



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



SECURITYMADEIN.LU



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG



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



*Computer Incident
Response Center
Luxembourg*



*Cyberworld Awareness
and Security Enhancement
Services*

**www.securitymadein.lu
www.cases.lu**



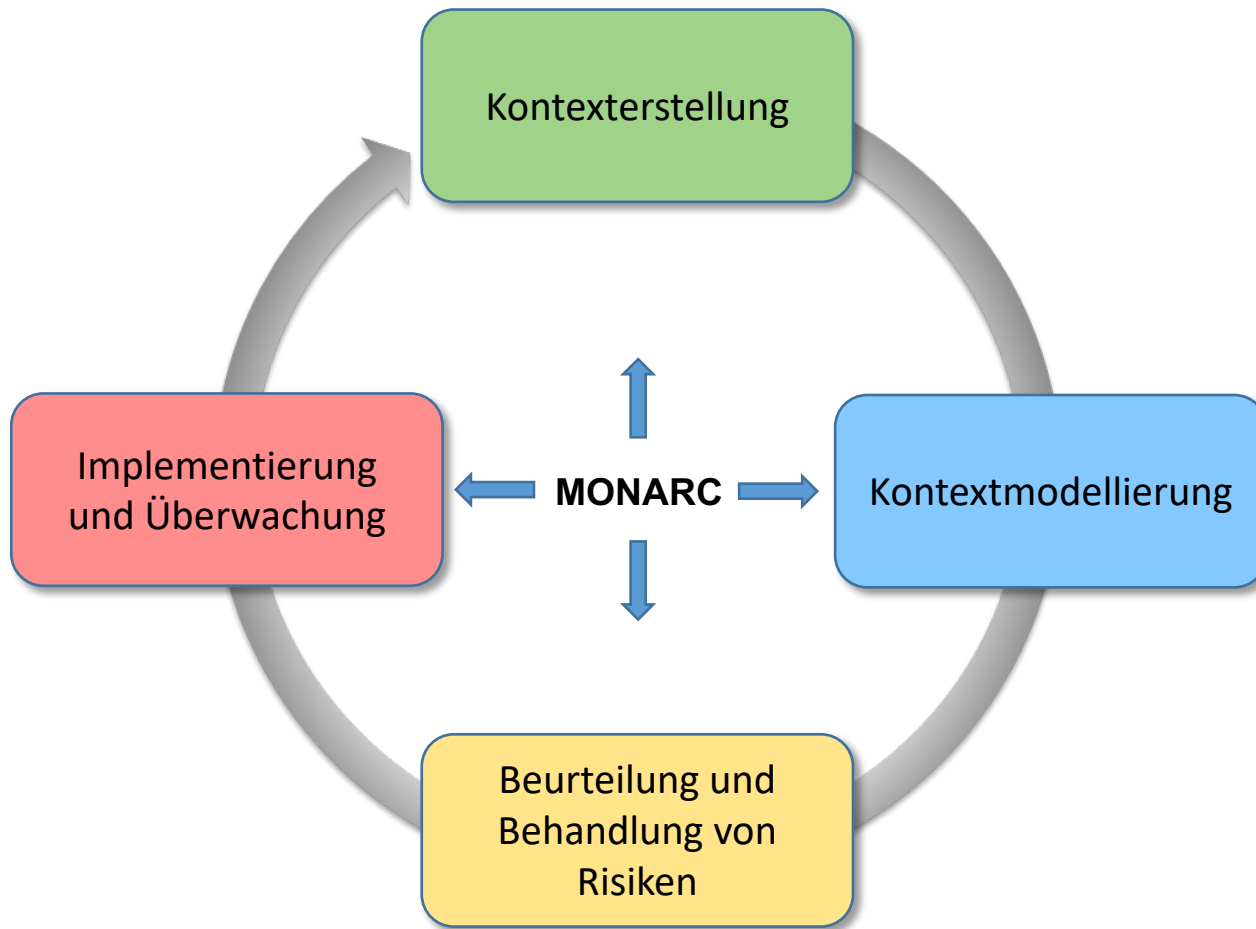
Was ist MONARC?

- 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 Code³ 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.

³ <https://github.com/monarc-project>



MONARC Methodik

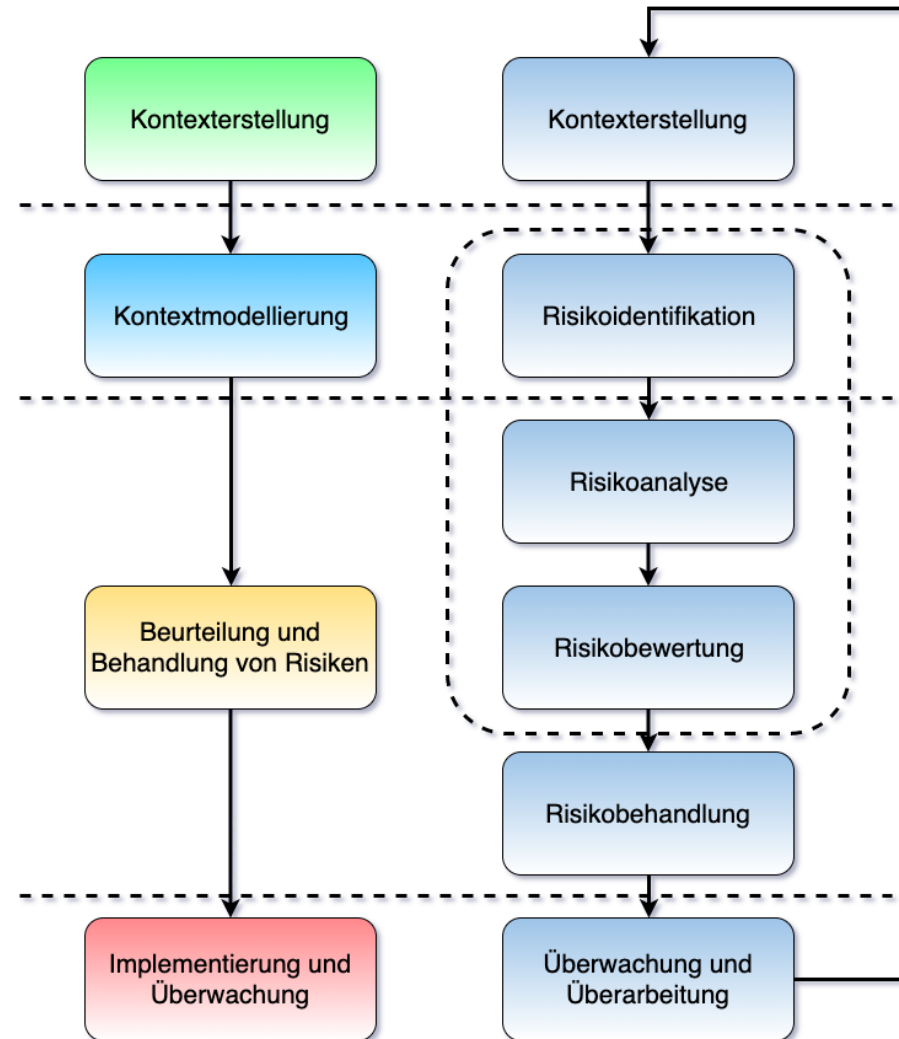


Methodik der Risikoanalyse

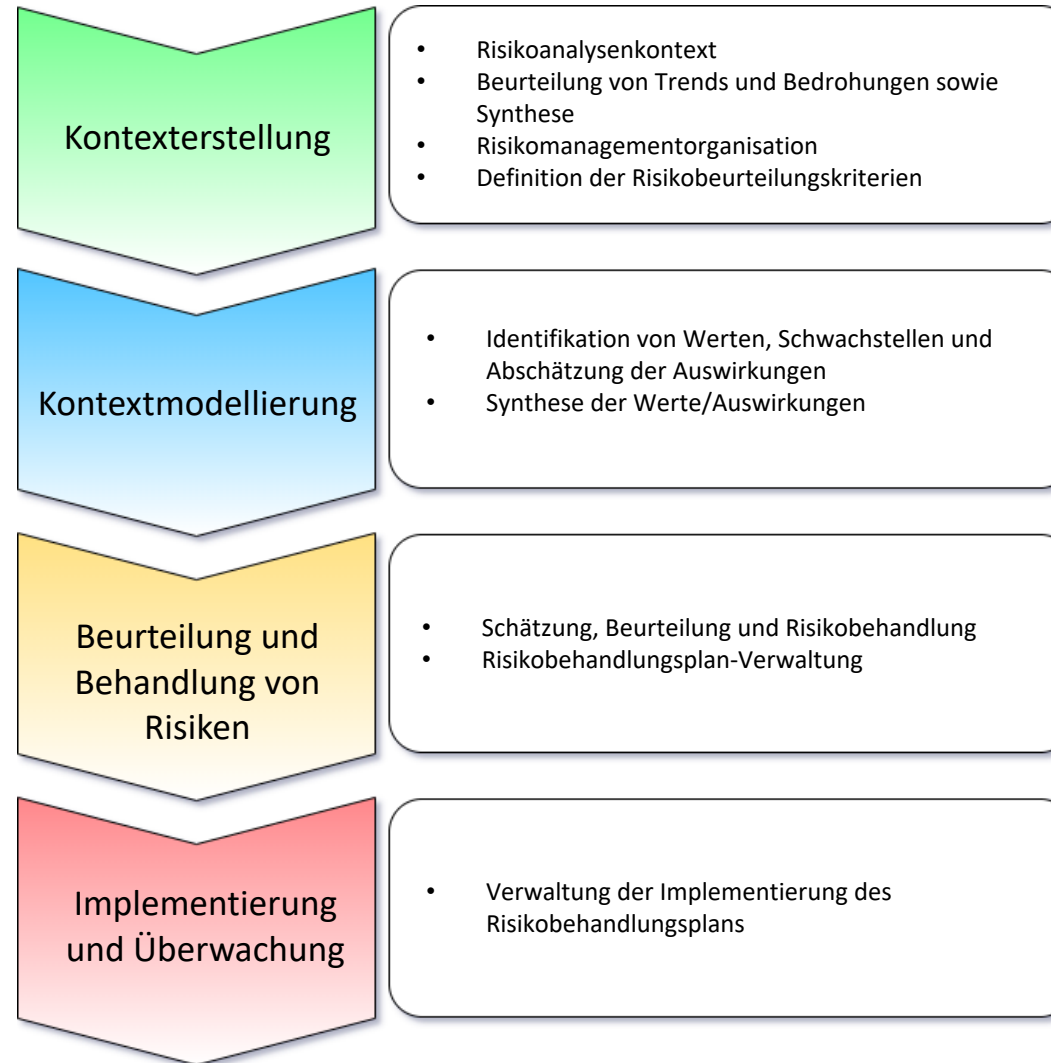
- **Strukturiertes Vorgehen**
 1. ...
 2. ...
 - n. ...
- **Prozessual**
 - Plan
 - Do
 - Check
 - Act
- **Qualitativ: Werte / Auswirkungen**
 - Reputation, Image
 - Betrieb
 - Legal
 - Finanziell
 - Personen / Menschen
 - ...



