



Informationssicherheit gestalten.

# Risikomanagement mit dem Tool MONARC (Optimised Risk Analysis Method)

# Agenda

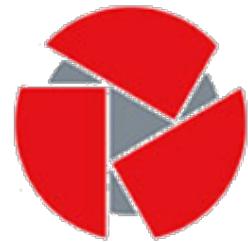
- Vorstellung
- Was ist MONARC?
- Die MONARC Methodik
- Aufbau und Nutzung des Tools
- Tipps & Tricks



LE GOUVERNEMENT  
DU GRAND-DUCHÉ DE LUXEMBOURG



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



**circL**

---

*Computer Incident  
Response Center  
Luxembourg*



**cases**

---

*Cyberworld Awareness  
and Security Enhancement  
Services*

[www.securitymadein.lu](http://www.securitymadein.lu)  
[www.cases.lu](http://www.cases.lu)



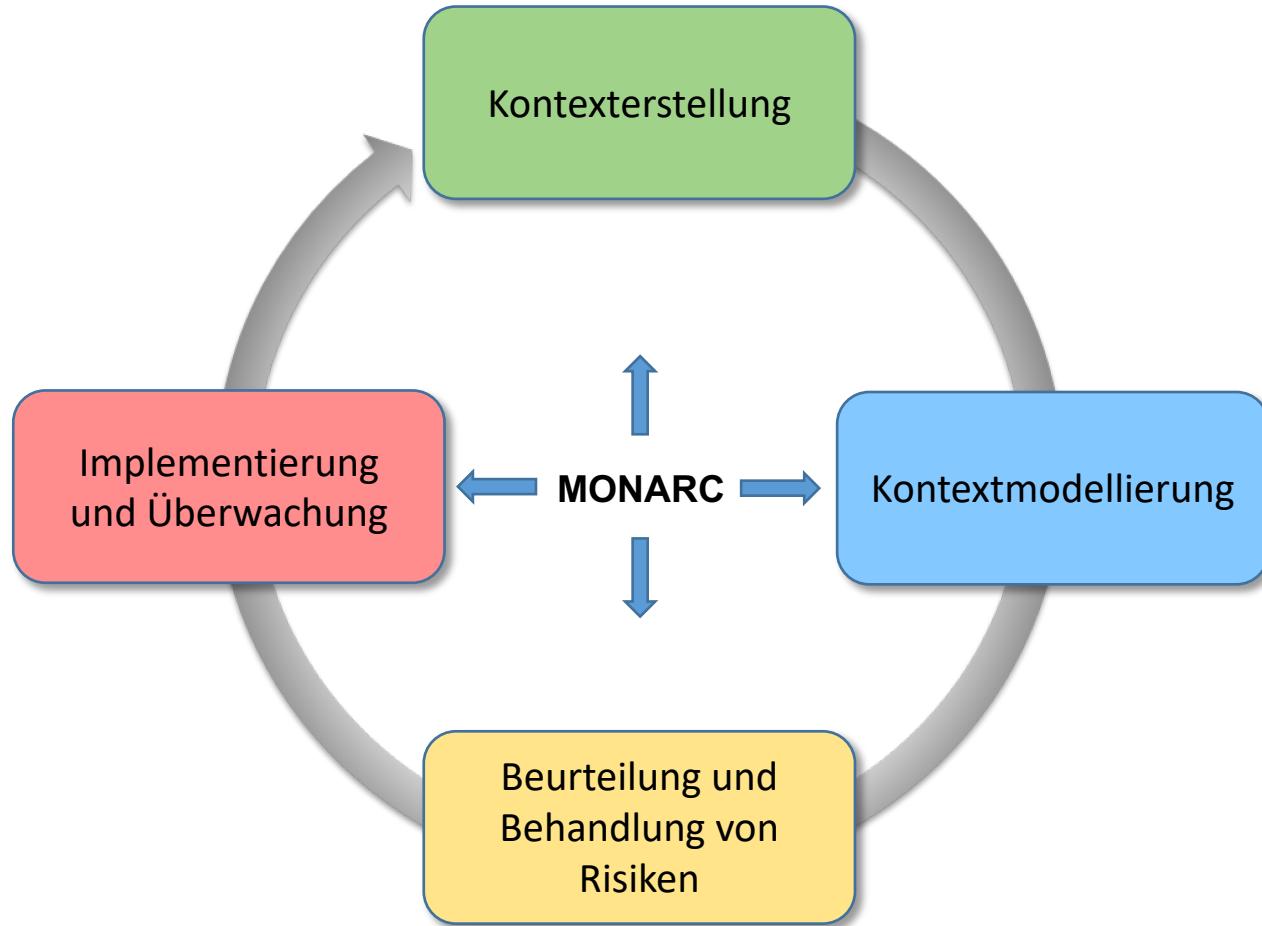
# Was ist MONARC?

- Optimised Risk Analysis Method (Méthode Optimisée d'Analyse des Risques)
- Open Source Software
- Web Applikation (SaaS, self-hosted, virtuelle Maschine, hosted by KonzeptAcht GmbH, etc.)
- Source Code<sup>3</sup> unter GNU Affero General Public License version 3
- Daten unterliegen CC0 1.0 Universal (CC0 1.0) – Public Domain Dedication
- 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.

<sup>3</sup> <https://github.com/monarc-project>



# MONARC Methodik

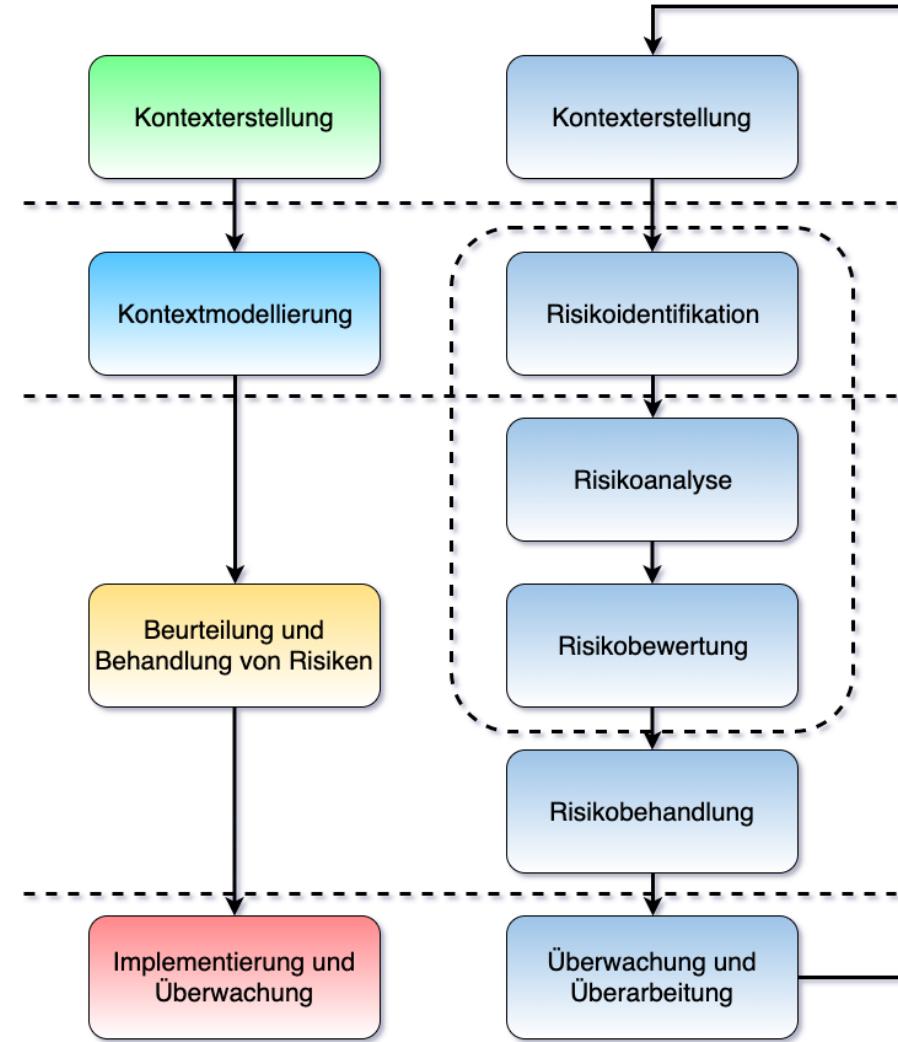


## Methodik der Risikoanalyse

- **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

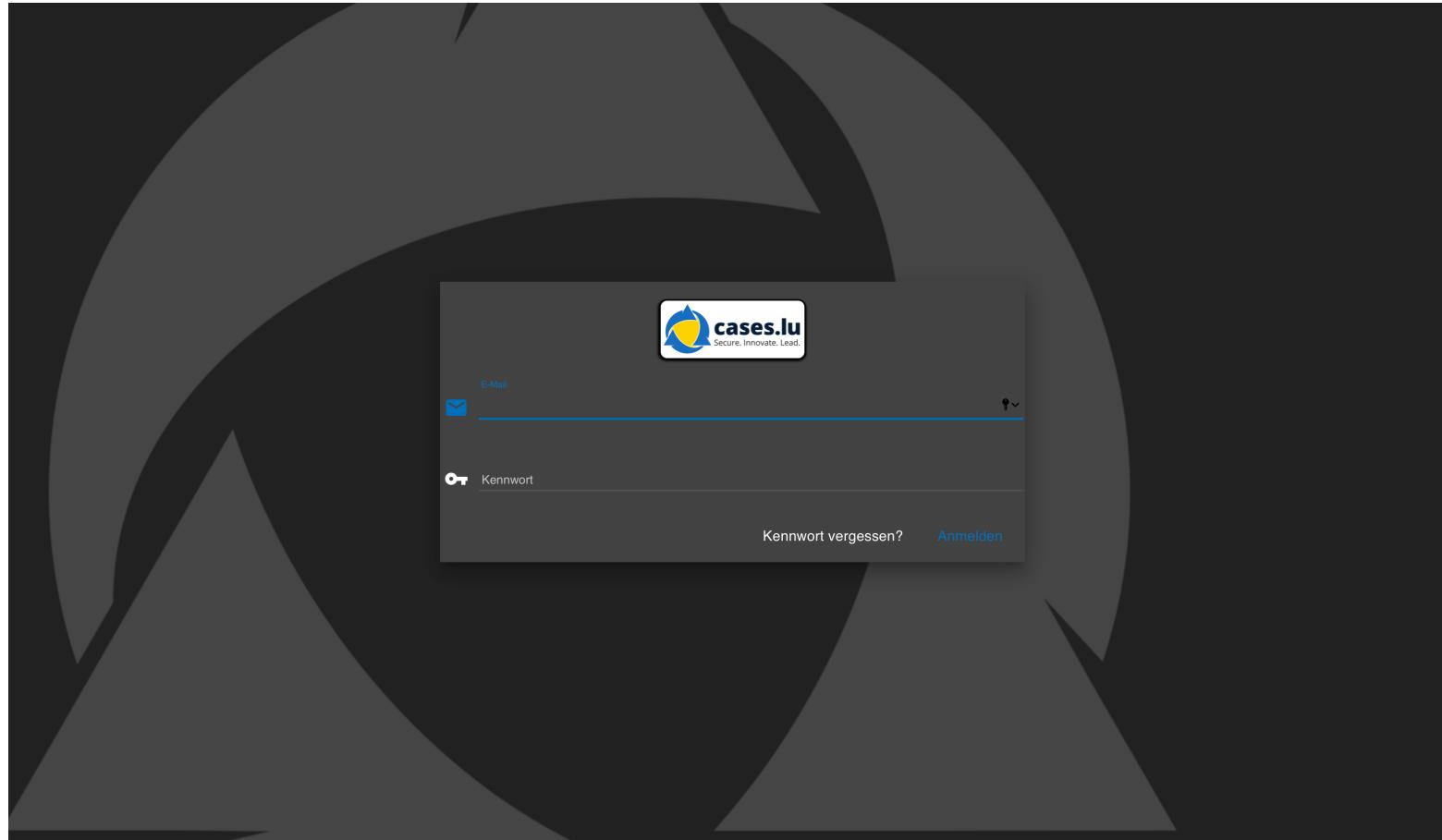
Die folgende Formel wird zur Berechnung des Risikos angewendet:

$$R = (P \times A) \times Q$$

**R:** Risiko, **P:** Eintrittswahrscheinlichkeit, **A:** Auswirkung, **Q:** Reifegrad der Maßnahme



# Erstellung Risikoanalyse in MONARC



# Erstellung Risikoanalyse in MONARC

Eine Risikoanalyse erstellen X

Quelle

Liste der Risikomodelle  Existierende Risikoanalyse

Beschreibung

 Sprache \* ▼

 Name \* .....

 Beschreibung .....

