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 27001:2022
- 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)

Zeitplan

Zeitraum	Inhalt
09:00 Uhr - 10:15 Uhr	Einführung MONARC
10:15 Uhr - 10:30 Uhr	Kaffeepause
10:30 Uhr - 12:00 Uhr	Aufbau und Nutzung des Tools
12:00 Uhr - 12:45 Uhr	Mittagspause
12:45 Uhr - 15:00 Uhr	Beurteilung und Behandlung von Risiken, Implementierung und Überwachung
15:00 Uhr - 15:15 Uhr	Kaffeepause
15:15 Uhr – 17:00 Uhr	Tools und Dashboards, Tipps & Tricks, Fragen / Feedback

Organisatorisches

❌ Keine Aufzeichnungen des Trainings!

❌ Keine Gruppenteilnahme!

LUXEMBOURG HOUSE OF CYBERSECURITY

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

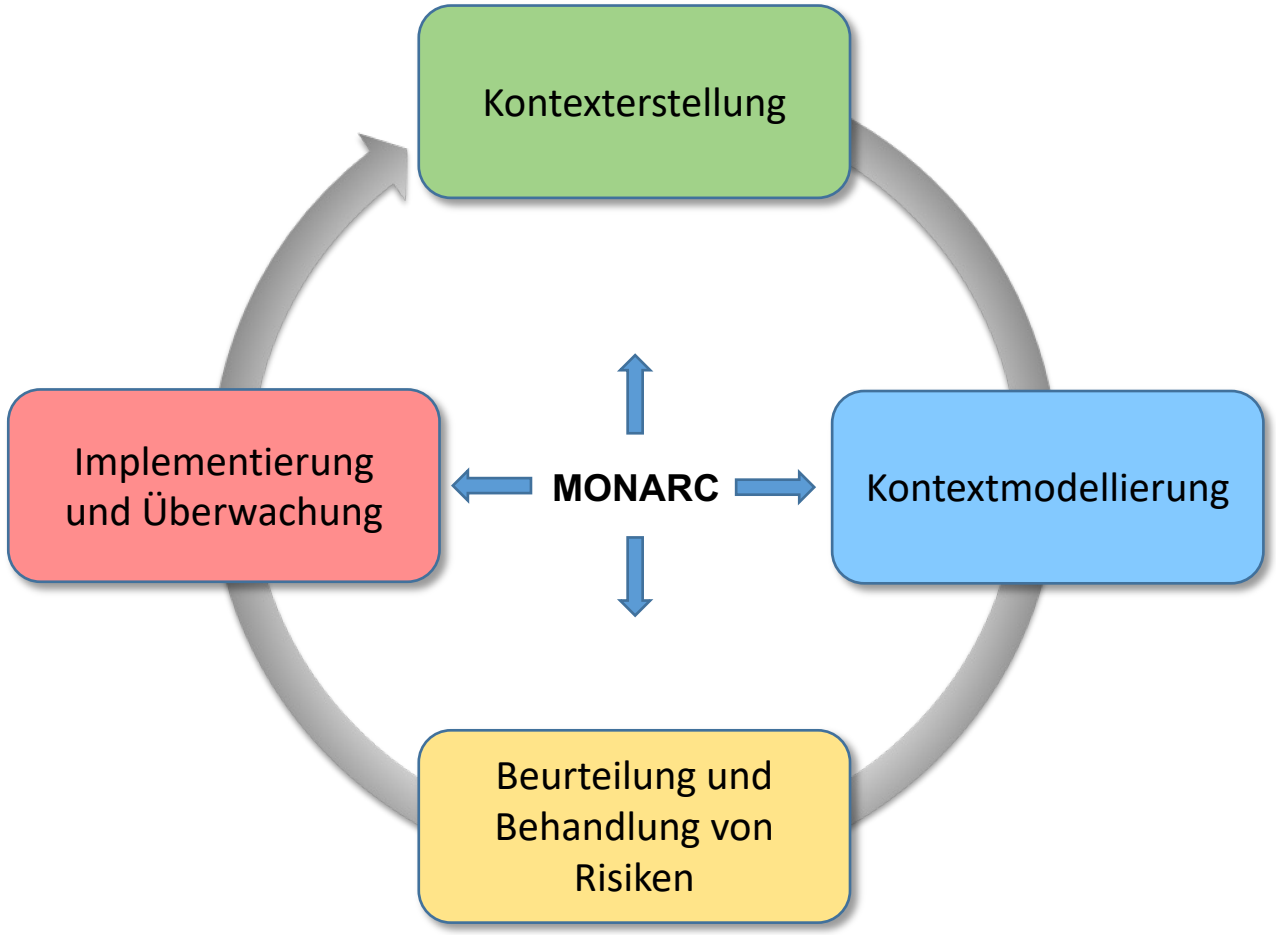
www.lhc.lu
www.nc3.lu

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

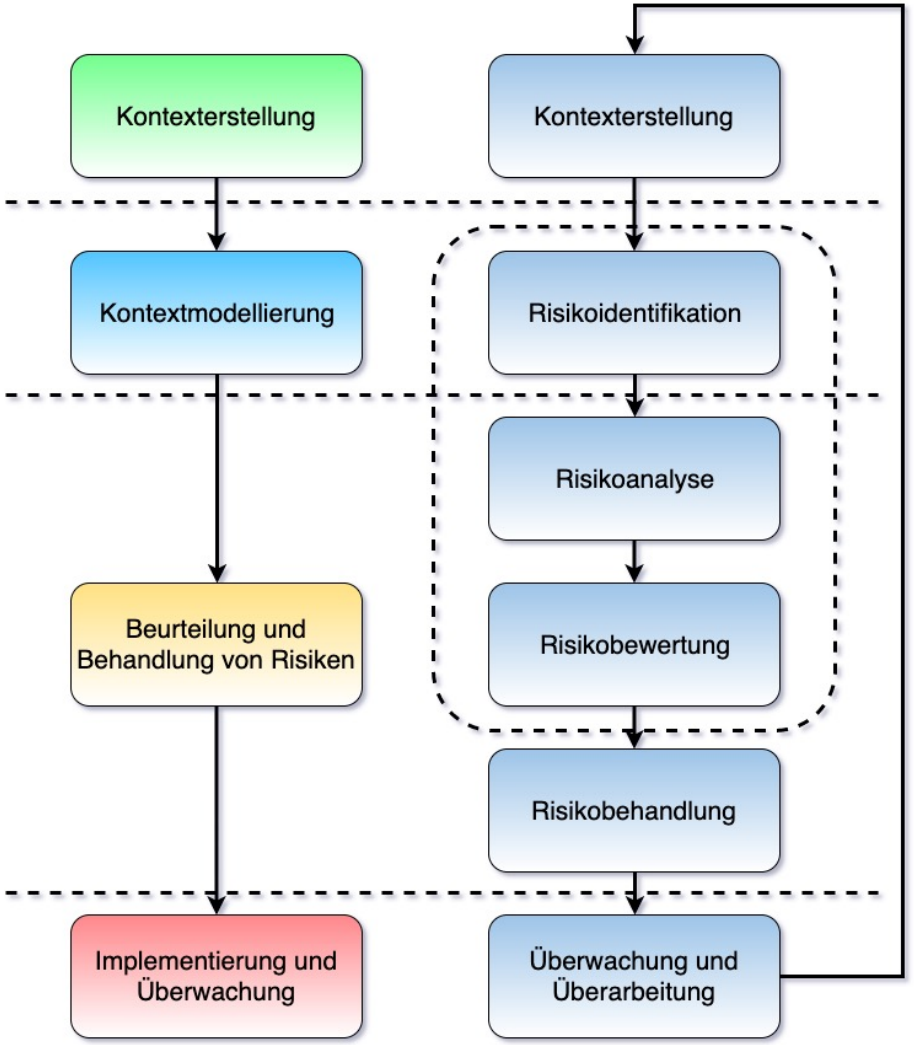
MONARC Methodik



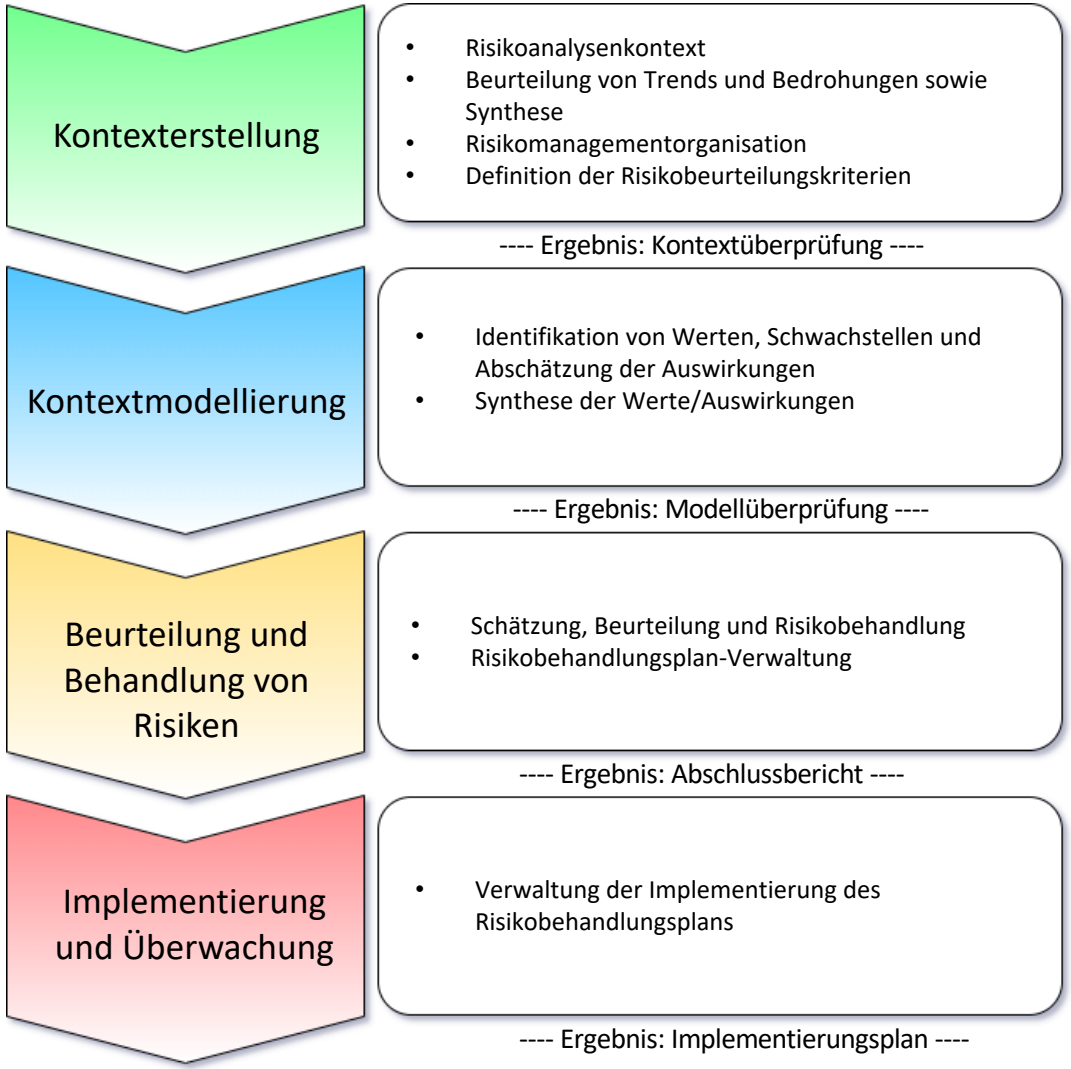
Methodik der Risikoanalyse

- **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 der Informationsrisiken angewendet:

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

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

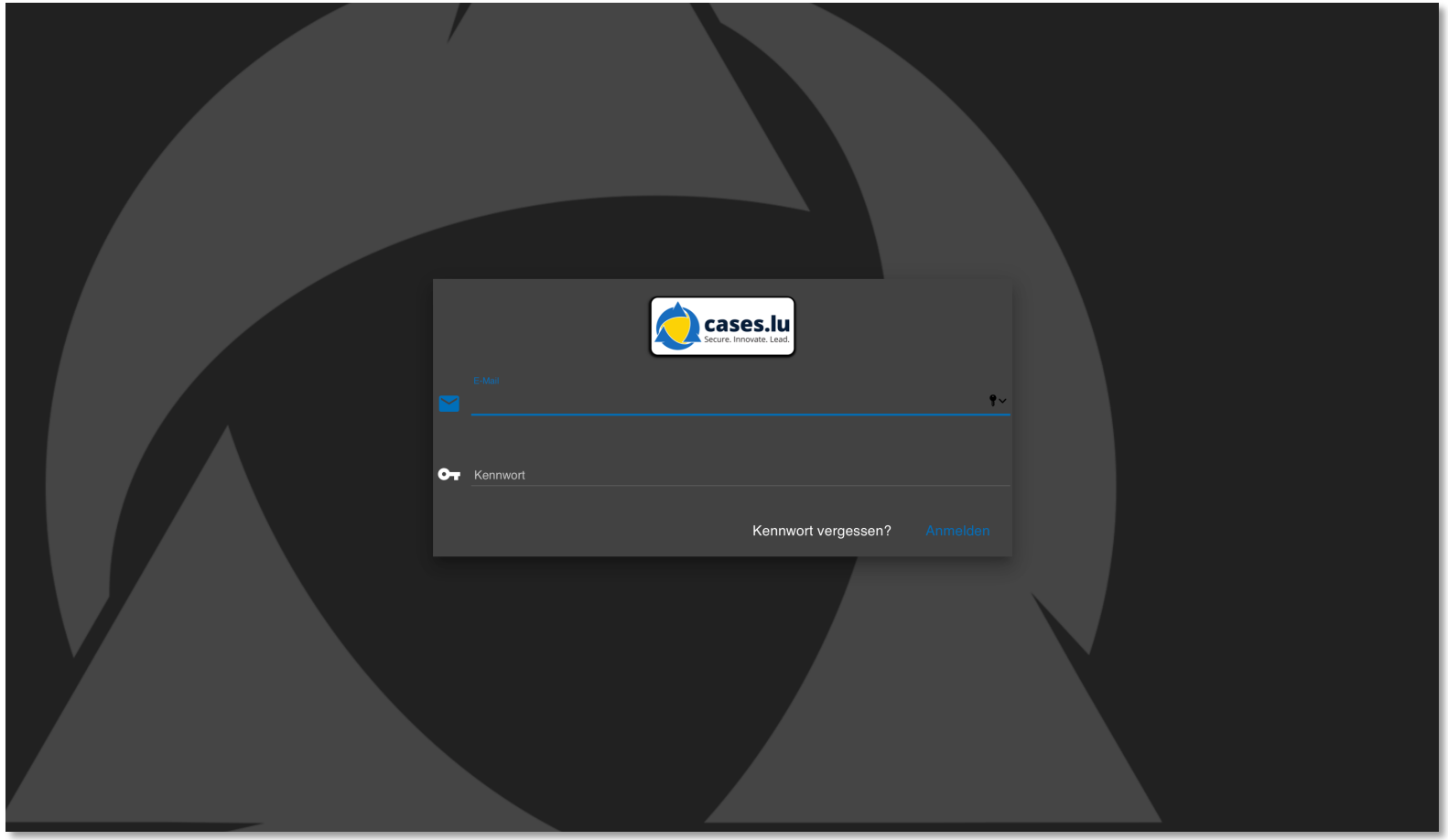
MONARC Methodik

Die folgende Formel wird zur Berechnung der operativen Risiken angewendet:

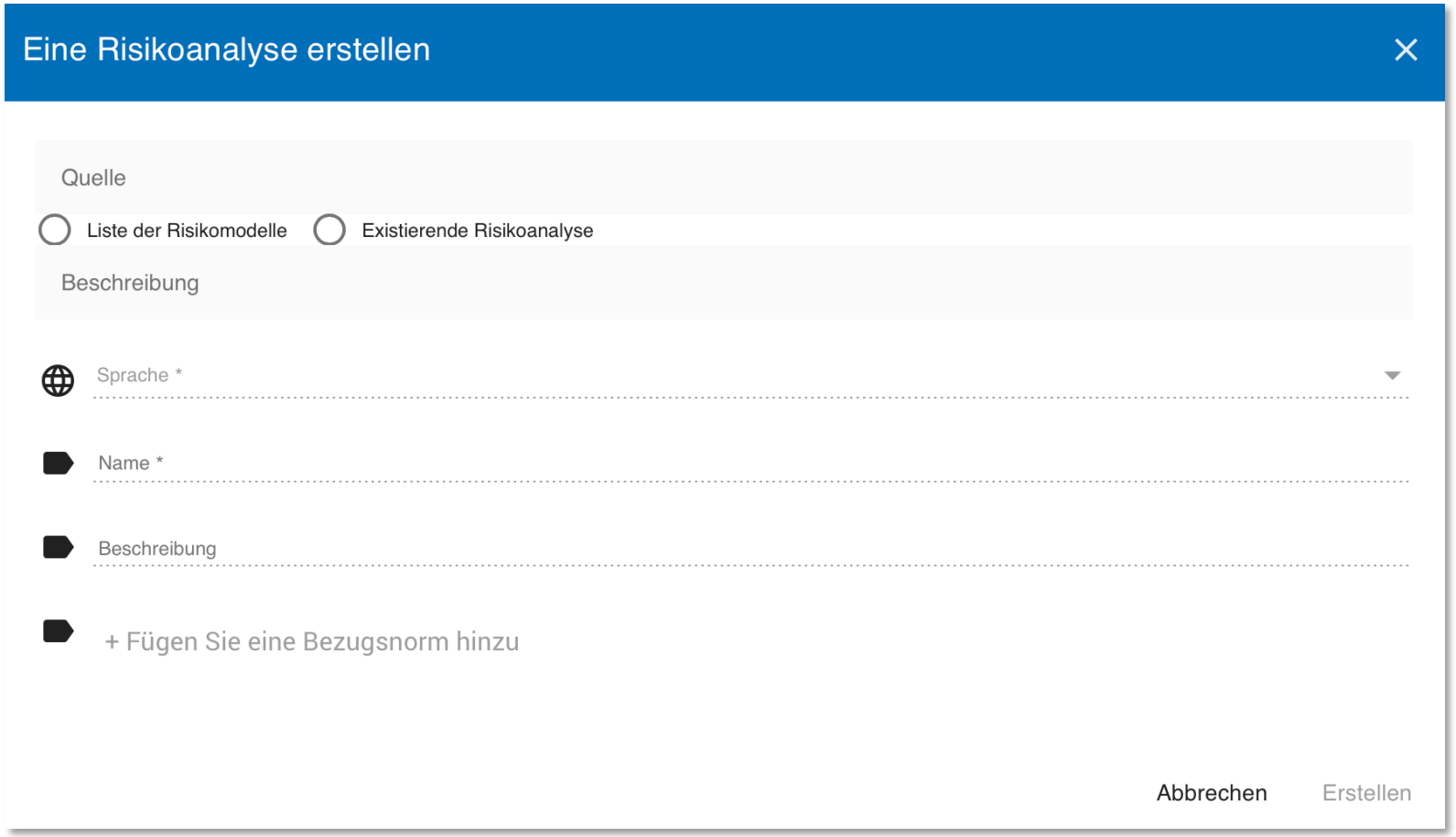
$$R = I \times P$$

R: Risiko; **I**: Auswirkung (Impact), **P:** Wahrscheinlichkeit (Probability)