MONARC Methodik



MONARC Methodik



MONARC Methodik

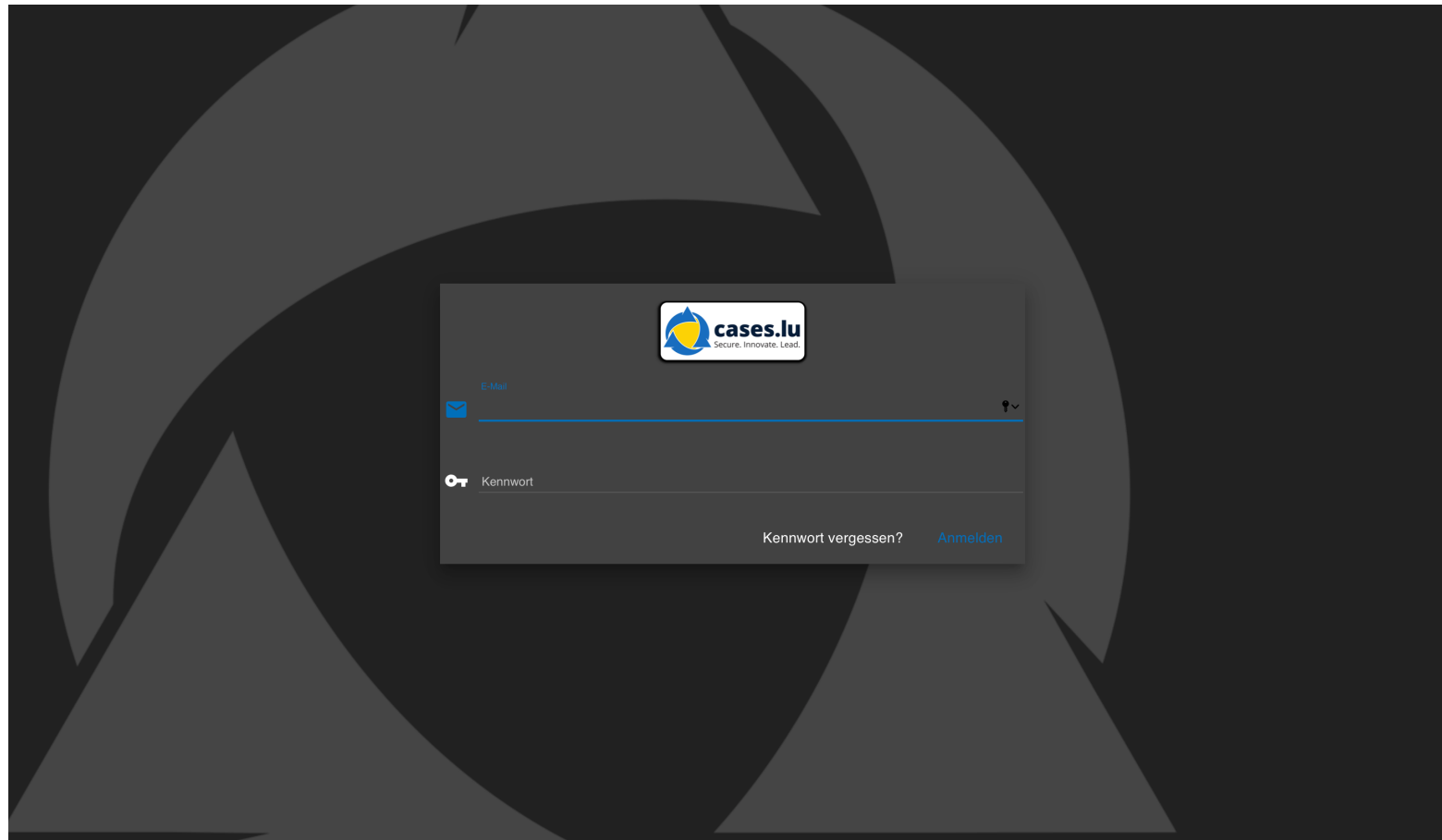
Die folgende Formel wird zur Berechnung des Risikos angewendet:

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

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



Erstellung Risikoanalyse in MONARC




Erstellung Risikoanalyse in MONARC


Eine Risikoanalyse erstellen


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



KonzeptAcht GmbH

MyPrintGER

+ Eine Risikoanalyse erstellen

Copyright 2012-2020 [CASES - Terms](#)

[MONARC v. 2.9.14](#)

Home > MyPrintGER

Risikoanalyse

Alles erweitern /Alle umschließen

Einen Wert suchen...

MyPrintGER

- Abteilung Druck
- Abteilung Grafik
- DSGVO gesetzliche Verpflichtungen

Wertbibliothek

Einen Wert suchen...

Grundlagen

EBIOS

MyPrintGER Risikoanalyse

Informationsrisiken Operative Risiken

143 Informationsrisiken

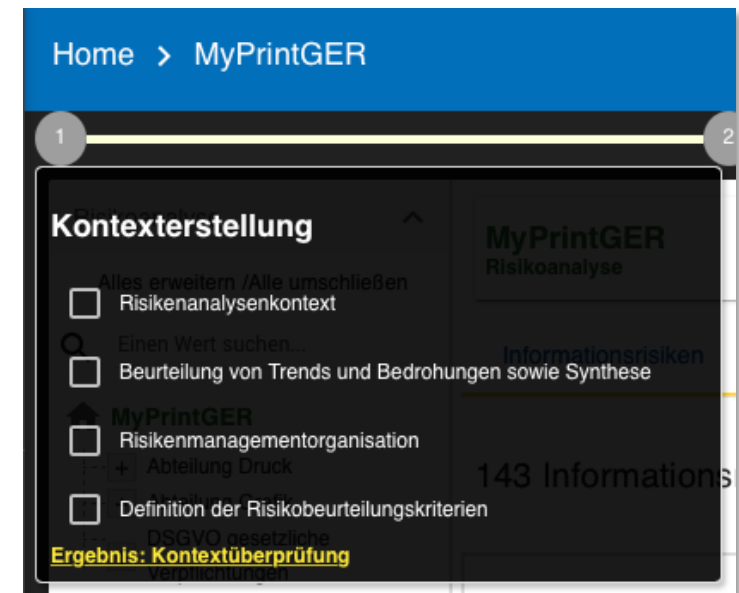
Risikoschwelle (bei max. CIA) ☒ ☐ ☐ ☐ ☐ Schlüsselwörter Art der Behandlung Suchen Sortieren MAX. Risiko Sortierrichtung Absteigend

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

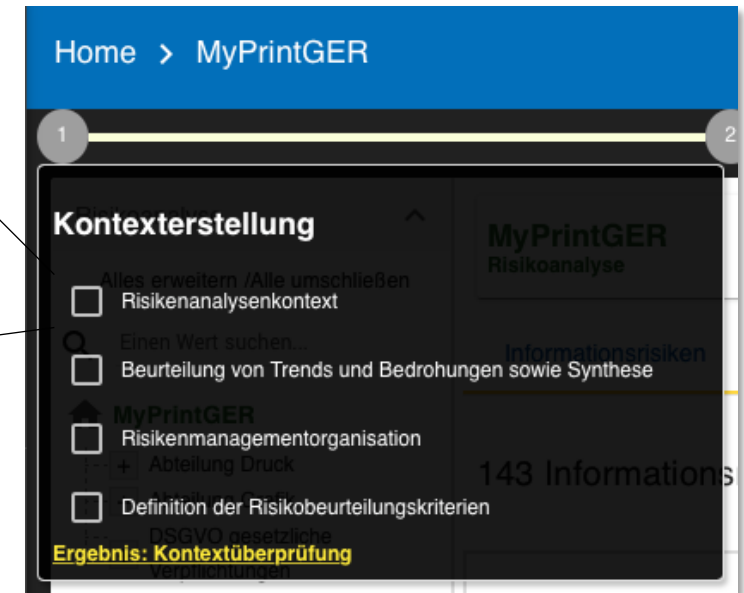
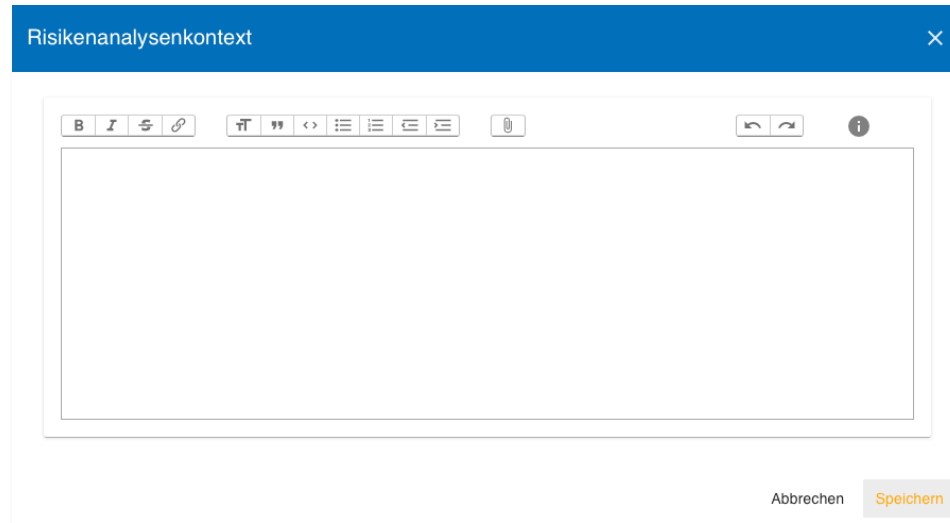