 + Fügen Sie eine Bezugsnorm hinzu

Abbrechen Erstellen

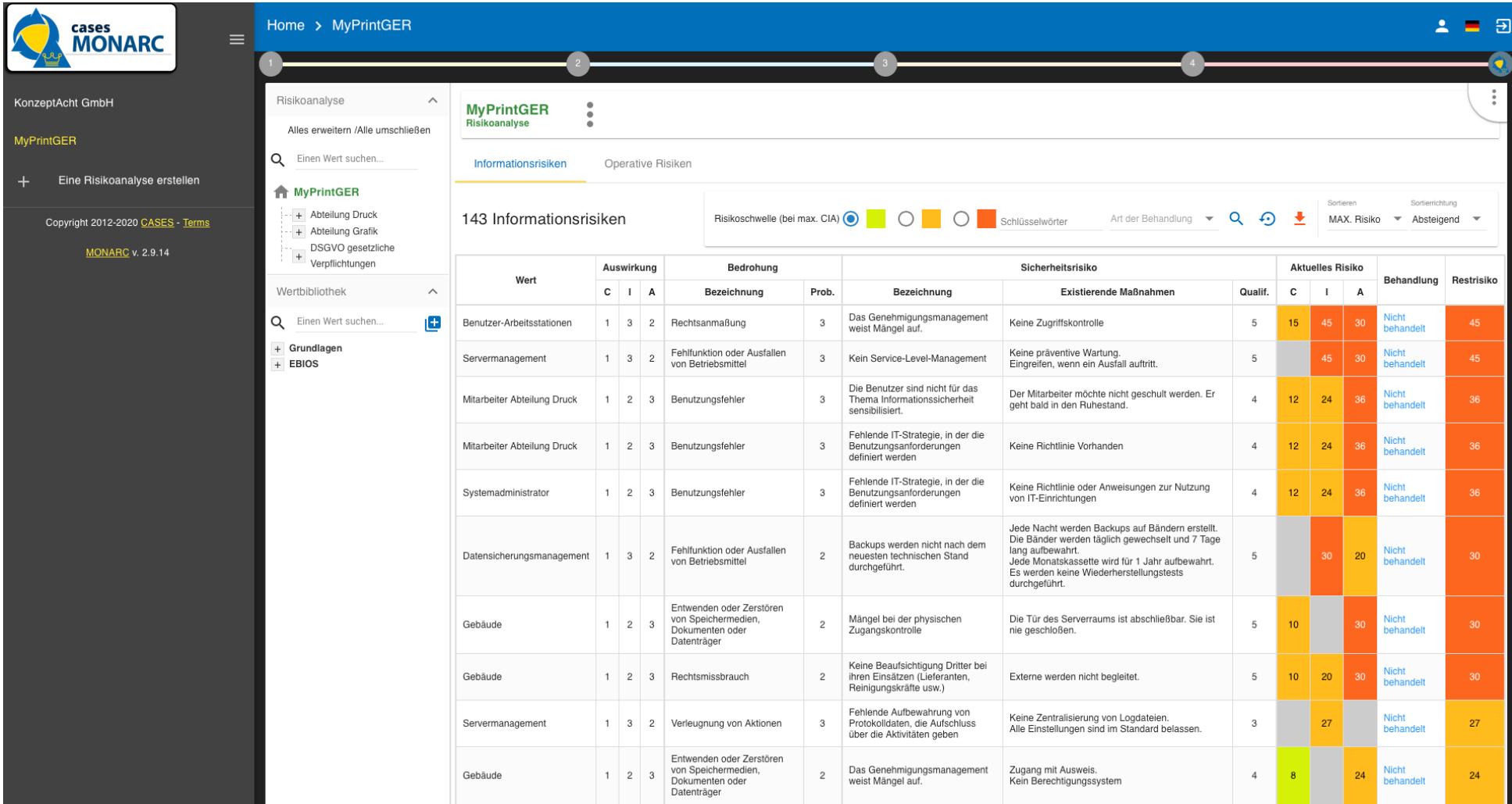
# Erstellung Risikoanalyse in MONARC

## 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



MyPrintGER Risikoanalyse

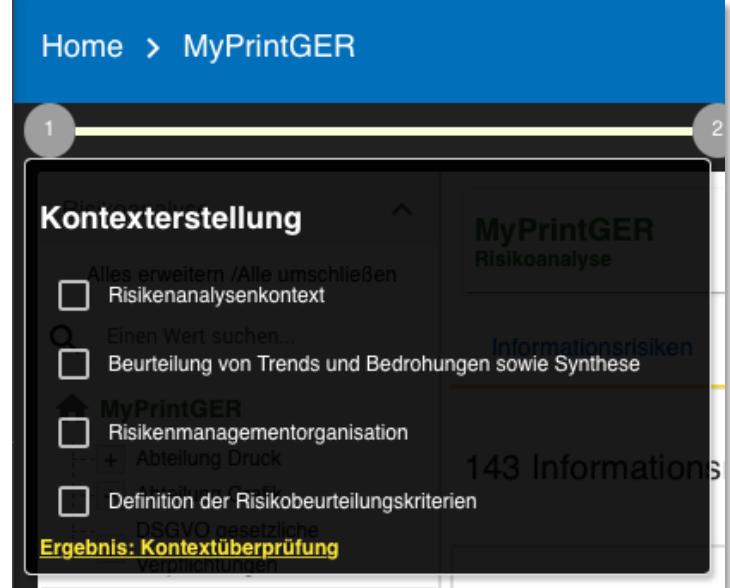
143 Informationsrisiken

Wert	Auswirkung			Bedrohung		Sicherheitsrisiko			Aktuelles Risiko			Behandlung	Restrisiko
	C	I	A	Bezeichnung	Prob.	Bezeichnung	Existierende Maßnahmen	Qualif.	C	I	A		
Benutzer-Arbeitsstationen	1	3	2	Rechtsanmaßung	3	Das Genehmigungsmanagement weist Mängel auf.	Keine Zugriffskontrolle	5	15	45	30	Nicht behandelt	45
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	Nicht behandelt	45
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	Nicht behandelt	36
Mitarbeiter Abteilung Druck	1	2	3	Benutzungsfehler	3	Fehlende IT-Strategie, in der die Benutzungsanforderungen definiert werden	Keine Richtlinie Vorhanden	4	12	24	36	Nicht behandelt	36
Systemadministrator	1	2	3	Benutzungsfehler	3	Fehlende IT-Strategie, in der die Benutzungsanforderungen definiert werden	Keine Richtlinie oder Anweisungen zur Nutzung von IT-Einrichtungen	4	12	24	36	Nicht behandelt	36
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	Nicht behandelt	30
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
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		Nicht behandelt	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



# 1. Kontexterstellung

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



Home > MyPrintGER

1 2

**Kontexterstellung**

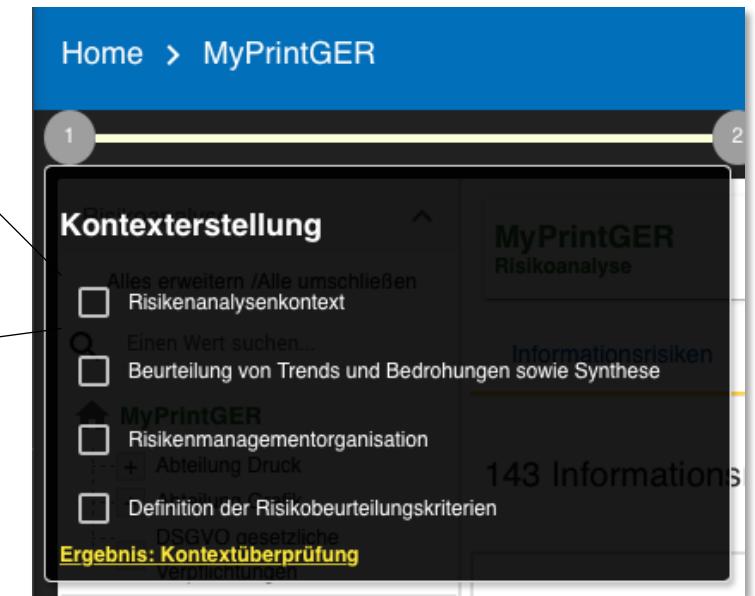
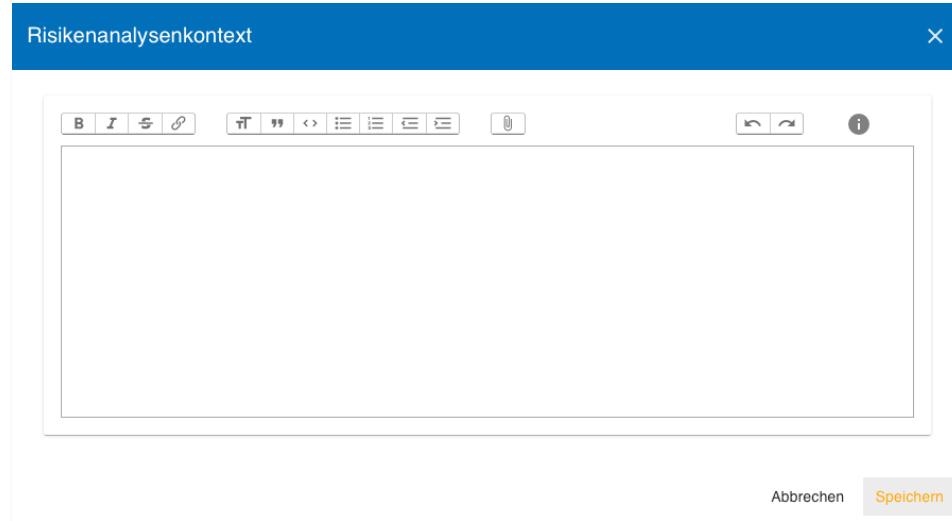
- Alles erweitern /Alle umschließen
- Risikoanalysenkontext
- Einen Wert suchen...
- Beurteilung von Trends und Bedrohungen sowie Synthese
- MyPrintGER Risikomanagementorganisation
  - + Abteilung Druck
- Definition der Risikobeurteilungskriterien
  - + DSGVO gesetzliche Verpflichtungen

**Ergebnis: Kontextüberprüfung**

143 Informations



# 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

Beurteilung von Trends und Bedrohungen sowie Synthese

Beurteilung von Trends   Beurteilung von Bedrohungen   Zusammenfassung

Was ist der Zweck Ihrer Organisation?

Welchen Verlauf hat Ihr Unternehmen in den letzten Jahren geschäftlich genommen?

Wie haben sich die externen Kriterien verändert (Wettbewerb, Marktentwicklung, rechtliche Rahmenbedingungen usw.)?

Welche Angriffsflächen könnte Ihre Struktur bieten?

Nennen Sie Ihre wichtigsten Geschäftsprozesse:

Home > MyPrintGER

1      2

**Kontexterstellung**

Alles erweitern /Alle umschließen  
 Risikenanalysenkontext

Einen Wert suchen...

Beurteilung von Trends und Bedrohungen sowie Synthese

**MyPrintGER**

Risikenmanagementorganisation  
 + Abteilung Druck

Definition der Risikobeurteilungskriterien  
 DSGVO gesetzliche Verpflichtungen

**Ergebnis: Kontextüberprüfung**

143 Informations

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



## 1.2.2 Beurteilung von Bedrohungen

Beurteilung von Trends und Bedrohungen sowie Synthese

Beurteilung von Trends Beurteilung von Bedrohungen Zusammenfassung

Analyse von Bedrohungen - 1 / 18

Thema: Physische Schadensfälle

Beschreibung:

Kommentare: Terroristische Akte sind bei der KonzeptAcht GmbH eher unwahrscheinlich.

Betroffene Kriterien:  C  I  A

Trend:  -  n  +  ++

Wahrscheinlichkeit: 1: gering: - Theoretisch möglich, aber ausgesprochen unwahrscheinlich - Ein Angreifer benötigt spezielle technische Fähigkeiten und Unterstützung sowie ein sehr hohes internes Expertenwissen - In der Praxis sehr unwahrscheinlich.  Wahrscheinlichkeit in der Analyse erzwingen

< Zurück Speichern Weiter >

Home > MyPrintGER

1 2

**Kontexterstellung**

Alles erweitern /Alle umschließen

Risikenanalysenkontext

Einen Wert suchen...