Erstellung Risikoanalyse in MONARC



Erstellung Risikoanalyse in MONARC



Erstellung Risikoanalyse in MONARC

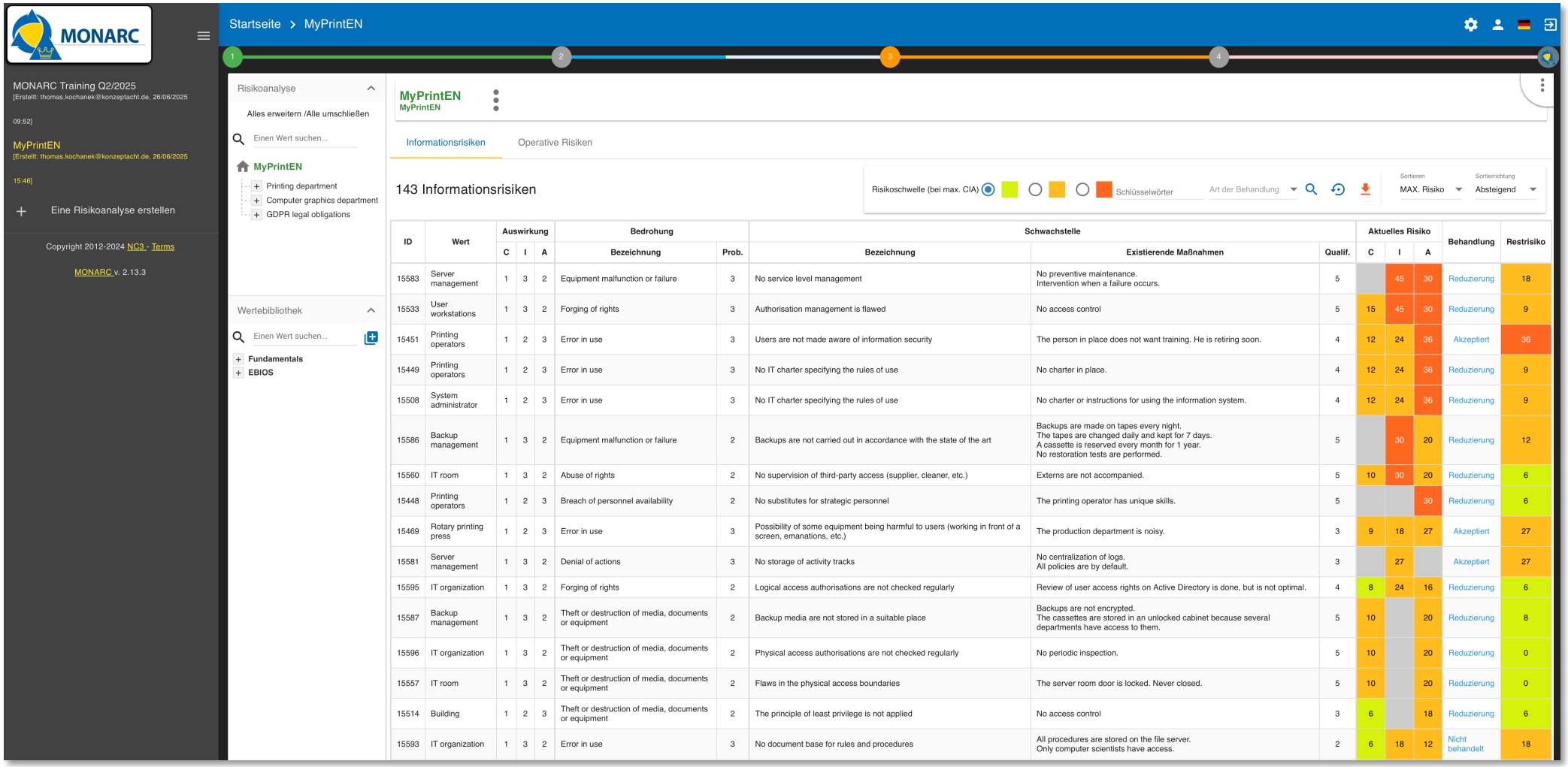
- Login Schulungsumgebung:
  - Hostname: `https://test.konzeptacht.de`
  - User: `K8-Training-xx@konzeptacht.de` *=> xx = 01 ≤ xx ≤ 15*
  - Passwort: `K8-Training-xx-serg516`

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`

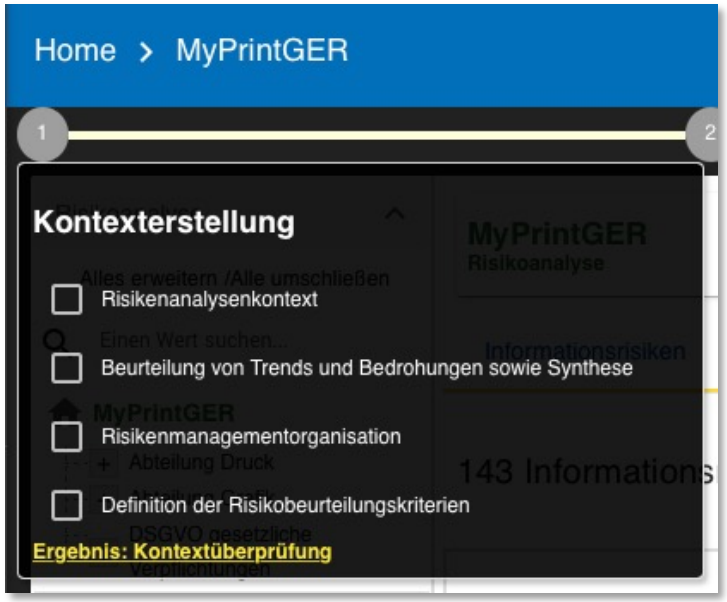
Aufbau und Nutzung des Tools



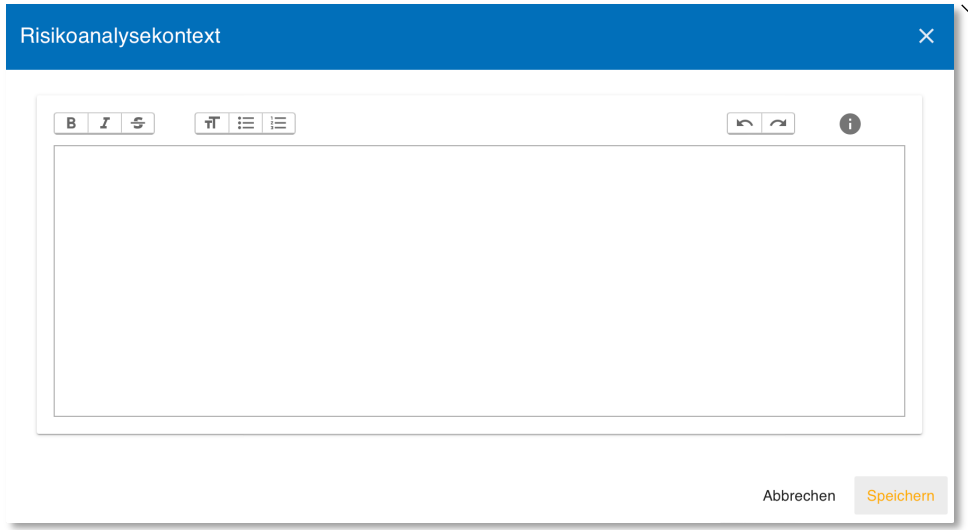
ID	Wert	Auswirkung			Bedrohung		Schwachstelle			Aktuelles Risiko			Behandlung	Restrisiko
		C	I	A	Bezeichnung	Prob.	Bezeichnung	Existierende Maßnahmen	Qualif.	C	I	A		
15583	Server management	1	3	2	Equipment malfunction or failure	3	No service level management	No preventive maintenance. Intervention when a failure occurs.	5		45	30	Reduzierung	18
15533	User workstations	1	3	2	Forging of rights	3	Authorisation management is flawed	No access control	5	15	45	30	Reduzierung	9
15451	Printing operators	1	2	3	Error in use	3	Users are not made aware of information security	The person in place does not want training. He is retiring soon.	4	12	24	36	Akzeptiert	36
15449	Printing operators	1	2	3	Error in use	3	No IT charter specifying the rules of use	No charter in place.	4	12	24	36	Reduzierung	9
15508	System administrator	1	2	3	Error in use	3	No IT charter specifying the rules of use	No charter or instructions for using the information system.	4	12	24	36	Reduzierung	9
15586	Backup management	1	3	2	Equipment malfunction or failure	2	Backups are not carried out in accordance with the state of the art	Backups are made on tapes every night. The tapes are changed daily and kept for 7 days. A cassette is reserved every month for 1 year. No restoration tests are performed.	5		30	20	Reduzierung	12
15560	IT room	1	3	2	Abuse of rights	2	No supervision of third-party access (supplier, cleaner, etc.)	Externs are not accompanied.	5	10	30	20	Reduzierung	6
15448	Printing operators	1	2	3	Breach of personnel availability	2	No substitutes for strategic personnel	The printing operator has unique skills.	5			30	Reduzierung	6
15469	Rotary printing press	1	2	3	Error in use	3	Possibility of some equipment being harmful to users (working in front of a screen, emanations, etc.)	The production department is noisy.	3	9	18	27	Akzeptiert	27
15581	Server management	1	3	2	Denial of actions	3	No storage of activity tracks	No centralization of logs. All policies are by default.	3		27		Akzeptiert	27
15595	IT organization	1	3	2	Forging of rights	2	Logical access authorisations are not checked regularly	Review of user access rights on Active Directory is done, but is not optimal.	4	8	24	16	Reduzierung	6
15587	Backup management	1	3	2	Theft or destruction of media, documents or equipment	2	Backup media are not stored in a suitable place	Backups are not encrypted. The cassettes are stored in an unlocked cabinet because several departments have access to them.	5	10		20	Reduzierung	8
15596	IT organization	1	3	2	Theft or destruction of media, documents or equipment	2	Physical access authorisations are not checked regularly	No periodic inspection.	5	10		20	Reduzierung	0
15557	IT room	1	3	2	Theft or destruction of media, documents or equipment	2	Flaws in the physical access boundaries	The server room door is locked. Never closed.	5	10		20	Reduzierung	0
15514	Building	1	2	3	Theft or destruction of media, documents or equipment	2	The principle of least privilege is not applied	No access control	3	6		18	Reduzierung	6
15593	IT organization	1	3	2	Error in use	3	No document base for rules and procedures	All procedures are stored on the file server. Only computer scientists have access.	2	6	18	12	Nicht behandelt	18

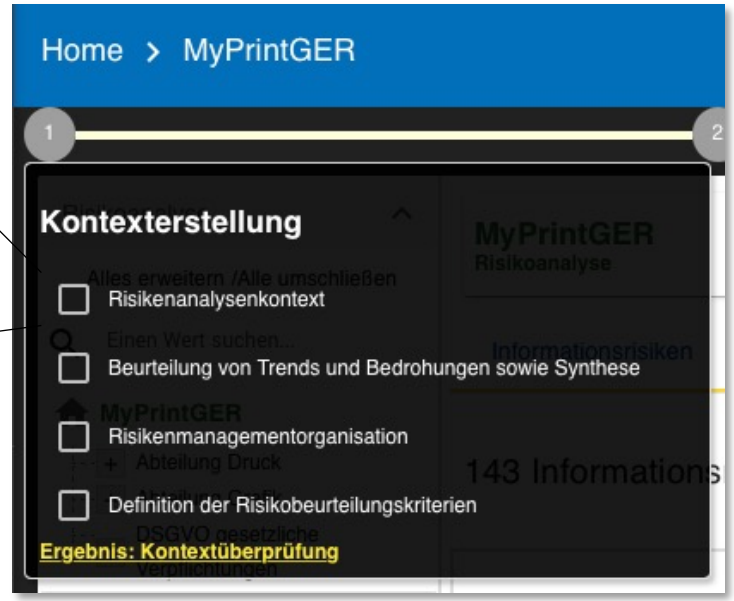
1. Kontexterstellung

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



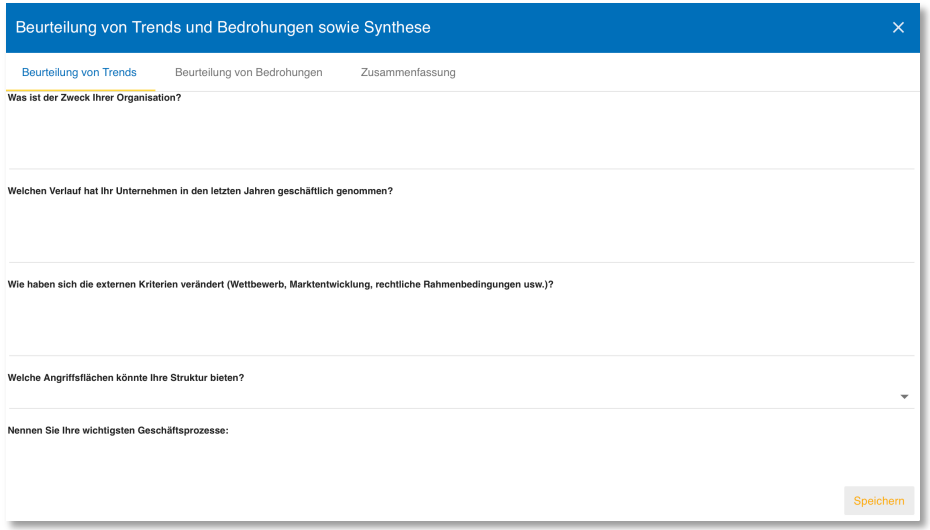
1.1 Risikoanalysekontext

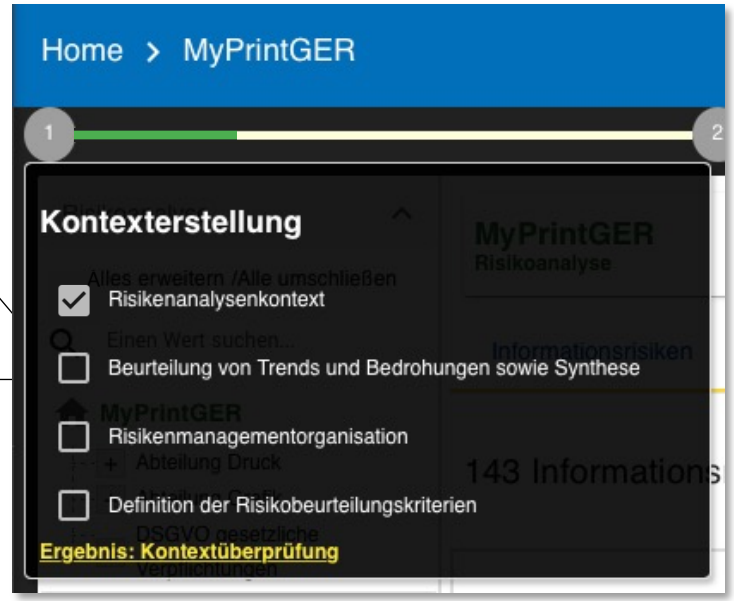




- Definition der Zielorganisation
- Referenz zu ISO/IEC 27005:2022:
  - Context establishment: Kap. 6

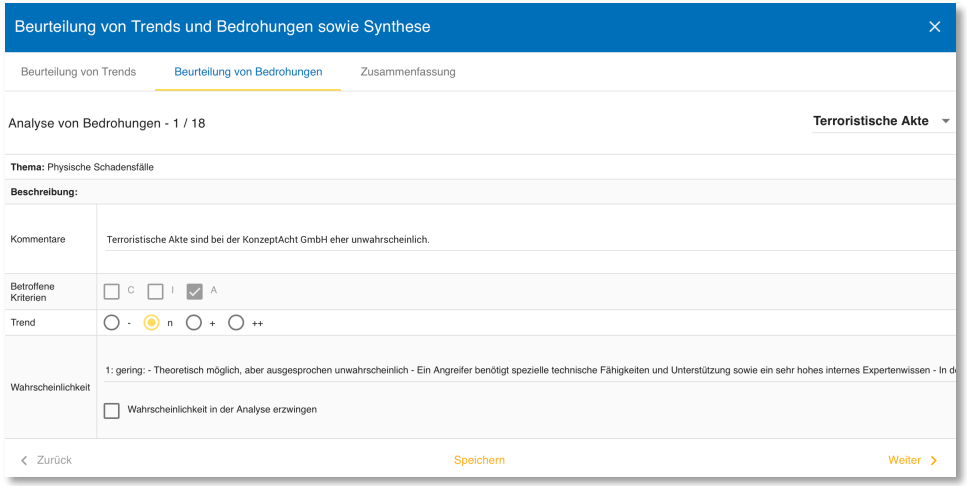
1.2.1 Beurteilung von Trends

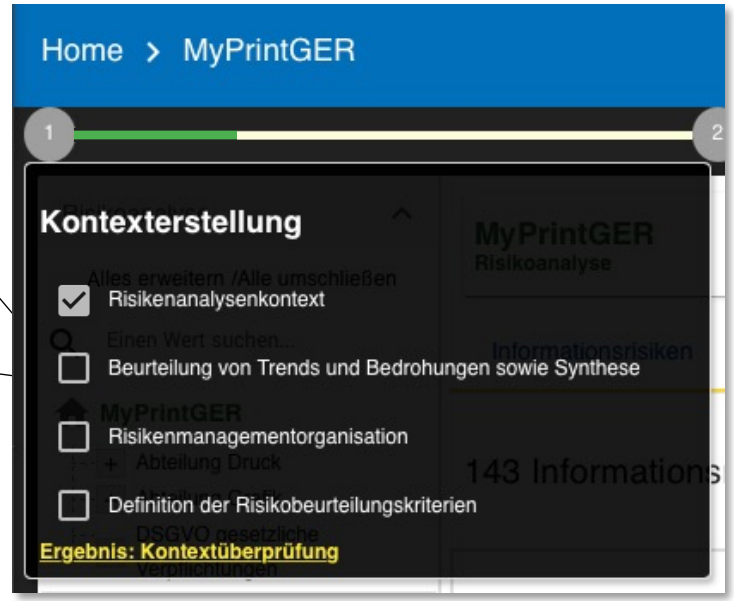




- Allgemeine Fragen zur Ermittlung des Kontexts
- Definieren Sie den Umfang und den Schwerpunkt der Analyse
- Sammlung von Informationen