1. Kontexterstellung

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



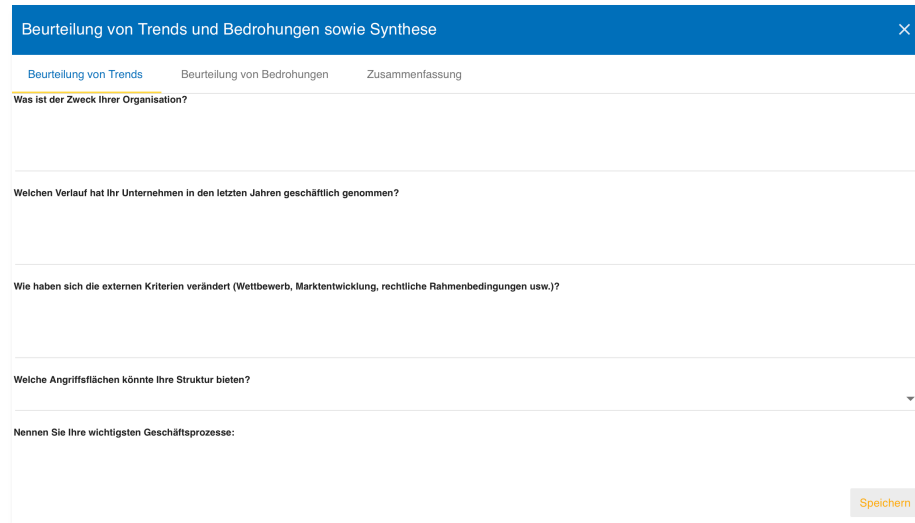
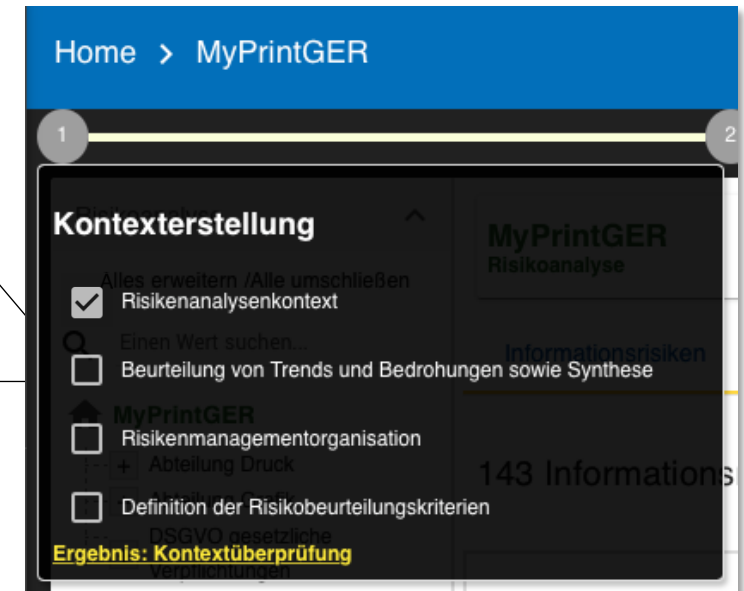
1.1 Risikoanalysekontext



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



1.2.1 Beurteilung von Trends

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



1.2.2 Beurteilung von Bedrohungen

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

☒ Risikensanalysenkontext

Einen Wert suchen...

☐ Beurteilung von Trends und Bedrohungen sowie Synthese

MyPrintGER

☐ Risikemanagementorganisation

+ Abteilung Druck

☐ Definition der Risikobeurteilungskriterien

Ergebnis: Kontextüberprüfung

MyPrintGER Risikoanalyse

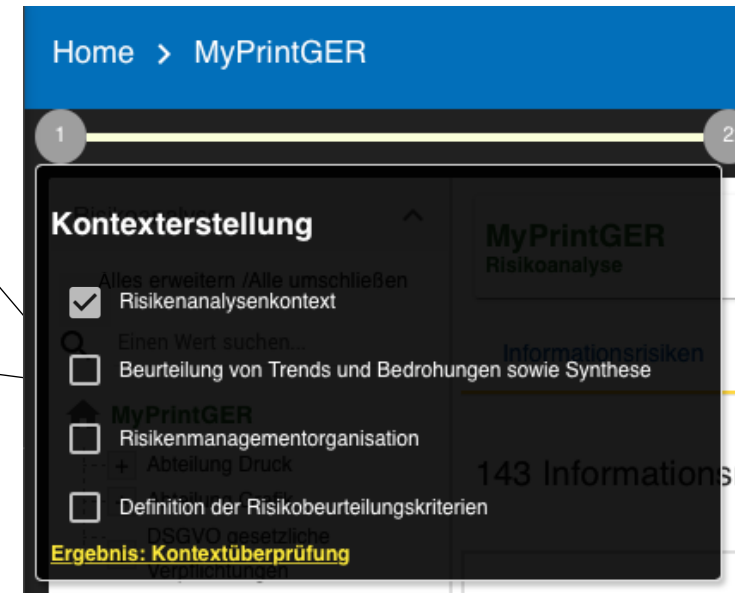
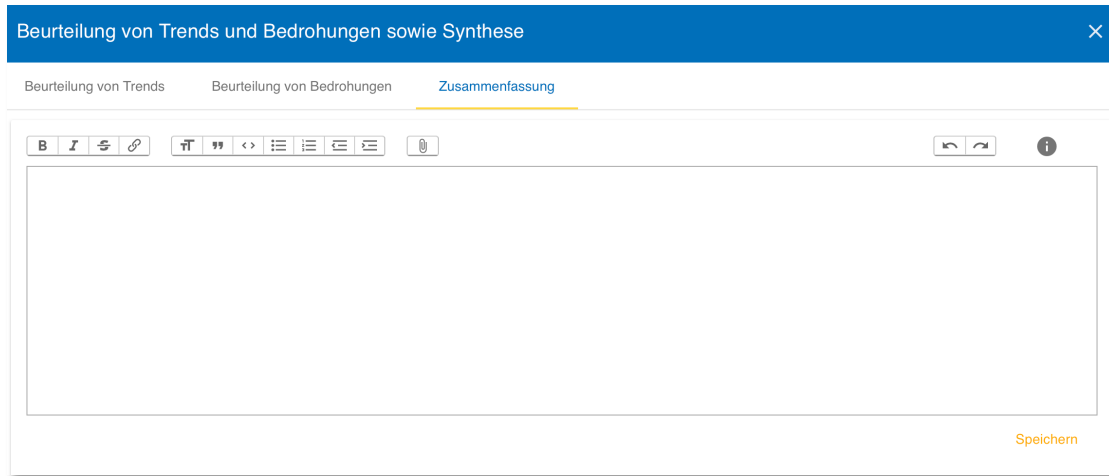
Informationen

143 Informations

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



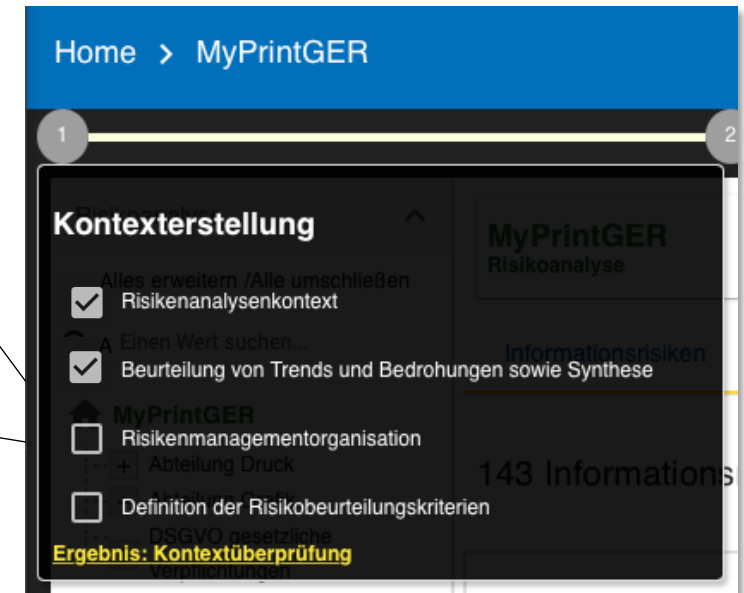
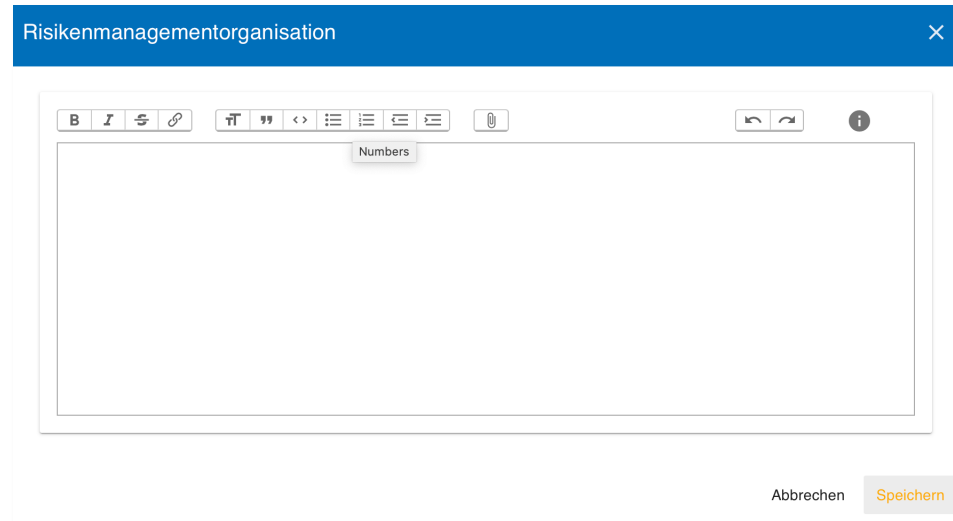
1.2.3 Zusammenfassung