Beurteilung von Trends und Bedrohungen sowie Synthese

**MyPrintGER**

Risikenmanagementorganisation

+ Abteilung Druck

Definition der Risikobeurteilungskriterien

DSGVO gesetzliche Verpflichtungen

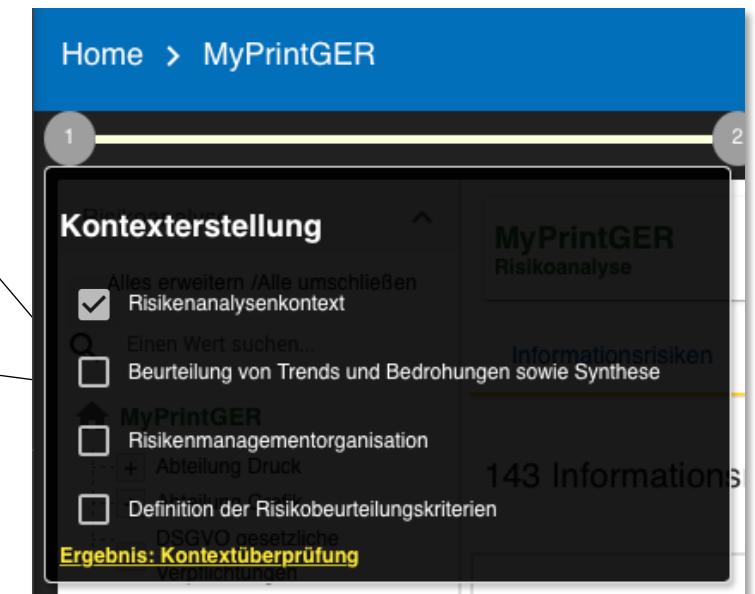
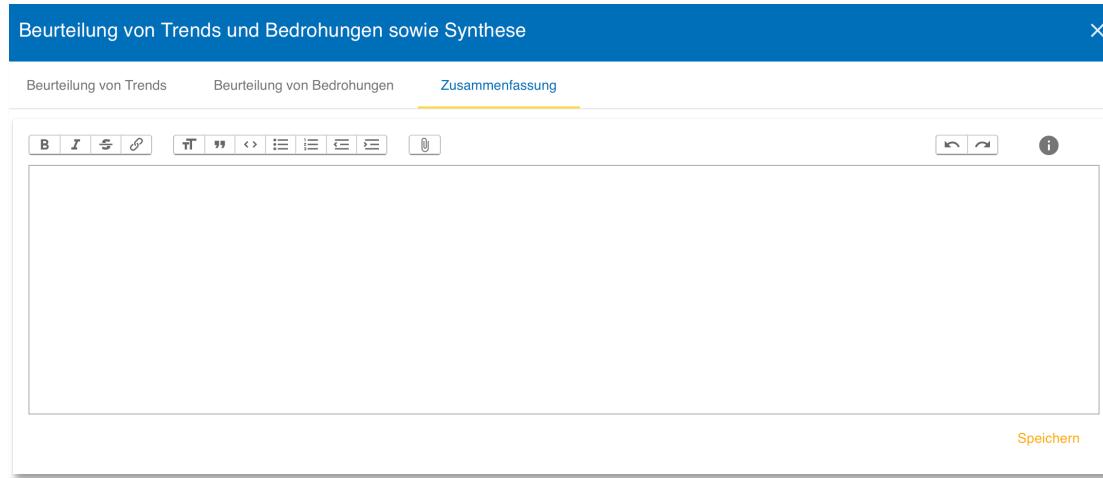
**Ergebnis: Kontexterstellung**

143 Informations

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



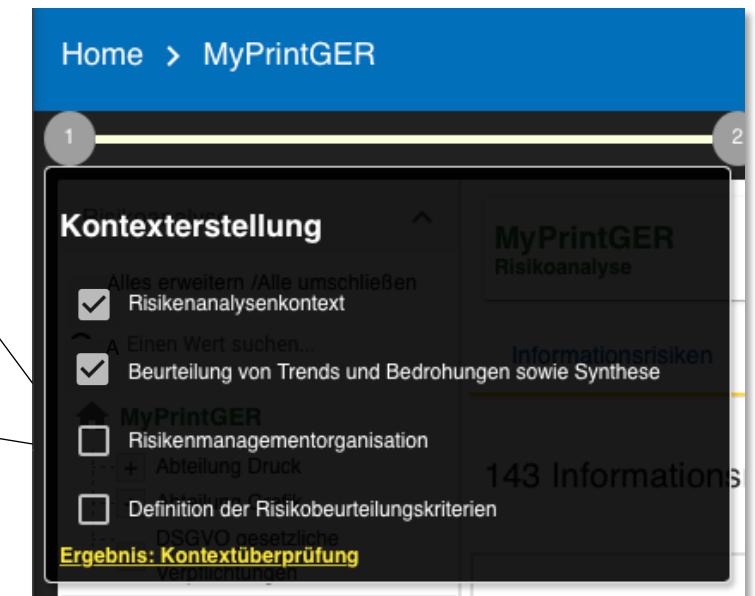
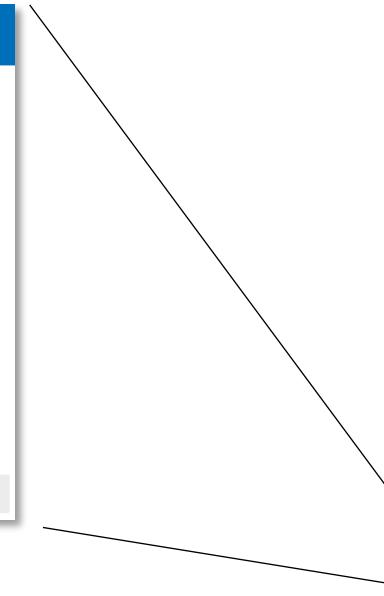
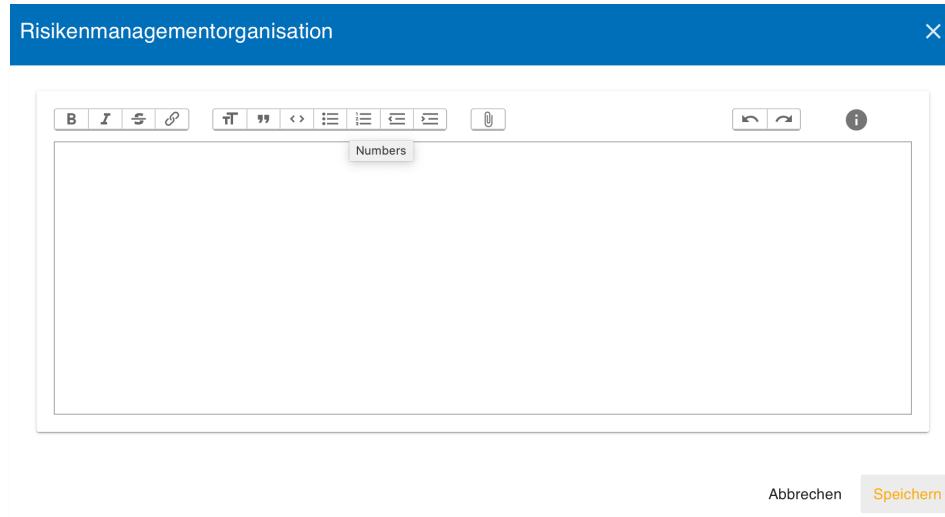
## 1.2.3 Zusammenfassung



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



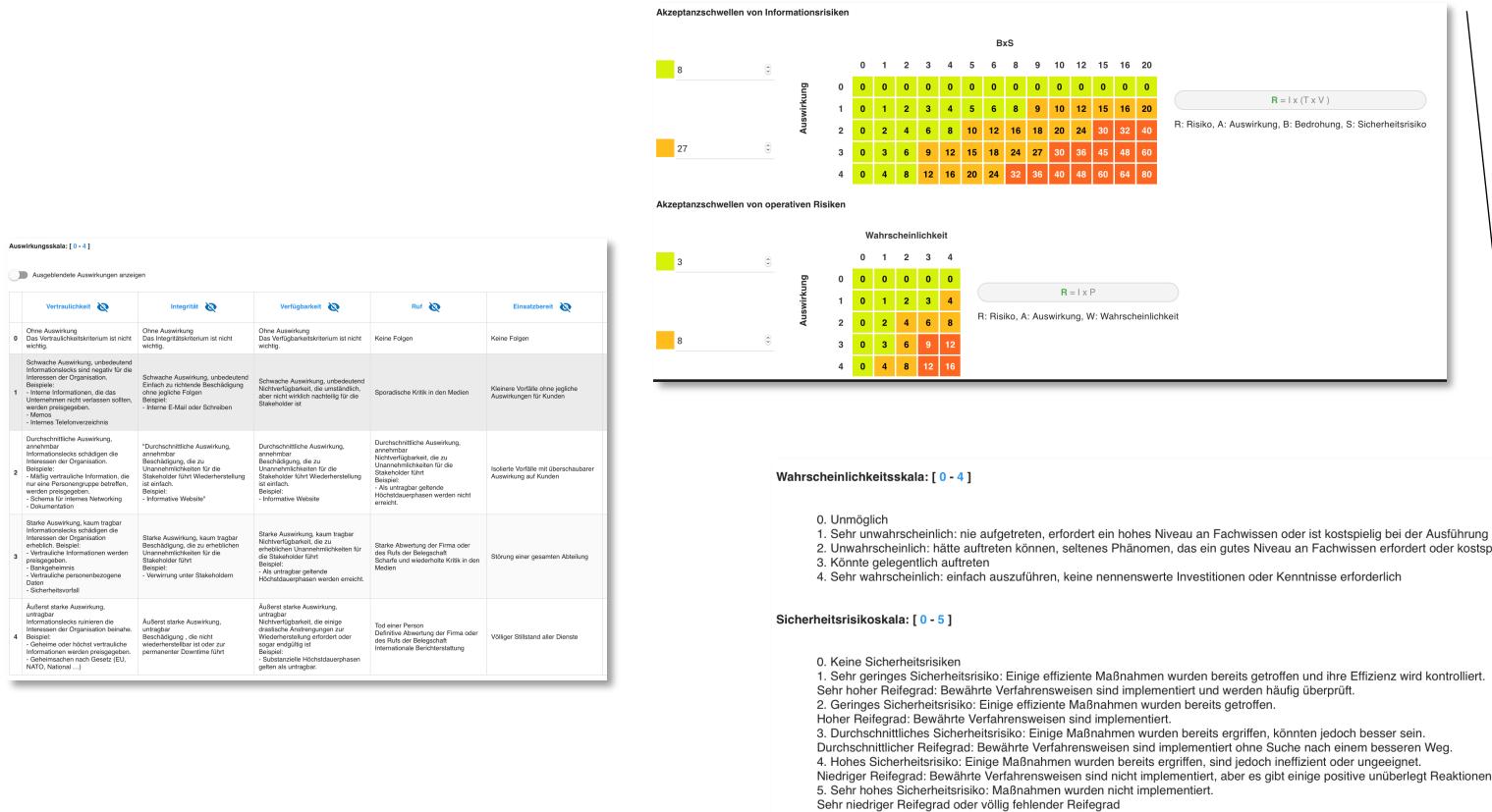
# 1.3 Risikomanagementorganisation



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



# 1.4 Definition der Risikobeurteilungskriterien



Home > MyPrintGER

1

**Kontexterstellung**

Alles erweitern /Alle umschließen Risikenanalysenkontext

Alles erweitern /Alle umschließen Risikenanalysenkontext

Einen Wert suchen...

