

Risikomanagement mit dem Tool MONARC (Optimised Risk Analysis Method)

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



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG



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



circl.lu
Computer Incident
Response Center
LUXEMBOURG



nc3.lu
National Cybersecurity
Competence Center
LUXEMBOURG

www.lhc.lu
www.nc3.lu

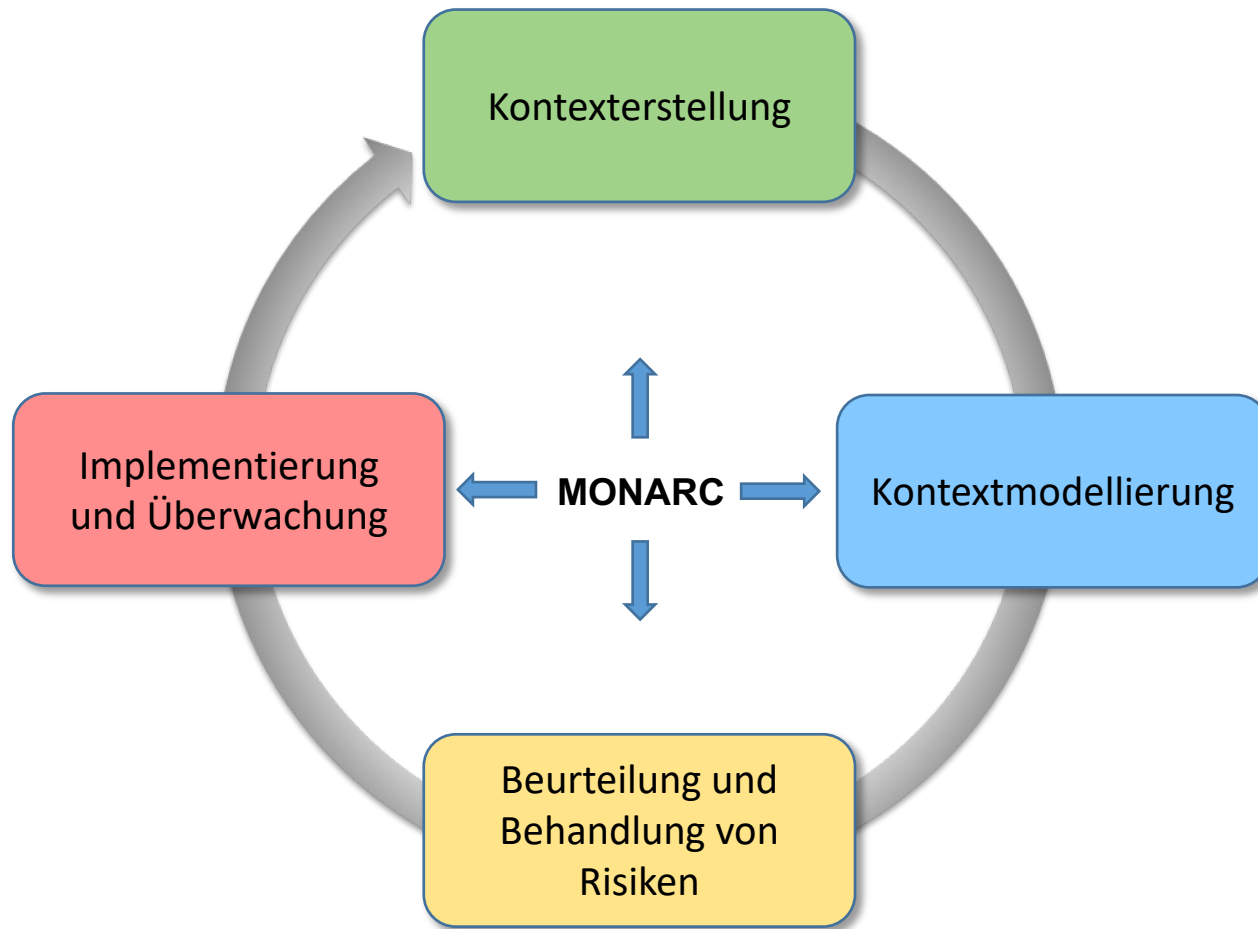


Was ist MONARC?

- Optimised Risk Analysis Method (**M**éthode **O**ptimisée d'**A**nalyse des **R**isques by **C**ASES.lu)
- Open Source Software
- Source Code³ 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>

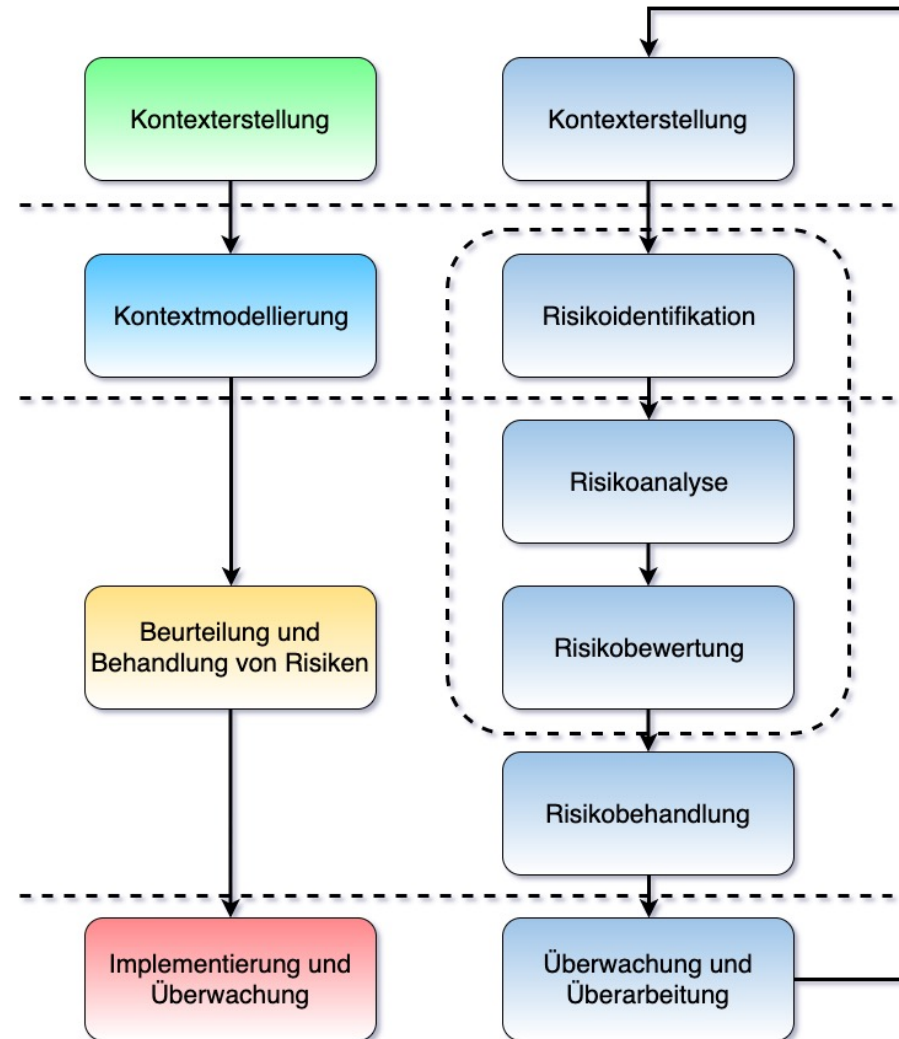
MONARC Methodik



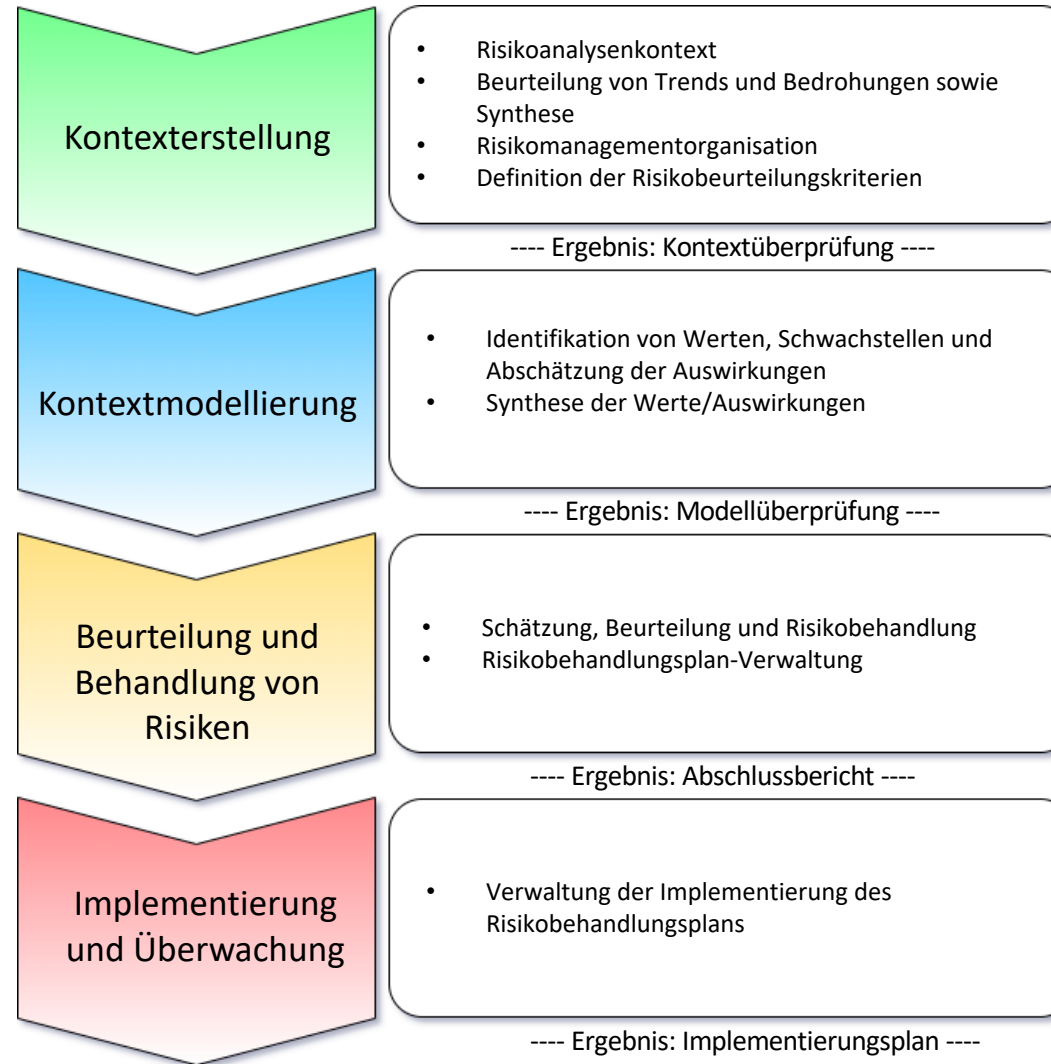
Methodik der Risikoanalyse

- **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)