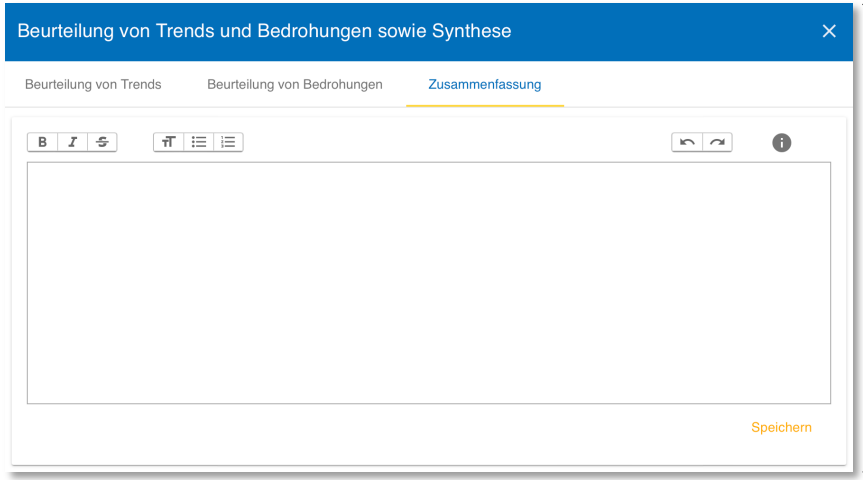
1.2.2 Beurteilung von Bedrohungen

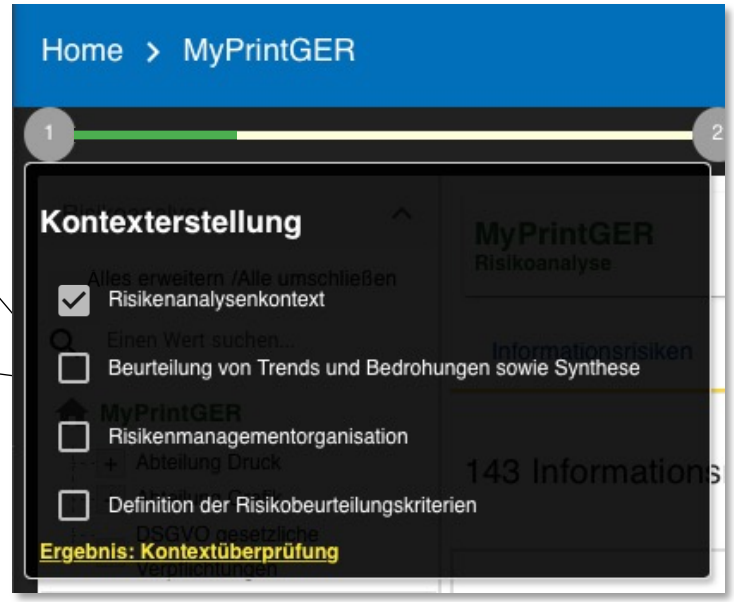




- Bewertung von Bedrohungen vor dem eigenen Kontext
- Sammeln von Informationen aller Beteiligten

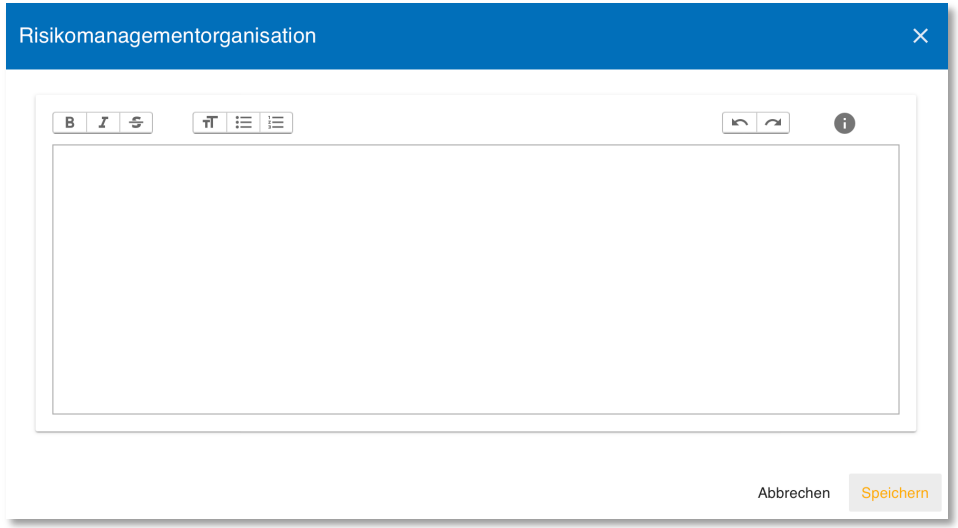
1.2.3 Zusammenfassung

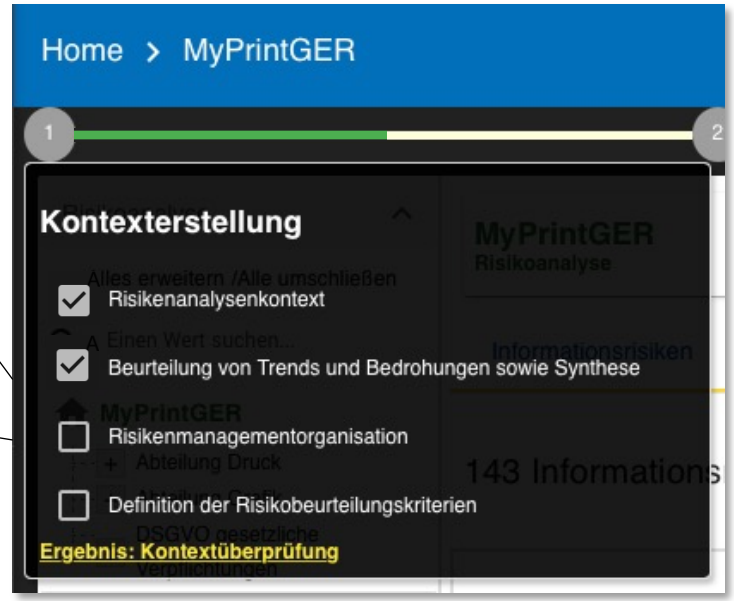




- Zusammenfassung der Ergebnisse von Trends und Bedrohungen
- Abschluss des ersten Arbeitsergebnisses

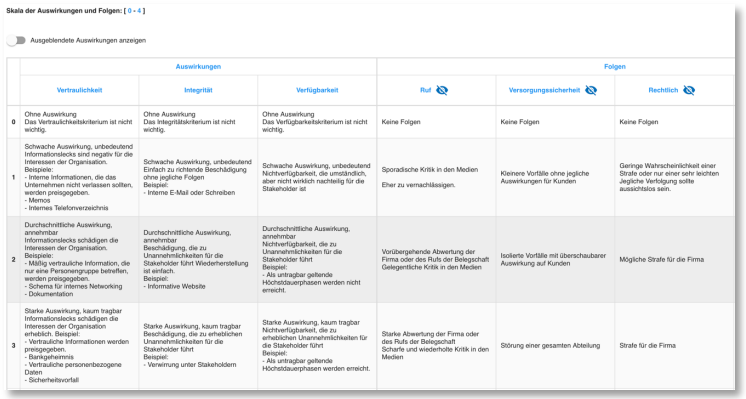
1.3 Risikomanagementorganisation





- Zusätzliche Informationen zur Risikomanagementorganisation
- Referenz zu ISO/IEC 27005:2022:
  - Organizational considerations: Kap. 6.1

1.4 Definition der Kriterien für Informationsrisiken

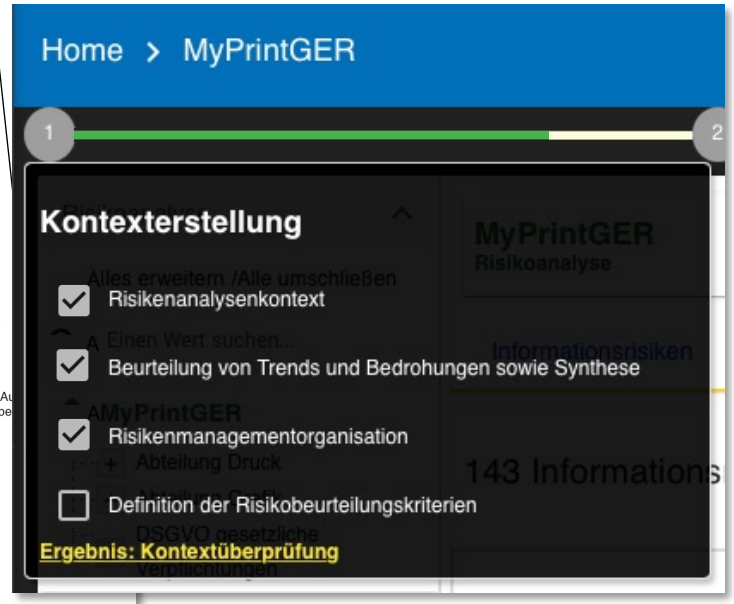


Wahrscheinlichkeitsskala: [0 - 4]

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

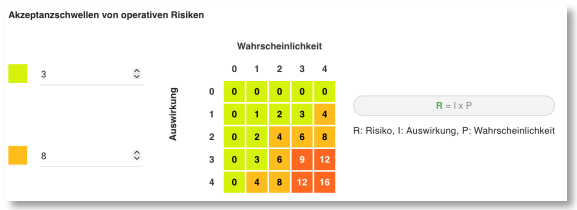
Qualifizierungsskala: [0 - 5]

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

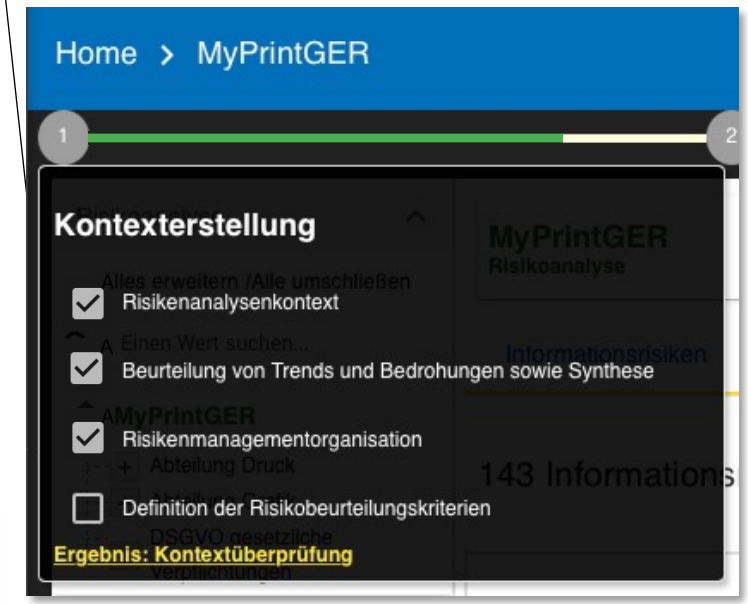


- Referenz zu ISO/IEC 27005:2022:
  - Establishing and maintaining information security risk criteria: Kapitel 6.4

1.4 Definition der Kriterien für Operative Risiken



	Reputation	Operational	Legal	Financial	Personal
0	No consequences	No consequences	No consequences	No consequences	No consequences
1	Sporadic media critics	Minor incidents without any impact on customers.	Small probability of any sentences, or really slight one. Any prosecution should be futile.	Brings some marginal fees (more or less 1% of the sales revenue).	Some inconvenience which will be topped without difficulty (Time waste, procedure reiteration, irritation, etc.).
2	Temporary degradation of the company or staff reputation. Occasional media critics	Isolated incidents with a manageable impact on customers.	Possible sentence for the company.	Brings some non-marginal fees (more or less 5% of the sales revenue).	Significative inconvenience which could be topped with some difficulties (Additional costs, denial of access to commercial delivery, fear, misunderstanding, stress, slight physical ailments, etc.).
3	Strong degradation of the company or staff reputation. Serious and repeated media critics.	Interruption of a whole department.	Sentence for the company.	Brings some heavy fees which can affect the company (more or less 10% of the sales revenue).	Significative consequences which could be topped, but with some serious difficulties (funds embezzlement, bank ban, deterioration of goods, job loss,
4	Death of someone. Definitive degradation of the company or staff reputation. Internationnal media coverage.	Complete stop of all services	Heavy sentence for the company.	Brings some deadly fees almost insurmontable (more or less 20% of the sales revenue).	Significative consequences almost irremediable, which can't be topped (financial distress, important financial debts, working impossibility, long periods psychological and physiological affection, death, etc.).



Wahrscheinlichkeitsskala: [0 - 4]

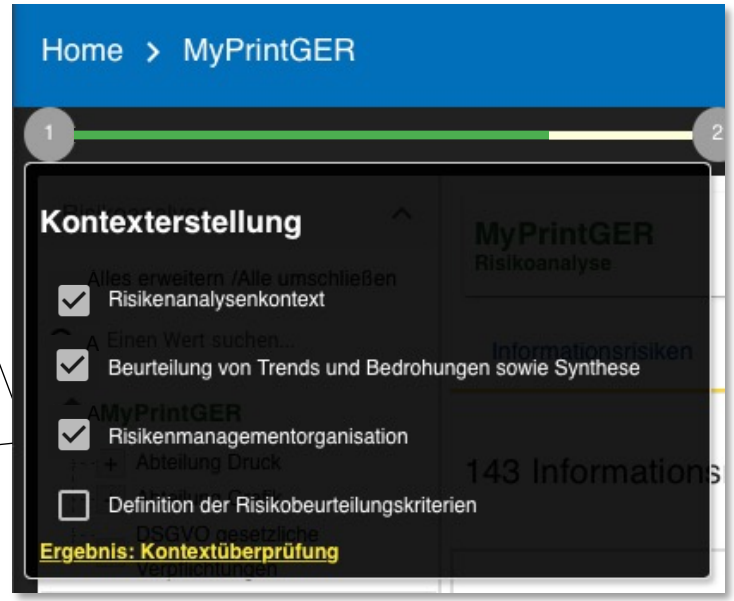
0. Impossible
1. Very unlikely: never happened, requires a high level of expert knowledge, or it is very expensive to execute.
2. Unlikely: might have happened, rare phenomenon which requires a good level of expert knowledge, or it is expensive to execute.
3. Could happen occasionally

- Referenz zu ISO/IEC 27005:2022:
  - Establishing and maintaining information security risk criteria: Kapitel 6.4

1.4 Definition der Konformitätsskala

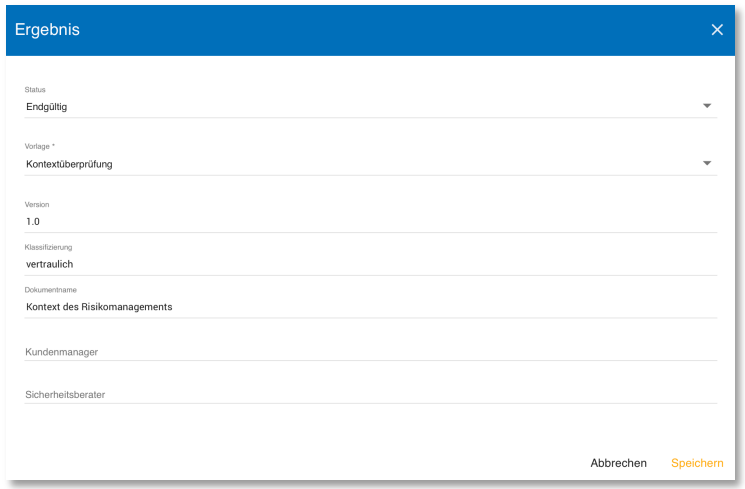
Konformitätsskala: 6 Ebenen

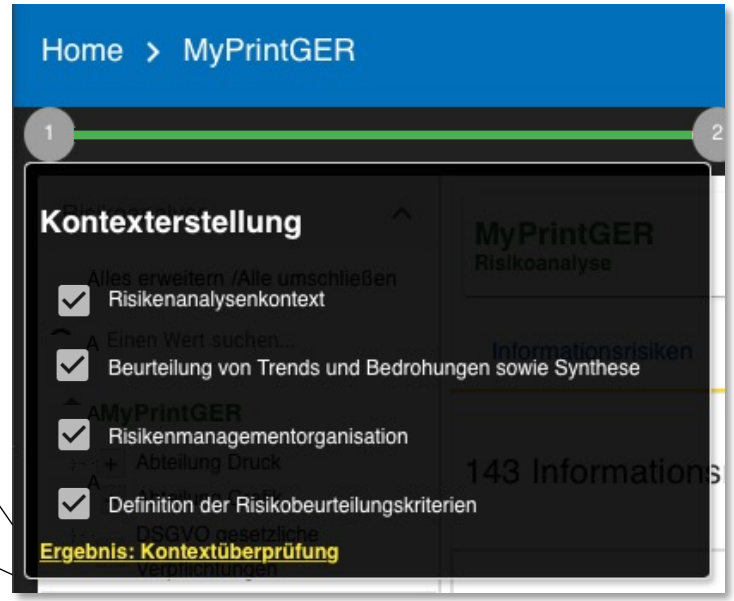
	Grad der Konformität	Farbe
0	Non-existent	
1	Initial	
2	Managed	
3	Defined	
4	Quantitatively managed	
5	Optimized	