Beurteilung von Trends und Bedrohungen sowie Synthese

MyPrintGER Risikoanalyse

Informationsrisiken

143 Informationsrisiken

AMyPrintGER Risikenmanagementorganisation

+ Abteilung Druck

Definition der Risikobeurteilungskriterien

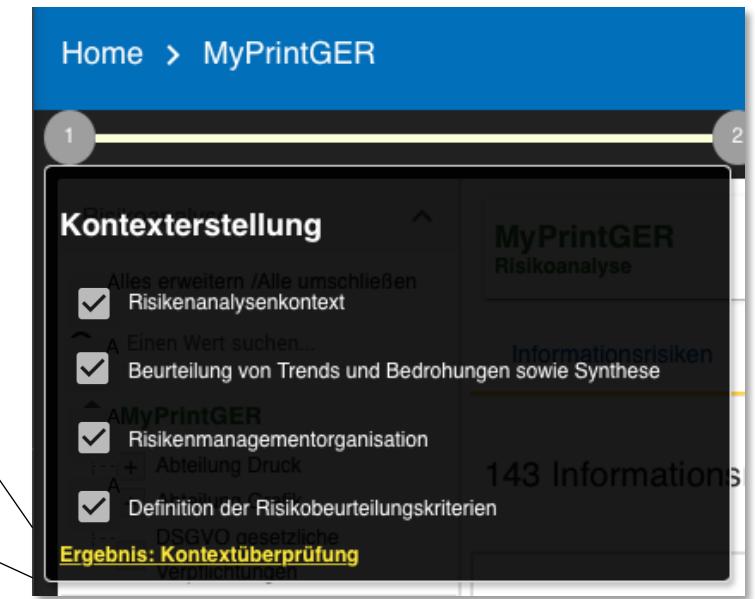
DSGVO gesetzliche Verpflichtungen

**Ergebnis: Kontextüberprüfung**



- 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

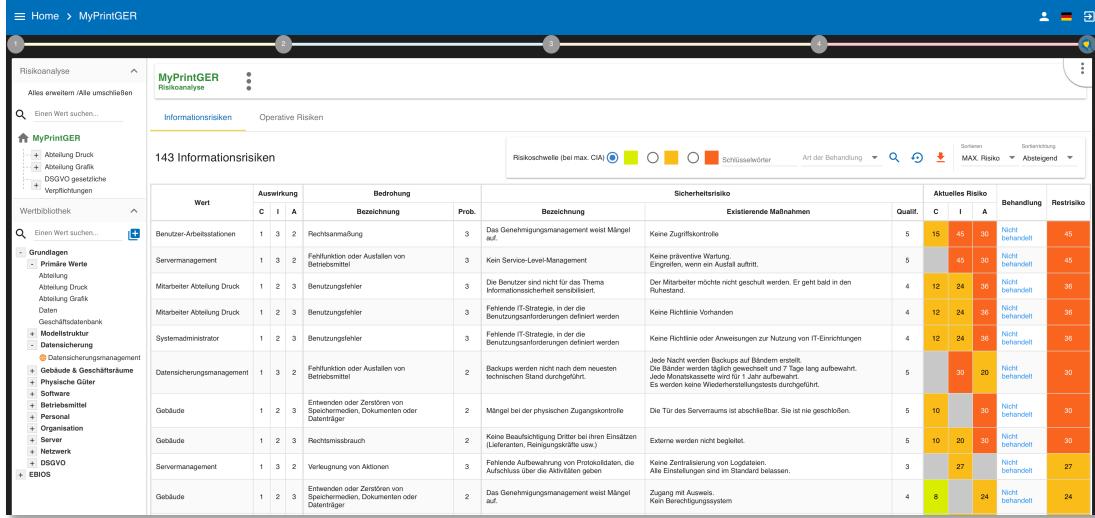
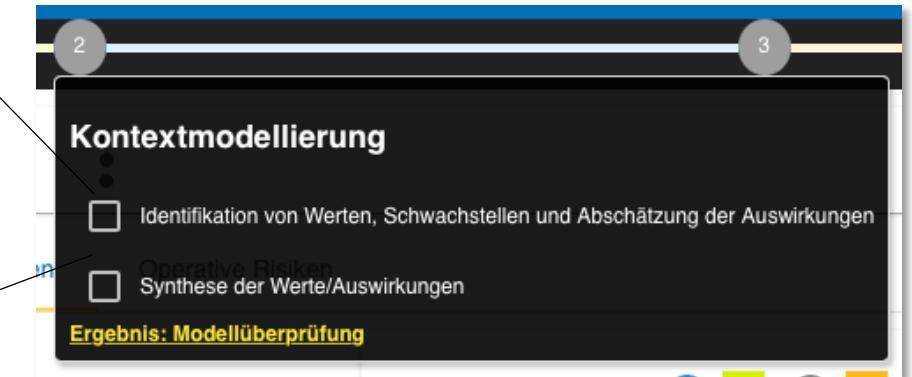


## 2. Kontextmodellierung

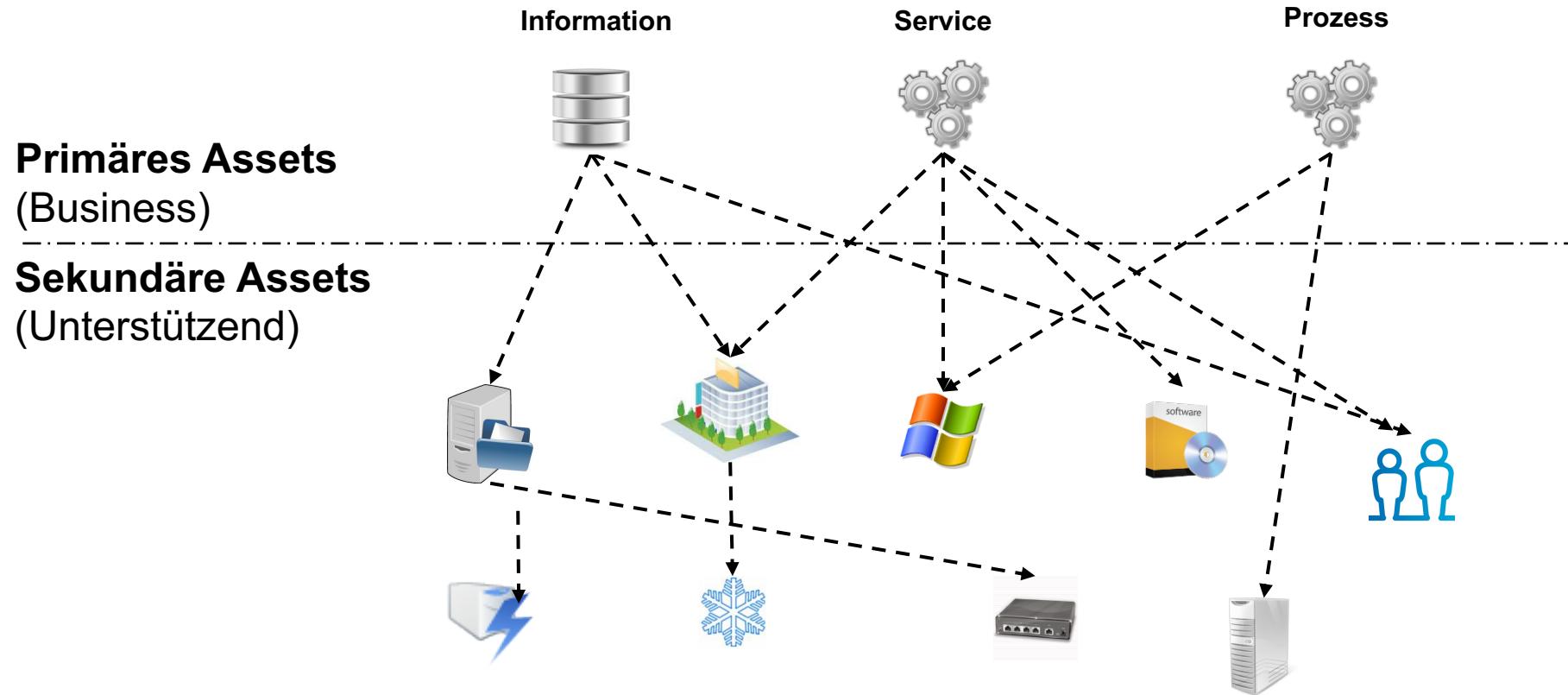
- Identifikation von Werten, Schwachstellen und Abschätzung der Auswirkungen
- Synthese der Werte/Auswirkungen



# 2.1 Identifikation von Werten, Schwachstellen und Abschätzung der Auswirkungen


## 2.1 Identifikation von Werten, Schwachstellen und Abschätzung der Auswirkungen

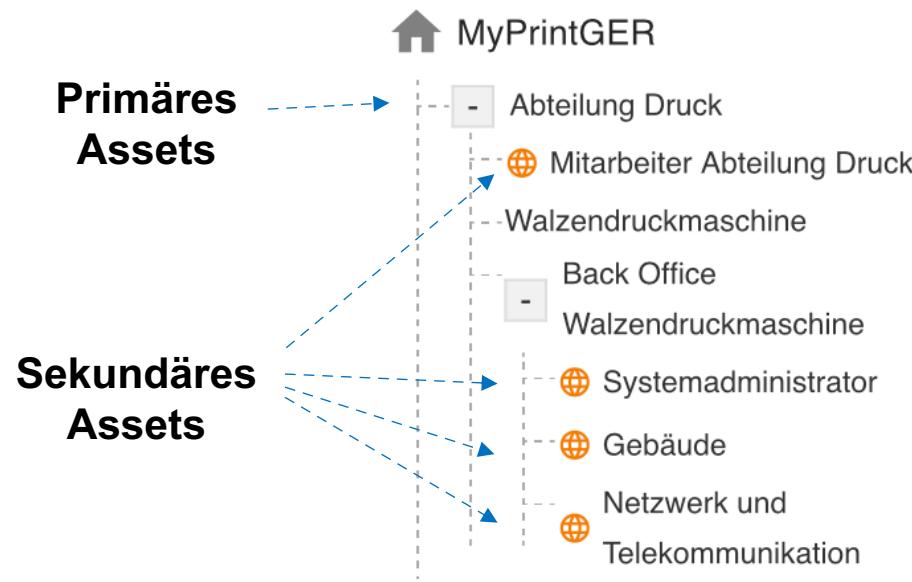


**Die Bewertung der Vertraulichkeit, Integrität und Verfügbarkeit wird von den primären Assets auf die sekundären Assets vererbt.**



# 2.1 Die Modellierung in MONARC

## Hierarchie der Assets



## Wertetyp

- [SERV]
- [OV\_UTIL]
- [MAT\_FIX]
- [CONT]
- [OV\_UTIL]
- [OV\_BATI]
- [OV\_RESEAU]

## 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, Smut, 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 risks**

Datenbank #1



Datenbank #2



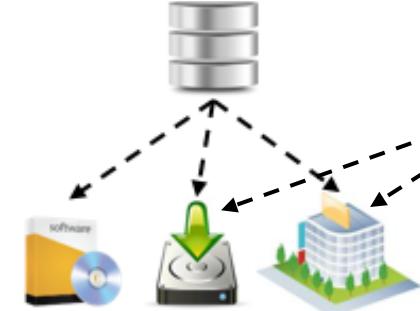
## “Global”