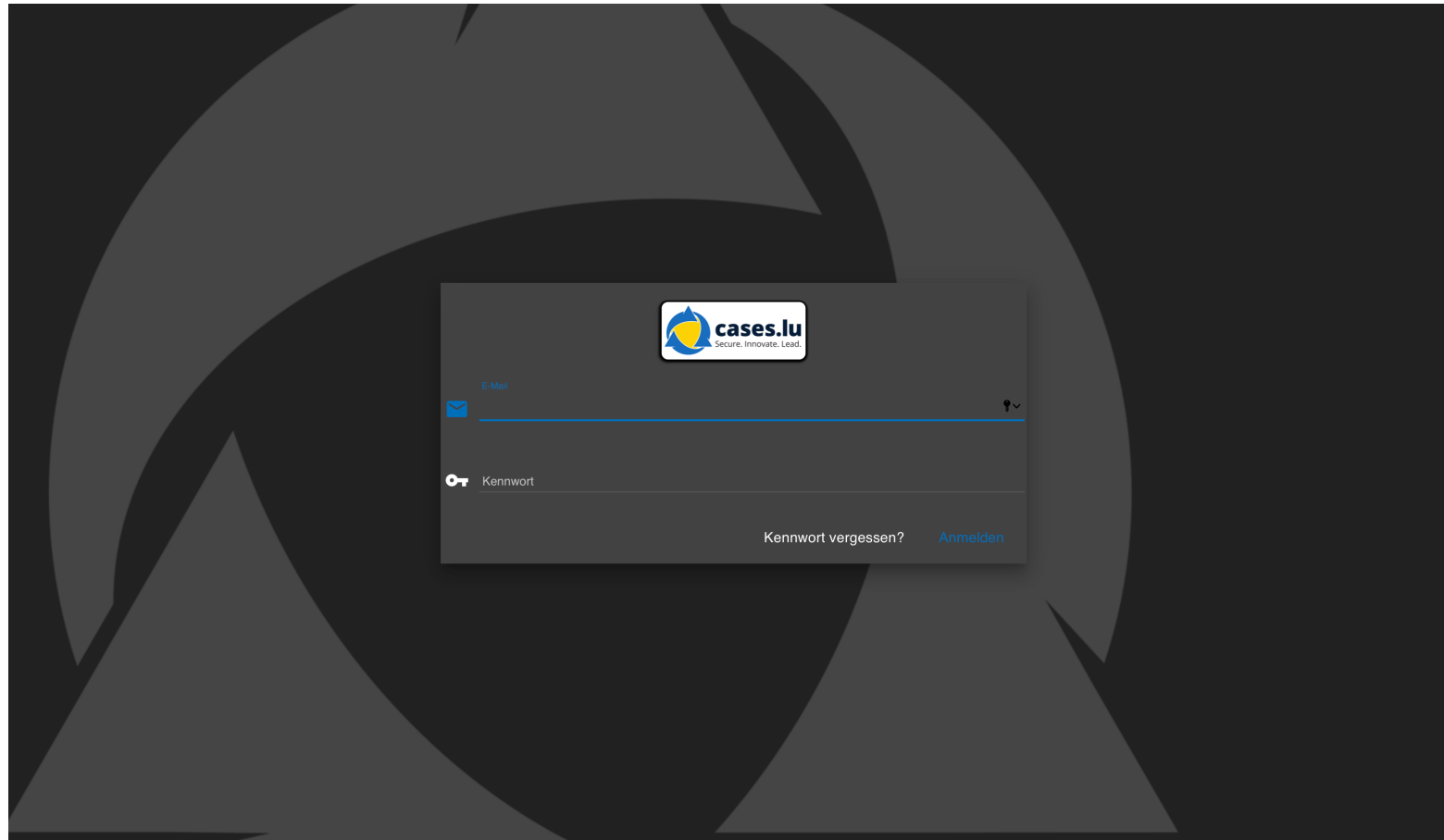
MONARC Methodik

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


Eine Risikoanalyse erstellen


Quelle


☐ Liste der Risikomodelle ☐ Existierende Risikoanalyse

Beschreibung

 Sprache *

 Name *

 Beschreibung

 + Fügen Sie eine Bezugsnorm hinzu

Abbrechen

Erstellen

Erstellung Risikoanalyse in MONARC


- Login Schulungsumgebung:
 - Hostname: `https://test.konzeptacht.de`
 - User: `K8-Training-xx@konzeptacht.de` $\Rightarrow xx = 01 \leq xx \leq 15$
 - 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



MONARC Training Q2/2025
[Erstellt: thomas.kochanek@konzeptacht.de, 26/06/2025]

09:52

MyPrintEN
[Erstellt: thomas.kochanek@konzeptacht.de, 26/06/2025]

15:46

+ Eine Risikoanalyse erstellen

Copyright 2012-2024 [NC3 - Terms](#)
[MONARC v. 2.13.3](#)

Risikoanalyse

Alles erweitern / Alle umschließen

Einen Wert suchen...

MyPrintEN

- Printing department
- Computer graphics department
- GDPR legal obligations

Wertebibliothek

Einen Wert suchen...

Fundamentals

- EBIOS

Startseite > MyPrintEN

1

2

3

4

MyPrintEN

Informationsrisiken

Operative Risiken

143 Informationsrisiken

Risikoschwelle (bei max. CIA) Schlüsselerwörter

Art der Behandlung

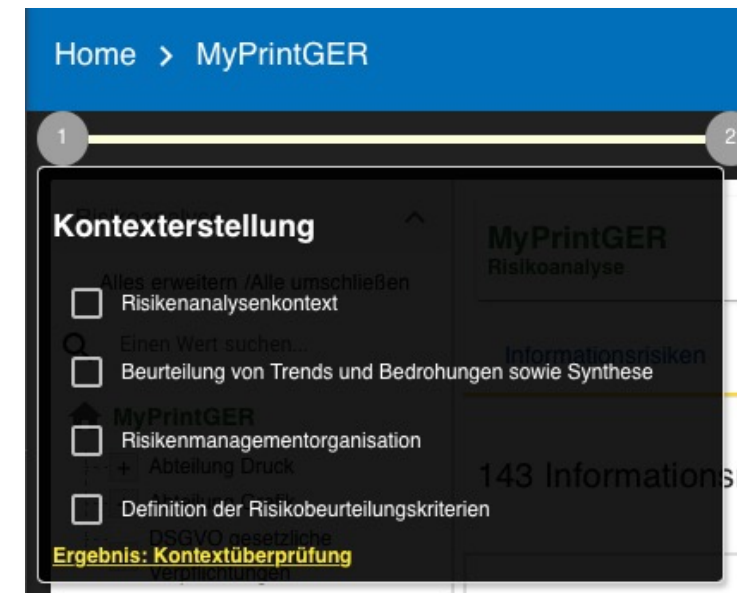
Sortieren

Sortierrichtung

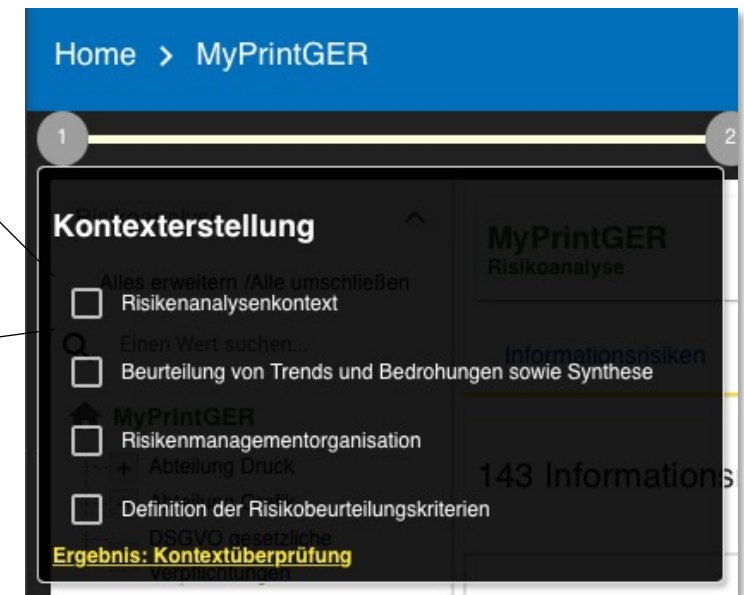
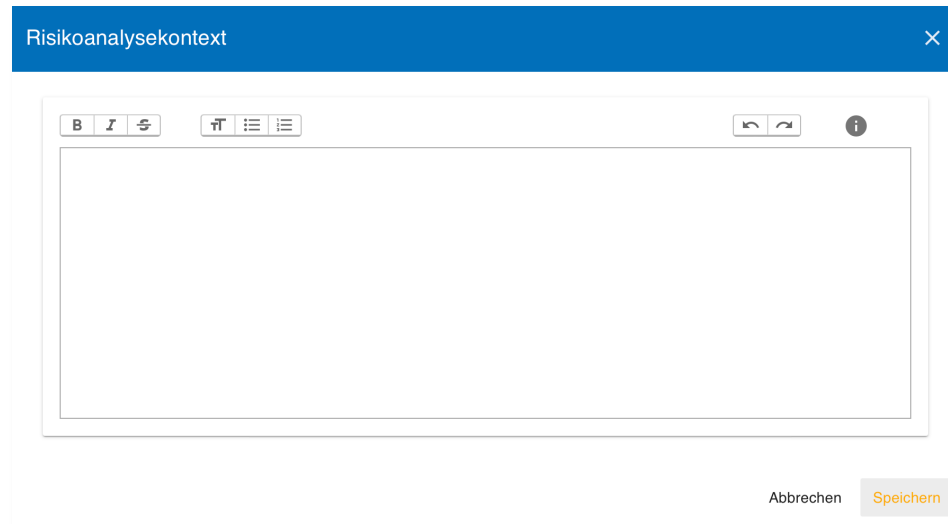
ID	Wert	Auswirkung			Bedrohung		Schwachstelle			Aktuelles Risiko			Behandlung	Restrisiko
		C	I	A	Bezeichnung	Prob.	Bezeichnung	Existierende Maßnahmen	Qualif.	C	I	A		
15583	Server management	1	3	2	Equipment malfunction or failure	3	No service level management	No preventive maintenance. Intervention when 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

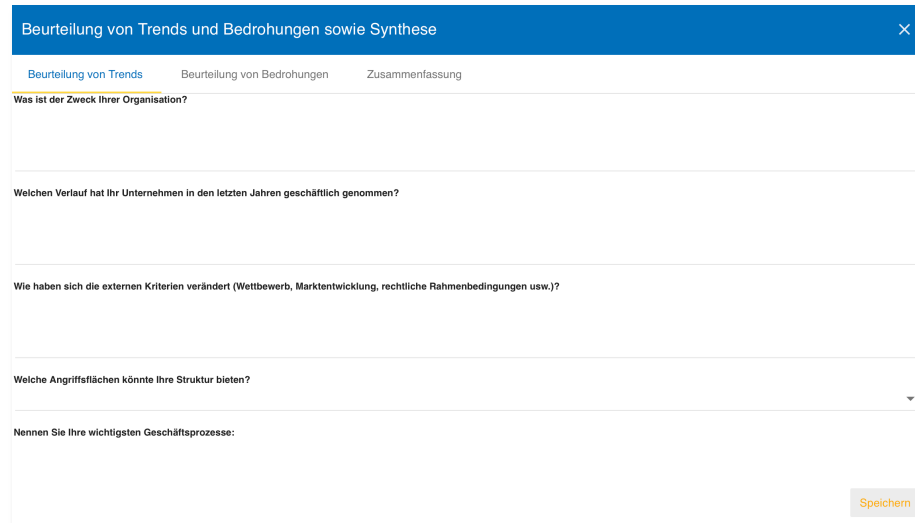
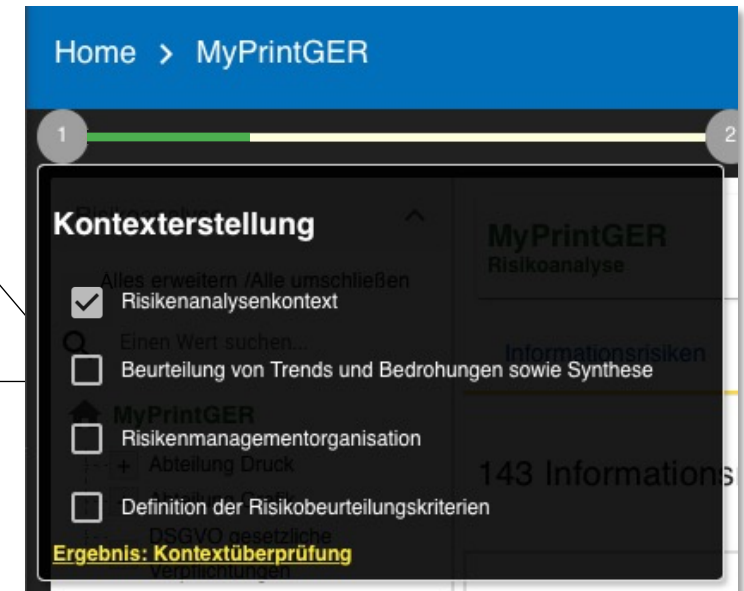


1.1 Risikoanalysekontext



- 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

Beurteilung von Trends und Bedrohungen sowie Synthese

Beurteilung von Trends **Beurteilung von Bedrohungen** Zusammenfassung

Analyse von Bedrohungen - 1 / 18 Terroristische Akte

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 d

☐ Wahrscheinlichkeit in der Analyse erzwingen

< Zurück Speichern Weiter >

Home > MyPrintGER

1 2

Kontexterstellung

Alles erweitern / Alle umschließen

☒ **Risikoplananalyse**

☐ **Beurteilung von Trends und Bedrohungen sowie Synthese**

MyPrintGER

☐ **Risikomanagementorganisation**

+ Abteilung Druck

☐ **Definition der Risikobeurteilungskriterien**

Ergebnis: Kontextüberprüfung

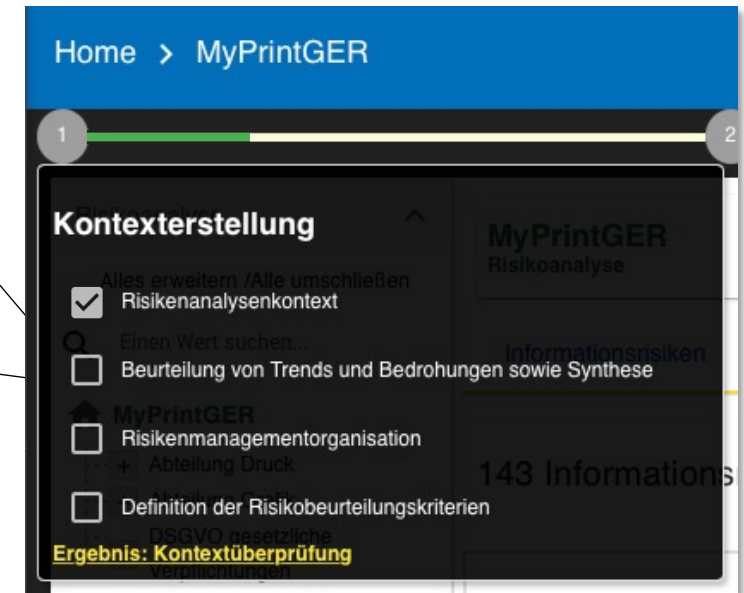
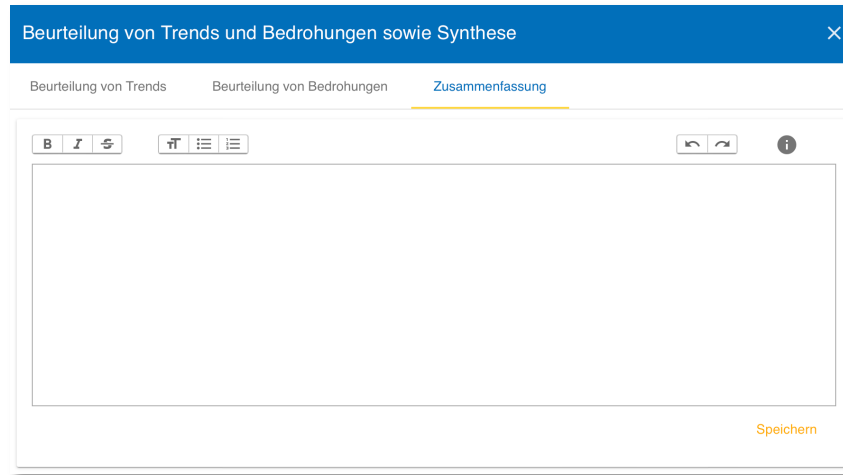
MyPrintGER Risikoanalyse