- Referenz zu ISO/IEC 27005:2022:
  - Establishing and maintaining information security risk criteria: Kapitel 6.4

1.5 Ergebnis: Kontextüberprüfung





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

1. Kontexterstellung - Übung

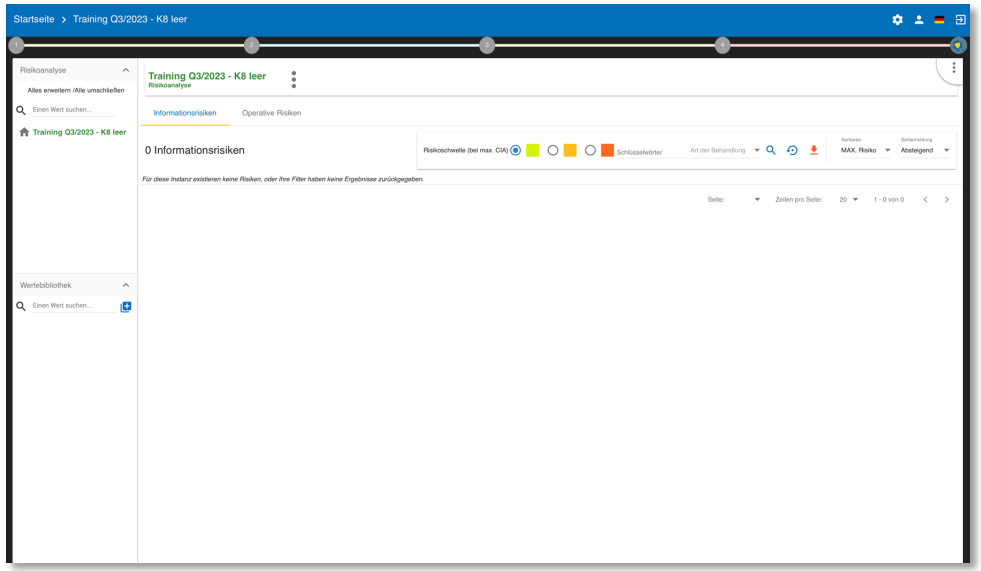
Übung: Durchführen der Kontexterstellung (30 Minuten)

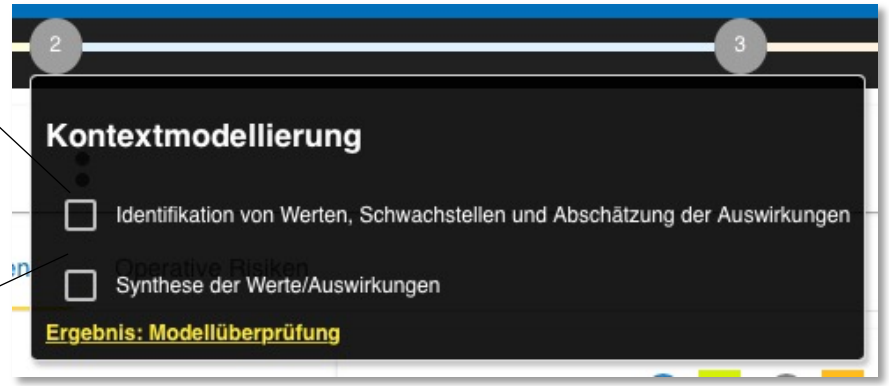
- **Ziel**: Definition des eigenen Kontextes
- **Vorgaben**:
  - Risikoanalysekontext: *<individuell>*
  - Beurteilung von Trends: *<individuell>*
  - Beurteilung von Bedrohungen: *<individuell>*
  - Zusammenfassung: *<individuell>*
  - Risikomanagementorganisation: *<individuell>*
  - Definition der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

2. Kontextmodellierung

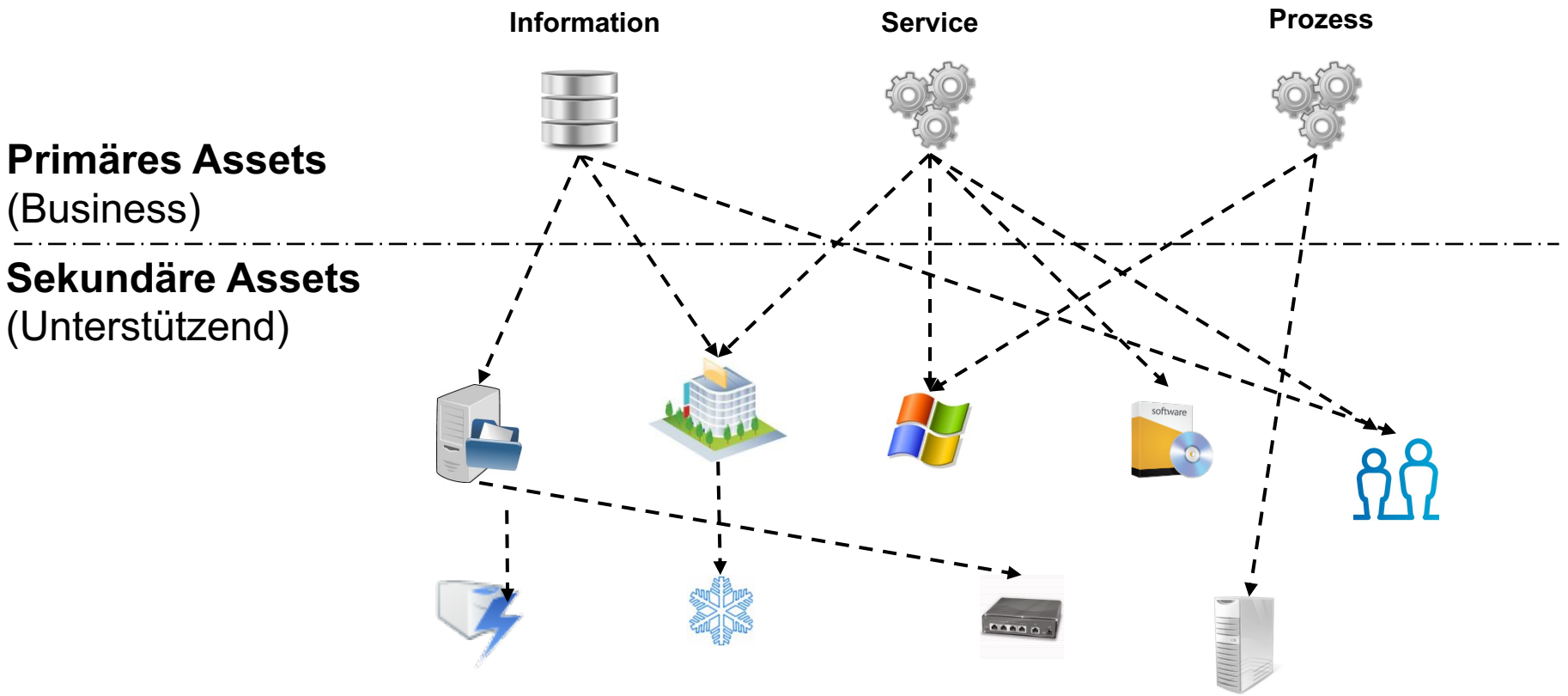
- Identifikation von Werten, Schwachstellen und Abschätzung der Auswirkungen
- Synthese der Werte/Auswirkungen

2.1 Identifikation von Werten, Schwachstellen und Abschätzung der Auswirkungen





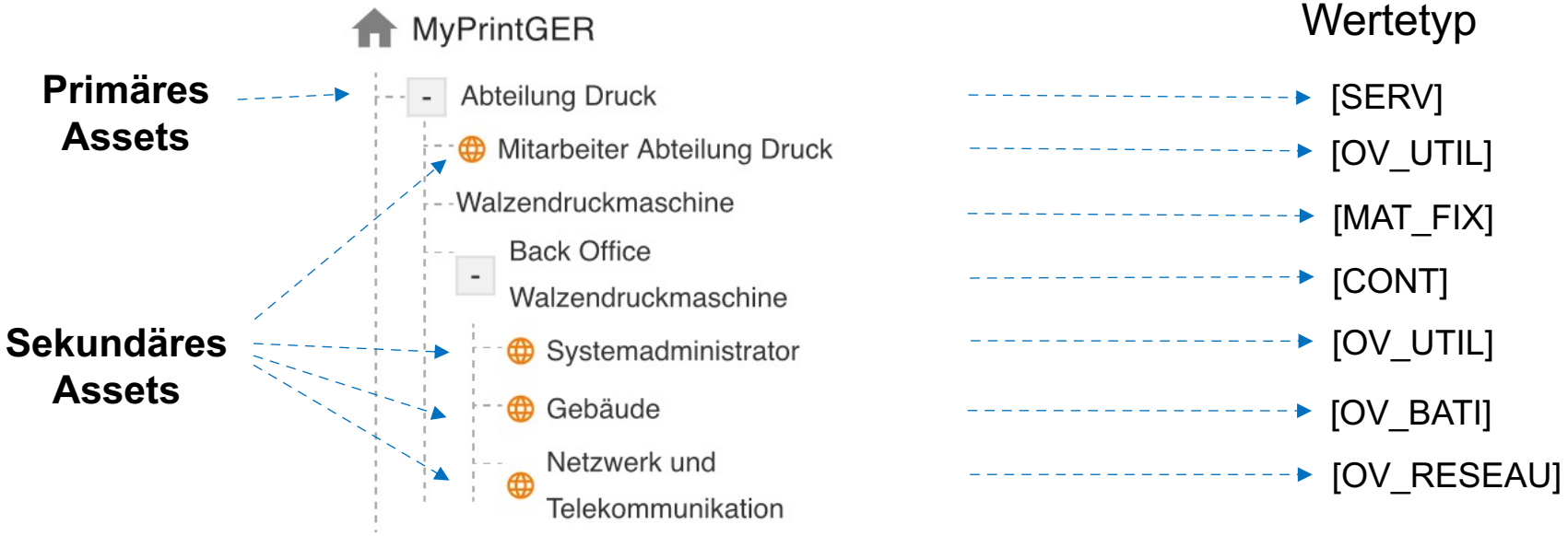
2.1 Identifikation von Werten, Schwachstellen und Abschätzung der Auswirkungen



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

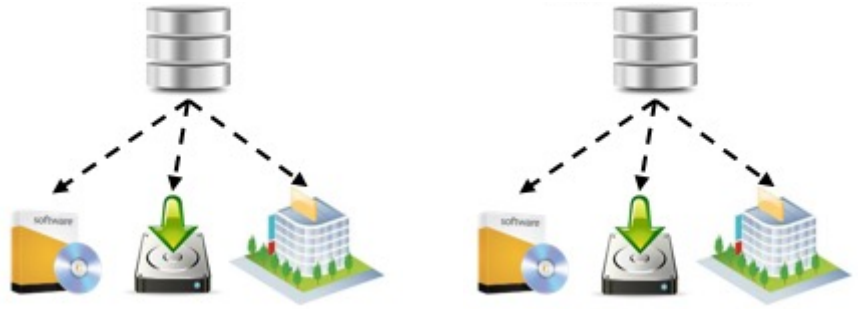
“Lokal”

Meine Risikoanalyse

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

30 Risiken

Datenbank #1 Datenbank #2



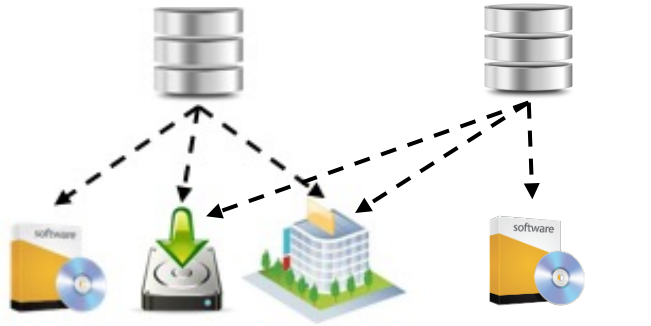
“Global”

Meine Risikoanalyse

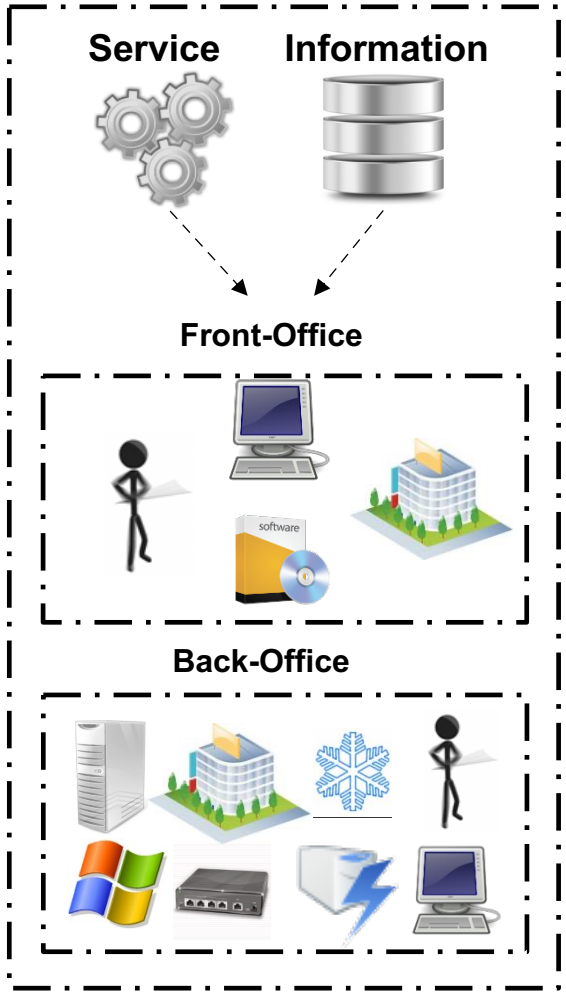
- Datenbank #1
  - Software
  - Backup NAS
  - Serverraum
- Datenbank #2
  - Software
  - Backup NAS
  - Serverraum

21 Risiken

Datenbank #1 Datenbank #2

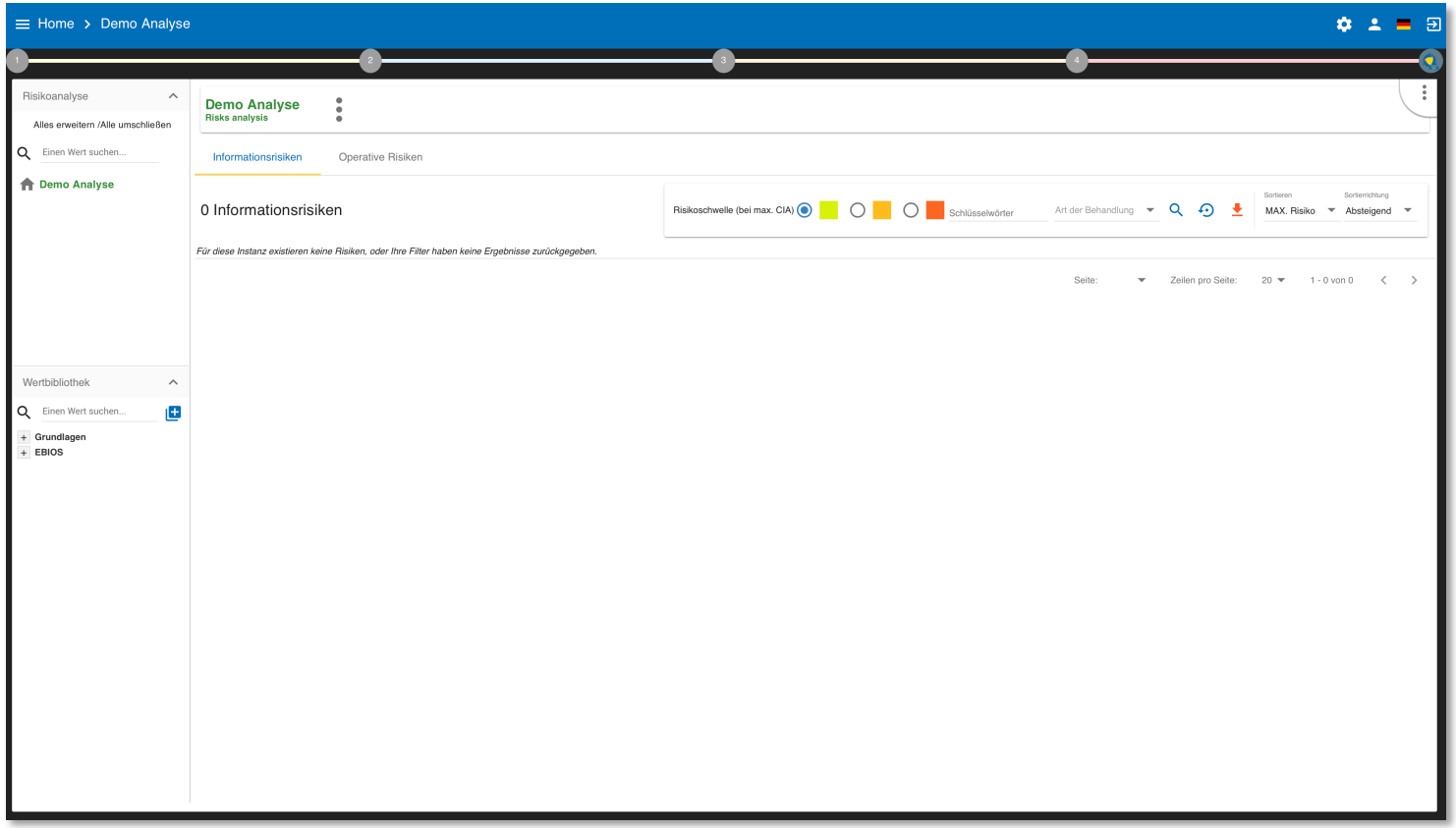


2.1 CASES Modellierung



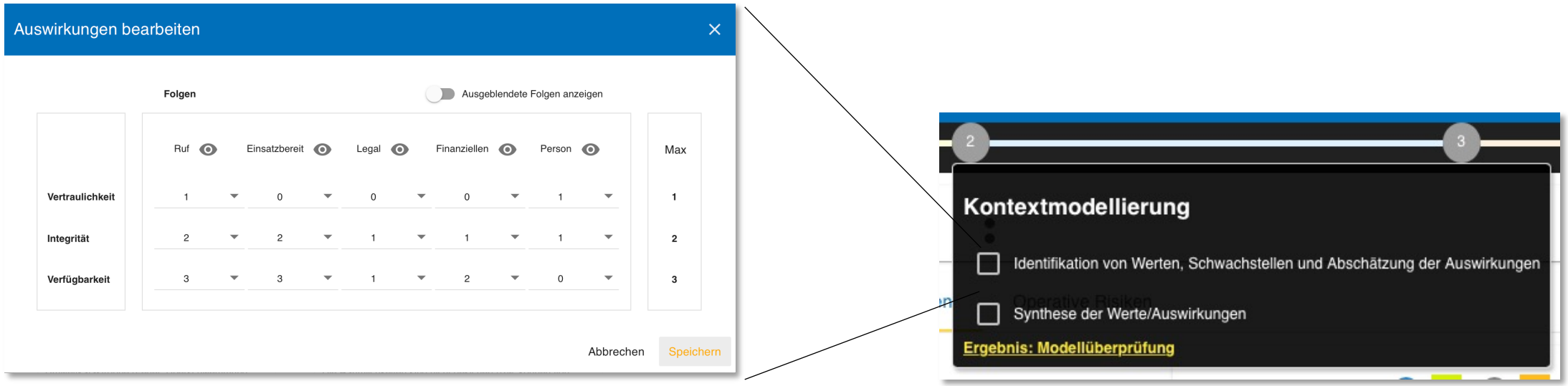
- MyPrintGER
  - Abteilung Druck
    - Mitarbeiter Abteilung Druck
    - Walzendruckmaschine
    - Back Office Walzendruckmaschine
      - Systemadministrator
      - Gebäude
      - Netzwerk und Telekommunikation
  - Abteilung Grafik
    - Frontoffice
      - Servicestelle
      - Mitarbeiter
      - 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