- 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

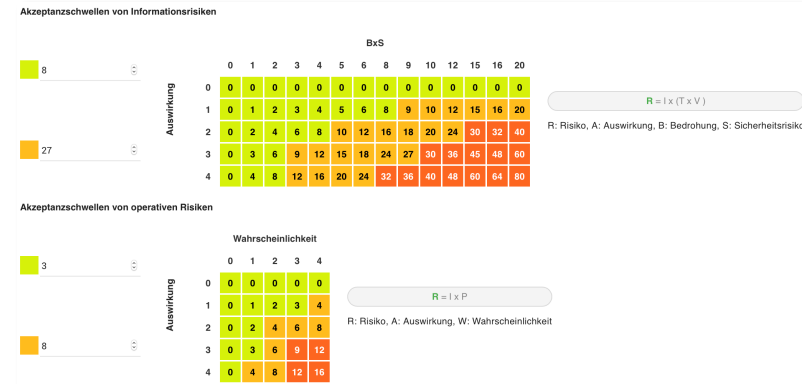


1.4 Definition der Risikobeurteilungskriterien

Auswertungsskala: [0 - 4]

☐ Ausgewählte Auswertungen anzeigen

	Vertraulichkeit	Integrität	Verfügbarkeit	Reif	Einsatzbereit
0	Ohne Auswirkung Das Vertraulichkeitskriterium ist nicht wichtig.	Ohne Auswirkung Das Integritätskriterium ist nicht wichtig.	Ohne Auswirkung Das Verfügbarkeitskriterium ist nicht wichtig.	Keine Folgen	Keine Folgen
1	Schwache Auswirkung, unbedeutend Informationslecks sind negativ für die Interessen der Organisation. Beispiele: - Interne Informationen, die das Unternehmen nicht verlassen sollten, werden preisgegeben. - Memos - Internes Telefonverzeichnis	Schwache Auswirkung, unbedeutend Einfach zu richtende Beschädigung ohne jegliche Folgen. Beispiel: - Interne E-Mail oder Schreiben	Schwache Auswirkung, unbedeutend Sicherheitsteil, das unbedeutend, aber nicht wirklich nachteilig für die Stakeholder ist.	Sporadische Kritik in den Medien	Keinere Vorfälle ohne jegliche Auswirkungen für Kunden
2	Durchschnittliche Auswirkung, annehmbar Informationslecks schädigen die Interessen der Organisation. Beispiele: - 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 Notwendigkeit, die zu Unannehmlichkeiten für die Stakeholder führt. Wiederherstellung ist einfach. Beispiel: - Informative Website	Durchschnittliche Auswirkung, annehmbar Notwendigkeit, die zu Unannehmlichkeiten für die Stakeholder führt. Wiederherstellung ist einfach. Beispiel: - Als untragbar geltende Höchstausgaben werden nicht erreicht.	Isolierte Vorfälle mit überschaubarer Auswirkung auf Kunden
3	Starke Auswirkung, kaum tragbar Informationslecks schädigen die Interessen der Organisation. Beispiel: - Vertrauliche Informationen werden preisgegeben. - Verstoß gegen Datenschutzgesetze. - Verstoß gegen personenbezogene Daten. - Sicherheitsvorfall	Starke Auswirkung, kaum tragbar Beschädigung, die zu erheblichen Unannehmlichkeiten für die Stakeholder führt. Beispiel: - Verstoß gegen Datenschutzgesetze. - Verstoß gegen personenbezogene Daten.	Starke Auswirkung, kaum tragbar Notwendigkeit, die zu erheblichen Unannehmlichkeiten für die Stakeholder führt. Beispiel: - Als untragbar geltende Höchstausgaben werden nicht erreicht.	Starke Abwertung der Firma oder des Reifegrad der Belegschaft. Schlechte und wiederholte Kritik in den Medien	Störung einer gesamten Abteilung
4	Äußerst starke Auswirkung, untragbar Informationslecks ruinieren die Interessen der Organisation. Beispiel: - Geheime oder hochvertrauliche Informationen werden preisgegeben. - Geheimnisse nach Gesetz (BSI, NATO, National ...)	Äußerst starke Auswirkung, untragbar Beschädigung, die nicht wiederherstellbar ist oder zur permanenter Downtime führt. Beispiel: - Geheime oder hochvertrauliche Informationen werden preisgegeben. - Geheimnisse nach Gesetz (BSI, NATO, National ...)	Äußerst starke Auswirkung, untragbar Beschädigung, die eine dauerhafte Notwendigkeit zur Wiederherstellung erfordert oder sogar eingetriggt ist. Beispiel: - Substanzielle Höchstausgaben werden nicht erreicht.	Tot einer Person Definitive Abwertung der Firma oder des Reifegrad der Belegschaft. Internationale Berichterstattung	Völliger Stillstand aller Dienste

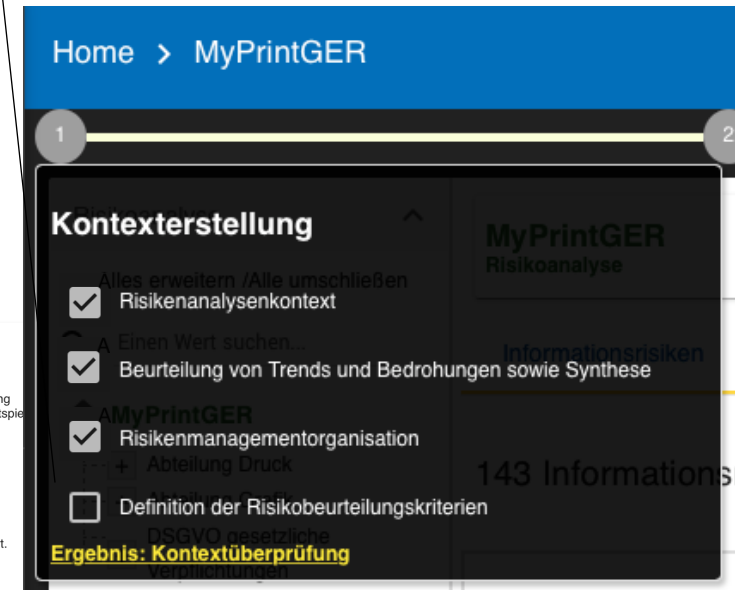


Wahrscheinlichkeitsskala: [0 - 4]

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

Sicherheitsrisikoskala: [0 - 5]

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



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



1.5 Ergebnis: Kontextüberprüfung



Ergebnis

Status: Endgültig

Vorlage: Kontextüberprüfung

Version: 1.0

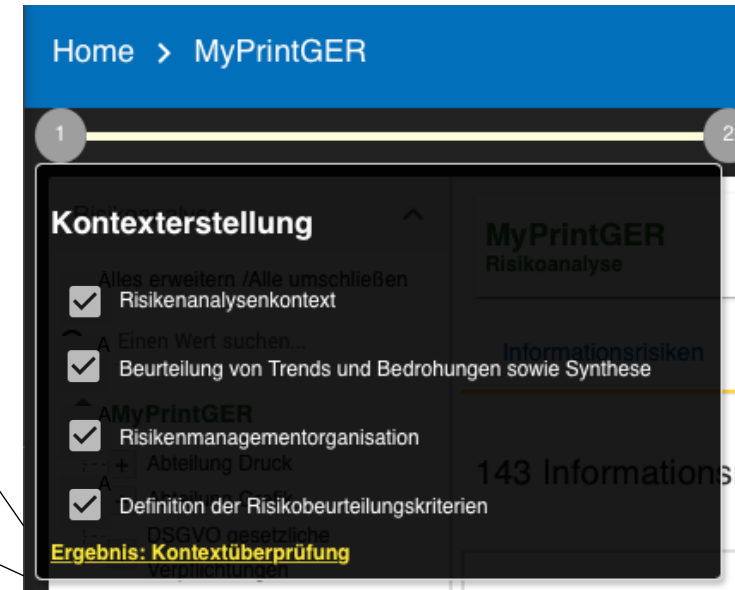
Klassifizierung: vertraulich

Dokumentname: Kontext des Risikomanagements

Kundenmanager:

Sicherheitsberater:

Abbrechen Speichern



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

Ergebnis: Kontextüberprüfung

MyPrintGER Risikoanalyse

Informationen

143 Informations

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

1. Kontexterstellung - Übung

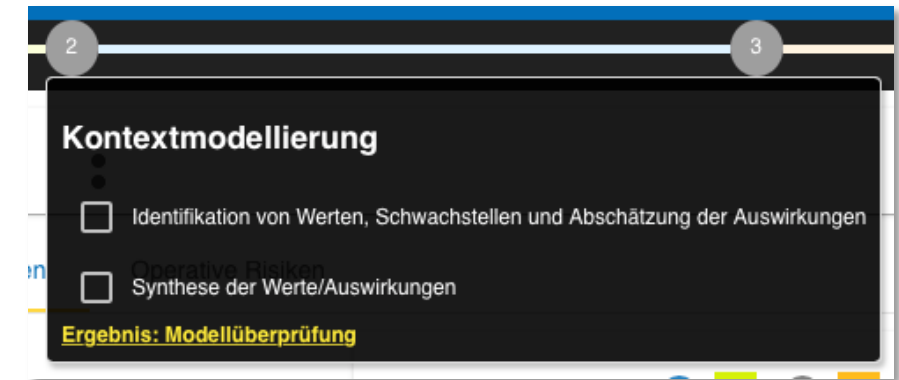
Übung: Durchführen der Kontexterstellung (30 Minuten)