### Meine Risikoanalyse

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

**21 risks**

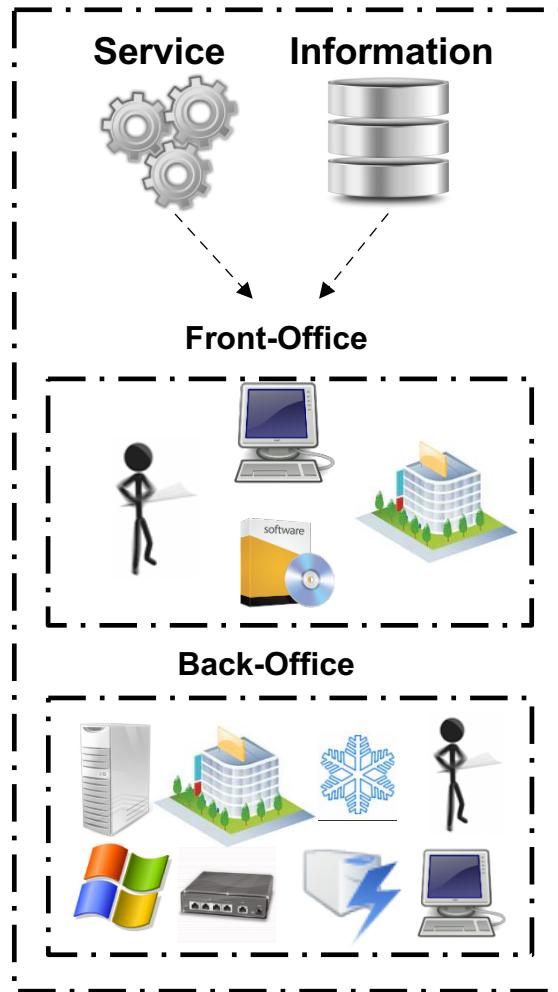
Datenbank #1



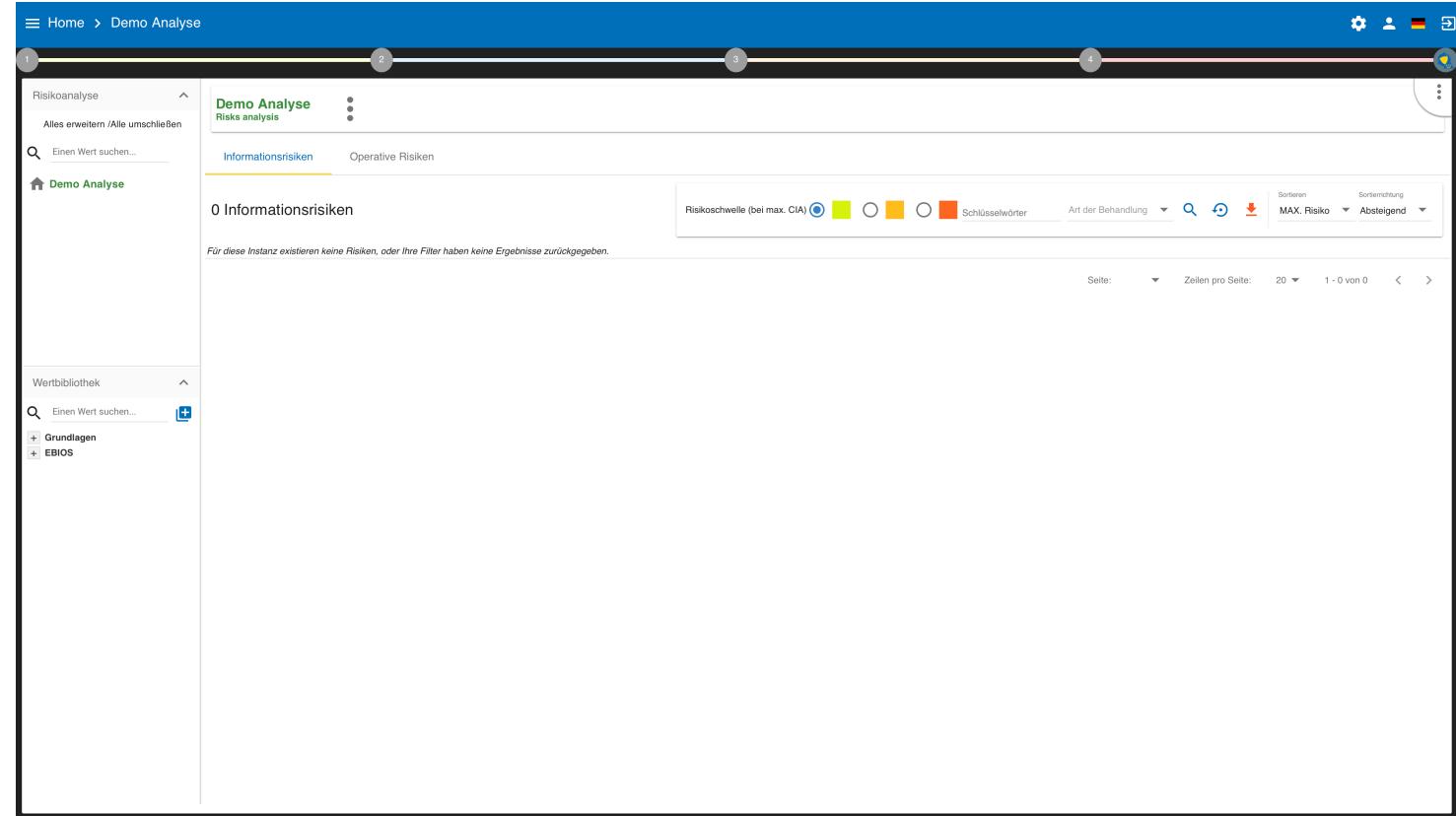
Datenbank #2



## 2.1 CASES Modellierung



# 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

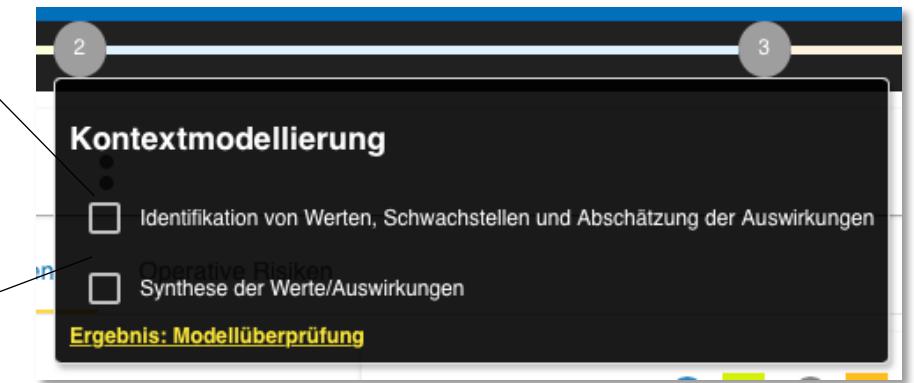
Auswirkungen bearbeiten

Folgen

Ausgeblendete Folgen anzeigen

	Ruf	Einsatzbereit	Legal	Finanziellen	Person	Max
Vertraulichkeit	1	0	0	0	1	1
Integrität	2	2	1	1	1	2
Verfügbarkeit	3	3	1	2	0	3

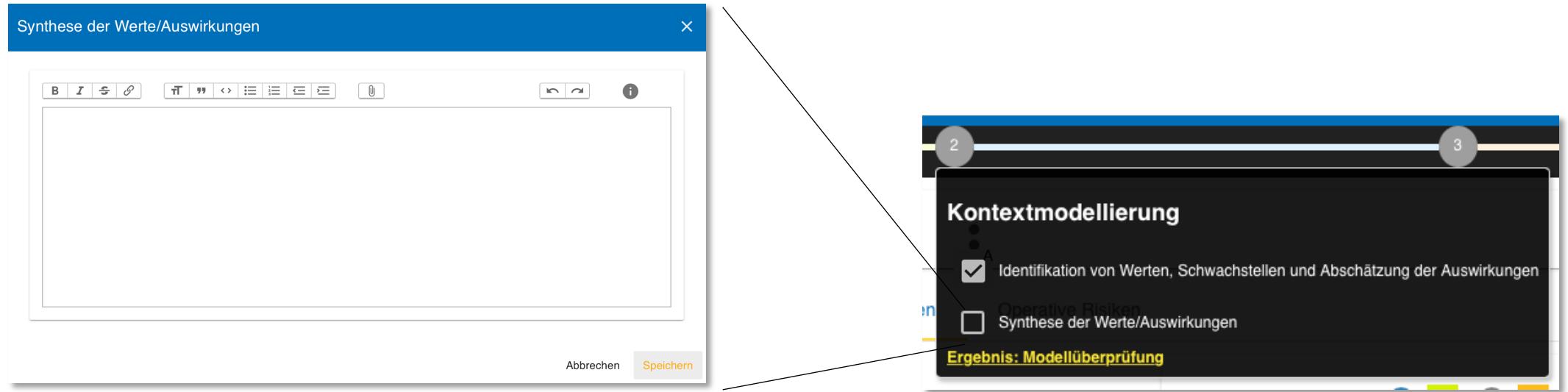
Abbrechen Speichern



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



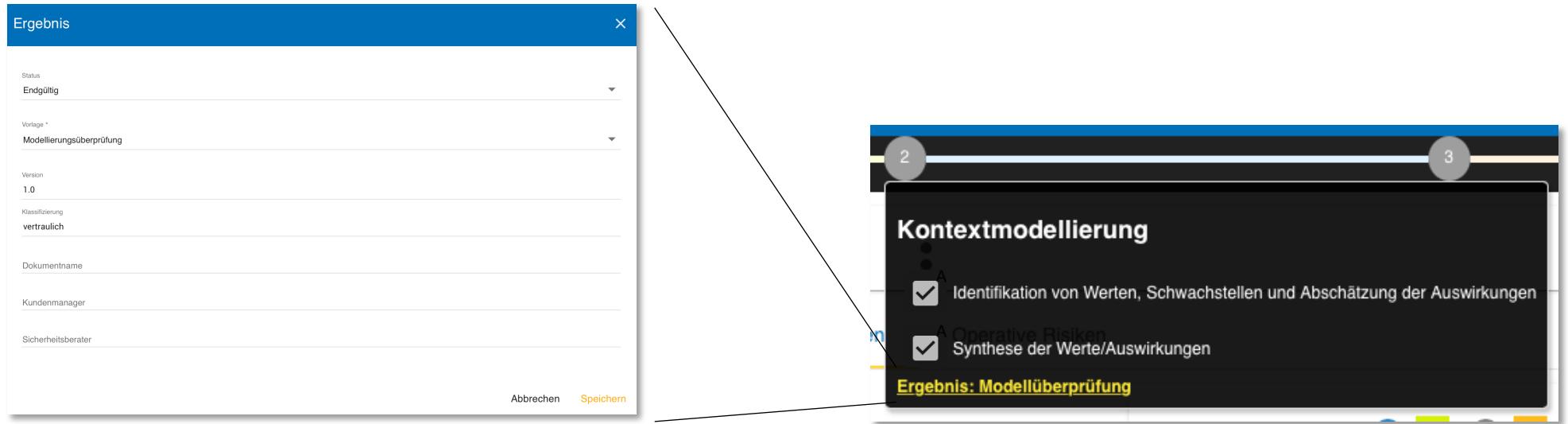
## 2.2 Synthese der Werte/Auswirkungen



- 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

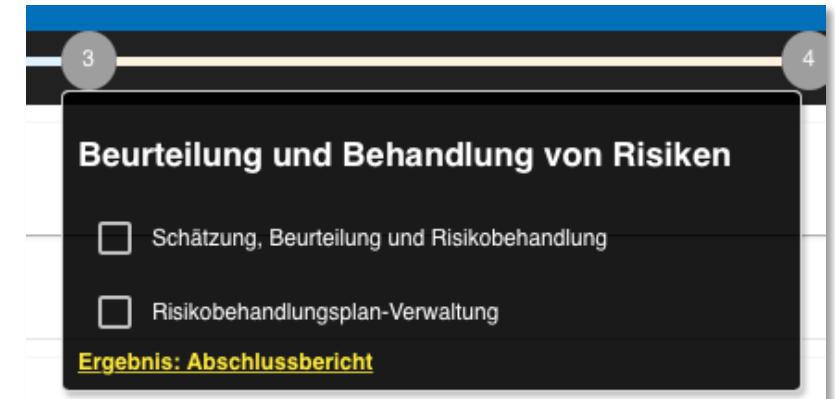
### Übung: Durchführen der Kontextmodellierung (30 Minuten)

- **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

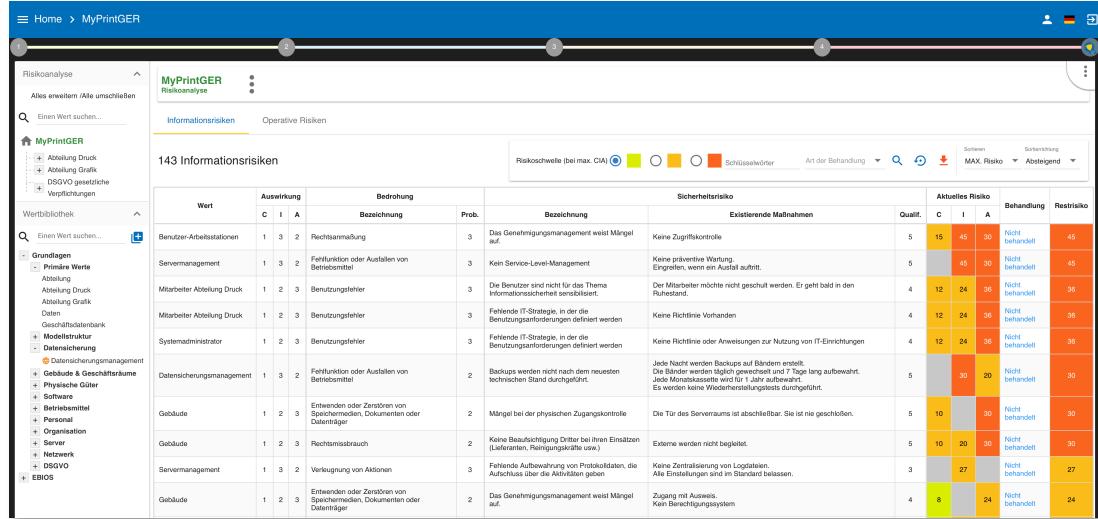
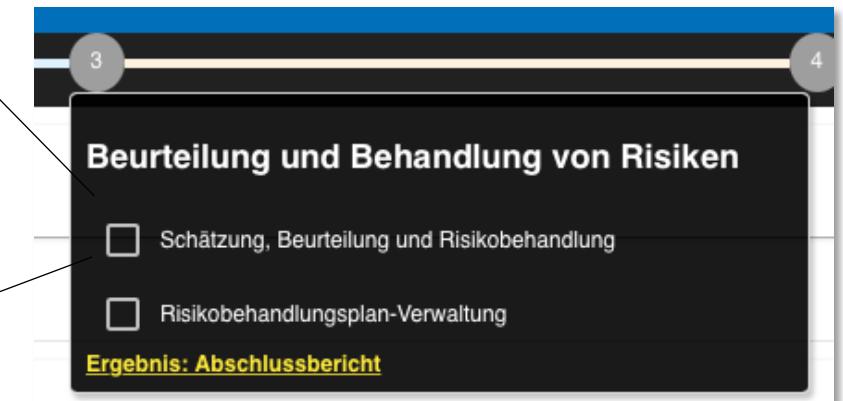