Informationsrisiken

143 Informations

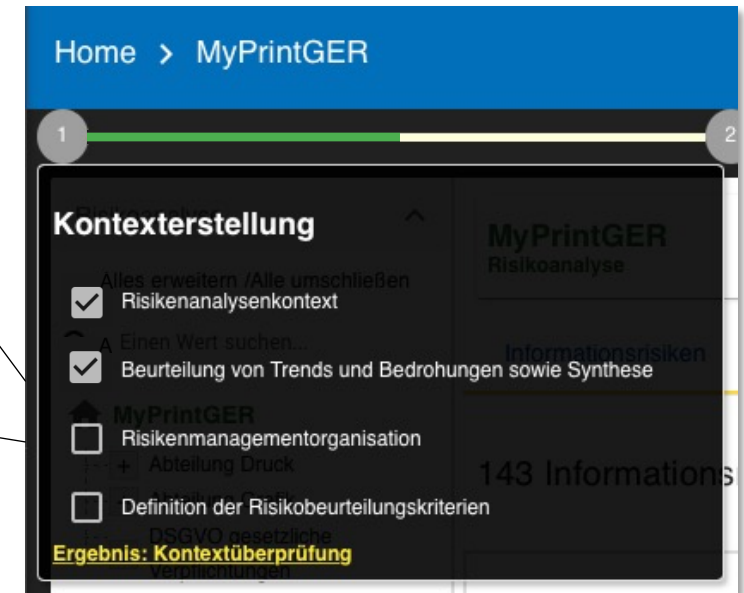
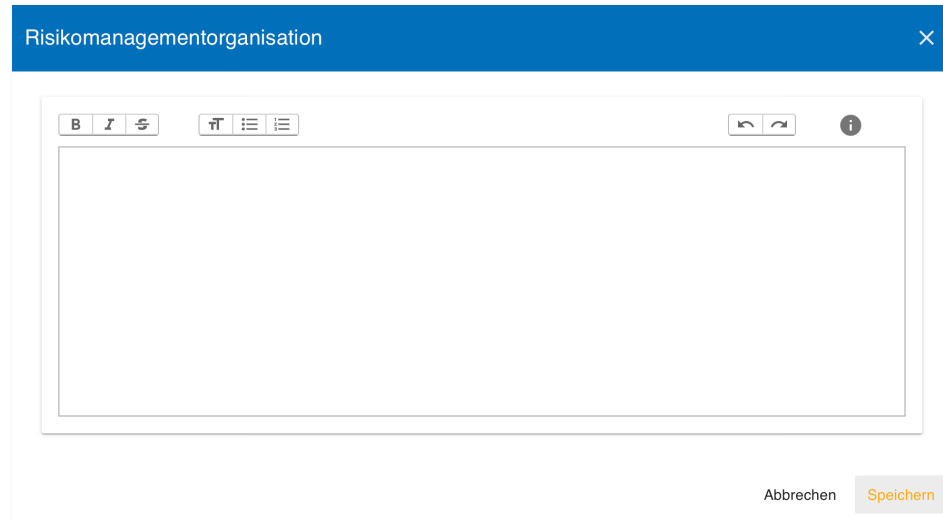
- Bewertung von Bedrohungen vor dem eigenen Kontext
- Sammeln von Informationen aller Beteiligten

1.2.3 Zusammenfassung



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

1.3 Risikomanagementorganisation



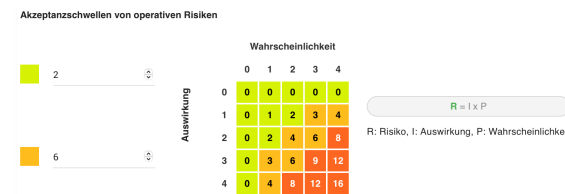
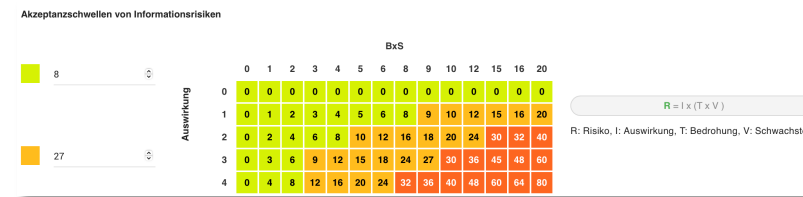
- Zusätzliche Informationen zur Risikomanagementorganisation
- Referenz zu ISO/IEC 27005:2022:
 - Organizational considerations: Kap. 6.1

1.4 Definition der Kriterien für Informationsrisiken

Skala der Auswirkungen und Folgen: [0 - 4]

☐ Ausgebildete Auswirkungen anzeigen

	Auswirkungen			Folgen		
	Vertraulichkeit	Integrität	Verfügbarkeit	Ruf	Versorgungssicherheit	Rechtlich
0	Ohne Auswirkung. Das Vertraulichkeitskriterium ist nicht wichtig. Schwache Auswirkung, unbedeutend. Informationsrisiko und negativ für die Interessen der Organisation. Beispiel: - Interne Informationen, die das Unternehmen nicht verlassen sollten, werden preisgegeben. - Mangel - Internes Telefonverzeichnis	Ohne Auswirkung. Das Integritätskriterium ist nicht wichtig. Schwache Auswirkung, unbedeutend. Einzelfall zu richtiger Beschädigung ohne jegliche Folgen. Beispiel: - Interne E-Mail oder Schreiben	Ohne Auswirkung. Das Verfügbarkeitskriterium ist nicht wichtig. Schwache Auswirkung, unbedeutend. Nichtverfügbarkeit, die unständlich, aber nicht kritisch nachteilig für die Stakeholder ist	Keine Folgen	Keine Folgen	Keine Folgen
1	Durchschnittliche Auswirkung, annehmbar. Informationsrisiko schädigen die Interessen der Organisation. Beispiel: - Mäßig vertrauliche Informationen, die nur eine Personengruppe betreffen, werden preisgegeben. - Schema für internes Networking - Dokumentation	Durchschnittliche Auswirkung, annehmbar. Beschädigung, die zu Unannehmlichkeiten für die Stakeholder führt. Wiederherstellung ist einfach. Beispiel: - Informative Website	Durchschnittliche Auswirkung, annehmbar. Nichtverfügbarkeit, die zu Unannehmlichkeiten für die Stakeholder führt. Beispiel: - Als untragbar geltende Höchstausgaben werden nicht erreicht.	Vorübergehende Abwertung der Firma oder des Rufs der Belegschaft. Gelegentliche Kritik in den Medien	Isolierte Vorfälle mit überschaubarer Auswirkung auf Kunden	Mögliche Strafe für die Firma
2	Starke Auswirkung, kaum tragbar. Informationsrisiko schädigen die Interessen der Organisation erheblich. Beispiel: - Vertrauliche Informationen werden preisgegeben. - Vertrauliche personenbezogene Daten - Sicherheitsvorfall	Starke Auswirkung, kaum tragbar. Beschädigung, die zu erheblichen Unannehmlichkeiten für die Stakeholder führt. Beispiel: - Verwundung unter Stakeholdern	Starke Auswirkung, kaum tragbar. Nichtverfügbarkeit, die zu erheblichen Unannehmlichkeiten für die Stakeholder führt. Beispiel: - Als untragbar geltende Höchstausgaben werden erreicht.	Starke Abwertung der Firma oder des Rufs der Belegschaft. Scharfe und wiederholte Kritik in den Medien	Störung einer gesamten Abteilung	Strafe für die Firma
3						
4						

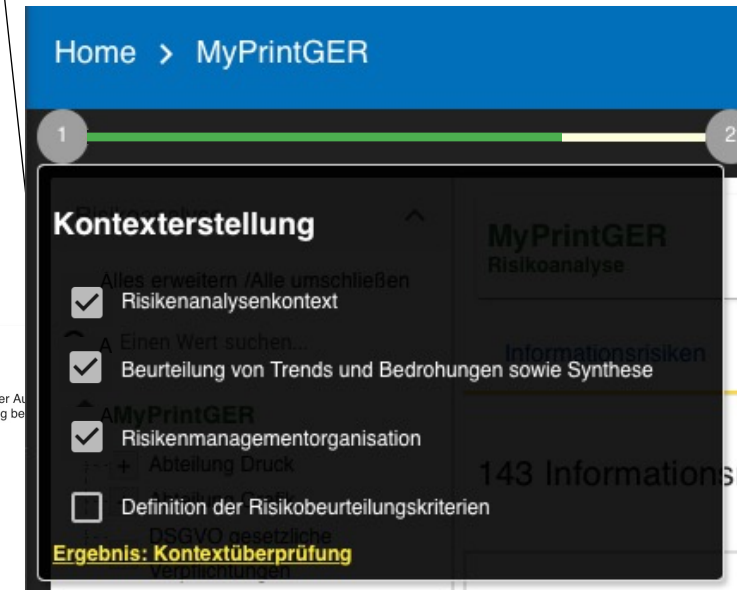


Wahrscheinlichkeitsskala: [0 - 4]

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

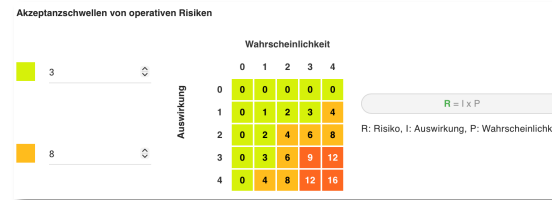
Qualifizierungsskala: [0 - 5]

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



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

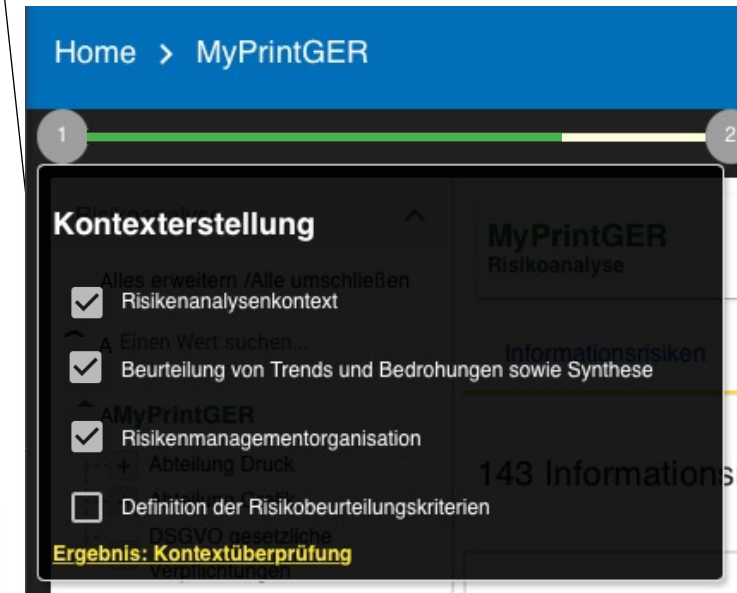
1.4 Definition der Kriterien für Operative Risiken



	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, imitation, 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).	Significant 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).	Significant 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. International media coverage.	Complete stop of all services	Heavy sentence for the company.	Brings some deadly fees almost insurmountable (more or less 20% of the sales revenue).	Significant 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

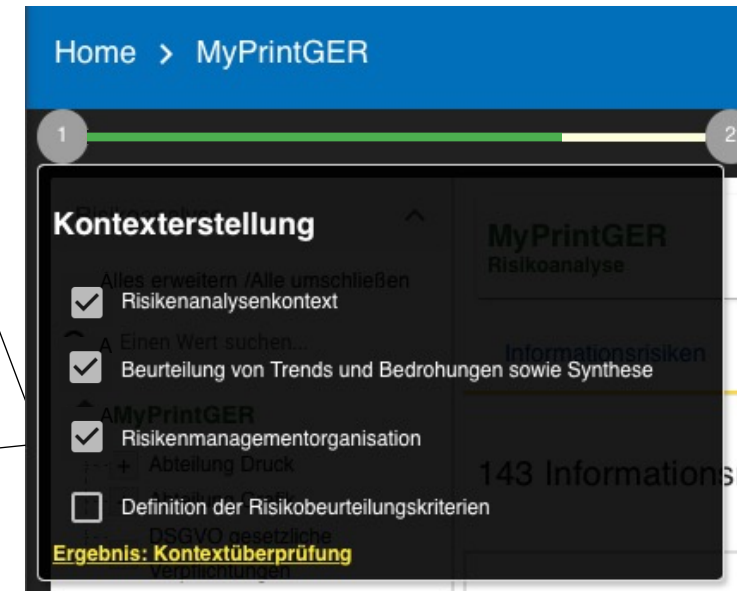


- Referenz zu ISO/IEC 27005:2022:
 - Establishing and maintaining information security risk criteria: Kapitel 6.4