- **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

Home > MyPrintGER

Risikoanalyse

Informationen Risiken

143 Informationsrisiken

Risikowerte (bei max. CIN)

Wert	Auswirkung			Bedrohung	Prob.	Bezeichnung	Sicherheitsrisiko	Qualif.	Aktuelles Risiko			Behandlung	Restrisiko
	C	I	A						C	I	A		
Benutzer-Arbeitsstationen	1	3	2	Fehlbedienung	3	Das Genehmigungsmanagement weist Mängel auf.	Keine Zugriffskontrolle	5	15	45	90	Nicht behandelt	45
Servermanagement	1	3	2	Funktions- oder Ausfällen von Benutzern	3	Kein Service-Level-Management	Keine präventive Wartung, Eingreifen, wenn ein Ausfall auftritt.	5	45	30	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	Funktions- oder Ausfällen von Benutzern	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	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	30	Nicht behandelt	30
Gebäude	1	2	3	Pflichtmissbrauch	2	Keine Beaufichtigung Dritter bei ihren Einsätzen (Lieferanten, Reinigungsfirma usw.)	Externe werden nicht begleitet.	5	10	20	30	Nicht behandelt	30
Servermanagement	1	3	2	Verletzung von Aktionen	3	Fehlende Aufbewahrung von Protokolldaten, die Aufschluss über die Aktivitäten geben	Keine Zentralisierung von Logdateien.	3	27	27	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	24	Nicht behandelt	24

2

3

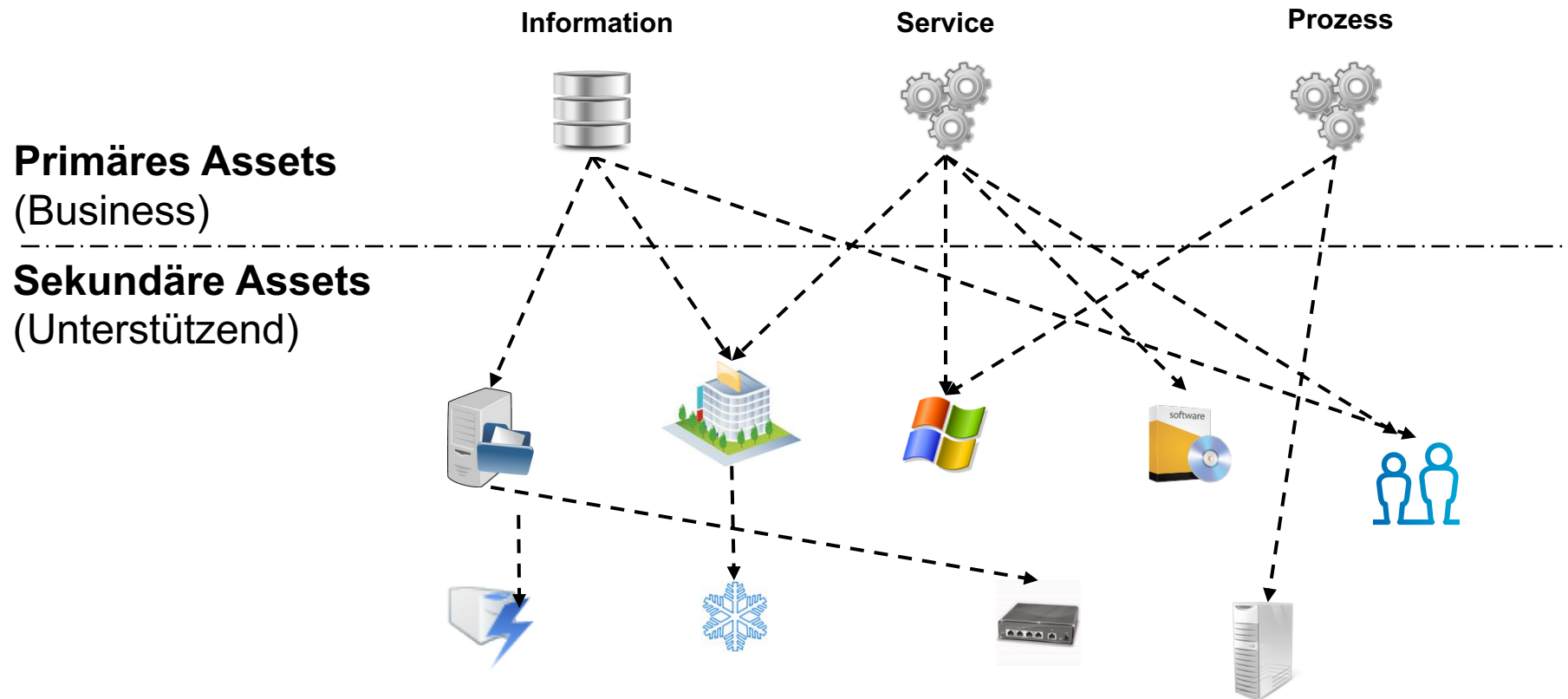
Kontextmodellierung

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

Ergebnis: Modellüberprüfung



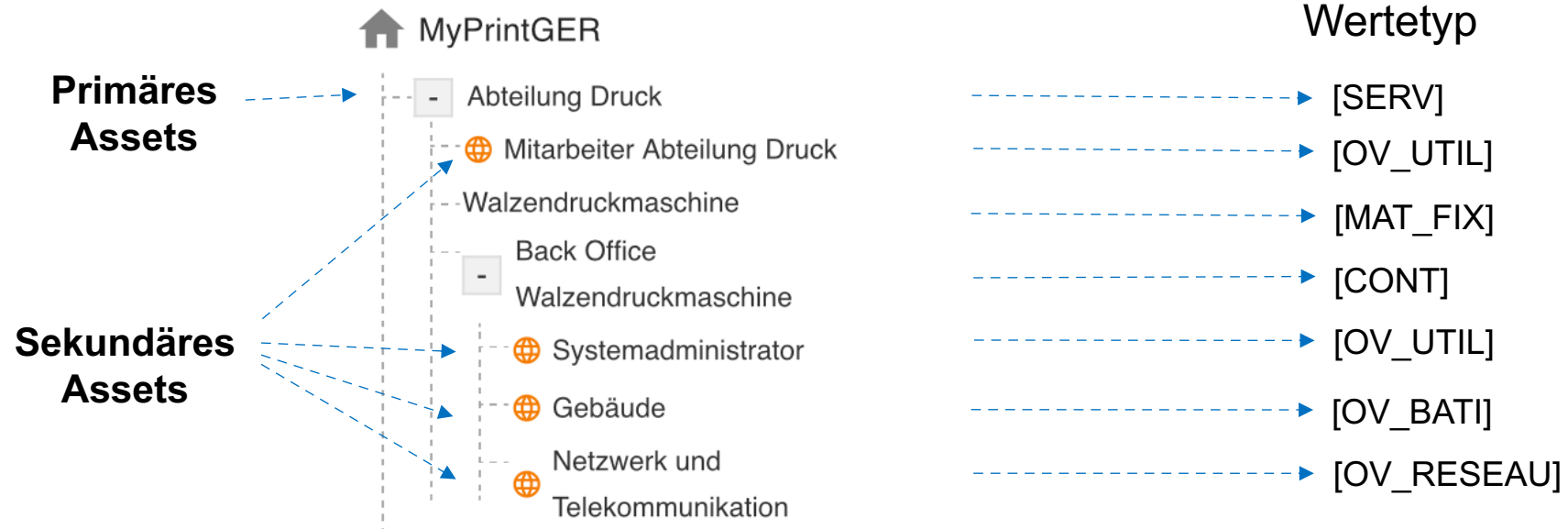
2.1 Identifikation von Werten, Schwachstellen und Abschätzung der Auswirkungen