### 3. Beurteilung und Behandlung von Risiken

- Schätzung, Beurteilung und Risikobehandlung
- Risikobehandlungsplan-Verwaltung



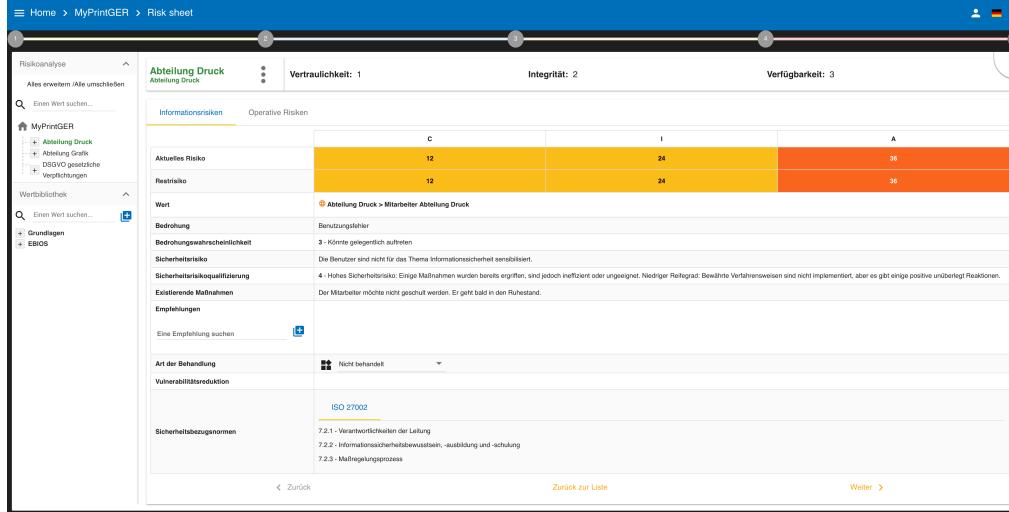
# 3.1 Schätzung, Beurteilung und Risikobehandlung

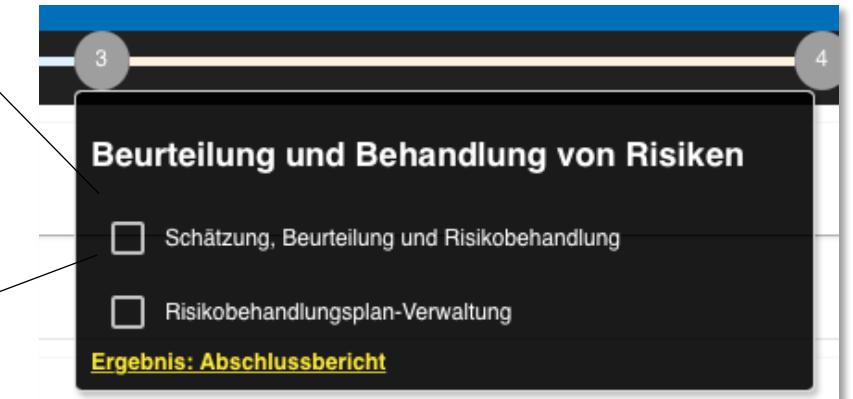
- Hauptansicht von MONARC
- Alle Risiken bewerten



# 3.1 Schätzung, Beurteilung und Risikobehandlung



The screenshot shows a risk matrix for the 'Abteilung Druck' department. The matrix is a 3x3 grid with columns labeled C, I, and A (Confidentiality, Integrity, Availability) and rows labeled C (Confidentiality), I (Integrity), and A (Availability). The values in the matrix are: C-C: 12, C-I: 24, C-A: 36, I-C: 12, I-I: 24, I-A: 36, A-C: 36, A-I: 36, A-A: 36. The matrix is titled 'Operative Risiken'.



**Beurteilung und Behandlung von Risiken**

- Schätzung, Beurteilung und Risikobehandlung
- Risikobehandlungsplan-Verwaltung

**Ergebnis: Abschlussbericht**

- Aktuelles Risiko und Restrisiko
- Risikobehandlung



# 3.1 Schätzung, Beurteilung und Risikobehandlung

**Eine Empfehlung hinzufügen**

Suchen Sie eine Empfehlung, um eine Empfehlung aus einer bestehenden zu erstellen

Wählen Sie einen Empfehlungssatz \*

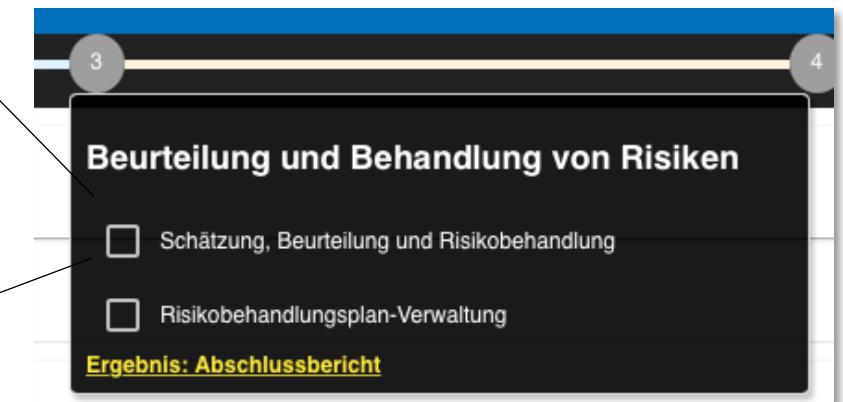
☰ Code \*

★ Gewichtung

- Hilfreiche Informationen zur Sicherheit, Beratung
- Empfehlung, die eine fest zugeordnete Aktion zur Lösung eines Sicherheitsrisikos oder einer fehlenden bewährten Methode erfordert
- Prioritätenempfehlung

↳ Beschreibung \*

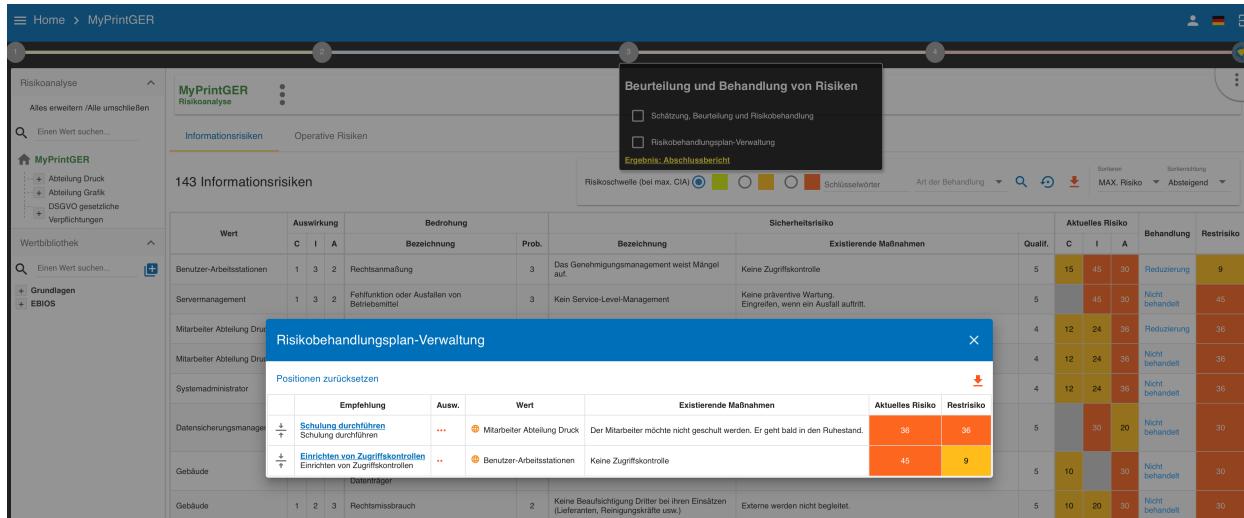
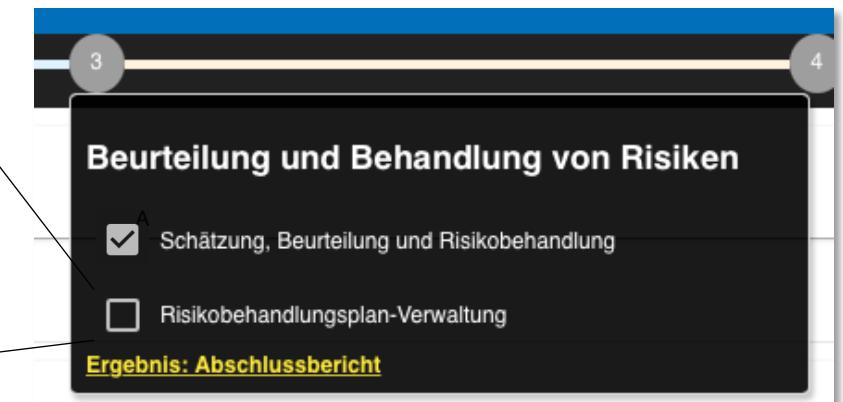
Abbrechen Erstellen



- Anlegen einer Maßnahme



## 3.2 Risikobehandlungsplan-Verwaltung

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



### 3.3 Ergebnis: Abschlussbericht

**Ergebnis**

Status: Endgültig

Vorlage: Risikobeurteilungsbericht

Version: 1.0

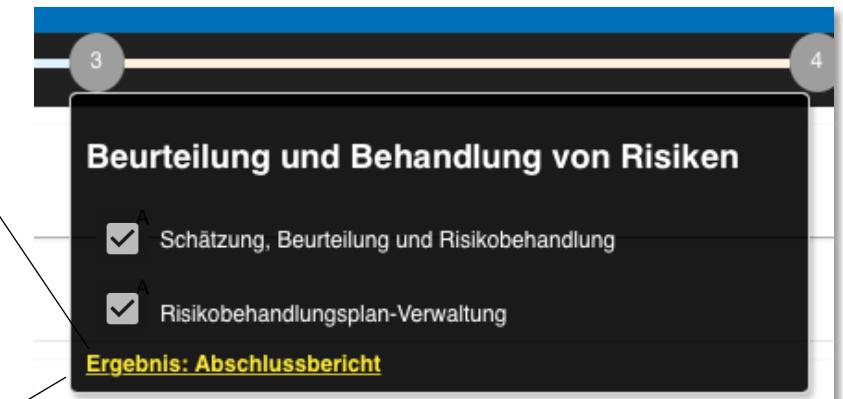
Klassifizierung: vertraulich

Dokumentname: Kundenmanager

Kundenmanager: Sicherheitsberater

Zusammenfassung der Risikobeurteilung:

Abbrechen Speichern



- 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

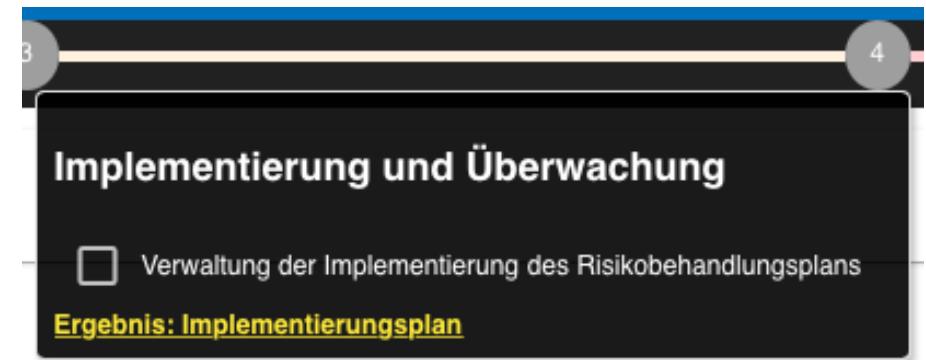
#### Übung: Durchführen der Beurteilung und Behandlung von Risiken (30 Minuten)

- **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

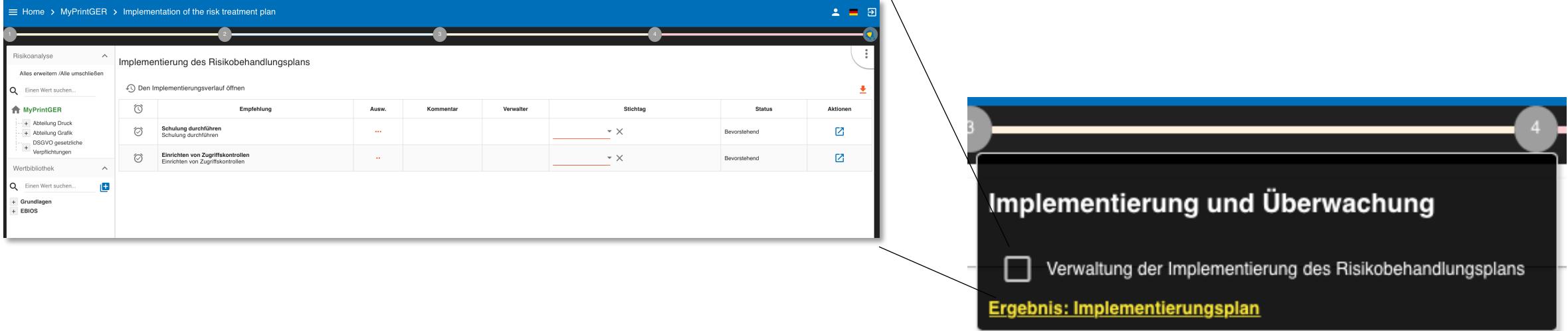


## 4. Implementierung und Überwachung

- Verwaltung der Implementierung des Risikobehandlungsplans



# 4.1 Verwaltung der Implementierung des Risikobehandlungsplans



Implementation of the risk treatment plan

Implementierung des Risikobehandlungsplans

Empfehlung	Ausw.	Kommentar	Verwalter	Stichtag	Status	Aktionen
Schulung durchführen	...			Stichtag	Bevorstehend	<a href="#">Aktion</a>
Einrichten von Zugriffskontrollen	...			Stichtag	Bevorstehend	<a href="#">Aktion</a>