1.4 Definition der Konformitätsskala

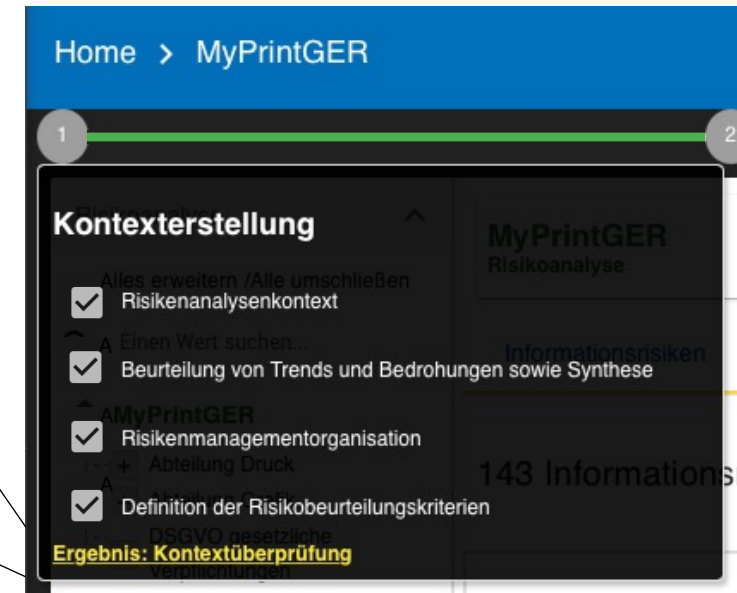
Konformitätsskala: 6 Ebenen

	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

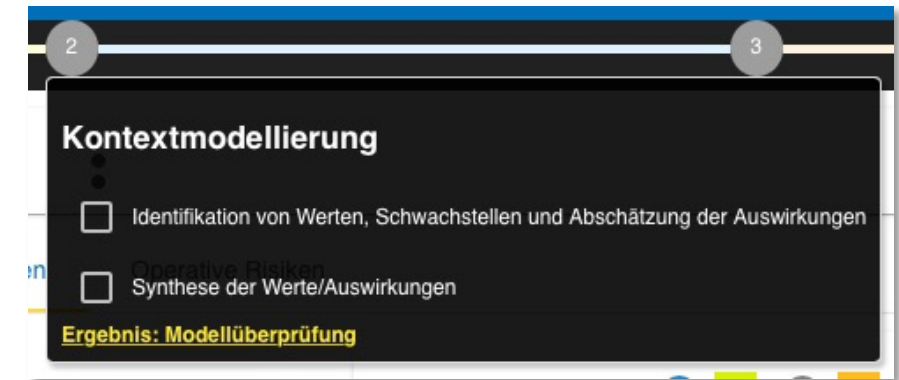
1. Kontexterstellung - Übung

Übung: Durchführen der Kontexterstellung (30 Minuten)

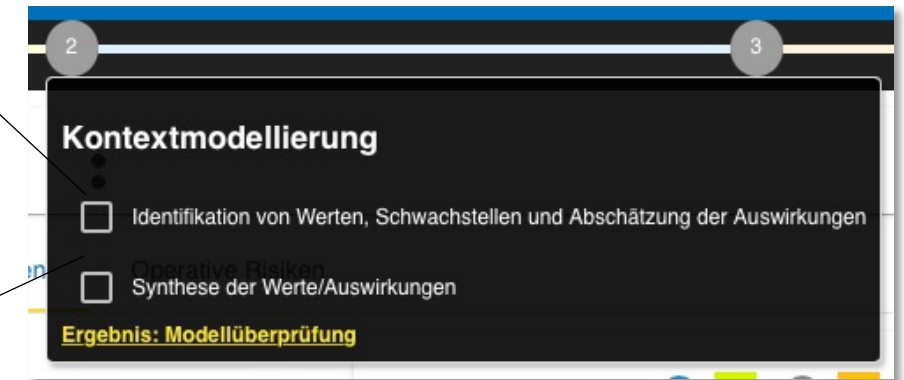
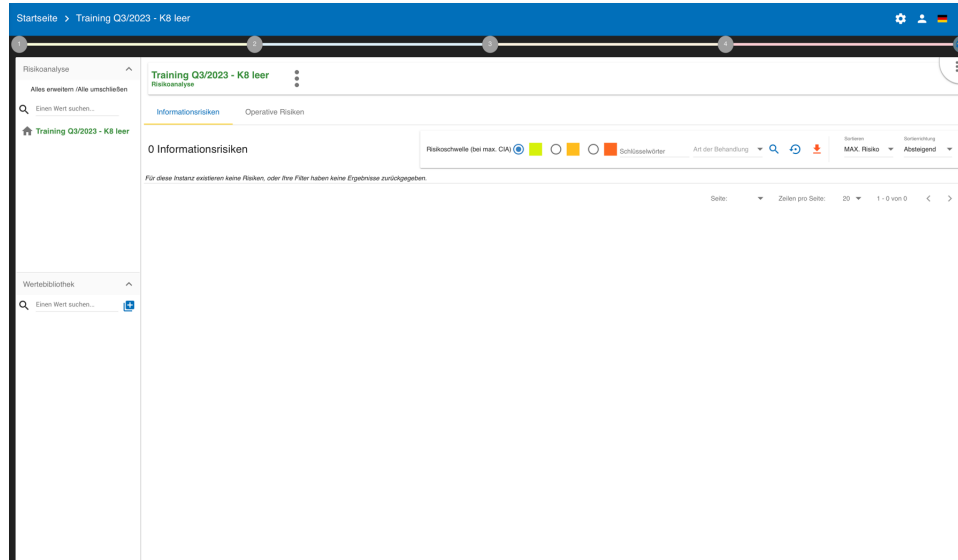
- **Ziel:** Definition des eigenen Kontextes
- **Vorgaben:**
 - Risikoanalysekontext: *<individuell>*
 - Beurteilung von Trends: *<individuell>*
 - Beurteilung von Bedrohungen: *<individuell>*
 - Zusammenfassung: *<individuell>*
 - Risikomanagementorganisation: *<individuell>*
 - Definition der Risikobeurteilungskriterien: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

2. Kontextmodellierung

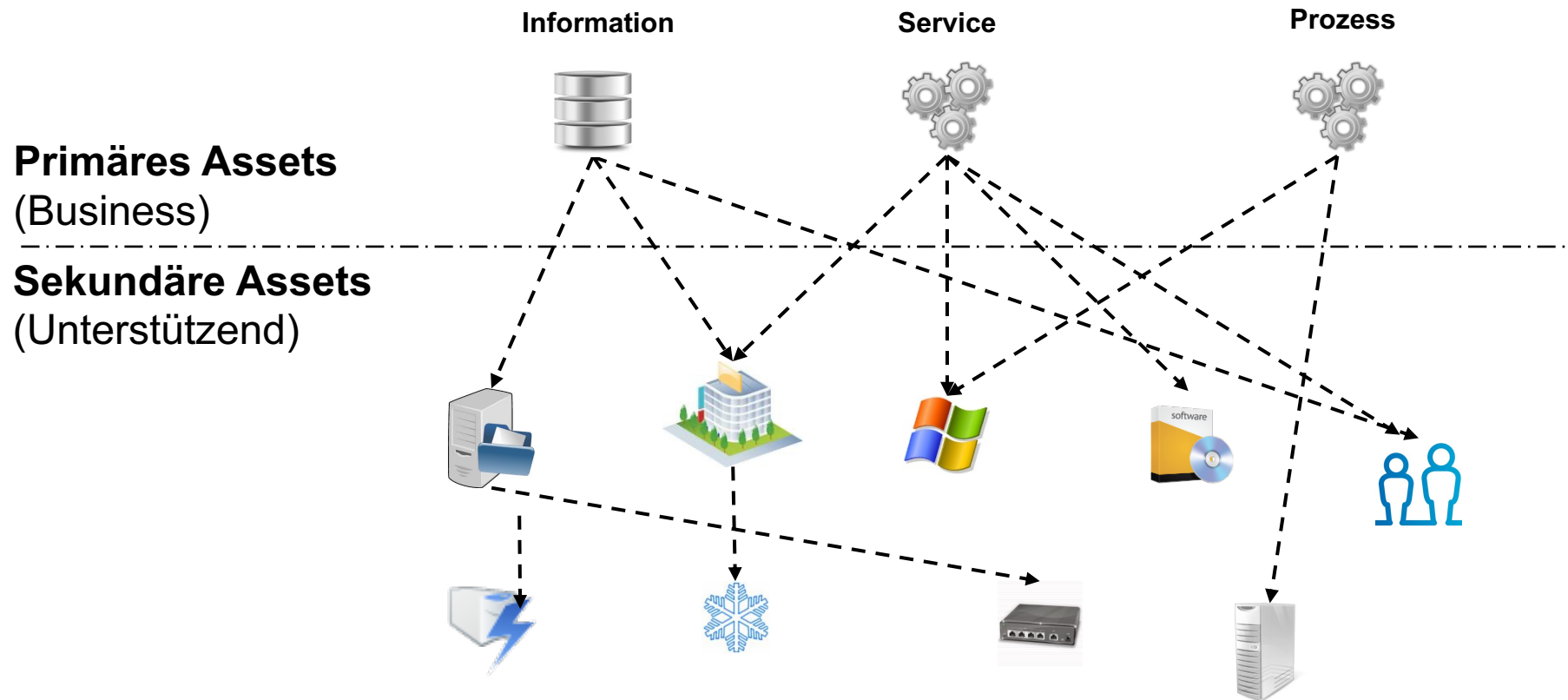
- Identifikation von Werten, Schwachstellen und Abschätzung der Auswirkungen
- Synthese der Werte/Auswirkungen



2.1 Identifikation von Werten, Schwachstellen und Abschätzung der Auswirkungen



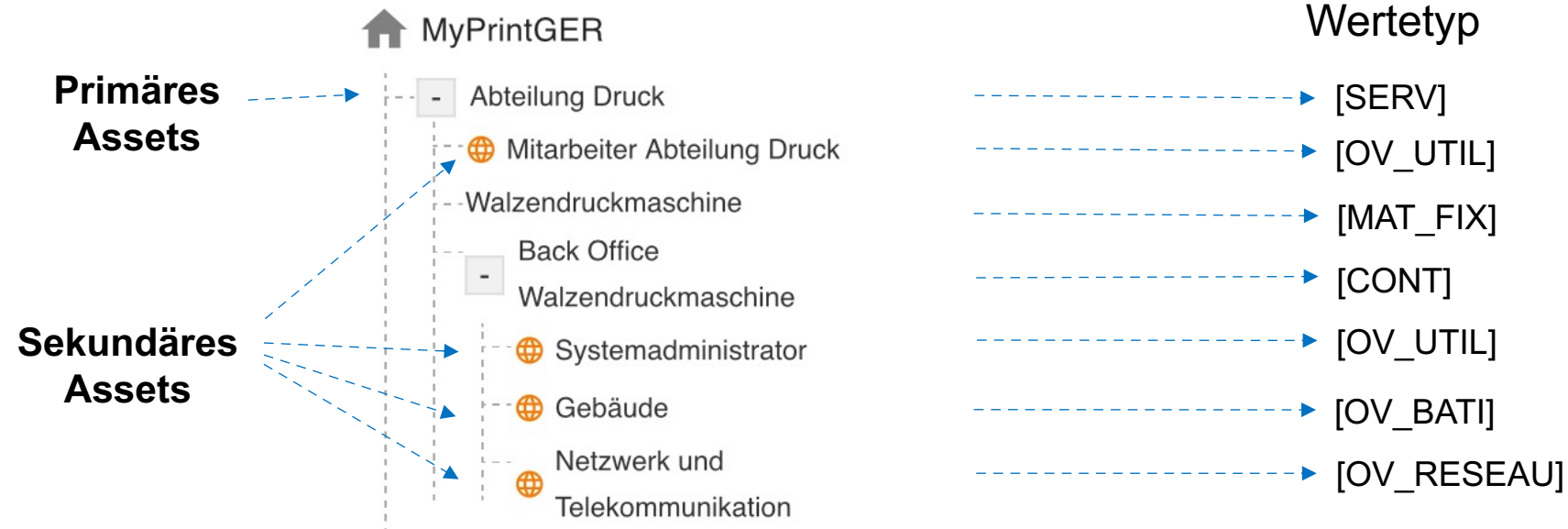
2.1 Identifikation von Werten, Schwachstellen und Abschätzung der Auswirkungen



