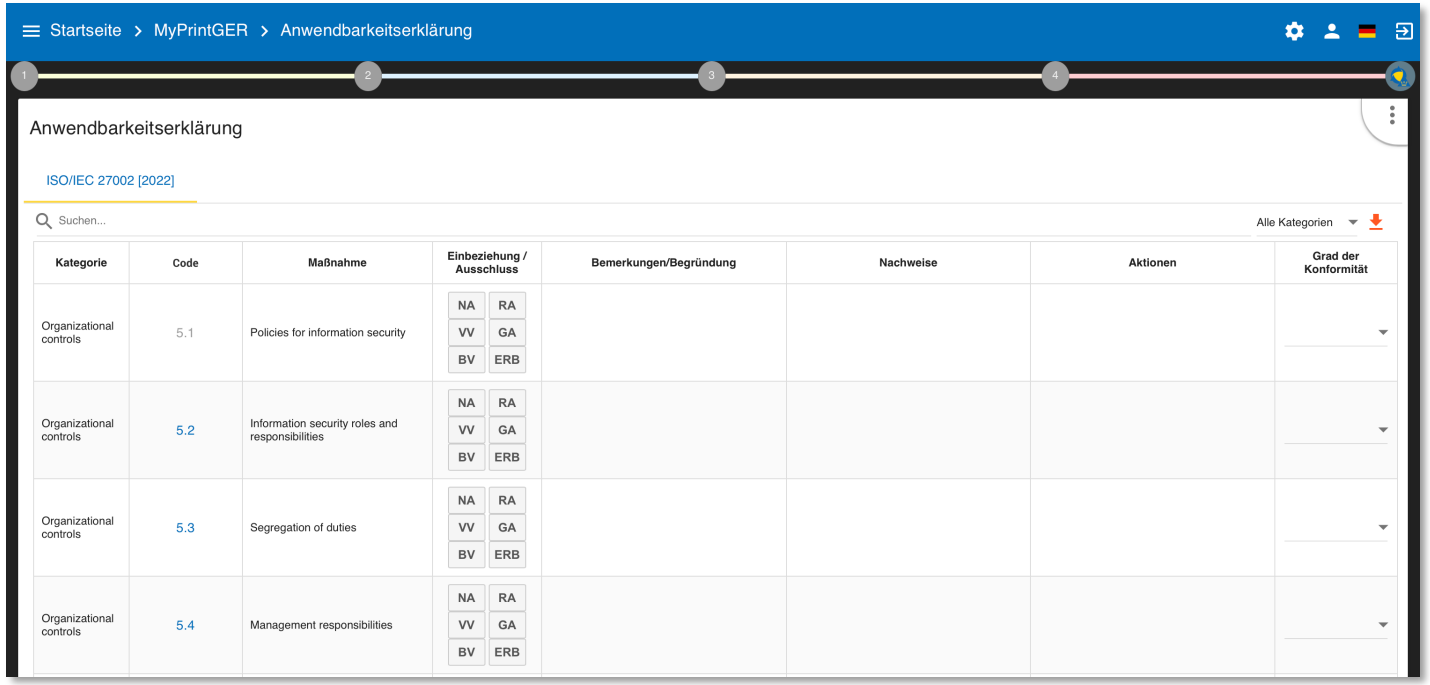


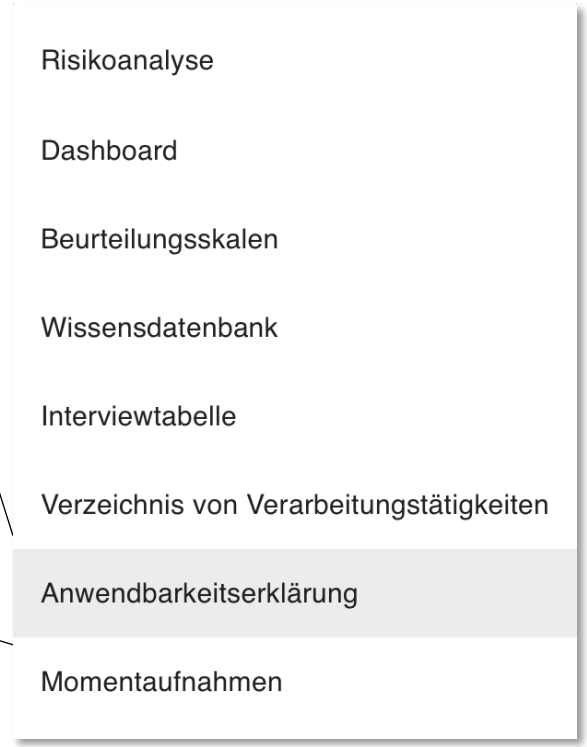


- Abbildung von EU-DSGVO Nachweisen

www.konzeptacht.de

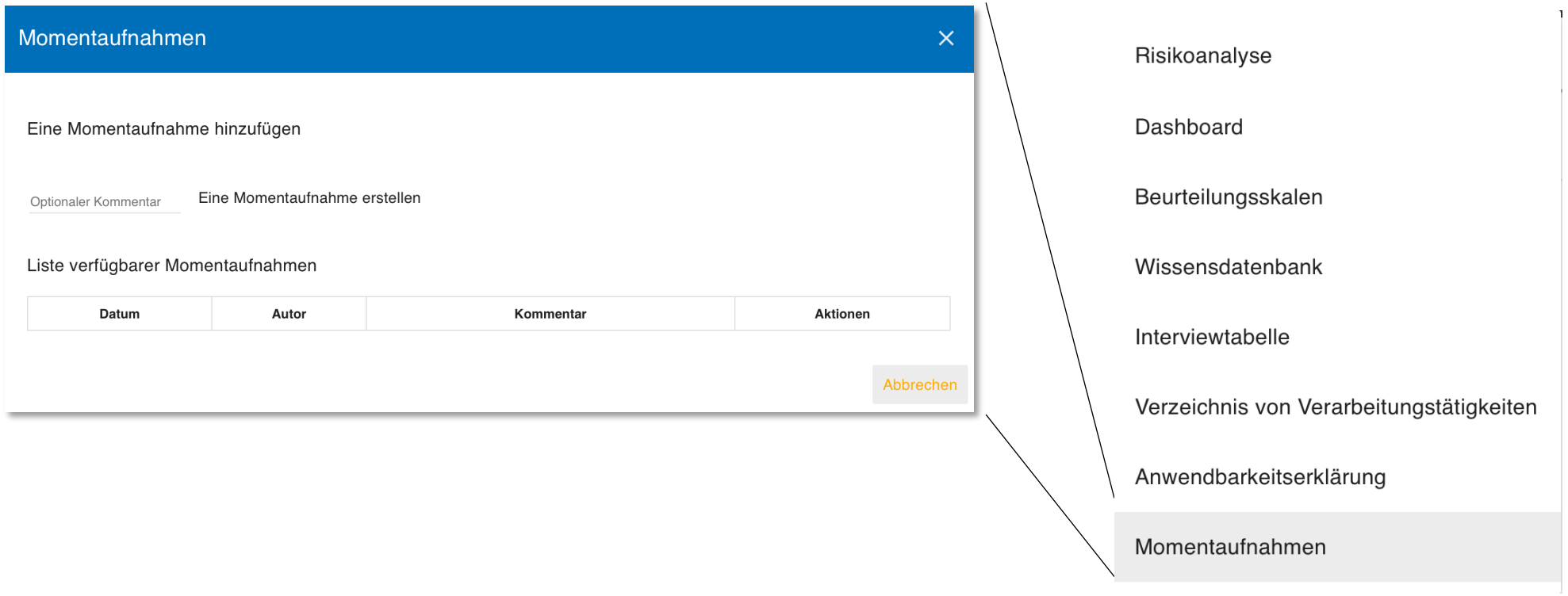
MONARC - Anwendbarkeitserklärung





- Abbildung einer Erklärung zur Anwendbarkeit / Statement of Applicability (SoA)

MONARC - Momentaufnahmen



- Momentaufnahmen erstellen als Nachweis für Versionierungen

Weitere Tipps & Tricks

- K8-Vorgehensweise unter Berücksichtigung der ISO 27001
  - Abbildung der ISO 27001 in den Schwachstellen
  - Spezielles für kritische Infrastrukturen unter KritisV und §8a BSIG
  - Spezielles für Betreiber von Strom- und Gasnetzen unter IT-SiKat § 11 Abs. 1a (08/2015)
  - Spezielle Kriterien VDA/ISA
  - Abbildung von Systemen zur Angriffserkennung (SzA)