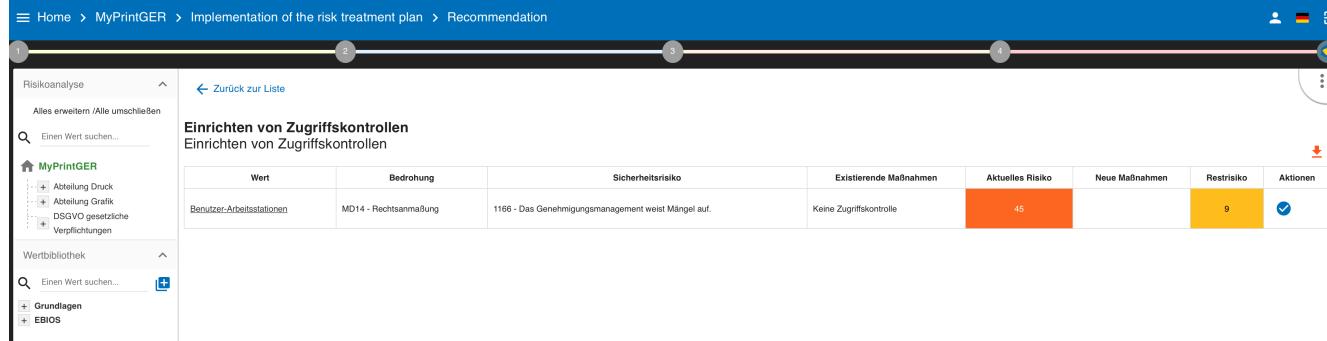
Implementierung und Überwachung

Ergebnis: Implementierungsplan

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



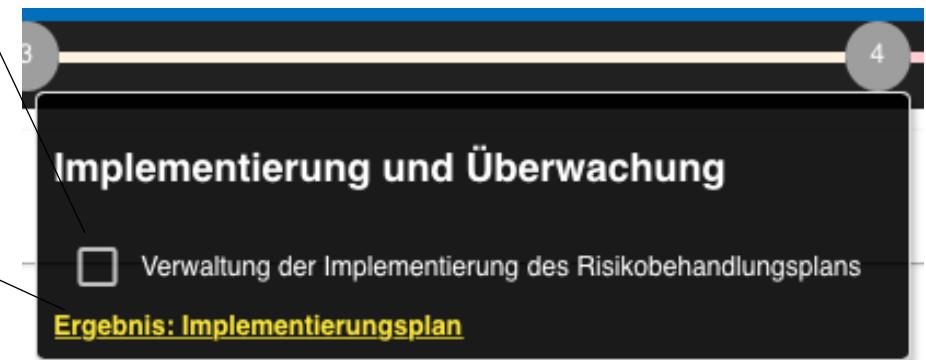
# 4.1 Verwaltung der Implementierung des Risikobehandlungsplans



The screenshot shows a software interface for risk management. The top navigation bar includes 'Home', 'MyPrintGER', 'Implementation of the risk treatment plan', and 'Recommendation'. The main content area is titled 'Einrichten von Zugriffskontrollen' (Setup of access controls). It displays a table with the following data:

Wert	Bedrohung	Sicherheitsrisiko	Existierende Maßnahmen	Aktuelles Risiko	Neue Maßnahmen	Restrisiko	Aktionen
Benutzer-Arbeitsstationen	MD14 - Rechtsanmaßung	1166 - Das Genehmigungsmanagement weist Mängel auf.	Keine Zugriffskontrolle	45		9	<input checked="" type="checkbox"/>

The sidebar on the left contains sections for 'Risikoanalyse', 'MyPrintGER' (with sub-options like 'Abteilung Druck', 'Abteilung Grafik', 'DSGVO gesetzliche Verpflichtungen'), and 'Wertbibliothek'.



**Implementierung und Überwachung**

Verwaltung der Implementierung des Risikobehandlungsplans

**Ergebnis: Implementierungsplan**

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



## 4.1 Verwaltung der Implementierung des Risikobehandlungsplans

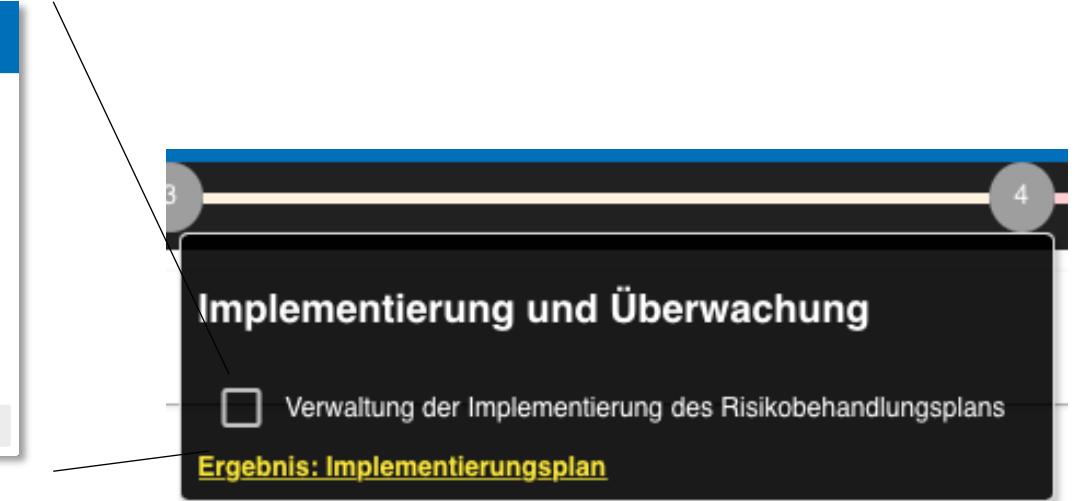
Einrichten von Zugriffskontrollen - Einrichten von Zugriffskontrollen X

Sie sind im Begriff, die Implementierung der Empfehlung **Einrichten von Zugriffskontrollen - Einrichten von Zugriffskontrollen** für das folgende Risiko zu überprüfen:

**Wert:** Benutzer-Arbeitsstationen  
**Bedrohung:** Rechtsanmaßung  
**Sicherheitsrisiko:** Das Genehmigungsmanagement weist Mängel auf.

Optionaler Kommentar

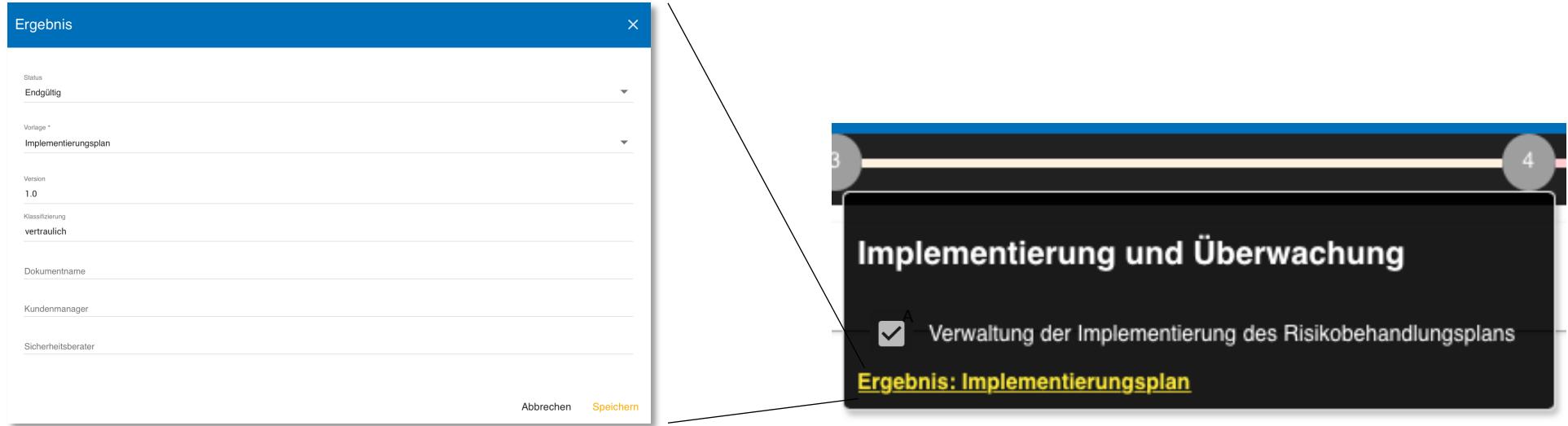
Abbrechen Überprüfen



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



## 4.2 Ergebnis: Implementierungsplan



The image shows a screenshot of the MONARC software interface. On the left, a modal window titled 'Ergebnis' (Result) displays the following details:

- Status: Endgültig
- Vorlage \*: Implementierungsplan
- Version: 1.0
- Klassifizierung: vertraulich
- Dokumentname: (empty)
- Kundenmanager: (empty)
- Sicherheitsberater: (empty)

At the bottom right of the modal are the buttons 'Abbrechen' (Cancel) and 'Speichern' (Save). A line from the 'Speichern' button points to a summary slide on the right. The summary slide has a dark background with a horizontal bar at the top numbered 3 and 4. The title is 'Implementierung und Überwachung' (Implementation and Monitoring). Below the title is a checked checkbox with the text 'Verwaltung der Implementierung des Risikobehandlungsplans' (Management of the implementation of the risk treatment plan). At the bottom of the slide is the text 'Ergebnis: Implementierungsplan' (Result: Implementation plan) in yellow.

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



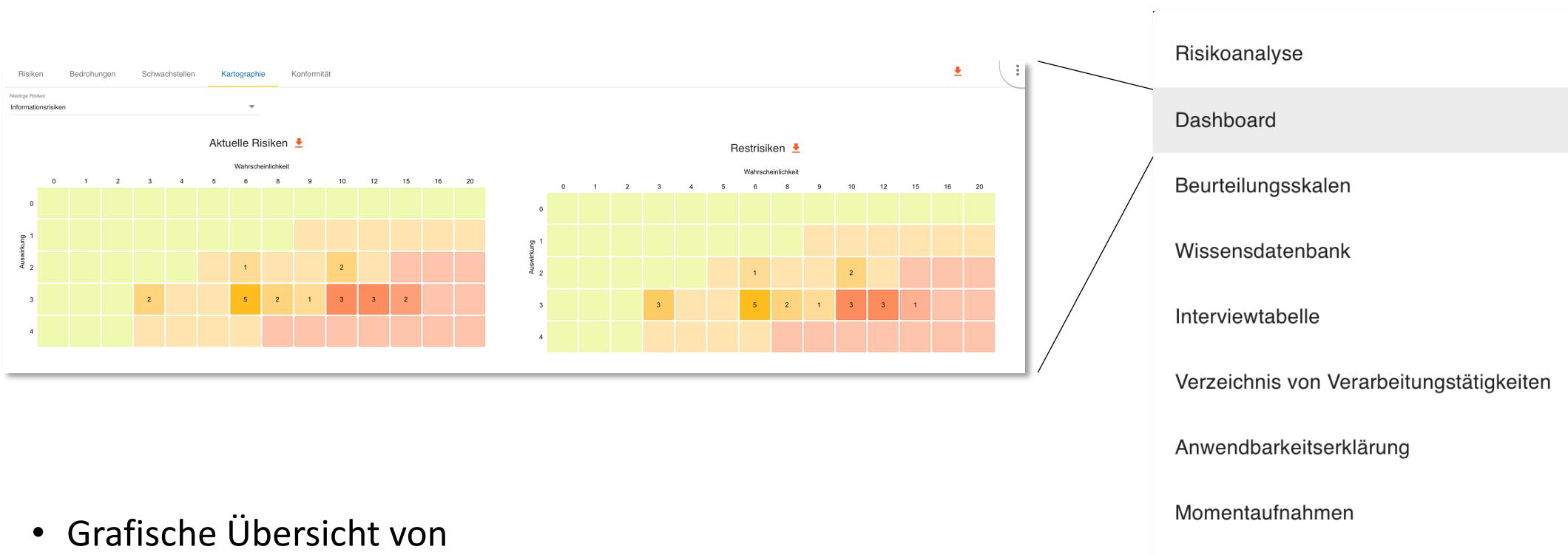
# 4. Implementierung und Überwachung - Übung

## 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



## Risikoanalyse

### Dashboard

### Beurteilungsskalen

### Wissensdatenbank

### Interviewtabelle

### Verzeichnis von Verarbeitungstätigkeiten

### Anwendbarkeitserklärung

### Momentaufnahmen

- Grafische Übersicht von
  - Risiken, Bedrohungen, Schwachstellen, Kartographie, Konformität

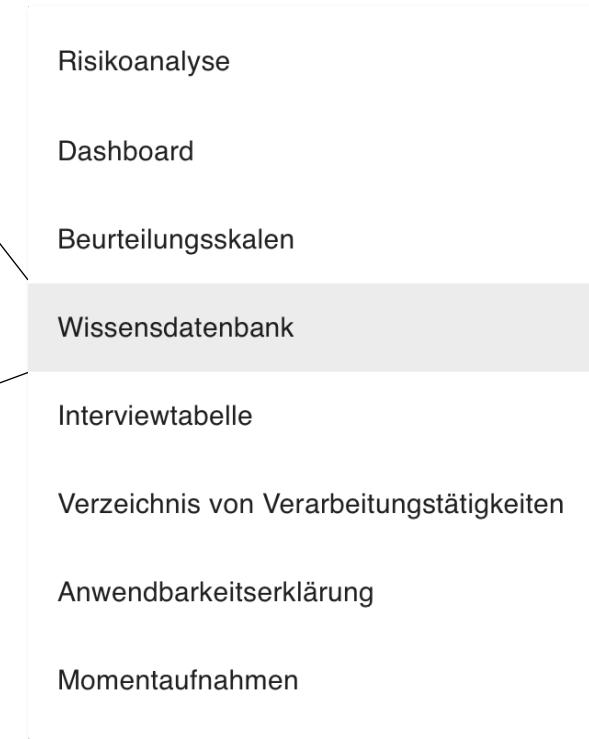


# MONARC - Wissensdatenbank

Werttypen    Bedrohungen    Schwachstellen    Bezugsnormen    Informationsrisiken    Tags    Operative Risiken    Empfehlungssets

Werttypen        Suchen...