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

2.1 Die Modellierung in MONARC

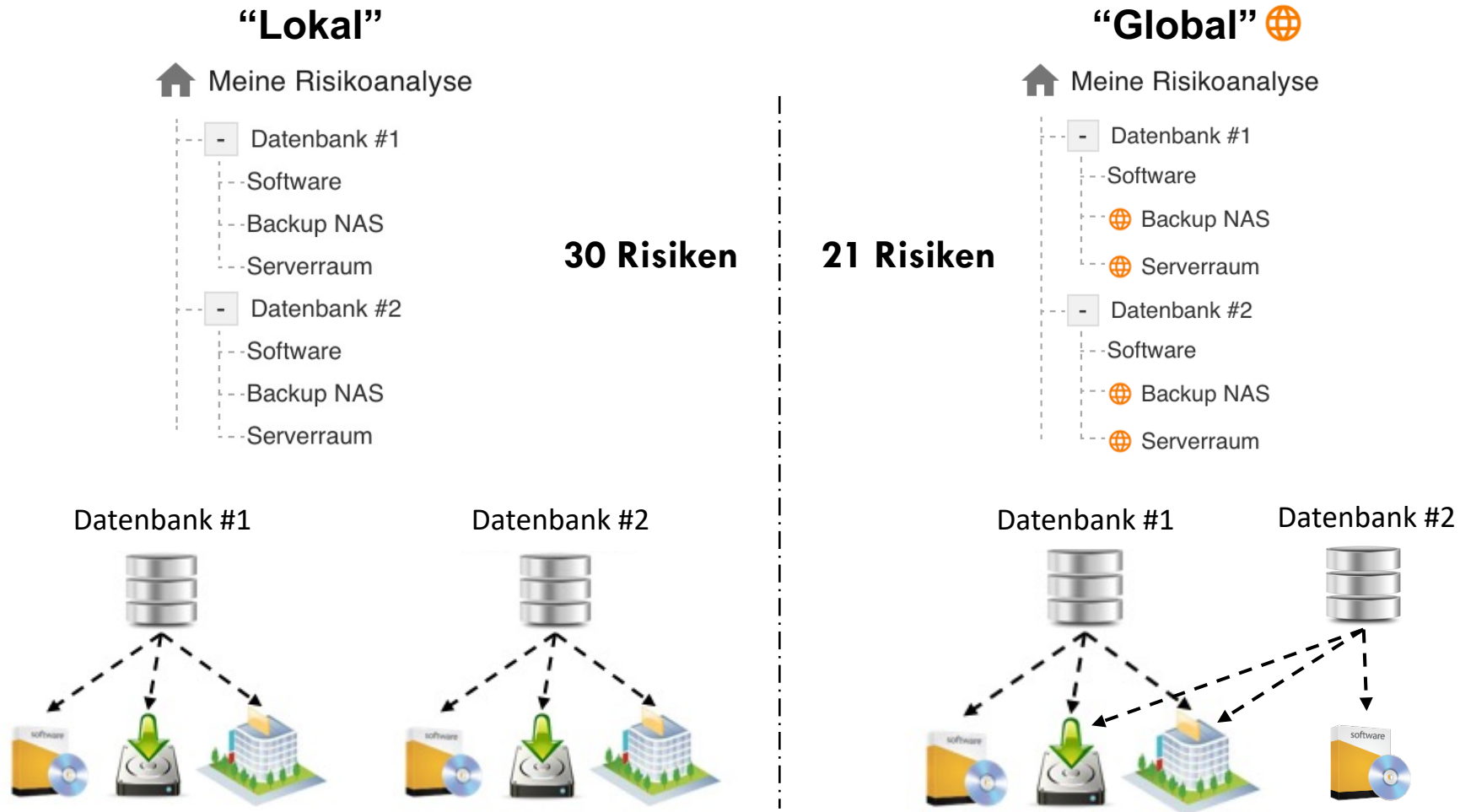
Hierarchie der Assets



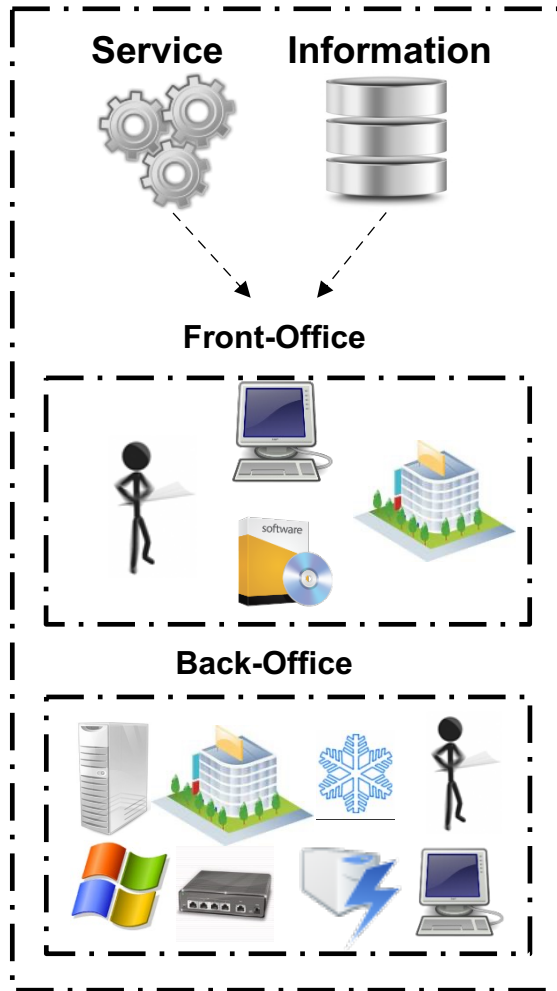
OV_BATI

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.

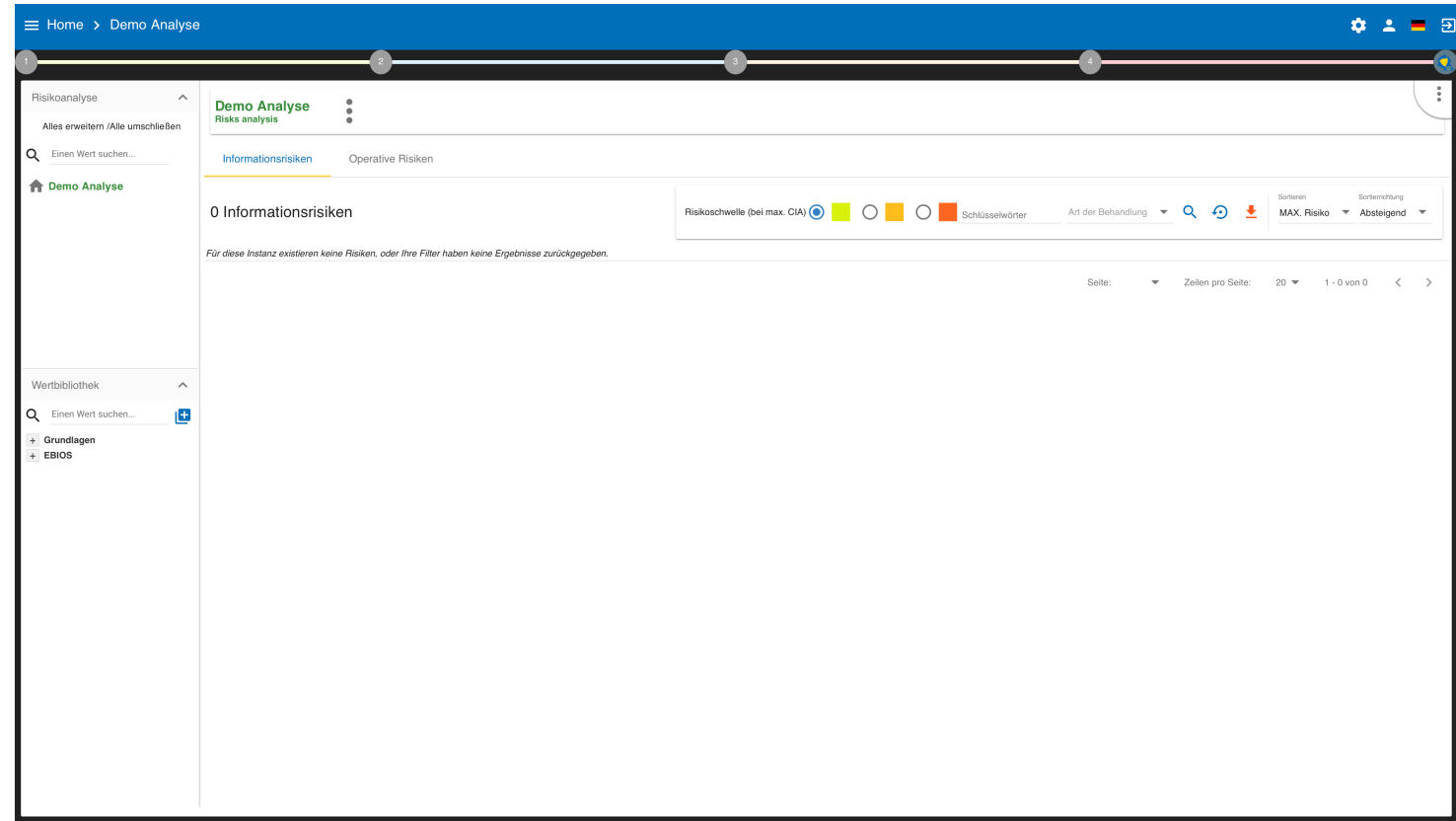
2.1 „Lokale“ und „Globale“ Assets



2.1 CASES Modellierung



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

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**

2 3

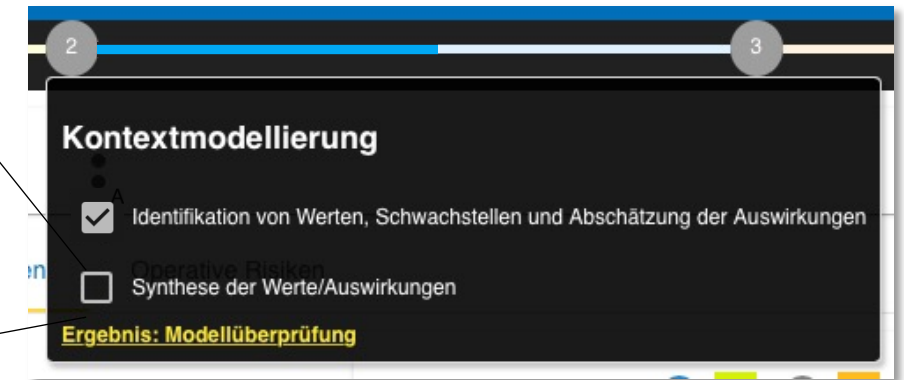
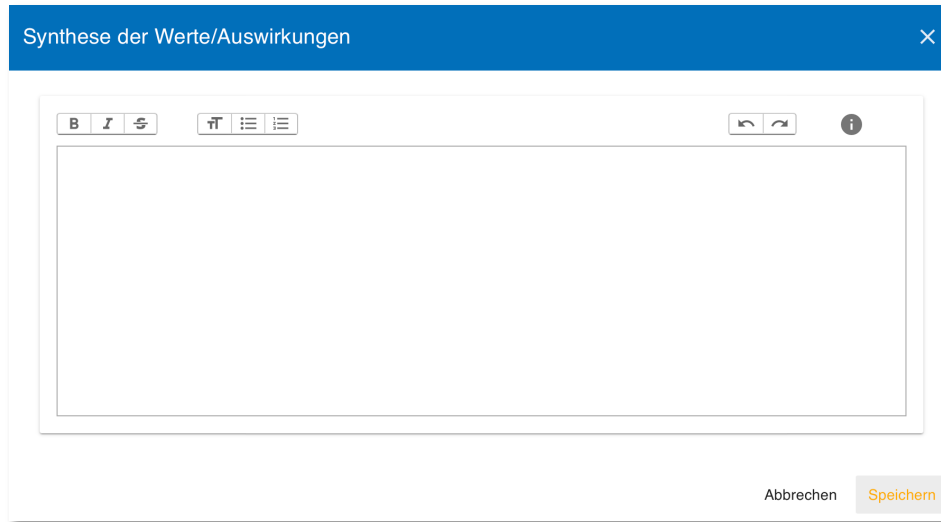
Kontextmodellierung