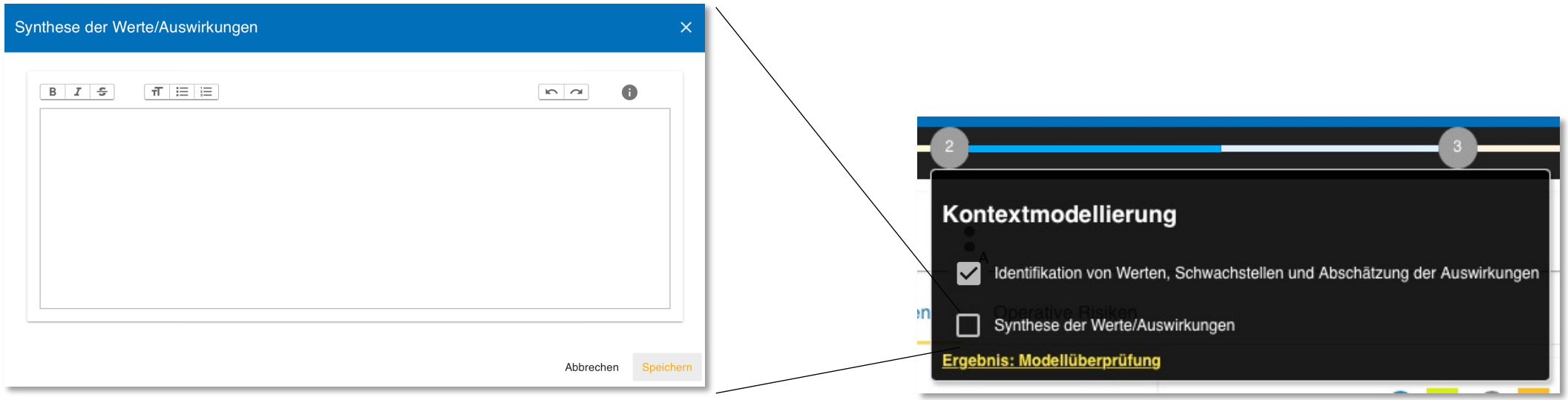
- Hauptansicht von MONARC
- Erstellung eines Risikomodells
- Referenz zu ISO/IEC 27005:2022:
  - Information security risk assessment process: Kapitel 7

2.1 Identifikation von Werten, Schwachstellen und Abschätzung der Auswirkungen



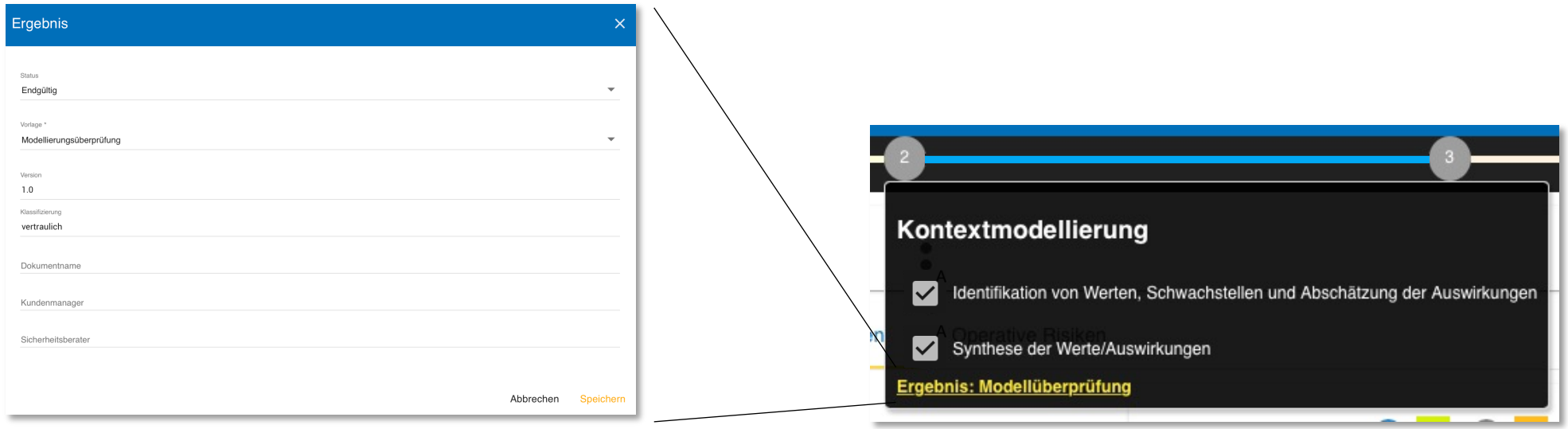
- Hauptansicht von MONARC
- Auswirkungen bearbeiten
- Referenz zu ISO/IEC 27005:2022:
  - Information security risk assessment process: Kapitel 7

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 / ODF

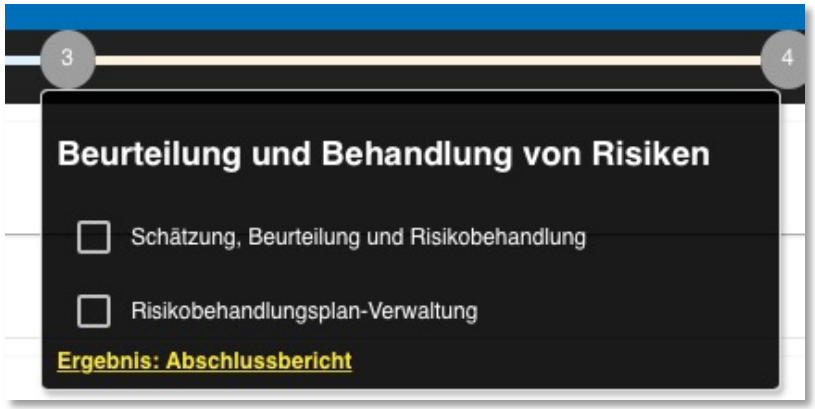
2. Kontextmodellierung - Übung

Übung: Durchführen der Kontextmodellierung (30 Minuten)

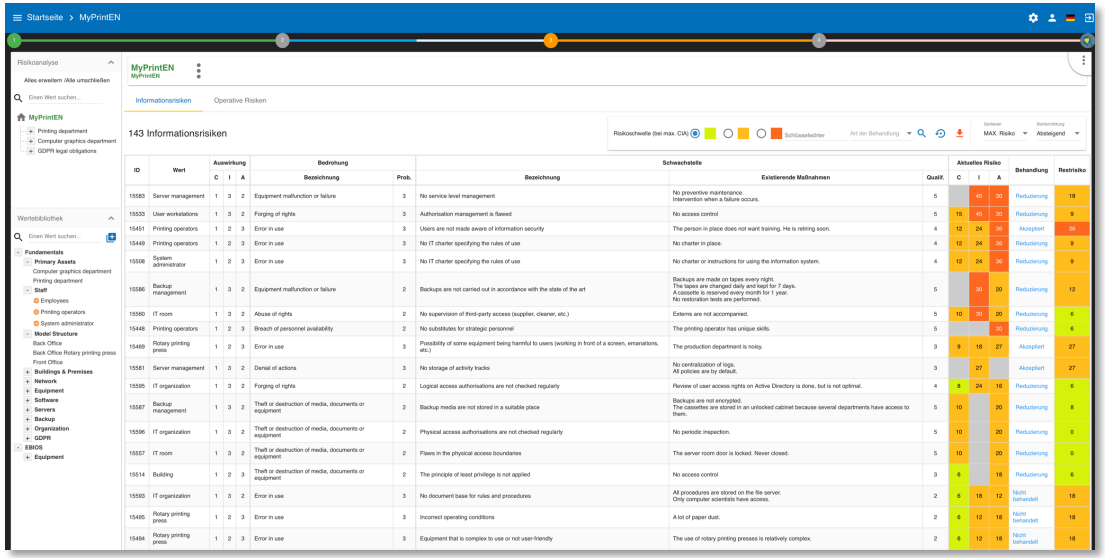
- **Ziel**: Definition des eigenen Kontextes
- **Vorgaben**:
  - Anlagen eigener
    - Lokaler und globaler Assets: *<individuell>*
    - Clonen von Assets: *<individuell>*
    - Asset-Kategorien: *<individuell>*
  - Modellierung von Abhängigkeiten: *<individuell>*
  - Erstellen der Risikoanalyse per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

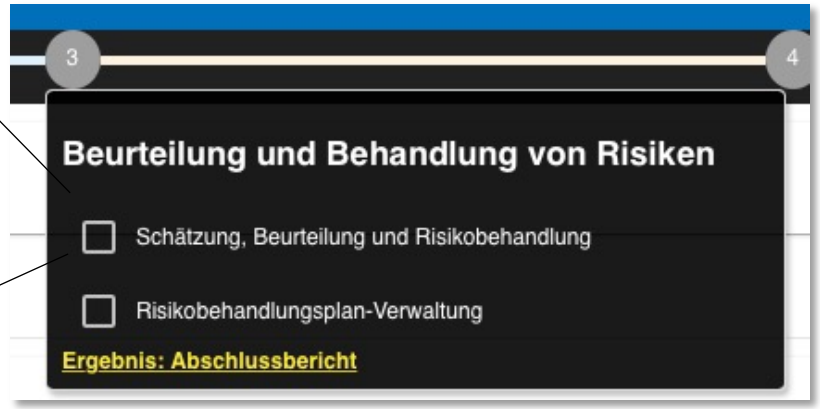
3. Beurteilung und Behandlung von Risiken

- Schätzung, Beurteilung und Risikobehandlung
- Risikobehandlungsplan-Verwaltung



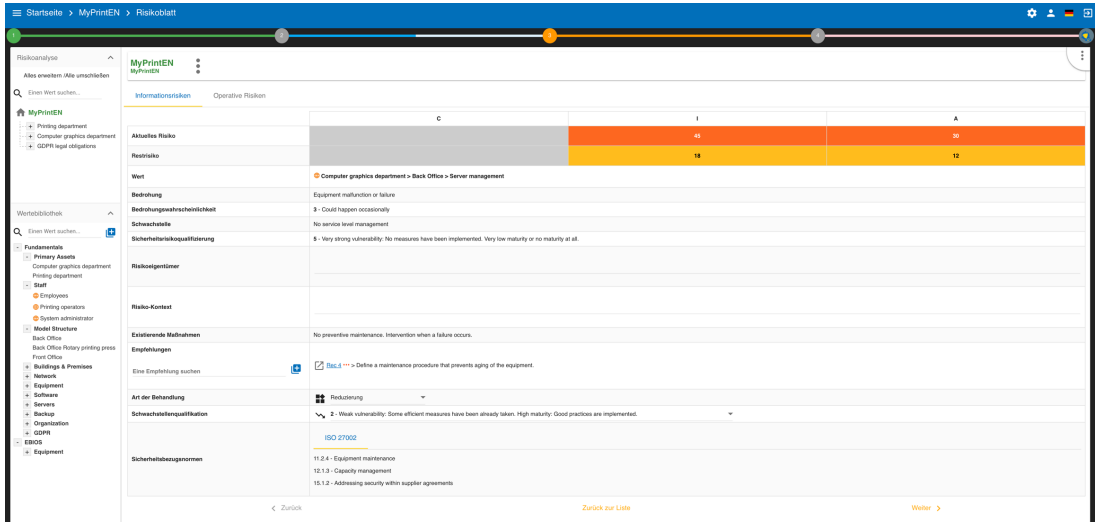
3.1 Schätzung, Beurteilung und Risikobehandlung

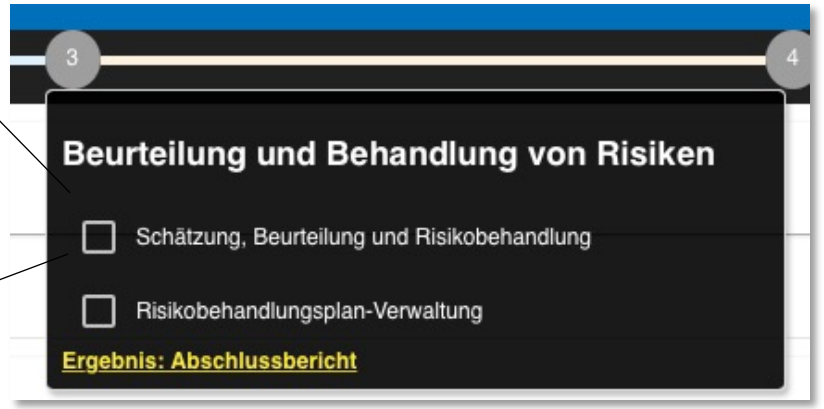




- Hauptansicht von MONARC
- Alle Risiken bewerten

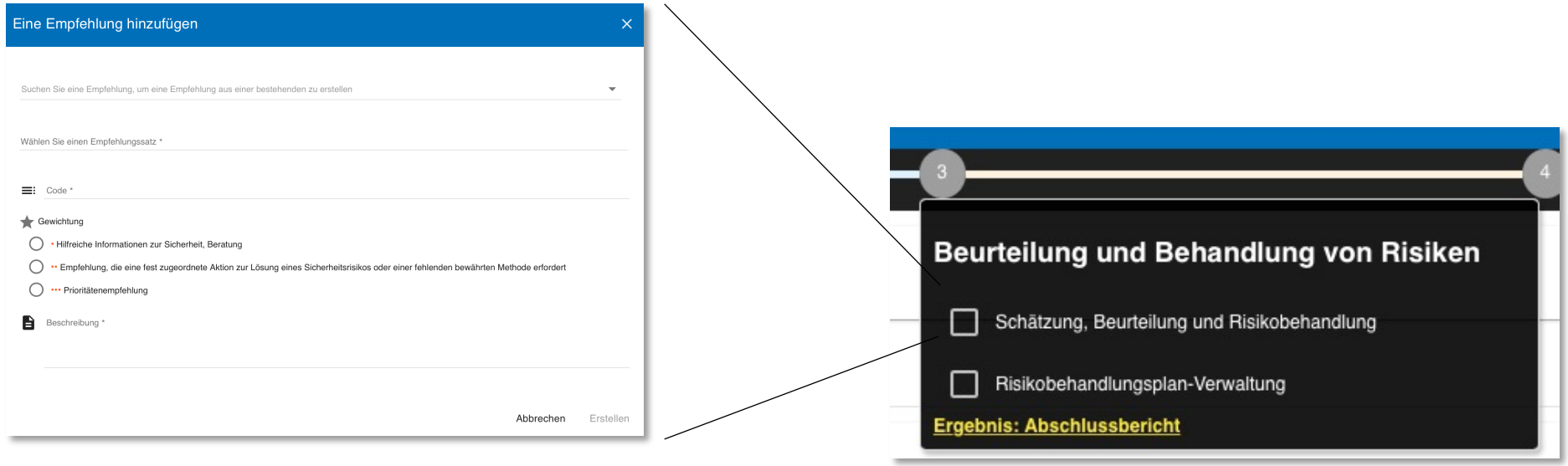
3.1 Schätzung, Beurteilung und Risikobehandlung





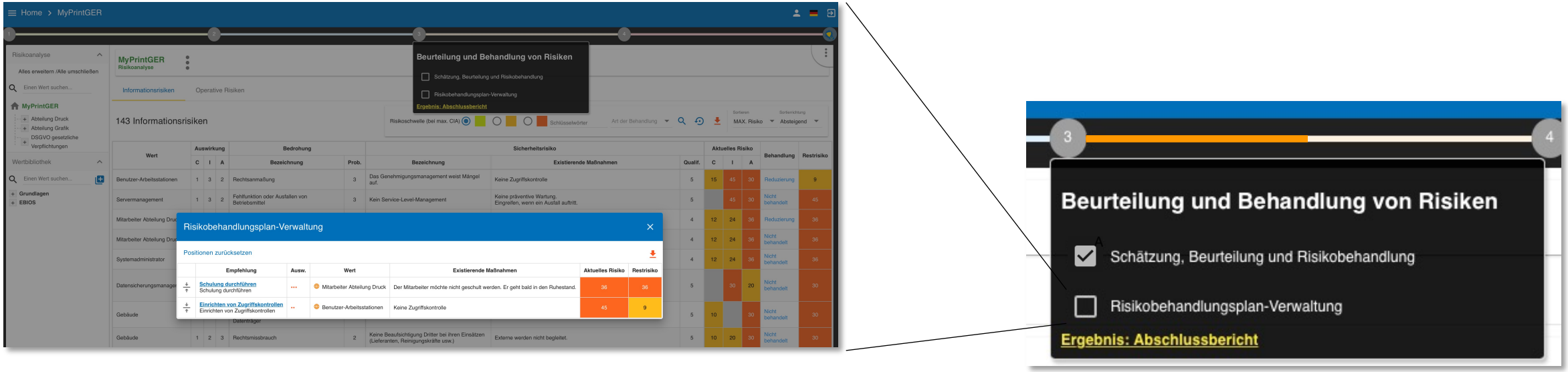
- Aktuelles Risiko und Restrisiko
- Risikobehandlung