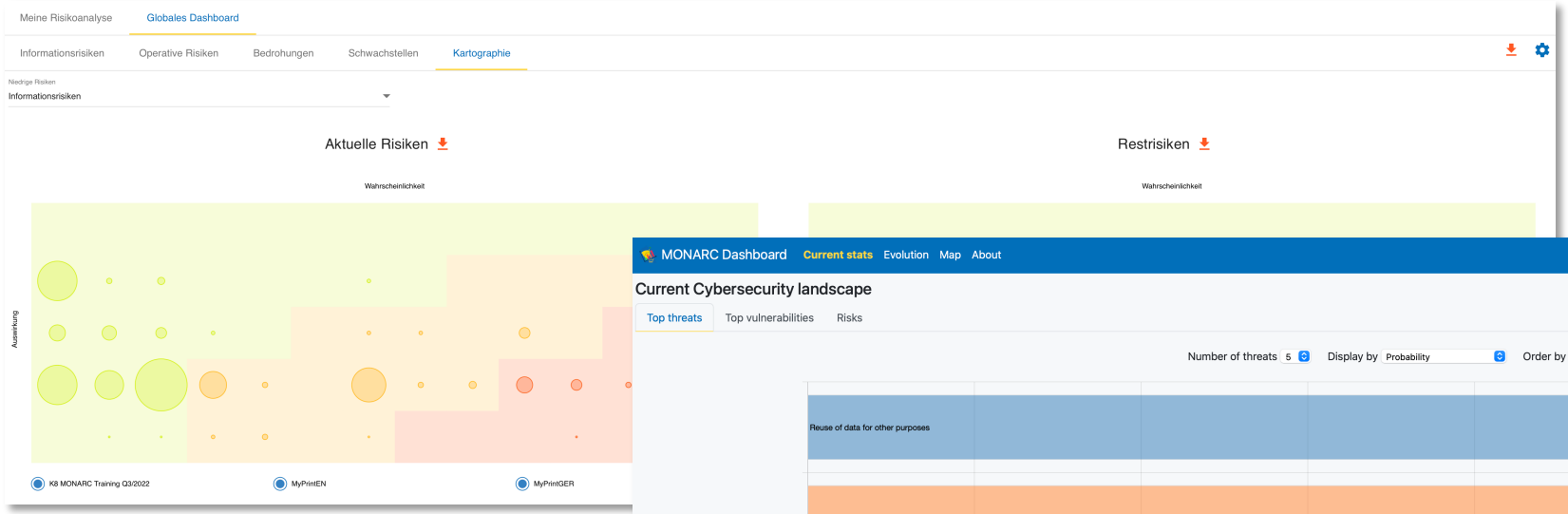
Weitere Tipps & Tricks

- Usermanagement und Berechtigungen
- Downloadmöglichleiten unter monarc.lu
- Transition zu ISO 27001:2022
- Import aus vorhandener Risikoanalyse
- Tipps & Tricks aus der Praxis

Technisches Wissen

- Wissenswertes zum technischen Aufsetzen der Plattform – bei Interesse
  - Installationsanleitung unter monarc.lu
  - Installationsanleitung auf der K8-Webseite
  - DB-Anbindung, PHP Timeouts etc.

Global Dashboard



Fragen / Feedback

- Zeit für offene Fragen / Feedback
- „Spielen“ im System

KonzeptAcht GmbH

Consulting

- Cyber Security Incident Response
- Aufbau von ISMS nach ISO 27001
- Aufbau von ISMS nach IT-Grundschutz
- ISMS nach VDA ISA
- Risikomanagement-Systeme
- Externer ISB / ISO
- MONARC Hosting

Audit & Prüfung

- Interne Audits
- Zertifizierungsaudits
- §8a (3) BSIG – KRITIS
- BSI TR-03109-6
- IT-Revisionsprüfungen
- Trusted ERP

Awareness / Schulung

- Cyber Security Awareness
- K8 macht Schule
- Phishing-Kampagnen
- Risikomanagement mit MONARC
- Inhouse Schulungen

Technische Sicherheit

- Penetrationstests
- Sicherheits-Analyse
- Prüfung von Sicherheits-konzepten
- Systeme zur Angriffserkennung (SzA)

Ihr Kontakt

https://www.konzeptacht.de

@konzeptacht

Thomas Kochanek

Thomas Kochanek

Ihr Kontakt

https://www.konzeptacht.de

@konzeptacht

Marc Sparwel