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

Ergebnis: Modellüberprüfung

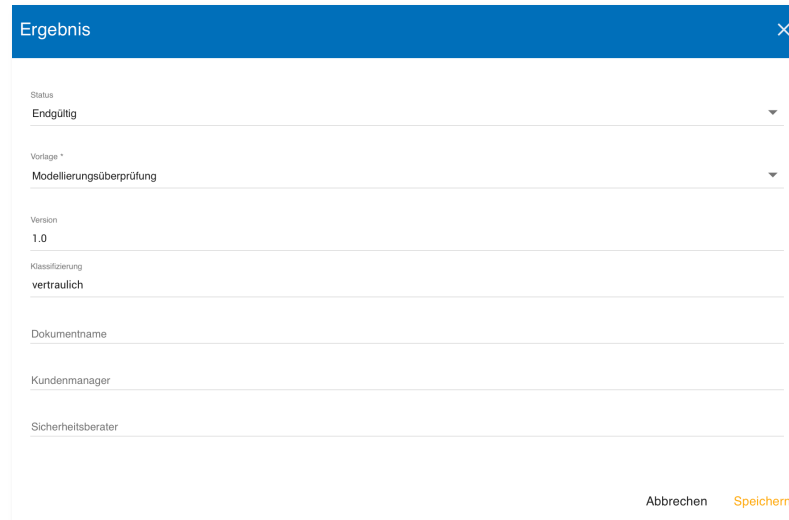
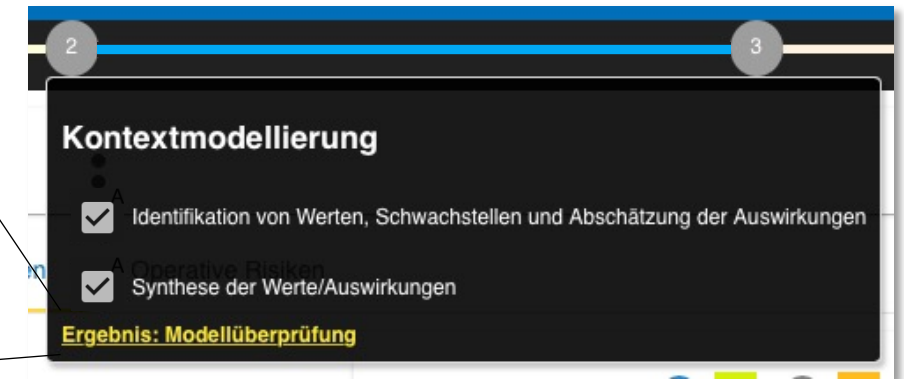
- Hauptansicht von MONARC
- Auswirkungen bearbeiten
- Referenz zu ISO/IEC 27005:2022:
 - Information security risk assessment process: Kapitel 7

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

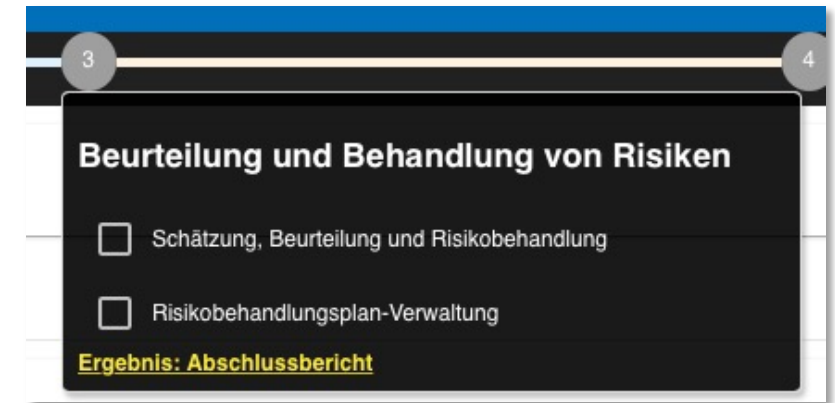
2. Kontextmodellierung - Übung

Übung: Durchführen der Kontextmodellierung (30 Minuten)

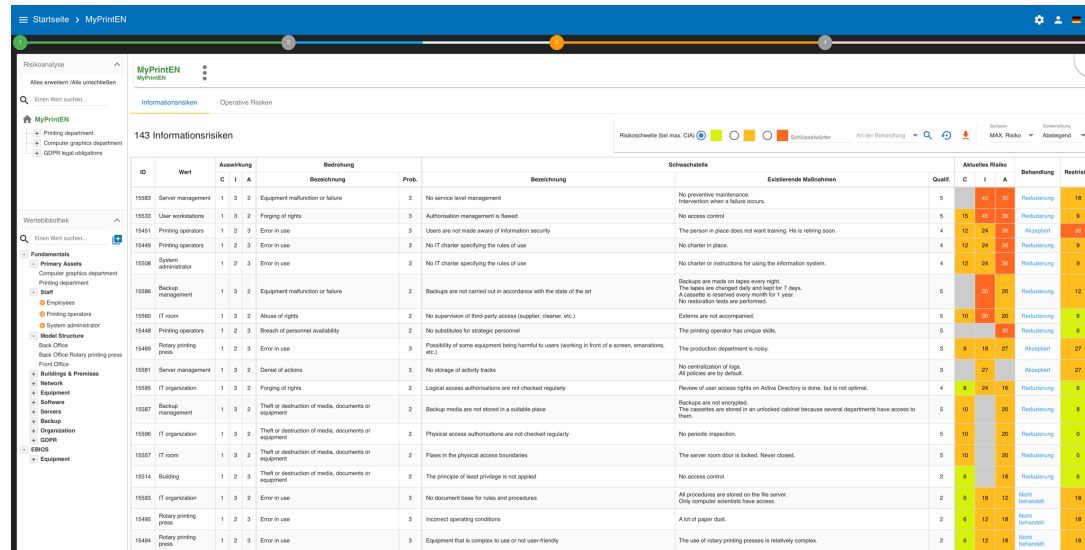
- **Ziel:** Definition des eigenen Kontextes
- **Vorgaben:**
 - Anlagen eigener
 - Lokaler und globaler Assets: *<individuell>*
 - Clonen von Assets: *<individuell>*
 - Asset-Kategorien: *<individuell>*
 - Modellierung von Abhängigkeiten: *<individuell>*
 - Erstellen der Risikoanalyse per Drag & Drop: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



ID	Wert	Auswirkung	Bedrohung	Prob.	Beschreibung	Schwachstelle	Existierende Maßnahmen	Qualif.	C	I	A	Behandlung	Risikost.
15352	Server management	1	3	2	Equipment malfunction or failure	3	No service level management	5	15	25	35	Risikobewertung	15
15353	User workstations	1	3	2	Forging of rights	3	Authorization management is flawed	5	15	25	35	Risikobewertung	15
15451	Printing operators	1	2	3	Error in use	3	Users are not made aware of information security	4	12	24	36	Akzeptiert	9
15452	Printing operators	1	2	3	Error in use	3	The person in place does not want training. He is retiring soon.	4	12	24	36	Risikobewertung	9
15453	Printing operators	1	2	3	Error in use	3	No IT charter specifying the rules of use	4	12	24	36	Risikobewertung	9
15555	System administrator	1	2	3	Error in use	3	No IT charter specifying the rules of use	4	12	24	36	Risikobewertung	9
15556	Backup management	1	3	2	Equipment malfunction or failure	2	Backups are not carried out in accordance with the state of the art	5	15	25	35	Risikobewertung	12
15557	IT room	1	3	2	Abuse of rights	2	No supervision of third-party access (supplier, cleaner, etc.)	5	15	25	35	Risikobewertung	9
15458	Printing operators	1	2	3	Breach of personnel availability	2	No substitutes for strategic personnel	5	15	25	35	Risikobewertung	9
15459	Rotary printing press	1	2	3	Error in use	3	Possibility of some equipment being harmful to users (looking in front of a screen, extensions, etc.)	3	9	18	27	Akzeptiert	27
15559	Server management	1	3	2	Denial of actions	3	No storage of activity tracks	3	9	18	27	Akzeptiert	27
15560	IT organization	1	3	2	Forging of rights	2	Logical access authorizations are not checked regularly	4	12	24	36	Risikobewertung	9
15561	Backup management	1	3	2	Theft or destruction of media, documents or equipment	2	Backup media are not stored in a suitable place	5	15	25	35	Risikobewertung	9
15562	IT organization	1	3	2	Theft or destruction of media, documents or equipment	2	Physical access authorizations are not checked regularly	5	15	25	35	Risikobewertung	9
15563	IT room	1	3	2	Theft or destruction of media, documents or equipment	2	Flaws in the physical access boundaries	5	15	25	35	Risikobewertung	9
15514	Building	1	2	3	The principle of least privilege is not applied	2	No access control	3	9	18	27	Risikobewertung	9
15555	IT organization	1	3	2	Error in use	3	No document base for rules and procedures	2	6	12	18	Nicht behandelt	18
15455	Rotary printing press	1	2	3	Error in use	3	Incorrect operating conditions	2	6	12	18	Nicht behandelt	18
15456	Rotary printing press	1	2	3	Error in use	3	Equipment that is complex to use or not user-friendly	2	6	12	18	Nicht behandelt	18

3

4

Beurteilung und Behandlung von Risiken

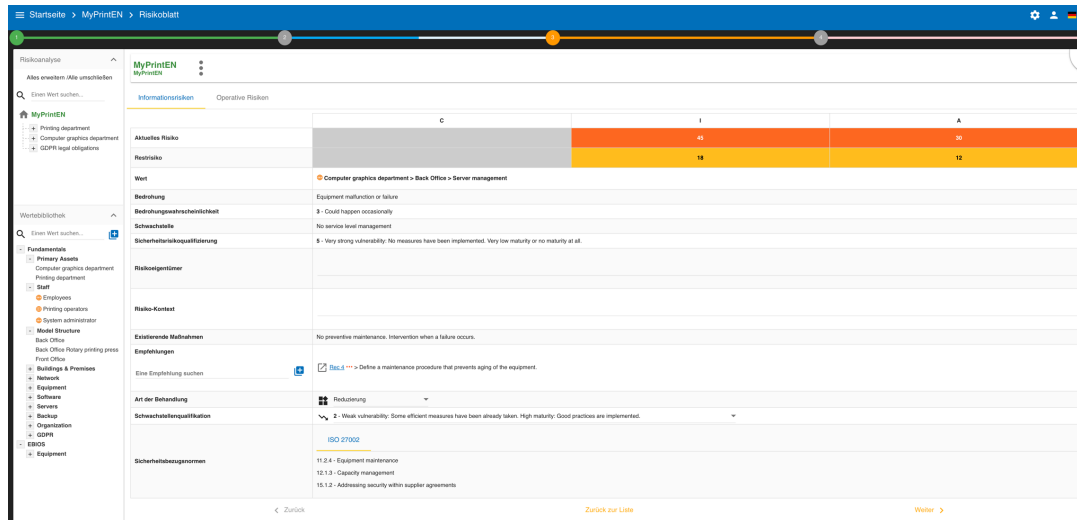
☐ Schätzung, Beurteilung und Risikobehandlung

☐ Risikobehandlungsplan-Verwaltung

Ergebnis: Abschlussbericht

- Hauptansicht von MONARC
- Alle Risiken bewerten

3.1 Schätzung, Beurteilung und Risikobehandlung



	C	I	A
Aktuelles Risiko		44	20
Restrisiko		18	12

Computer graphics department > Back Office > Server management

Equipment malfunction or failure

Bedrohung

Bedrohungsgefahr

Schwachstelle

Sicherheitsbewertung

Sehr starke Vulnerabilität: No measures have been implemented. Very low maturity or no maturity at all.

Risikogestaltung

Risiko-Kontext

Existierende Maßnahmen

Keine präventive Wartung. Intervention when a failure occurs.

Empfehlungen

Eine Empfehlung suchen

Act der Behandlung

Schwachstellenqualifikation

2 - Weak vulnerability: Some efficient measures have been already taken. High maturity: Good practices are implemented.

ISO 27002

Sicherheitsmaßnahmen

11.2.4 - Equipment maintenance

12.1.3 - Capacity management

15.1.2 - Addressing security within supplier agreements

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

3 4

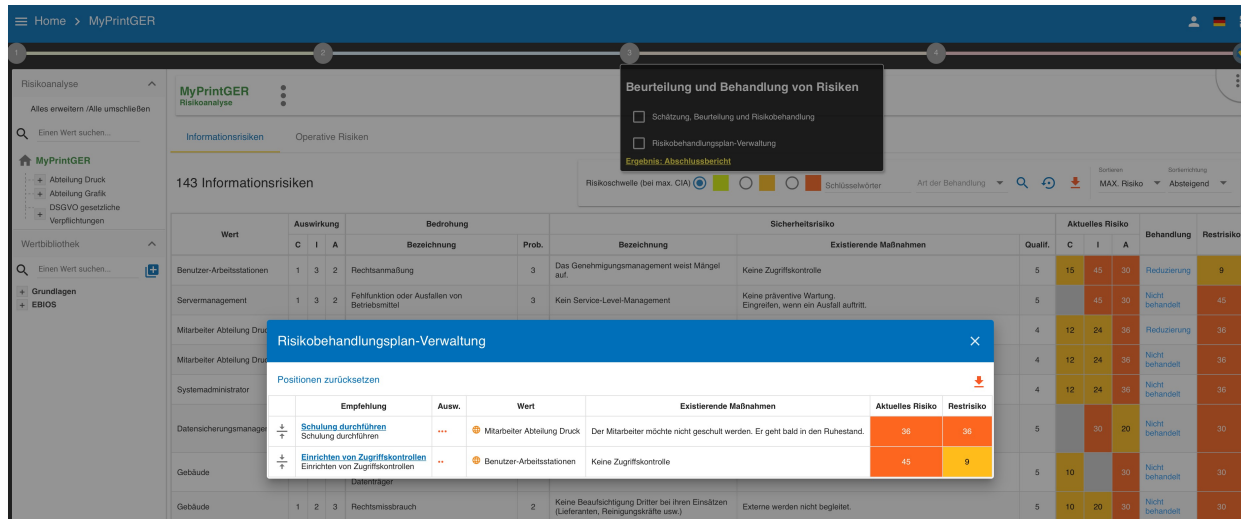
Beurteilung und Behandlung von Risiken

- ☐ Schätzung, Beurteilung und Risikobehandlung
- ☐ Risikobehandlungsplan-Verwaltung

Ergebnis: Abschlussbericht

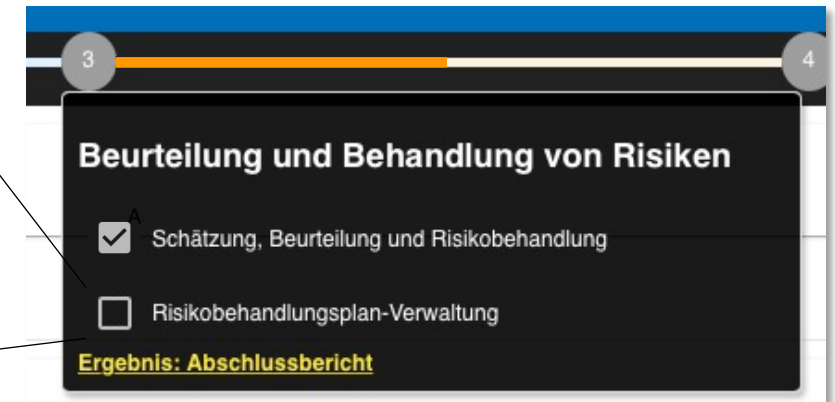
- Anlegen einer Maßnahme

3.2 Risikobehandlungsplan-Verwaltung



The screenshot shows the MyPrintGER Risk Management interface. A modal titled "Risikobehandlungsplan-Verwaltung" is open, displaying a table with columns: Empfehlung, Ausw., Wert, Existierende Maßnahmen, Aktuelles Risiko, and Restrisiko. The table lists several recommendations and their corresponding risk levels.