3.1 Schätzung, Beurteilung und Risikobehandlung



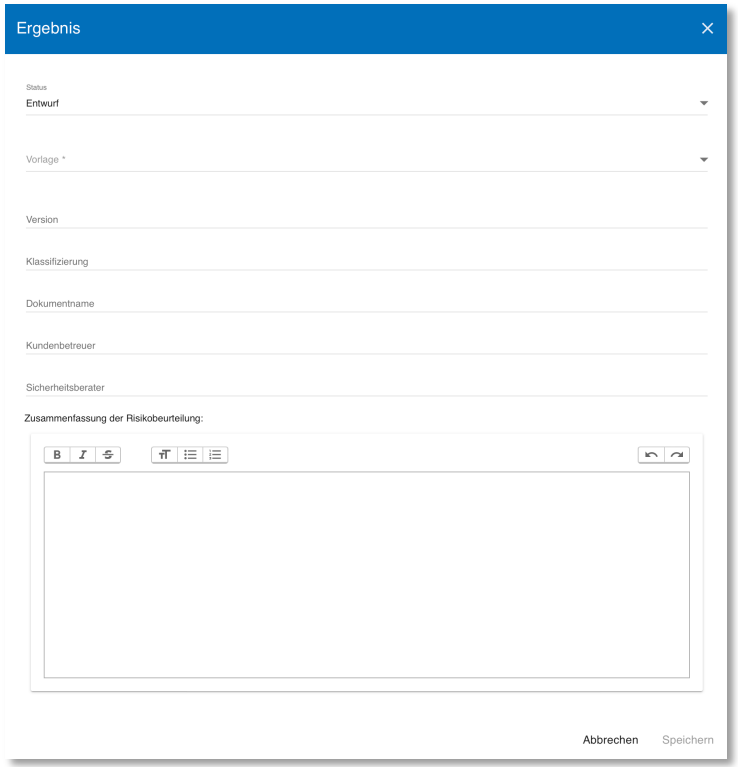
- Anlegen einer Maßnahme

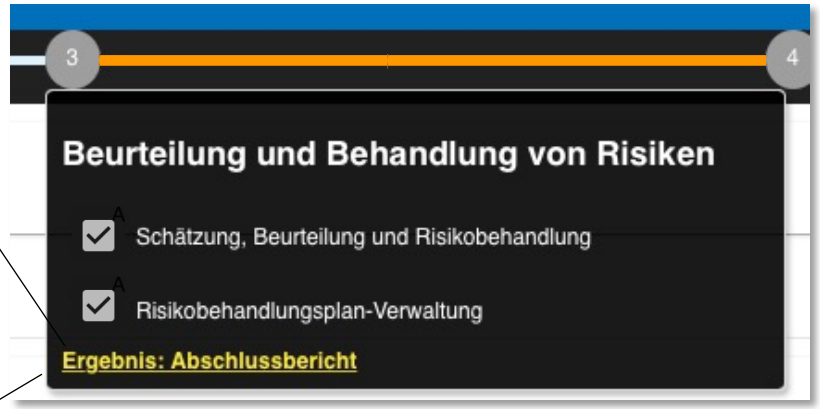
3.2 Risikobehandlungsplan-Verwaltung



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

3.3 Ergebnis: Abschlussbericht





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

3. Beurteilung und Behandlung von Risiken - Übung

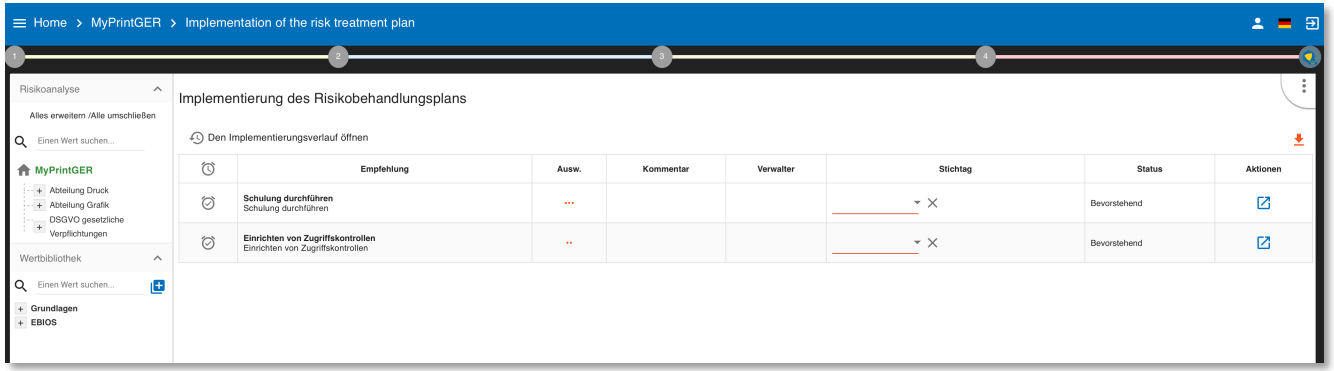
Übung: Durchführen der Beurteilung und Behandlung von Risiken (30 Minuten)

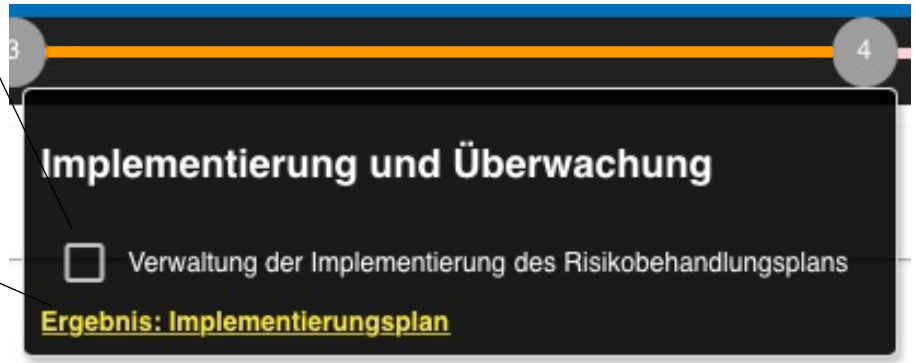
- **Ziel**: Durchführen einer eigenen Risikobeurteilung mit Behandlungsmaßnahmen
- **Vorgaben**:
  - Nennung existierender Maßnahmen: *<individuell>*
  - Beurteilung des Reifegrads existierender Maßnahmen: *<individuell>*
  - Auswahl der Risikobehandlung: *<individuell>*
  - Anlegen von Maßnahmen / Empfehlungen: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

4. Implementierung und Überwachung

- Verwaltung der Implementierung des Risikobehandlungsplans

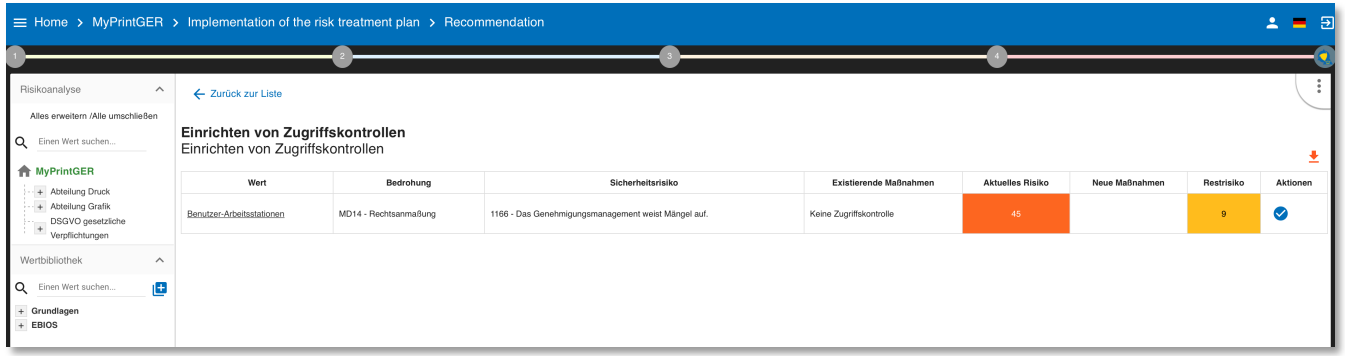
4.1 Verwaltung der Implementierung des Risikobehandlungsplans

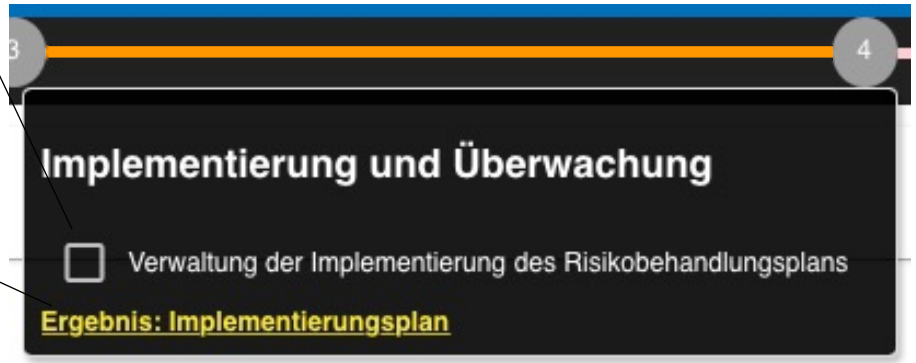




- Festlegen eines Verantwortlichen
- Hinterlegen von Kommentaren
- Definition eines Stichtages
- Verifikation des Umsetzungsstatus

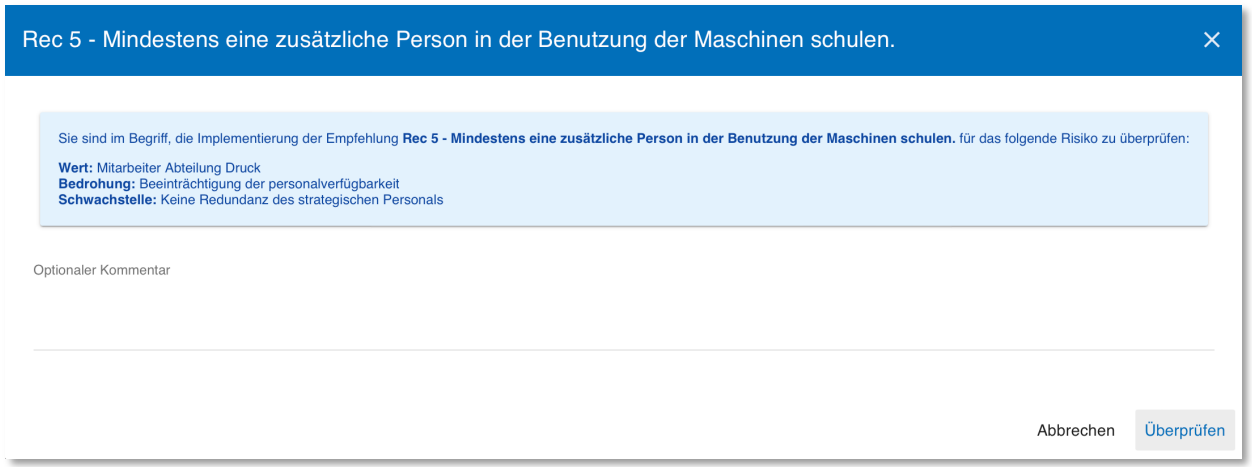
4.1 Verwaltung der Implementierung des Risikobehandlungsplans

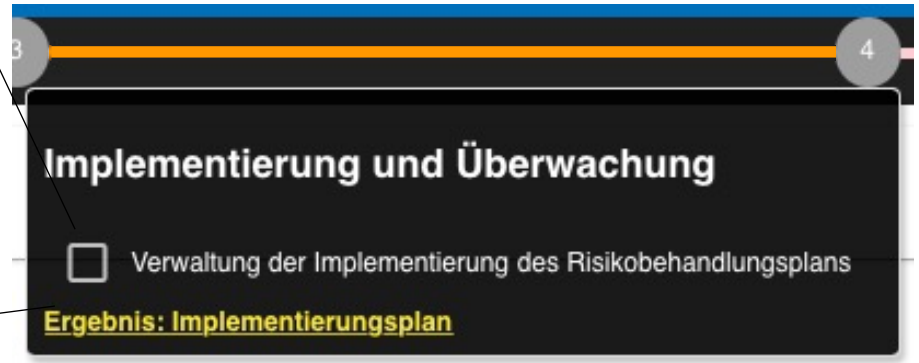




- Änderung des Risikos:
  Das „Restrisiko“ wird zum „aktuellen Risiko“
- Die „neue Maßnahme“ wird zur „existierenden Maßnahme“

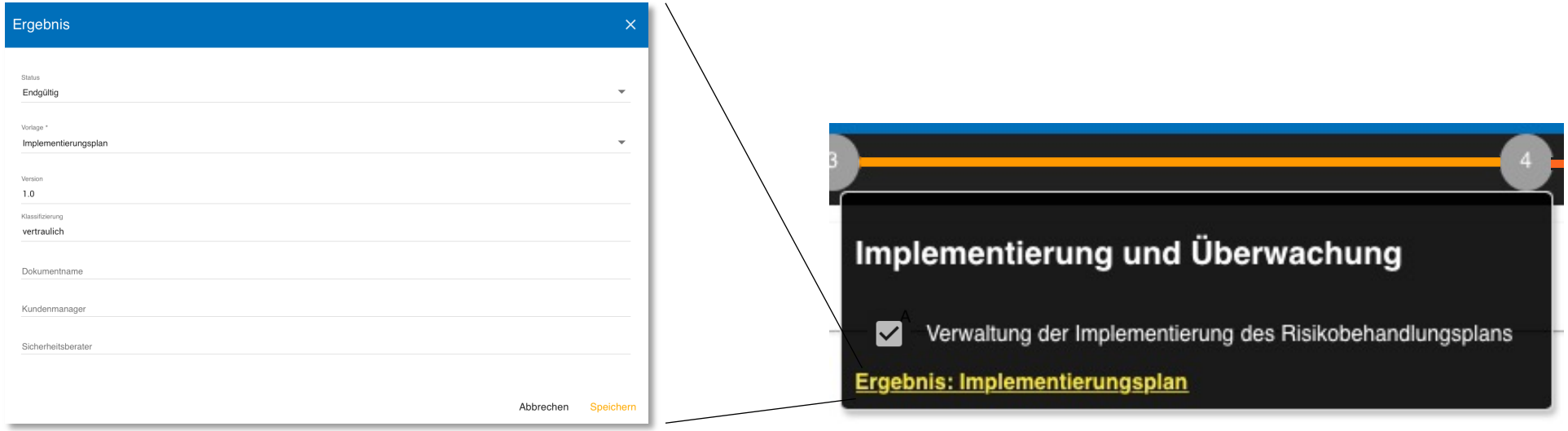
4.1 Verwaltung der Implementierung des Risikobehandlungsplans





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

4.2 Ergebnis: Implementierungsplan



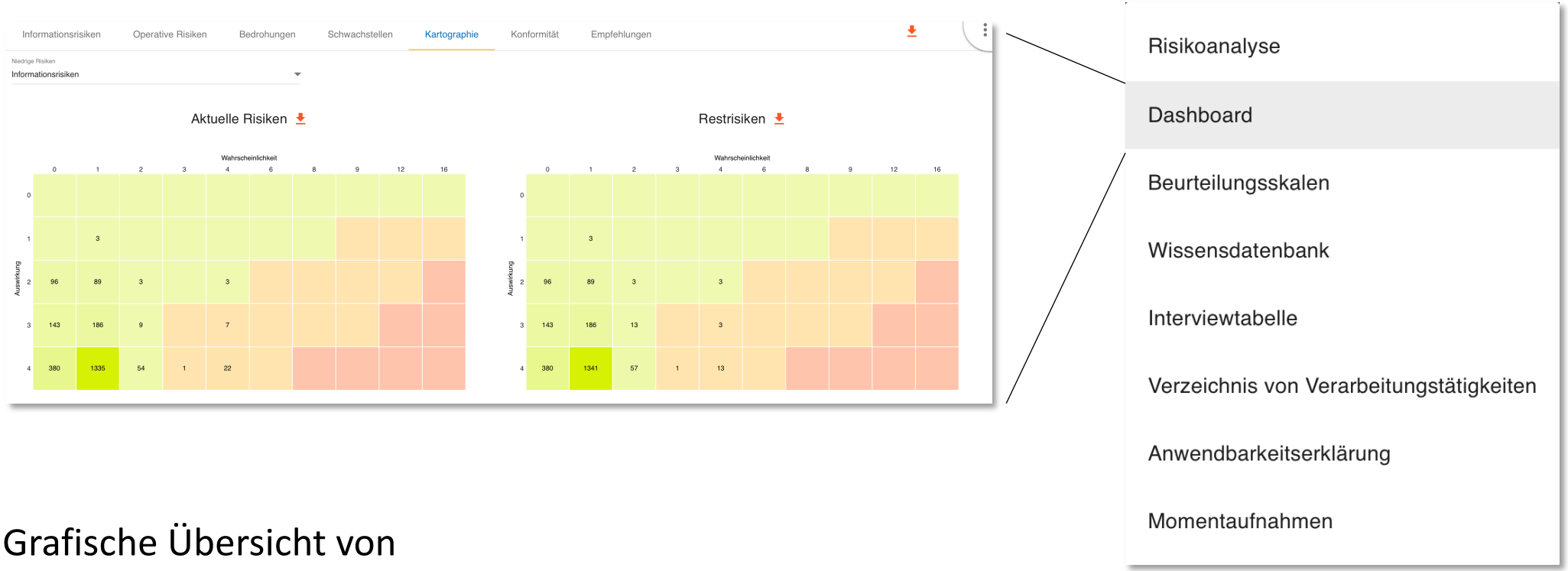
- Zusammenfassung des Risikobehandlungsplanes
- Aufstellung der bereits umgesetzten Maßnahmen
- Ziel: Offizieller Bericht zur Risikobehandlung
- Format: MS Word / ODF