<input type="checkbox"/> Status	Bezeichnung	Code	Typ	Beschreibung	Aktionen
<input checked="" type="checkbox"/>	Behälter	CONT	Primär	Vermögenswert-Behälter	 
<input checked="" type="checkbox"/>	Benutzer	OV_UTIL	Sekundär	Benutzer	 
<input checked="" type="checkbox"/>	Benutzer	PER_UTI	Sekundär	Nutzer	 
<input checked="" type="checkbox"/>	Betreiber / Wartung	PER_EXP	Sekundär	Betreiber / Wartung	 
<input checked="" type="checkbox"/>	Betriebssystem	LOG_OS	Sekundär	Windows 7, MAC OS 10, Linux	 



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



# MONARC - Wissensdatenbank

Interviewtabelle

Ein Interview hinzufügen

Datum	Abteilung / Kontakte	Inhalt	Aktionen
-------	----------------------	--------	----------

Abbrechen

- Risikoanalyse
- Dashboard
- Beurteilungsskalen
- Wissensdatenbank
- Interviewtabelle
- Verzeichnis von Verarbeitungstätigkeiten
- Anwendbarkeitserklärung
- Momentaufnahmen

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



# MONARC - Verzeichnis Verarbeitungstätigkeiten

Verzeichnis von Verarbeitungstätigkeiten

VVA

**Beschreibung**

Name	VVA
Erstellungsdatum	2020-05-08
Aktualisierungsdatum	
Zweck(e)	
Datensicherheitsbeschreibung	

**Agenten**

Agent	Name	Kontaktdaten
Verantwortliche		
Datenschutzbeauftragter		
Vertreter		
Gemeinsam		
Verantwortliche		

**Kategorien der betroffenen Personen und personenbezogene Daten**

Kategorien der betroffenen Person	Datenkategorien	Beschreibung	Aufbewahrungsfrist für Daten	Beschreibung der Aufbewahrungsfrist

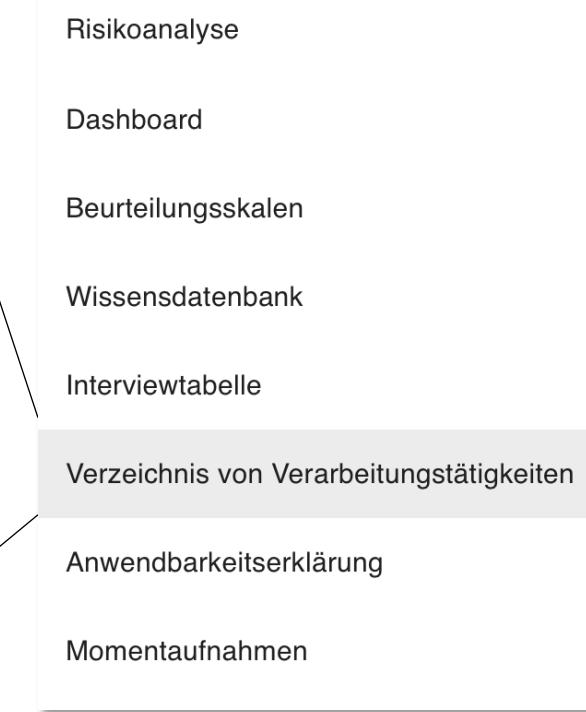
**Empfänger**

Empfänger	Empfängertyp	Beschreibung

**Internationale Datenübertragung**

Organisation	Beschreibung	Land	Dokumente

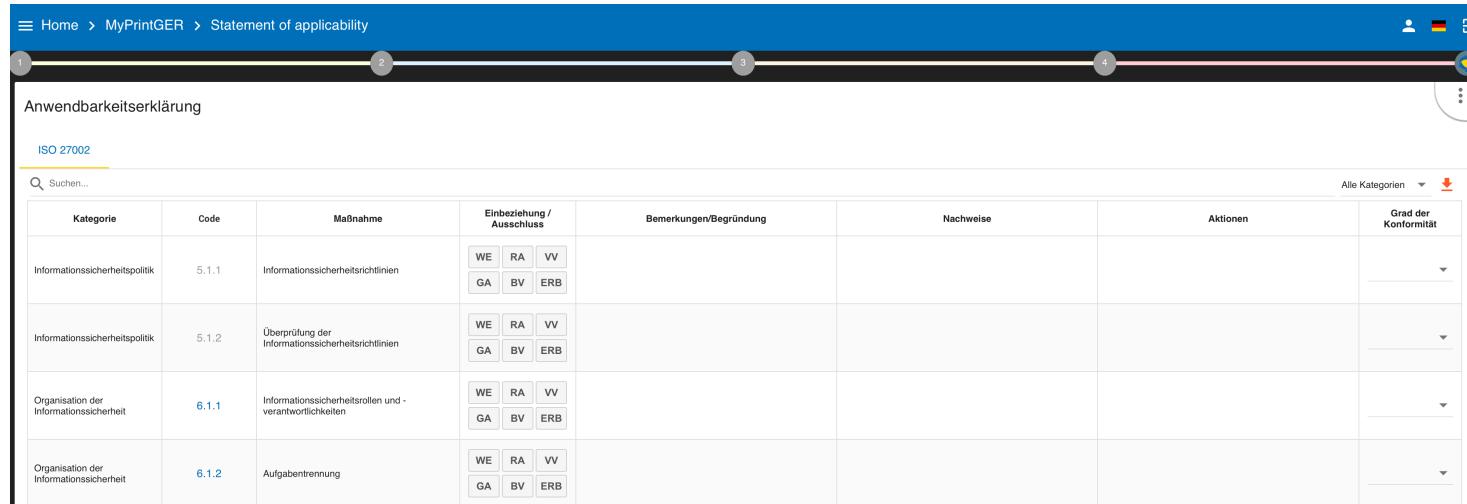
**Auftragsverarbeiter**



- Abbildung von EU-DSGVO Nachweisen



# MONARC - Anwendbarkeitserklärung



The screenshot shows a table with columns for Kategorie (Category), Code (Code), Maßnahme (Measure), Einbeziehung / Ausschluss (Inclusion / Exclusion), Bemerkungen/Begründung (Remarks/Reasoning), Nachweise (Proofs), Aktionen (Actions), and Grad der Konformität (Degree of Conformity). The table lists measures for Informationssicherheitspolitik (Information Security Policy) and Organisation der Informationssicherheit (Organization of Information Security), including sub-measures like Überprüfung der Informationssicherheitsrichtlinien (Review of Information Security Policies) and Aufgabentrennung (Task Separation).

Risikoanalyse

Dashboard

Beurteilungsskalen

Wissensdatenbank

Interviewtabelle

Verzeichnis von Verarbeitungstätigkeiten

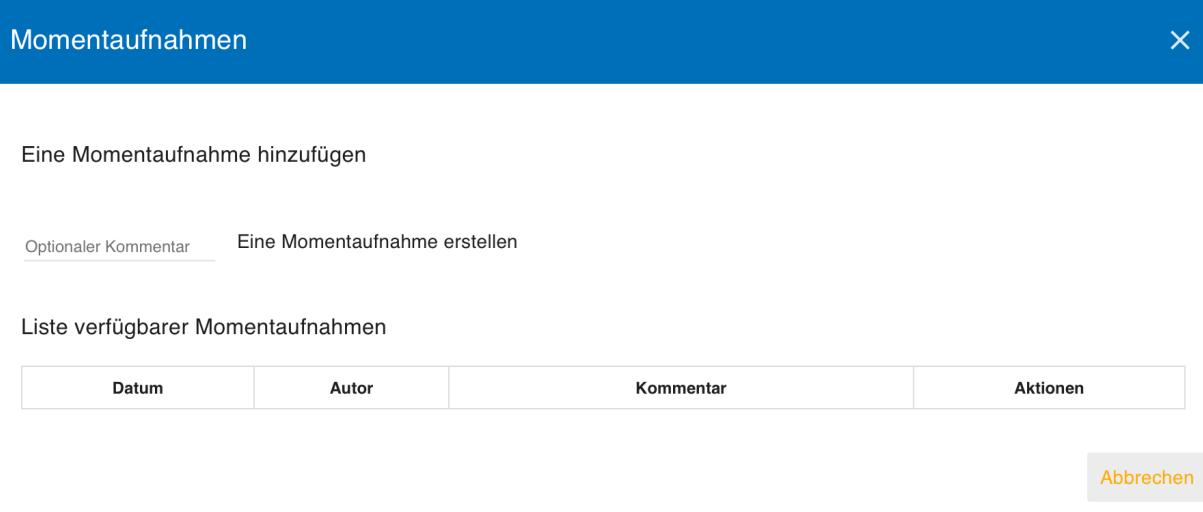
Anwendbarkeitserklärung

Momentaufnahmen

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



# MONARC - Momentaufnahmen



The screenshot shows the 'Momentaufnahmen' (Screenshots) module of the MONARC system. The interface includes a header with a blue bar, a main content area with a table for managing screenshots, and a sidebar with various links. A callout box highlights the 'Momentaufnahmen' module in the sidebar.

- Risikoanalyse
- Dashboard
- Beurteilungsskalen
- Wissensdatenbank
- Interviewtabelle
- Verzeichnis von Verarbeitungstätigkeiten
- Anwendbarkeitserklärung
- Momentaufnahmen

- Momentaufnahmen erstellen als Nachweis für Versionierungen



# Weitere Tipps & Tricks

- Usermanagement und Berechtigungen
- Downloadmöglichkeiten unter [monarc.lu](http://monarc.lu)
- Import aus vorhandener Risikoanalyse
- Tipps & Tricks aus der Praxis
- 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)



# Technisches Wissen

- Wissenswertes zum technischen Aufsetzen der Plattform – bei Interesse
  - Installationsanleitung unter [monarc.lu](http://monarc.lu)
  - Installationsanleitung auf der K8-Webseite
  - DB-Anbindung, PHP Timeouts etc.

# Fragen / Feedback

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



Consulting	Audit & Prüfung	Awareness / Schulung	Technische Sicherheit
<ul style="list-style-type: none"><li>• Cyber Security Incident Response</li><li>• Aufbau von ISMS nach ISO 27001</li><li>• Aufbau von ISMS nach IT-Grundschutz</li><li>• ISMS nach VDA ISA</li><li>• Risikomanagement-Systeme</li><li>• Externer ISB / ISO</li><li>• MONARC Hosting</li></ul>	<ul style="list-style-type: none"><li>• Interne Audits</li><li>• Zertifizierungsaudits</li><li>• §8a (3) BSIG – KRITIS</li><li>• BSI TR-03109-6</li><li>• IT-Revisionsprüfungen</li><li>• Trusted ERP</li></ul>	<ul style="list-style-type: none"><li>• Cyber Security Awareness</li><li>• K8 macht Schule</li><li>• Phishing-Kampagnen</li><li>• Risikomanagement mit MONARC</li><li>• Inhouse Schulungen</li></ul>	<ul style="list-style-type: none"><li>• Penetrationstests</li><li>• Sicherheits-Analyse</li><li>• Prüfung von Sicherheitskonzepten</li></ul>

# Ihr Kontakt



 <https://www.konzeptacht.de>

 [@konzeptacht](#)

 [Thomas Kochanek](#)

 [Thomas Kochanek](#)

# Ihr Kontakt



<https://www.konzeptacht.de>

[@konzeptacht](https://twitter.com/konzeptacht)

[Marc Sparwel](https://www.linkedin.com/in/marc-sparwel-1a114a110)