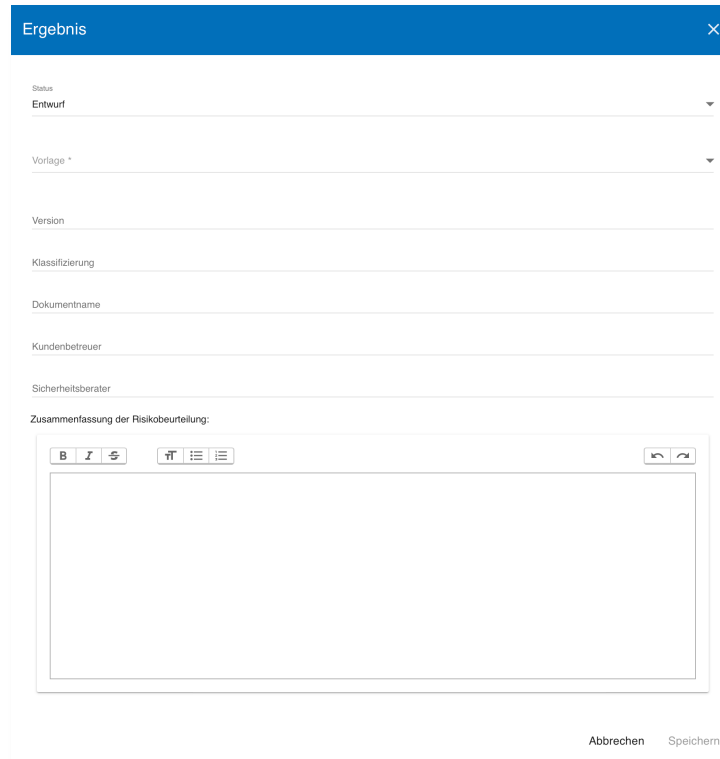
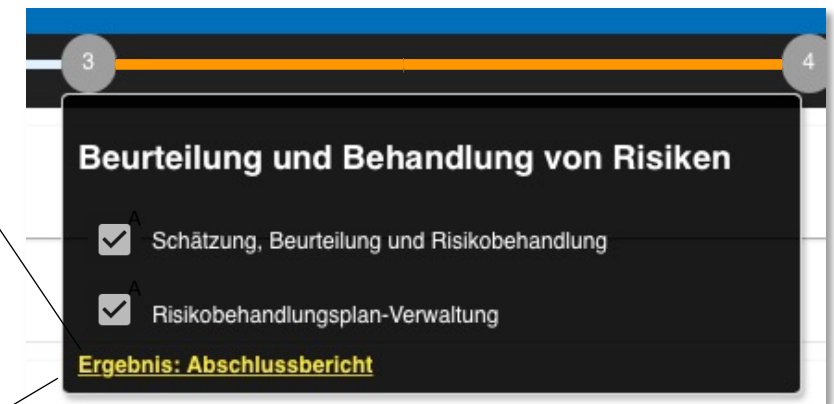
Empfehlung	Ausw.	Wert	Existierende Maßnahmen	Aktuelles Risiko	Restrisiko
Schulung durchführen	...	Mitarbeiter Abteilung Druck	Der Mitarbeiter möchte nicht geschult werden. Er geht bald in den Ruhestand.	36	36
Einrichten von Zugriffskontrollen	...	Benutzer-Arbeitsstationen	Keine Zugriffskontrolle	45	9



The diagram illustrates the process flow for risk assessment and treatment plan management. It shows a sequence of steps: 3. Beurteilung und Behandlung von Risiken, which includes two sub-steps: Schätzung, Beurteilung und Risikobehandlung (checked) and Risikobehandlungsplan-Verwaltung (unchecked). The final result is labeled "Ergebnis: Abschlussbericht".

- 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

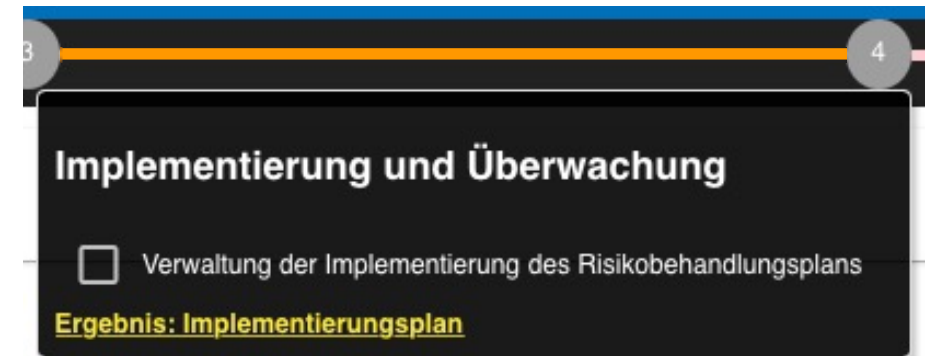
3. Beurteilung und Behandlung von Risiken - Übung

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



The screenshot shows a software interface with a progress bar at the top. The progress bar has a blue segment on the left and an orange segment on the right, with a grey circle containing the number 4 on the right side. Below the progress bar, there is a dark grey box with the title "Implementierung und Überwachung" in white. Below the title, there is a checkbox followed by the text "Verwaltung der Implementierung des Risikobehandlungsplans". At the bottom of the box, the text "Ergebnis: Implementierungsplan" is displayed in yellow.

4.1 Verwaltung der Implementierung des Risikobehandlungsplans

Home > MyPrintGER > Implementation of the risk treatment plan

Risikoanalyse

Alles erweitern / Alle umschließen

Einen Wert suchen...

MyPrintGER

- Abteilung Druck
- Abteilung Grafik
- DSGVO gesetzliche Verpflichtungen

Wertbibliothek

Einen Wert suchen...

- Grundlagen
- EBIOS

Implementierung des Risikobehandlungsplans

Den Implementierungsverlauf öffnen

	Empfehlung	Ausw.	Kommentar	Verwalter	Stichtag	Status	Aktionen
	Schulung durchführen Schulung durchführen	...			▼ ×	Bevorstehend	🔗
	Einrichten von Zugriffskontrollen Einrichten von Zugriffskontrollen	..			▼ ×	Bevorstehend	🔗

Implementierung und Überwachung

☐ Verwaltung der Implementierung des Risikobehandlungsplans

Ergebnis: Implementierungsplan

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

4.1 Verwaltung der Implementierung des Risikobehandlungsplans

Home > MyPrintGER > Implementation of the risk treatment plan > Recommendation

Risikoanalyse

← Zurück zur Liste

Einrichten von Zugriffskontrollen

Einrichten von Zugriffskontrollen

Wert	Bedrohung	Sicherheitsrisiko	Existierende Maßnahmen	Aktuelles Risiko	Neue Maßnahmen	Restrisiko	Aktionen
Benutzer-Arbeitsstationen	MD14 - Rechtsanwaltschaft	1166 - Das Genehmigungsmanagement weist Mängel auf.	Keine Zugriffskontrolle	45		9	

Wertbibliothek

Ein Wert suchen...

Grundlagen

EBIOS

3 4

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

Rec 5 - Mindestens eine zusätzliche Person in der Benutzung der Maschinen schulen. ×

Sie sind im Begriff, die Implementierung der Empfehlung **Rec 5 - Mindestens eine zusätzliche Person in der Benutzung der Maschinen schulen.** für das folgende Risiko zu überprüfen:

Wert: Mitarbeiter Abteilung Druck
Bedrohung: Beeinträchtigung der personalverfügbarkeit
Schwachstelle: Keine Redundanz des strategischen Personals

Optionaler Kommentar

Abbrechen Überprüfen

3
4

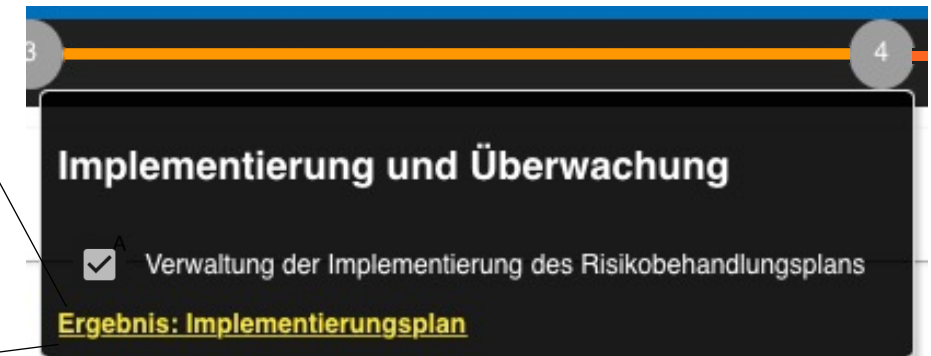
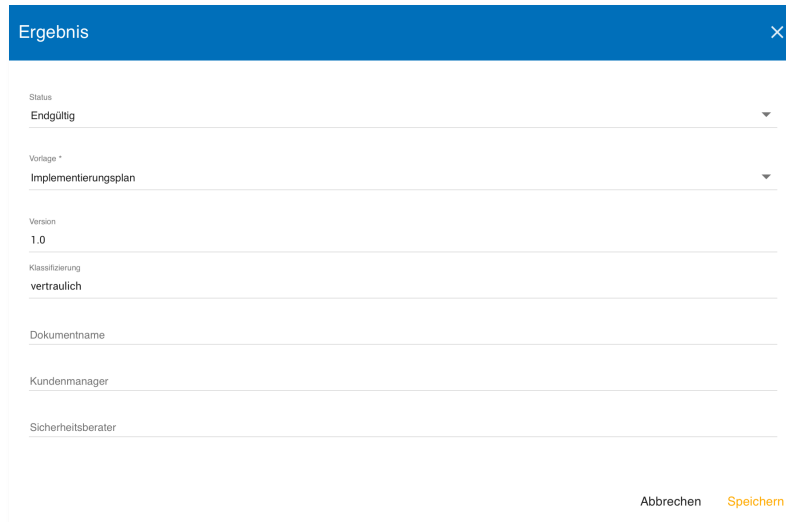
Implementierung und Überwachung

☐ Verwaltung der Implementierung des Risikobehandlungsplans

Ergebnis: Implementierungsplan

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

4.2 Ergebnis: Implementierungsplan



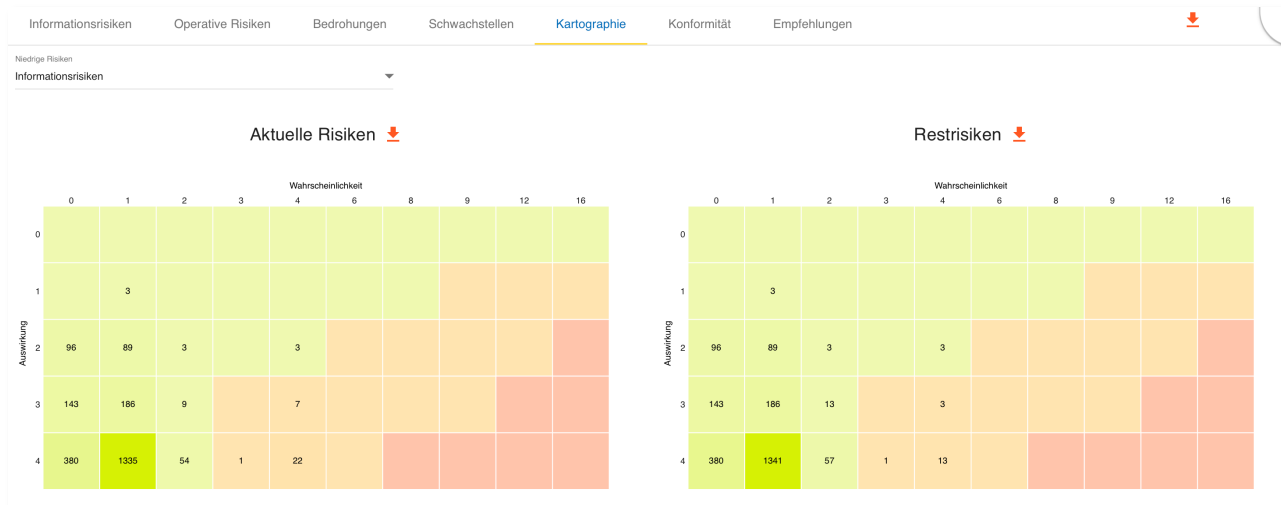
- Zusammenfassung des Risikobehandlungsplanes
- Aufstellung der bereits umgesetzten Maßnahmen
- Ziel: Offizieller Bericht zur Risikobehandlung
- Format: MS Word / ODF