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

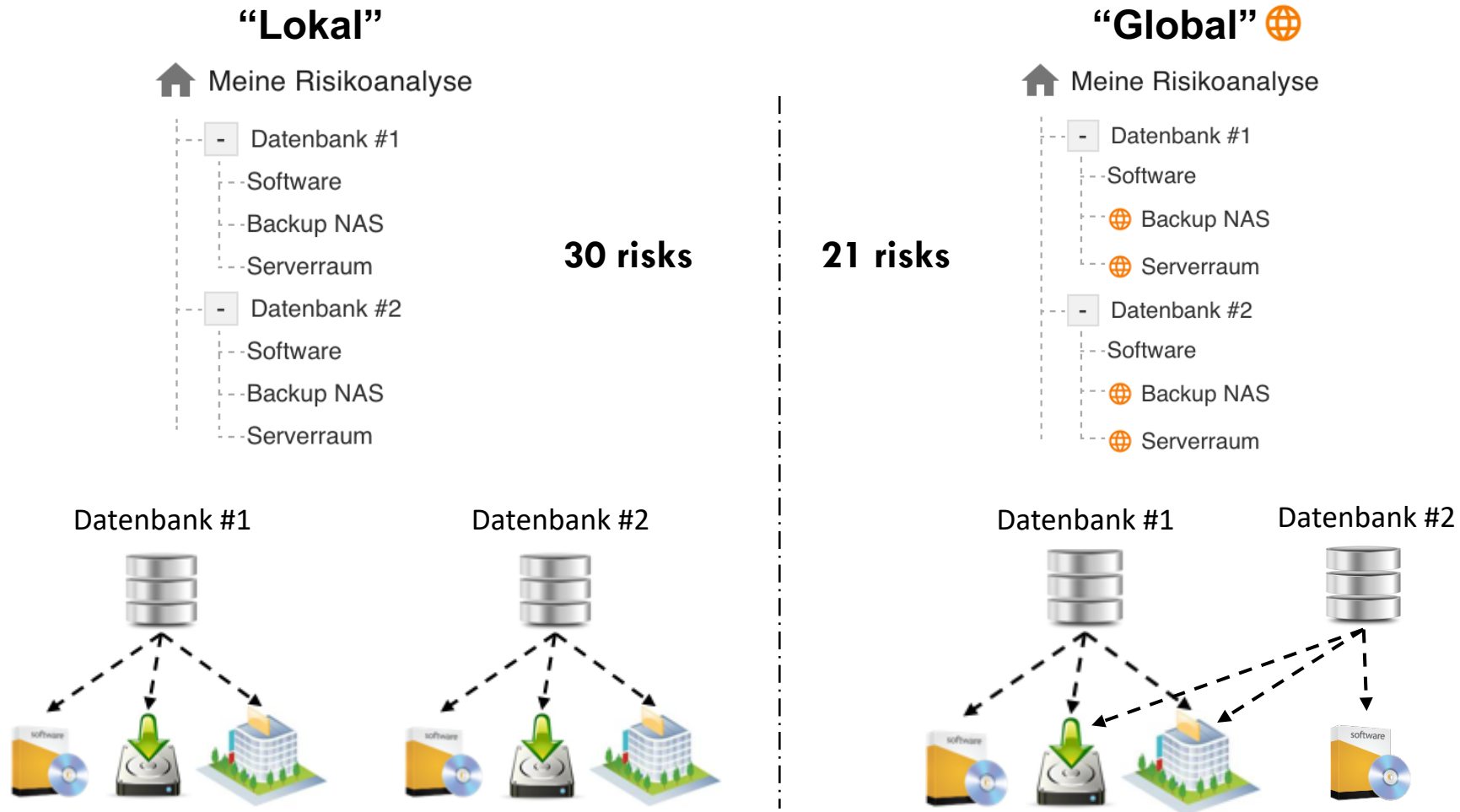


OV_BATI

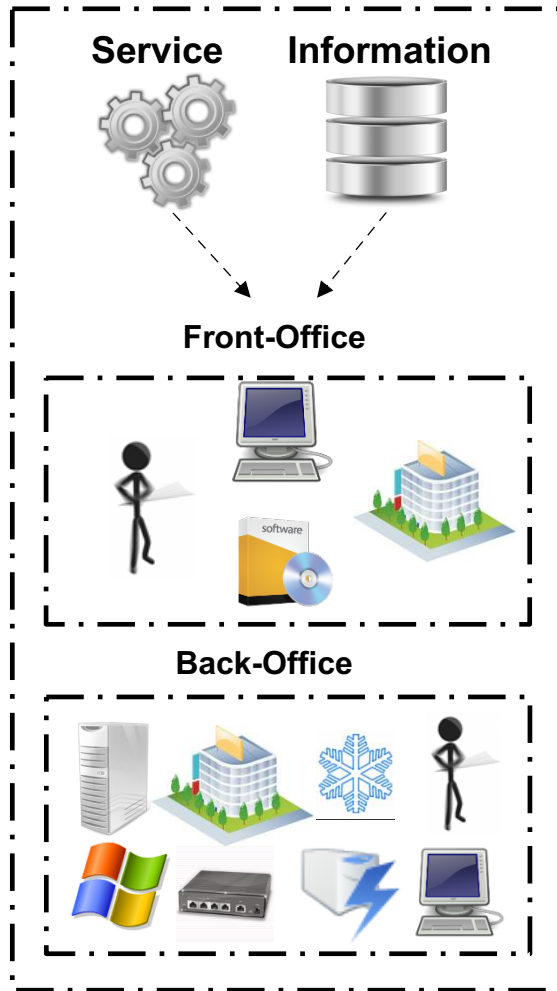
Bedrohung	Sicherheitsrisiko
Entwenden oder Zerstören von Speichermedien, Dokumenten oder Datenträger	Mängel bei der physischen Zugangskontrolle
Entwenden oder Zerstören von Speichermedien, Dokumenten oder Datenträger	Der Least-Privileg-Grundsatz wird nicht angewendet
Entwenden oder Zerstören von Speichermedien, 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.



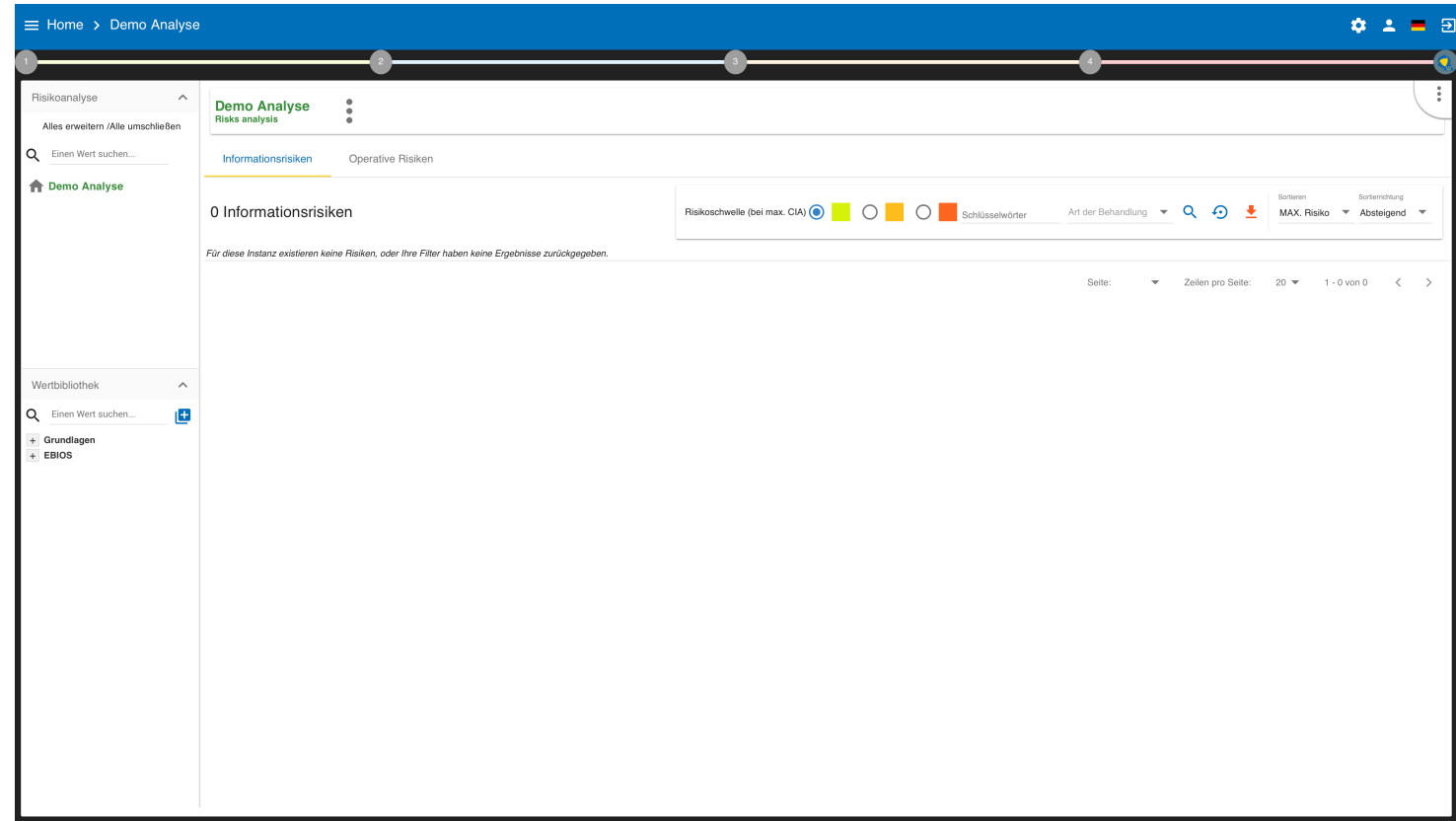
2.1 „Lokale“ und „Globale“ Assets



2.1 CASES Modellierung



2.1 Identifikation von Werten, Schwachstellen und Abschätzung der Auswirkungen



- Hauptansicht von MONARC
- Erstellung eines Risikomodells
- Referenz zu ISO 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

2 3

Kontextmodellierung

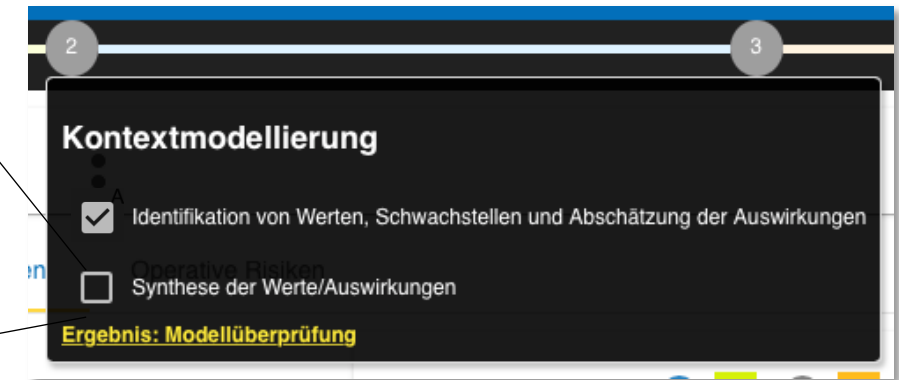
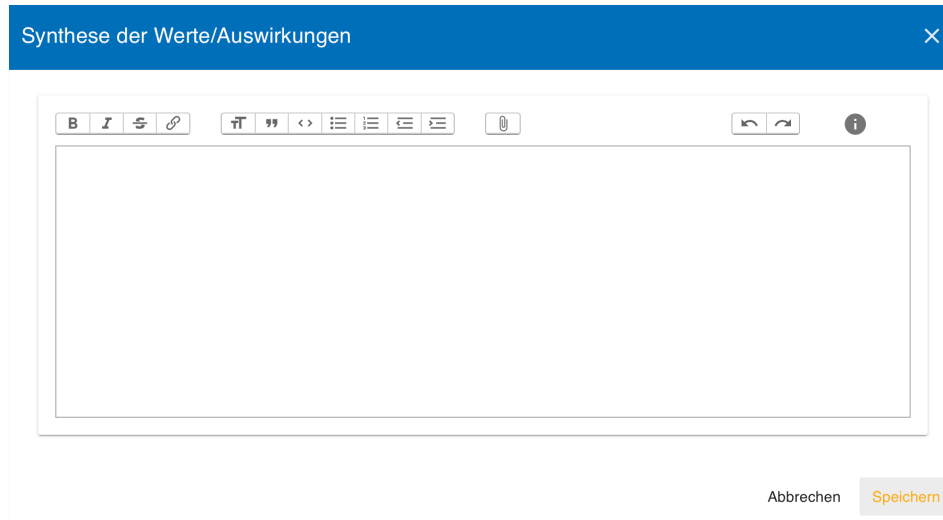
- ☐ Identifikation von Werten, Schwachstellen und Abschätzung der Auswirkungen
- ☐ Operative Risiken
- ☐ Synthese der Werte/Auswirkungen