4. Implementierung und Überwachung - Übung

Übung: Implementierung und Überwachung von Maßnahmen (30 Minuten)

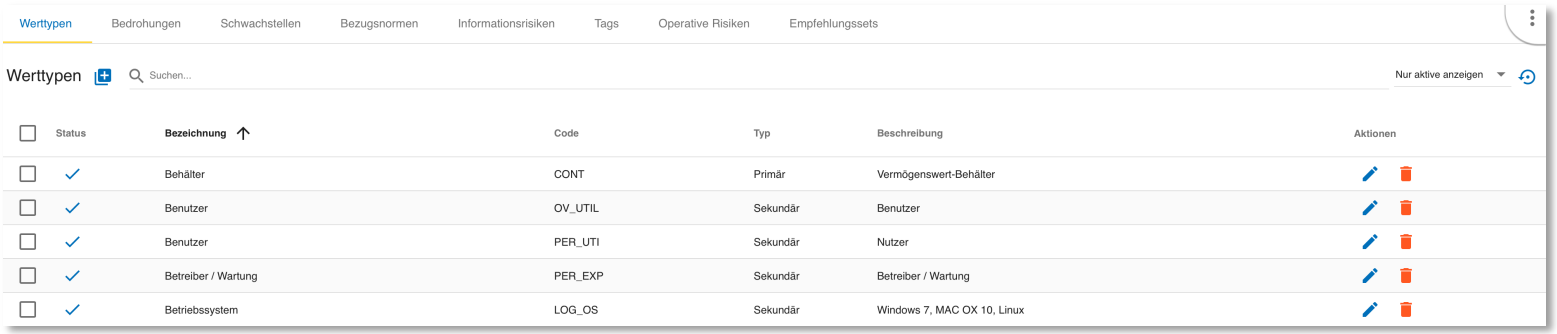
- **Ziel**: Durchführen einer eigenen Maßnahmenplanung und Umsetzung
- **Vorgaben**:
  - Import der einheitlichen Testumgebung: `MyPrintGER.json`
  - Bestimmung eigener Maßnahmenplanungen: *<individuell>*
  - Umsetzung von Maßnahmen dokumentieren: *<individuell>*
  - Erstellung eines eigenen Reports

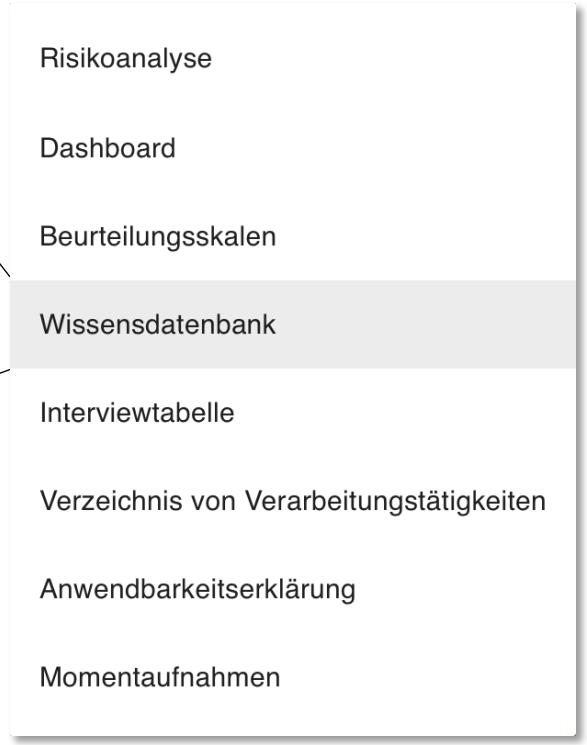
MONARC - Dashboard



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

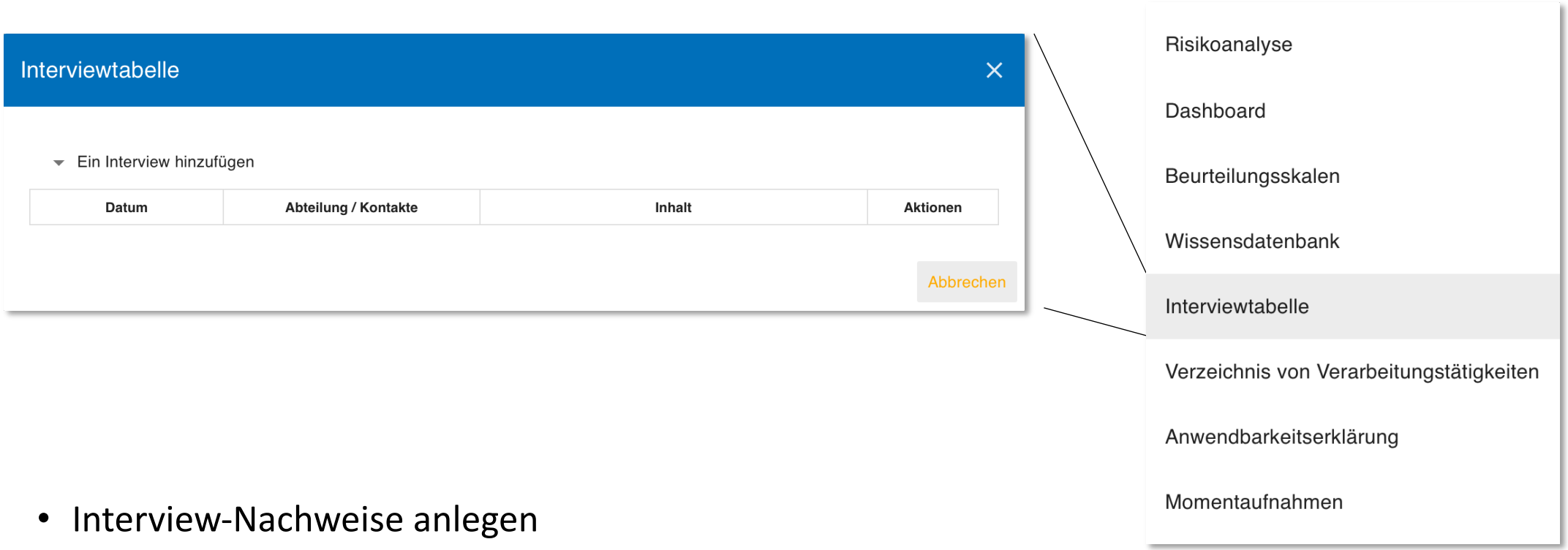
MONARC - Wissensdatenbank





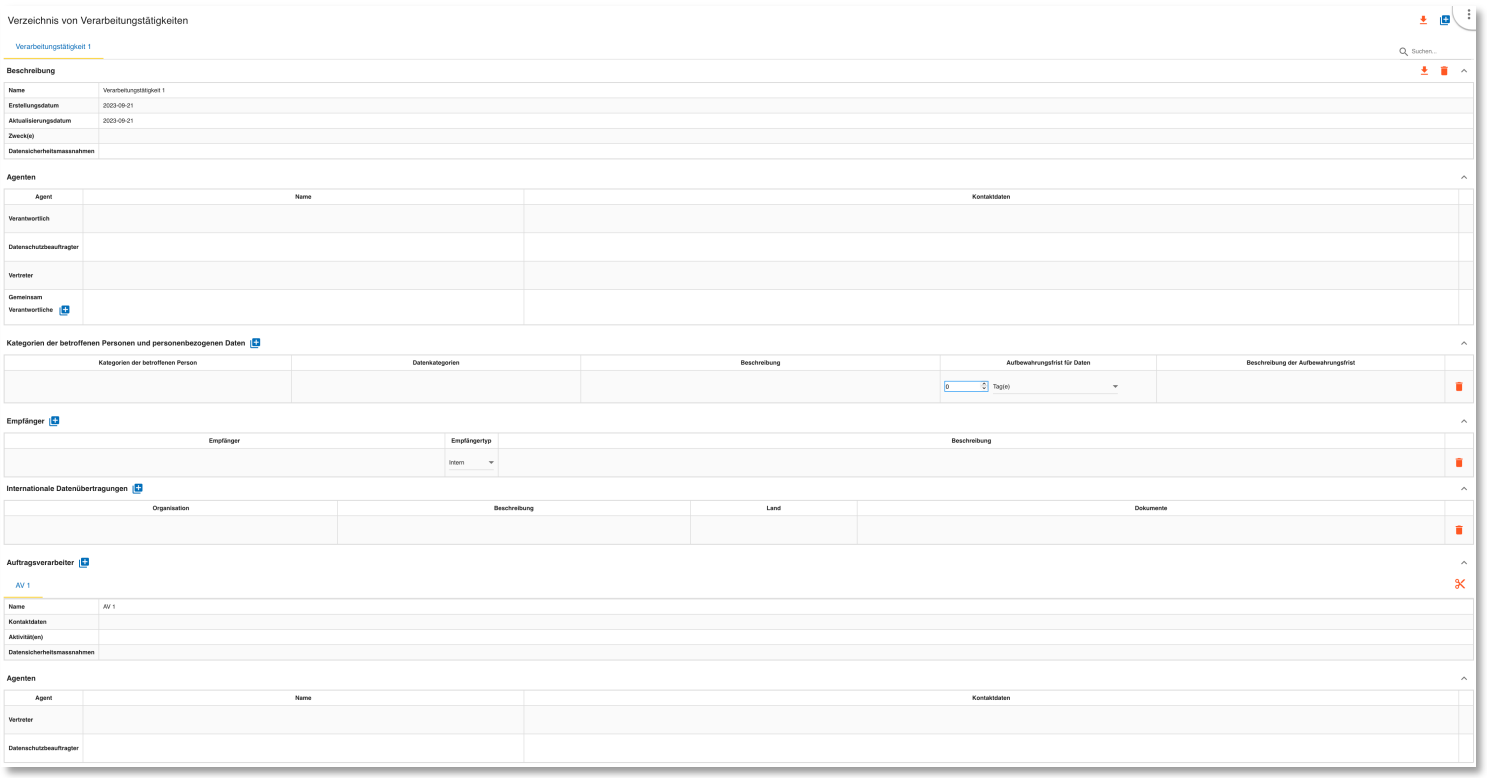
- Wissensdatenbank mit
  - Wertetypen, Bedrohungen, Schwachstellen, Bezugsnormen, Informationsrisiken, Tags, Operative Risiken, Empfehlungssets

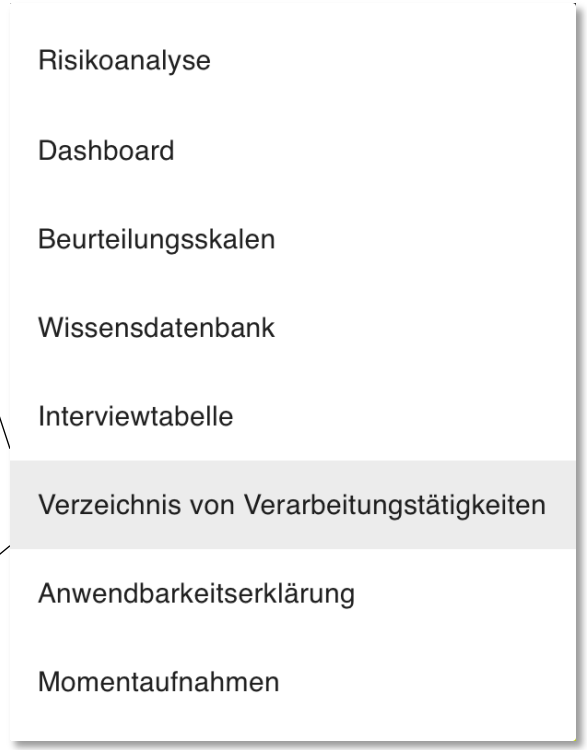
MONARC - Interviewtabelle



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

MONARC - Verzeichnis Verarbeitungstätigkeiten

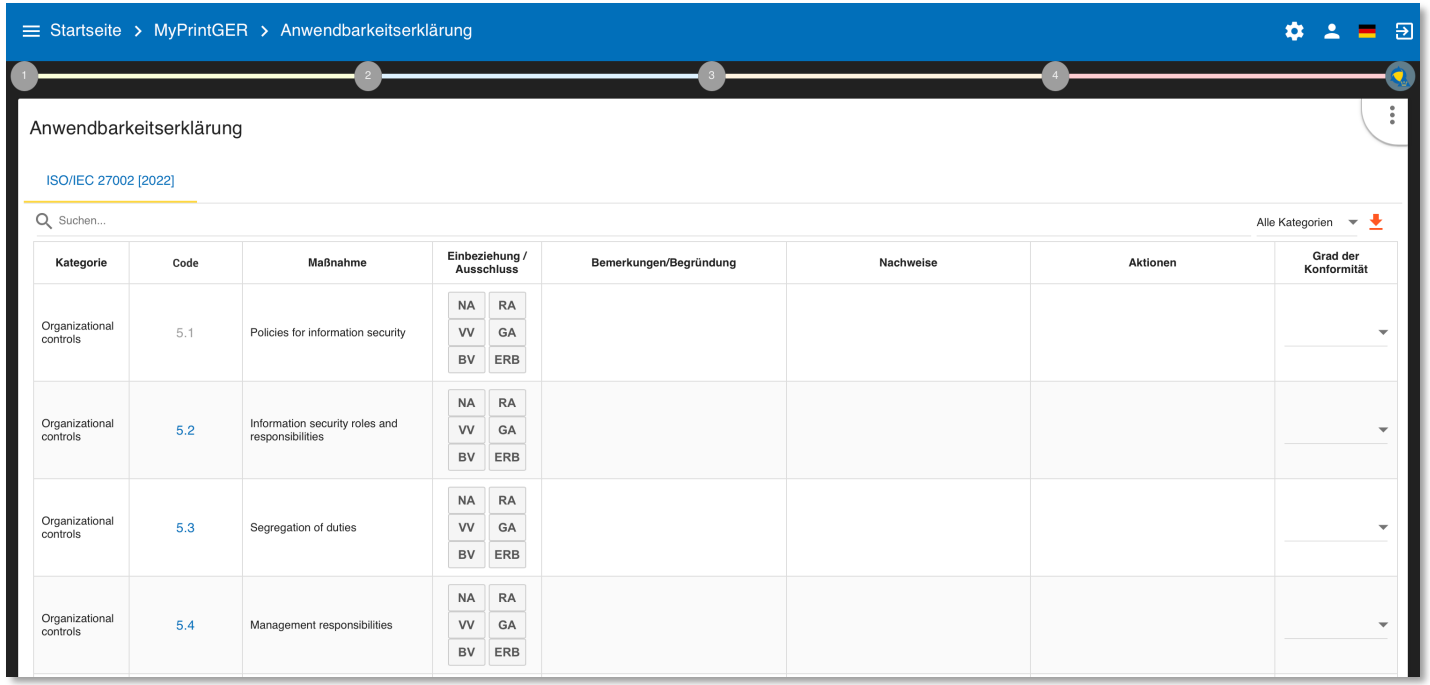


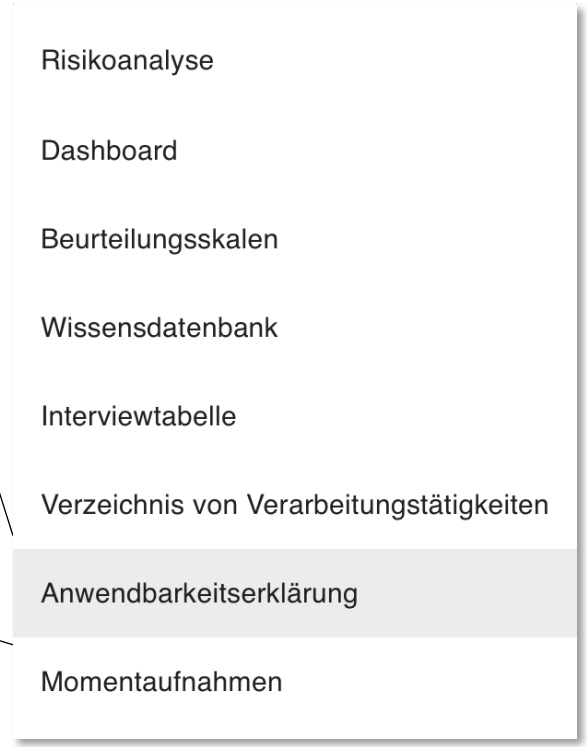


- Abbildung von EU-DSGVO Nachweisen

www.konzeptacht.de

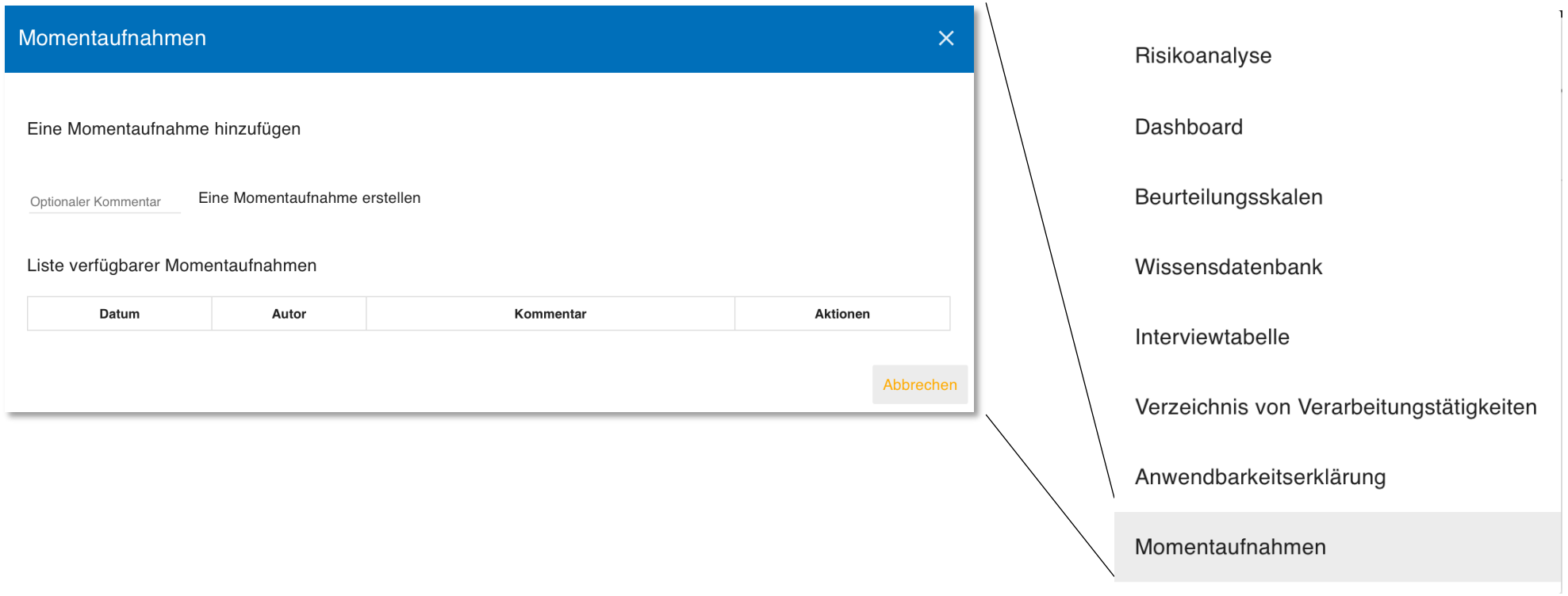
MONARC - Anwendbarkeitserklärung





- 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)