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



Risikoanalyse

Dashboard

Beurteilungsskalen

Wissensdatenbank

Interviewtabelle




















Verzeichnis von Verarbeitungstätigkeiten

Anwendbarkeitserklärung

Momentaufnahmen

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

MONARC - Wissensdatenbank

Werttypen					
Bedrohungen Schwachstellen Bezugsnormen Informationsrisiken Tags Operative Risiken Empfehlungssets					
Werttypen   Suchen...					
Nur aktive anzeigen 					
<input type="checkbox"/> Status	Bezeichnung 	Code	Typ	Beschreibung	Aktionen
<input type="checkbox"/> 	Behälter	CONT	Primär	Vermögenswert-Behälter	 
<input type="checkbox"/> 	Benutzer	OV_UTIL	Sekundär	Benutzer	 
<input type="checkbox"/> 	Benutzer	PER_UTI	Sekundär	Nutzer	 
<input type="checkbox"/> 	Betreiber / Wartung	PER_EXP	Sekundär	Betreiber / Wartung	 
<input type="checkbox"/> 	Betriebssystem	LOG_OS	Sekundär	Windows 7, MAC OS X 10, Linux	 

Risikoanalyse

Dashboard

Beurteilungsskalen

Wissensdatenbank

Interviewtabelle

Verzeichnis von Verarbeitungstätigkeiten

Anwendbarkeitserklärung

Momentaufnahmen

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

MONARC - Interviewtabelle

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

Verarbeitungstätigkeit 1

Beschreibung

Name	Verarbeitungstätigkeit 1
Erstellungsdatum	2023-09-21
Aktualisierungsdatum	2023-09-21
Zweck	
Datensicherheitsmaßnahmen	

Agenten

Agent	Name	Kontaktdaten
Verantwortlich		
Datenschutzbeauftragter		
Vertreter		
Gemeinsam Verantwortliche		

Kategorien der betroffenen Personen und personenbezogenen Daten

Kategorien der betroffenen Person	Datenkategorien	Beschreibung	Aufbewahrungstzeit für Daten	Beschreibung der Aufbewahrungstzeit
			0 Tage(n)	

Empfänger

Empfänger	Empfängertyp	Beschreibung
	Intern	

Internationale Datenübertragungen

Organisation	Beschreibung	Land	Dokumente

Auftragsverarbeiter

AV 1

Name	AV 1
Kontaktdaten	
Aktivitäten	
Datensicherheitsmaßnahmen	

Agenten

Agent	Name	Kontaktdaten
Vertreter		
Datenschutzbeauftragter		

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

- Abbildung von EU-DSGVO Nachweisen

MONARC - Anwendbarkeitserklärung

Startseite > MyPrintGER > Anwendbarkeitserklärung

Anwendbarkeitserklärung

ISO/IEC 27002 [2022]

Suchen...

Alle Kategorien

Kategorie	Code	Maßnahme	Einbeziehung / Ausschluss	Bemerkungen/Begründung	Nachweise	Aktionen	Grad der Konformität
Organizational controls	5.1	Policies for information security	<div>NA</div> <div>RA</div> <div>VV</div> <div>GA</div> <div>BV</div> <div>ERB</div>				
Organizational controls	5.2	Information security roles and responsibilities	<div>NA</div> <div>RA</div> <div>VV</div> <div>GA</div> <div>BV</div> <div>ERB</div>				
Organizational controls	5.3	Segregation of duties	<div>NA</div> <div>RA</div> <div>VV</div> <div>GA</div> <div>BV</div> <div>ERB</div>				
Organizational controls	5.4	Management responsibilities	<div>NA</div> <div>RA</div> <div>VV</div> <div>GA</div> <div>BV</div> <div>ERB</div>				

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

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

- Momentaufnahmen erstellen als Nachweis für Versionierungen

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

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)

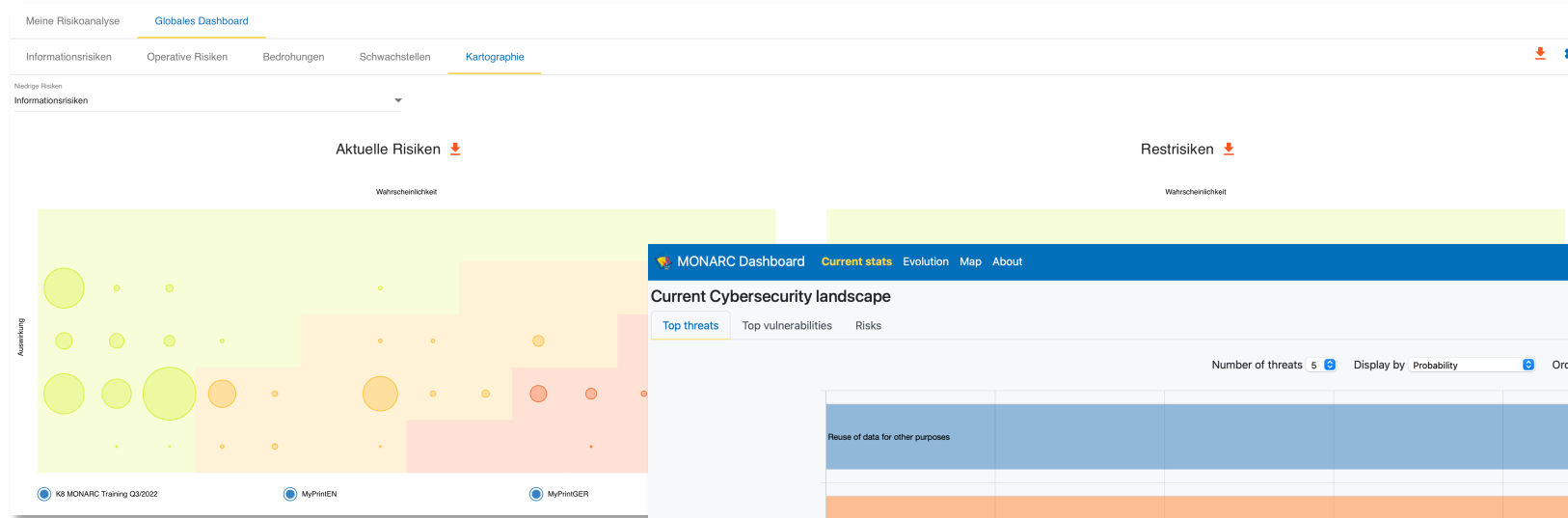
Weitere Tipps & Tricks

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

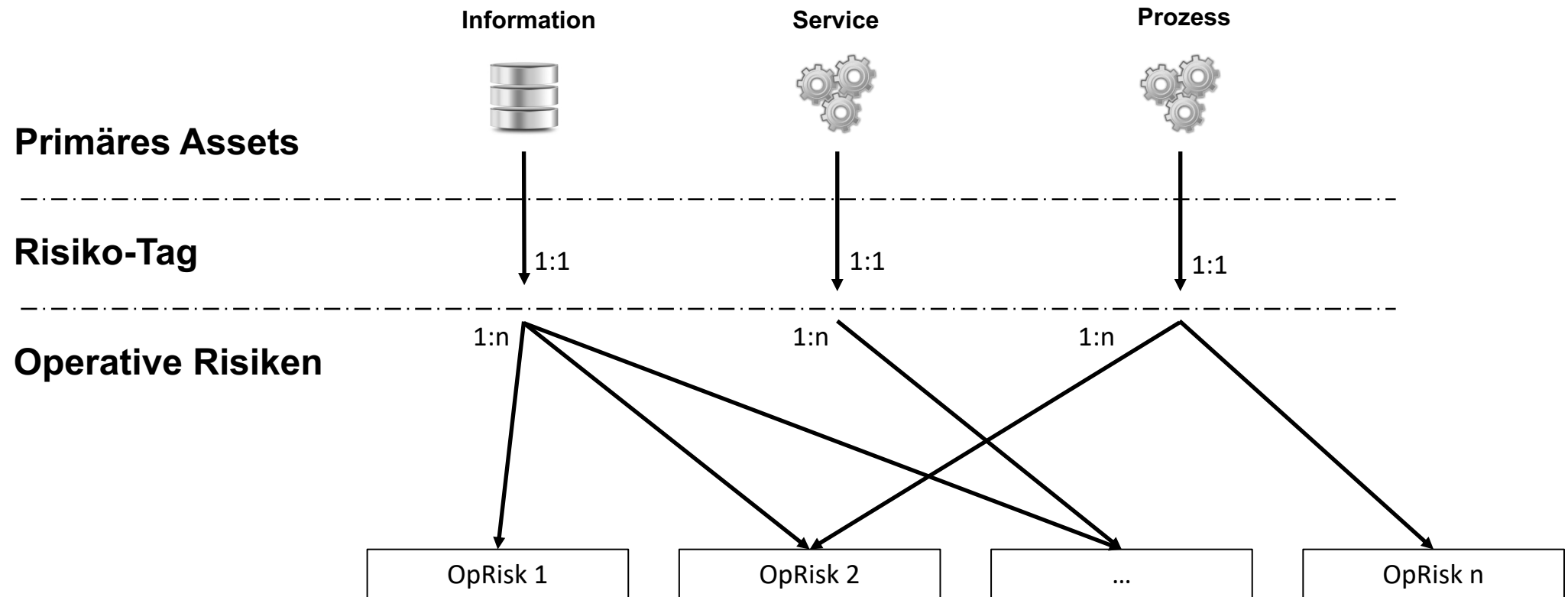
Technisches Wissen

- Wissenswertes zum technischen Aufsetzen der Plattform – bei Interesse
 - Installationsanleitung unter [GitHub](#)
 - Stats-Service

Global Dashboard



Exkurs: Operative Risiken



Exkurs: Operative Risiken

Startseite > MyPrintEN

1

2

3

4

Risikoanalyse

Alles erweitern /Alle umschließen

Einen Wert suchen...

MyPrintEN

- Printing department
- Computer graphics department
- GDPR legal obligations

Wertebibliothek

Einen Wert suchen...

Fundamentals

- Primary Assets
- Staff
- Model Structure
- Buildings & Premises
- Network
- Equipment
- Software
- Servers
- Backup
- Organization
- GDPR

Components

Consent

- Direct subcontracting
- DPO

Governance

- Lawfulness and legitimacy
- Principles relating to processing of personal data

Processor

- Recipients

Right of access

Right to erasure

Right to information

Right to object

Right to portability

Right to rectification

Right to restriction of

MyPrintEN

Informationsrisiken

Operative Risiken

62 operative Risiken

Risikoschwelle (bei max. NETTORISIKO)

Schlüsselwörter

Art der Behandlung

Suchen

Erneuern

Drucken

Sortieren

Nettorisiko

Sortierreichtung

Absteigend

ID	Wert	Risikobeschreibung	Wahrsch.	Auswirkung					Aktuelles Risiko	Nettorisiko	Existierende Maßnahmen	Behandlung	Restrisiko
				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

Seite:

1

Zeilen pro Seite:

20

1 - 20 von 62

Exkurs: Operative Risiken

MyPrintEN

MyPrintEN

Informationsrisiken

Operative Risiken

	Wahrsch.	Auswirkung					MAX. Risiko
		Reputation	Operational	Legal	Financial	Personal	
Aktuelles Risiko	4	1	3	3	2	3	12
Restrisiko	1	1	3	3	2	3	3
Wert	DPO						
Risikobeschreibung	Low communication between DPO and the commission						
Risikoeigentümer							
Risiko-Kontext							
Risikowahrscheinlichkeit	4 - Very likely: easy to execute, no mentionable investment or knowledge necessary						
Existierende Maßnahmen	Absence of DPO						
Empfehlungen							
Eine Empfehlung suchen	<div>Rec 12 --> Designate a DPO compliant with the GDPR</div>						
Art der Behandlung	<div>Reduzierung</div>						
Sicherheitsbezugsnormen	<div>ISO 27002</div>						

< Zurück

Zurück zur Liste

Weiter >

Fragen / Feedback



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



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 Sicherheitskonzepten
- Systeme zur Angriffserkennung (SzA)
- Threat Intelligence

Ihr Kontakt



 <https://www.konzeptacht.de>

 [Thomas Kochanek](#)

 [Thomas Kochanek](#)



Ihr Kontakt



konzeptacht GmbH

Marc Sparwel
Security Consultant

Hohenzollernring 57 · 50672 Köln
Tel.: +49 (0)221-291949-71 · Mobil: +49 (0)162-7745206
marc.sparwel@konzeptacht.de · www.konzeptacht.de

 <https://www.konzeptacht.de>

 [Marc Sparwel](#)