Ergebnis: Modellüberprüfung

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

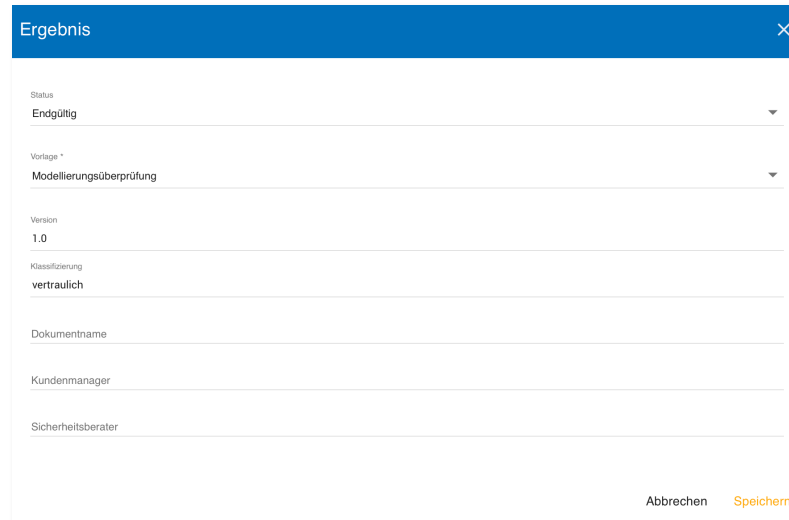
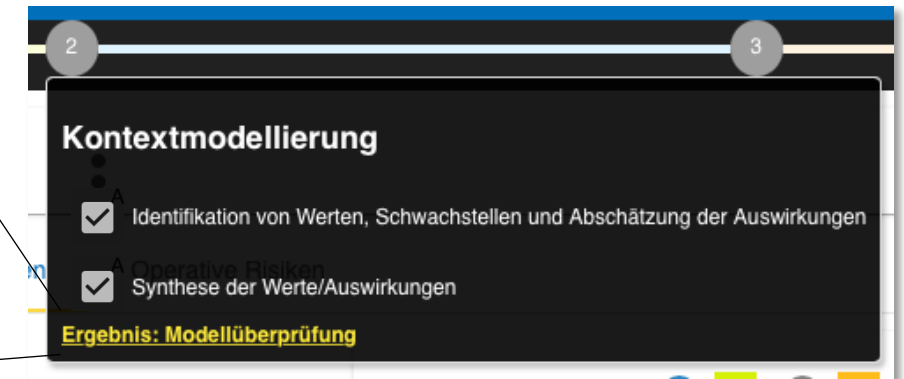


2.2 Synthese der Werte/Auswirkungen



- 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

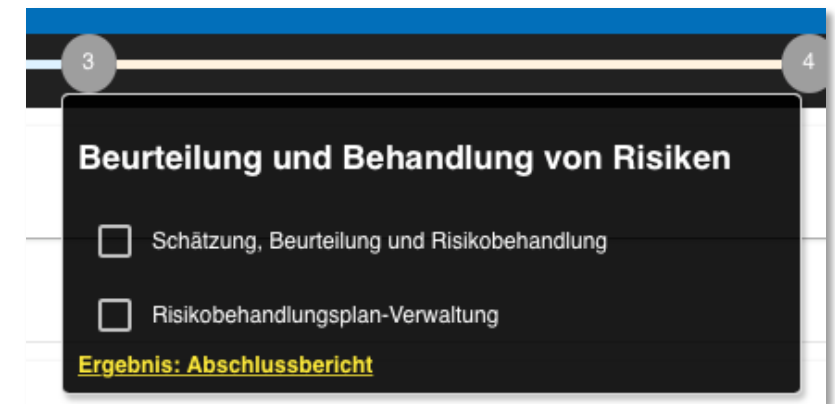
Übung: Durchführen der Kontextmodellierung (30 Minuten)

- **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

Home > MyPrintGER

Risikoanalyse

Alles erweitern (Alle unsichtbar)

Einen Wert suchen...

MyPrintGER

4 Abteilung Druck

4 Abteilung Grafik

4 DSGVO gesetzliche Verpflichtungen

Wertbibliothek

Einen Wert suchen...

Grundlagen

Primäre Werte

Abteilung

Abteilung Druck

Abteilung Grafik

Daten

Geschäftsdatenbank

Modellstruktur

Datensicherung

Datensicherungsmanagement

Gebäude & Geschäftsräume

Physische Güter

Software

Betriebsmittel

Personal

Organisation

Server

Netzwerk

DSGVO

BIBOS

MyPrintGER

Risikoanalyse

Informationsrisiken

Operative Risiken

143 Informationsrisiken

Risikowerte (bei max. CIA)

Schlüsselwörter

Art der Behandlung

Sortieren

MAX, Risiko

Absteigend

Wert	Auswirkung			Bedrohung	Prob.	Bezeichnung	Sicherheitsrisiko	Aktuelles Risiko			Behandlung	Restrisiko	
	C	I	A					C	I	A			
Benutzer-Arbeitsstationen	1	3	2	Rechtsanmaßung	3	Das Genehmigungsmanagement weist Mängel auf.	Keine Zugriffskontrolle	5	15	45	60	Nicht behandelt	45
Servermanagement	1	3	2	Funktions- oder Ausfällen von Benutzern	3	Kein Service-Level-Management	Keine präventive Wartung. Eingreifen, wenn ein Ausfall auftritt.	5	45	30	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	Funktions- oder Ausfällen von Benutzern	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	20	Nicht behandelt	30
Gebäude	1	2	3	Entwerfen 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	20	30	Nicht behandelt	30
Gebäude	1	2	3	Rechtsmissbrauch	2	Keine Beaufsichtigung Dritter bei ihren Einsätzen (Lieferanten, Reinigungskraft etc.)	Externe werden nicht begleitet.	5	10	20	30	Nicht behandelt	30
Servermanagement	1	3	2	Verletzung 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	27	27	Nicht behandelt	27
Gebäude	1	2	3	Entwerfen oder Zerstören von Speichermedien, Dokumenten oder Datenträger	2	Das Genehmigungsmanagement weist Mängel auf.	Zugang mit Ausweis. Kein Berechtigungssystem	4	8	24	24	Nicht behandelt	24

3

4

Beurteilung und Behandlung von Risiken

☐ Schätzung, Beurteilung und Risikobehandlung

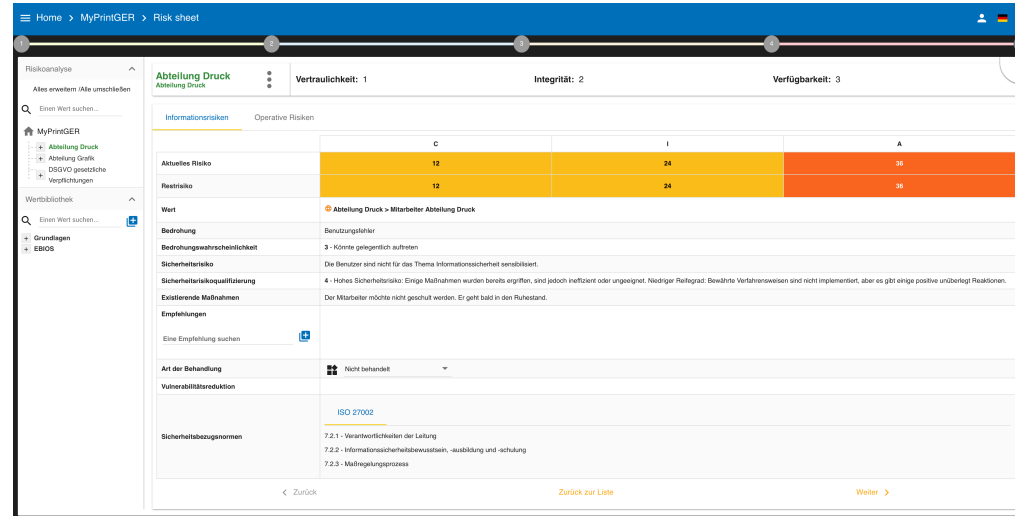
☐ Risikobehandlungsplan-Verwaltung

Ergebnis: Abschlussbericht

- Hauptansicht von MONARC
- Alle Risiken bewerten



3.1 Schätzung, Beurteilung und Risikobehandlung



		C	I	A
Aktuelles Risiko		12	24	36
Restrisiko		12	24	36

Wert
 Bedrohung: Benutzungsfehler
 Bedrohungswahrscheinlichkeit: 3 - Könnte gelegentlich auftreten
 Sicherheitsrisiko: Die Benutzer sind nicht für das Thema Informationssicherheit sensibilisiert.
 Sicherheitsrisikopräqualifizierung: 4 - Hohes Sicherheitsrisiko: Einige Maßnahmen wurden bereits ergriffen, sind jedoch ineffizient oder ungeeignet. Niedriger Restgrad: Bewährte Verfahrenswesen sind nicht implementiert, aber es gibt einige positive unberogte Reaktionen.
 Existierende Maßnahmen: Der Mitarbeiter möchte nicht geschult werden. Er geht bald in den Ruhestand.
 Empfehlungen:
 Eine Empfehlung suchen
 Art der Behandlung: Nicht behandelt
 Vulnerabilitätsreduktion: ISO 27002
 Sicherheitsbezugsnormen: 7.2.1 - Verantwortlichkeit der Leitung, 7.2.2 - Informationssicherheitsbewusstheit, -ausbildung und -schulung, 7.2.3 - Mafregelungsprozess