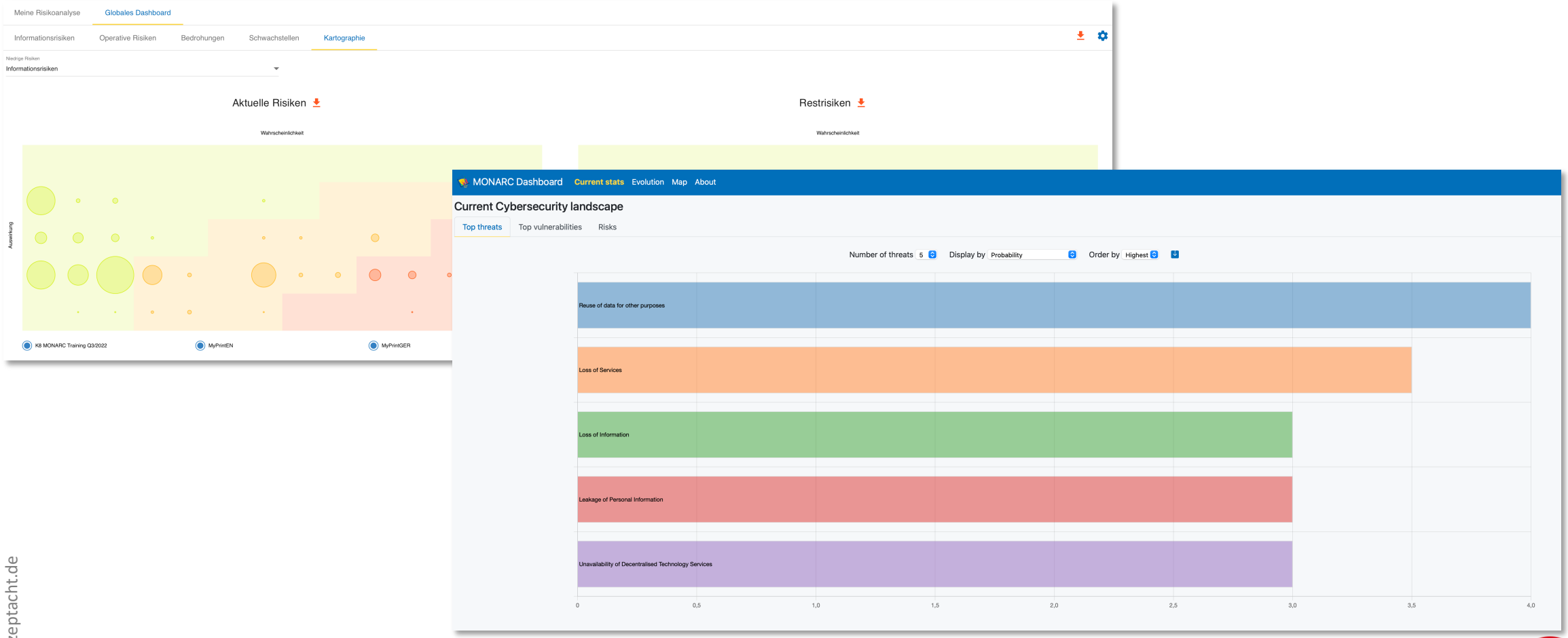
Weitere Tipps & Tricks

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

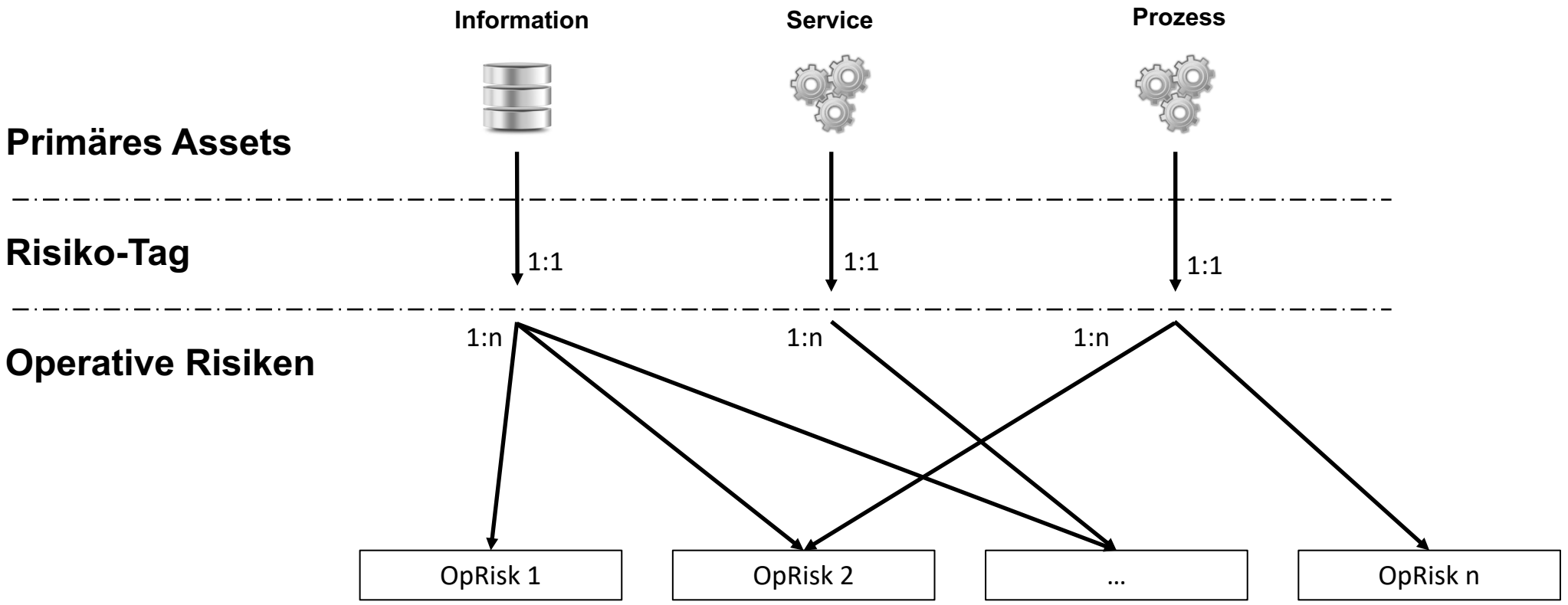
Technisches Wissen

- Wissenswertes zum technischen Aufsetzen der Plattform – bei Interesse
  - Installationsanleitung unter GitHub
  - Stats-Service

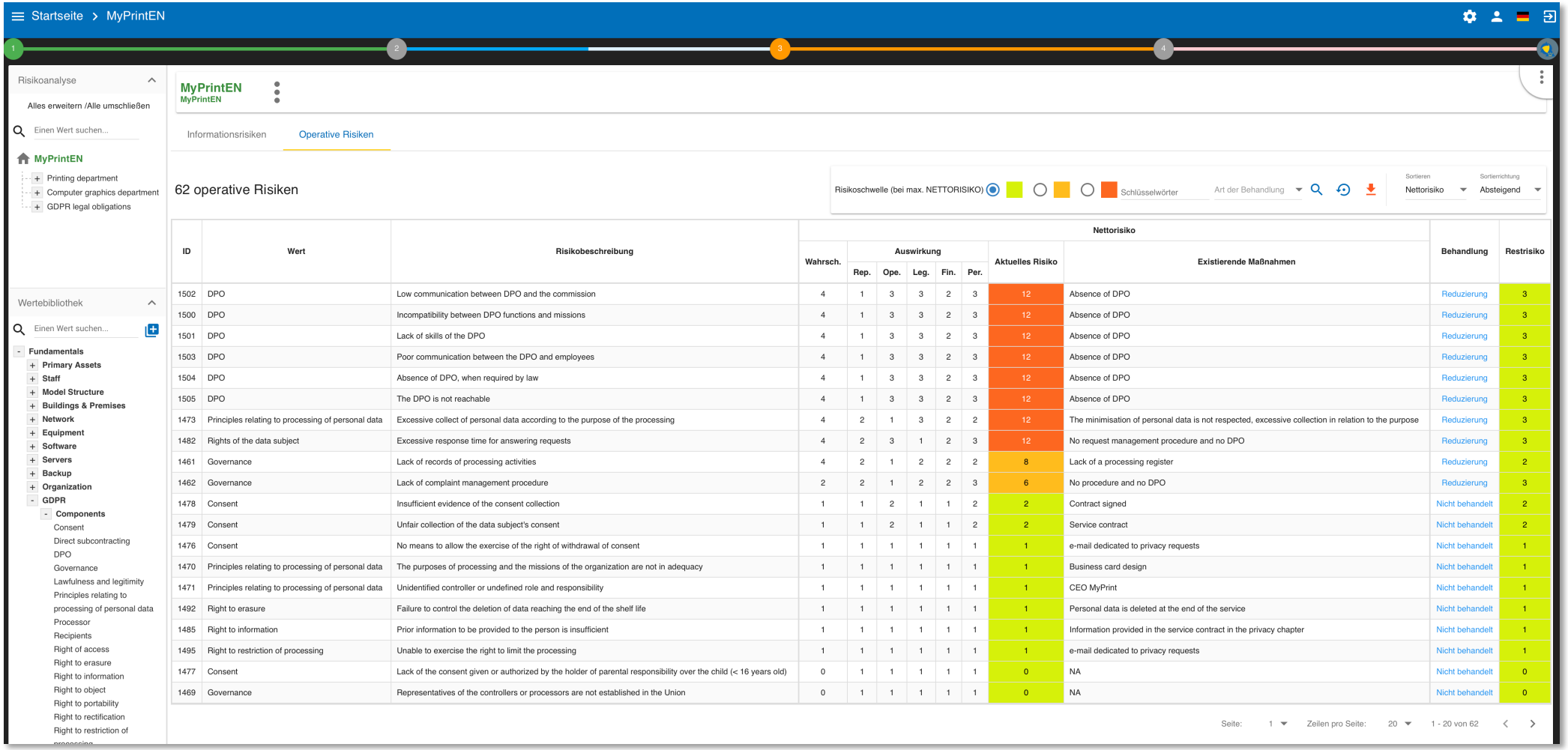
Global Dashboard



Exkurs: Operative Risiken

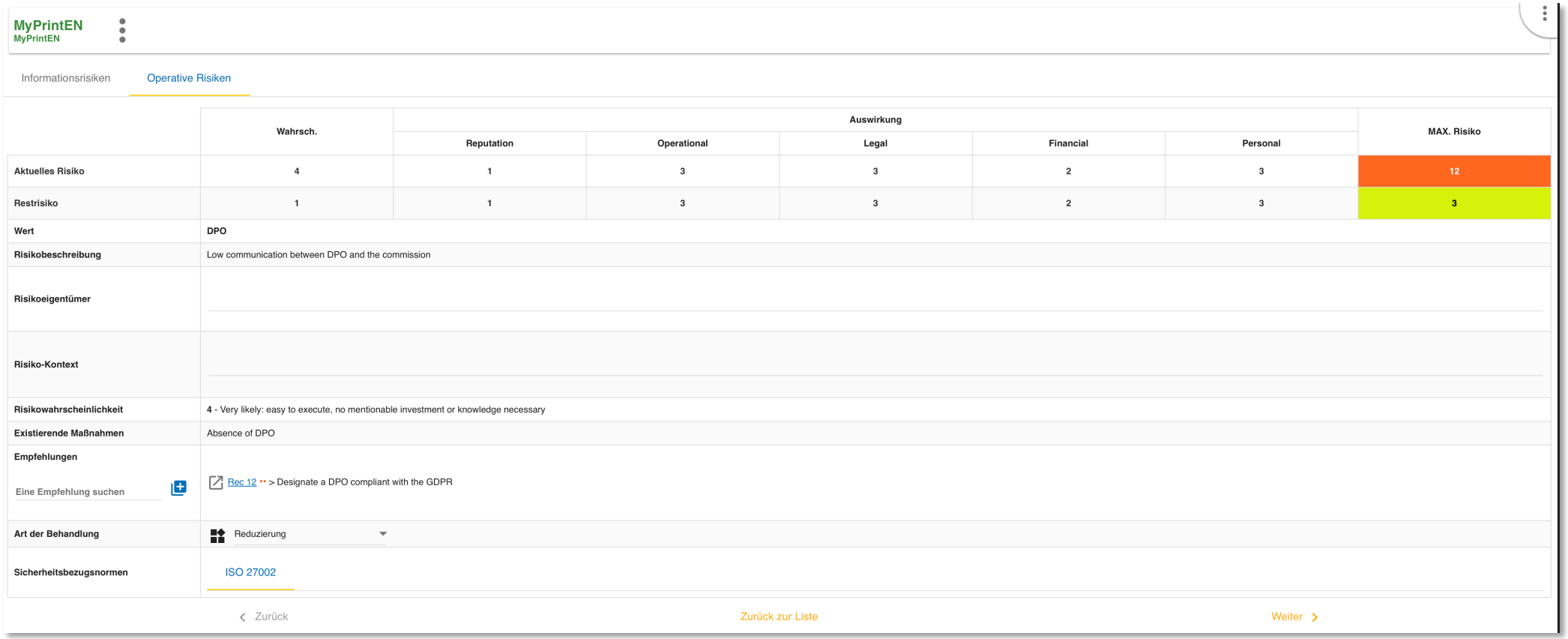


Exkurs: Operative Risiken



ID	Wert	Risikobeschreibung	Nettorisiko							Behandlung	Restrisiko
			Wahrsch.	Auswirkung					Aktuelles Risiko	Existierende Maßnahmen	
				Rep.	Ope.	Leg.	Fin.	Per.			
1502	DPO	Low communication between DPO and the commission	4	1	3	3	2	3	12	Absence of DPO	Reduzierung	3
1500	DPO	Incompatibility between DPO functions and missions	4	1	3	3	2	3	12	Absence of DPO	Reduzierung	3
1501	DPO	Lack of skills of the DPO	4	1	3	3	2	3	12	Absence of DPO	Reduzierung	3
1503	DPO	Poor communication between the DPO and employees	4	1	3	3	2	3	12	Absence of DPO	Reduzierung	3
1504	DPO	Absence of DPO, when required by law	4	1	3	3	2	3	12	Absence of DPO	Reduzierung	3
1505	DPO	The DPO is not reachable	4	1	3	3	2	3	12	Absence of DPO	Reduzierung	3
1473	Principles relating to processing of personal data	Excessive collect of personal data according to the purpose of the processing	4	2	1	3	2	2	12	The minimisation of personal data is not respected, excessive collection in relation to the purpose	Reduzierung	3
1482	Rights of the data subject	Excessive response time for answering requests	4	2	3	1	2	3	12	No request management procedure and no DPO	Reduzierung	3
1461	Governance	Lack of records of processing activities	4	2	1	2	2	2	8	Lack of a processing register	Reduzierung	2
1462	Governance	Lack of complaint management procedure	2	2	1	2	2	3	6	No procedure and no DPO	Reduzierung	3
1478	Consent	Insufficient evidence of the consent collection	1	1	2	1	1	2	2	Contract signed	Nicht behandelt	2
1479	Consent	Unfair collection of the data subject's consent	1	1	2	1	1	2	2	Service contract	Nicht behandelt	2
1476	Consent	No means to allow the exercise of the right of withdrawal of consent	1	1	1	1	1	1	1	e-mail dedicated to privacy requests	Nicht behandelt	1
1470	Principles relating to processing of personal data	The purposes of processing and the missions of the organization are not in adequacy	1	1	1	1	1	1	1	Business card design	Nicht behandelt	1
1471	Principles relating to processing of personal data	Unidentified controller or undefined role and responsibility	1	1	1	1	1	1	1	CEO MyPrint	Nicht behandelt	1
1492	Right to erasure	Failure to control the deletion of data reaching the end of the shelf life	1	1	1	1	1	1	1	Personal data is deleted at the end of the service	Nicht behandelt	1
1485	Right to information	Prior information to be provided to the person is insufficient	1	1	1	1	1	1	1	Information provided in the service contract in the privacy chapter	Nicht behandelt	1
1495	Right to restriction of processing	Unable to exercise the right to limit the processing	1	1	1	1	1	1	1	e-mail dedicated to privacy requests	Nicht behandelt	1
1477	Consent	Lack of the consent given or authorized by the holder of parental responsibility over the child (< 16 years old)	0	1	1	1	1	1	0	NA	Nicht behandelt	0
1469	Governance	Representatives of the controllers or processors are not established in the Union	0	1	1	1	1	1	0	NA	Nicht behandelt	0

Exkurs: Operative Risiken



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

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)
- Threat Intelligence

Ihr Kontakt

https://www.konzeptacht.de

Thomas Kochanek

Thomas Kochanek

www.konzeptacht.de

Ihr Kontakt

https://www.konzeptacht.de

Marc Sparwel