3

4

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

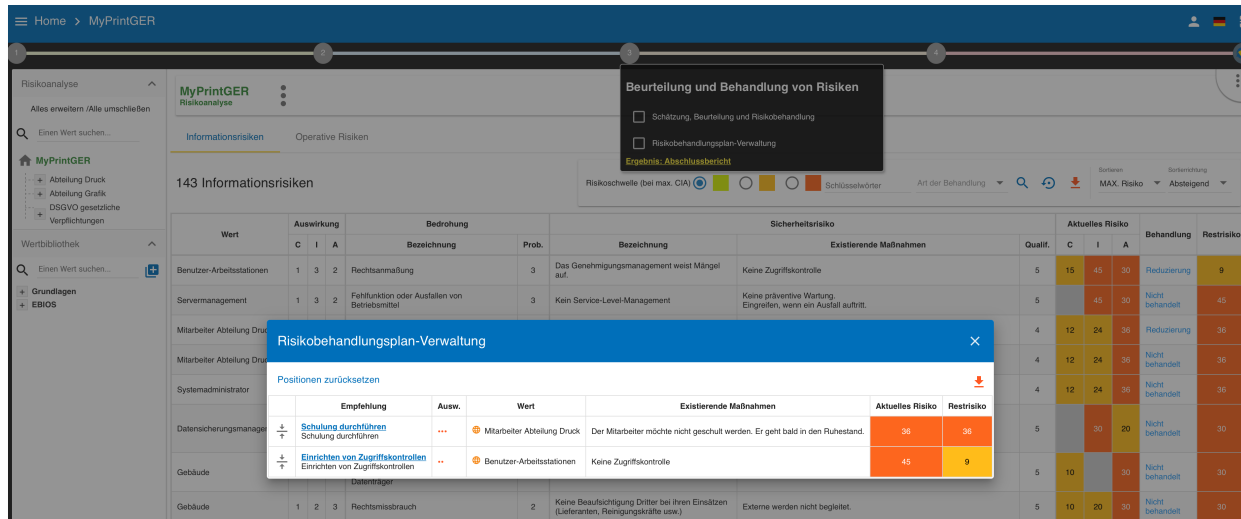
- ☐ Schätzung, Beurteilung und Risikobehandlung
- ☐ Risikobehandlungsplan-Verwaltung

Ergebnis: Abschlussbericht

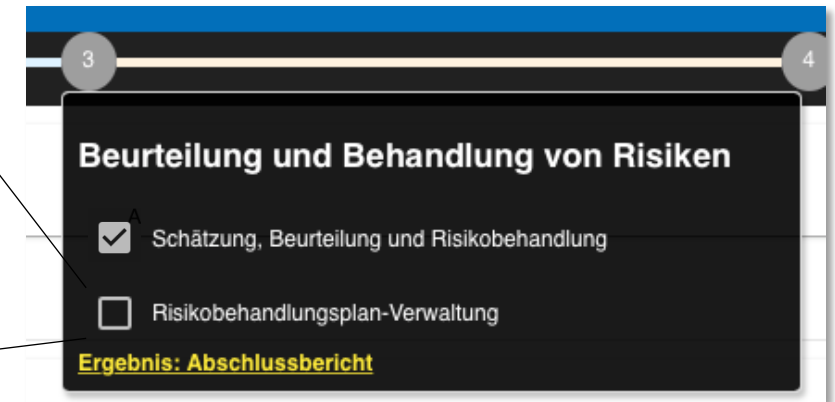
- Anlegen einer Maßnahme



3.2 Risikobehandlungsplan-Verwaltung



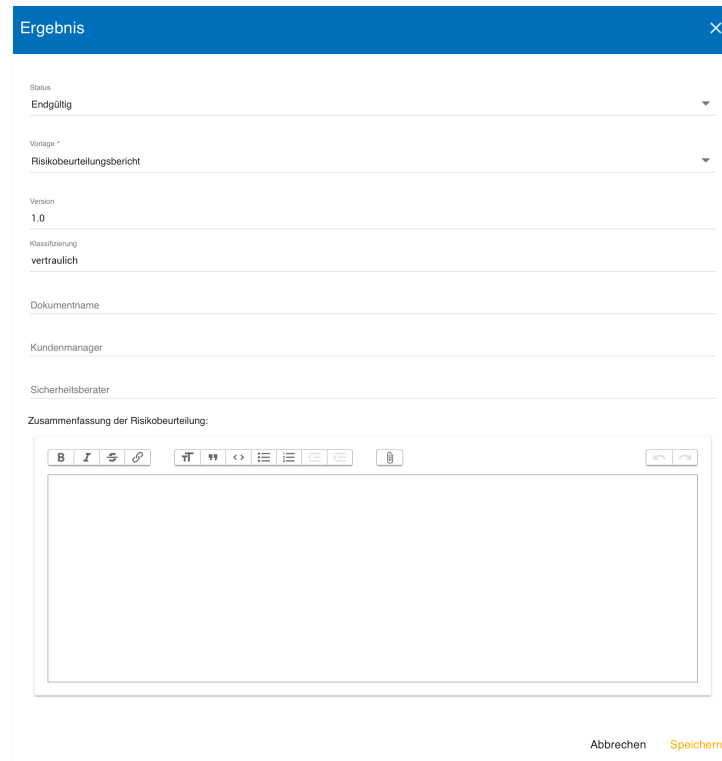
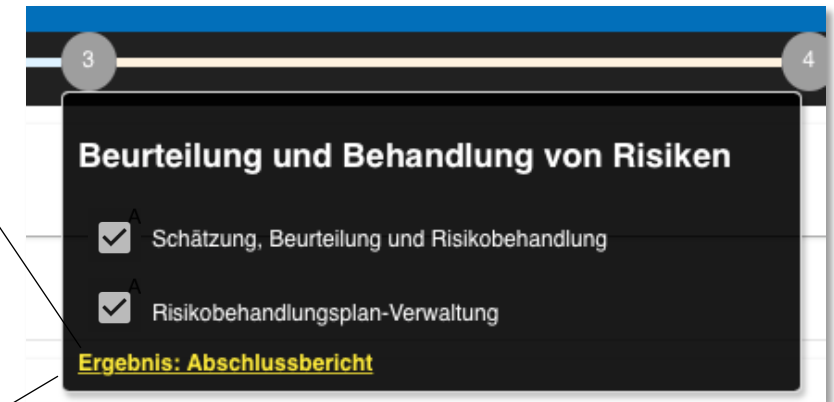
The screenshot shows the 'MyPrintGER Risikoanalyse' interface. A modal titled 'Beurteilung und Behandlung von Risiken' is open, displaying two options: 'Schätzung, Beurteilung und Risikobehandlung' (checked) and 'Risikobehandlungsplan-Verwaltung' (unchecked). Below the modal, a table lists 143 information risks. The table has columns for 'Wert', 'Auswirkung', 'Bedrohung', 'Bezeichnung', 'Prob.', 'Bezeichnung', 'Existierende Maßnahmen', 'Qualif.', 'C', 'I', 'A', 'Behandlung', and 'Restrisiko'. A 'Risikobehandlungsplan-Verwaltung' modal is also open, showing a table with columns for 'Empfehlung', 'Ausw.', 'Wert', 'Existierende Maßnahmen', 'Aktuelles Risiko', and 'Restrisiko'.



The diagram shows a flow from step 3 to step 4. Step 3 is titled 'Beurteilung und Behandlung von Risiken' and includes two options: 'Schätzung, Beurteilung und Risikobehandlung' (checked) and 'Risikobehandlungsplan-Verwaltung' (unchecked). Step 4 is titled 'Ergebnis: Abschlussbericht'.

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

3.3 Ergebnis: Abschlussbericht

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

3. Beurteilung und Behandlung von Risiken - Übung

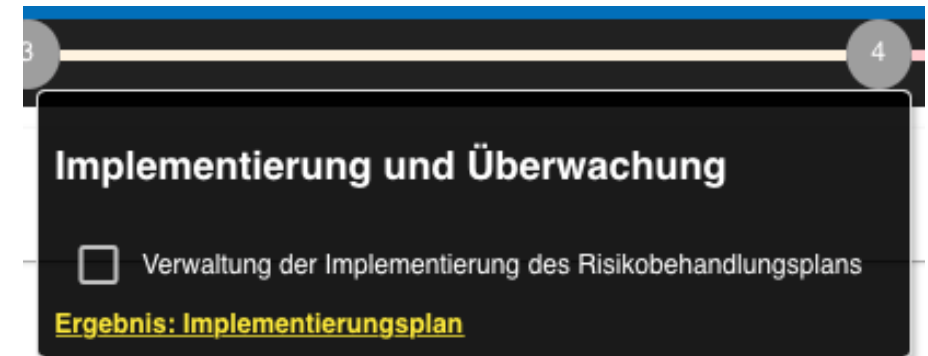
Übung: Durchführen der Beurteilung und Behandlung von Risiken (30 Minuten)

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



4. Implementierung und Überwachung

- Verwaltung der Implementierung des Risikobehandlungsplans



4.1 Verwaltung der Implementierung des Risikobehandlungsplans

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	🔗

3 4

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		0	

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

Einrichten von Zugriffskontrollen - Einrichten von Zugriffskontrollen

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

3
4

Implementierung und Überwachung

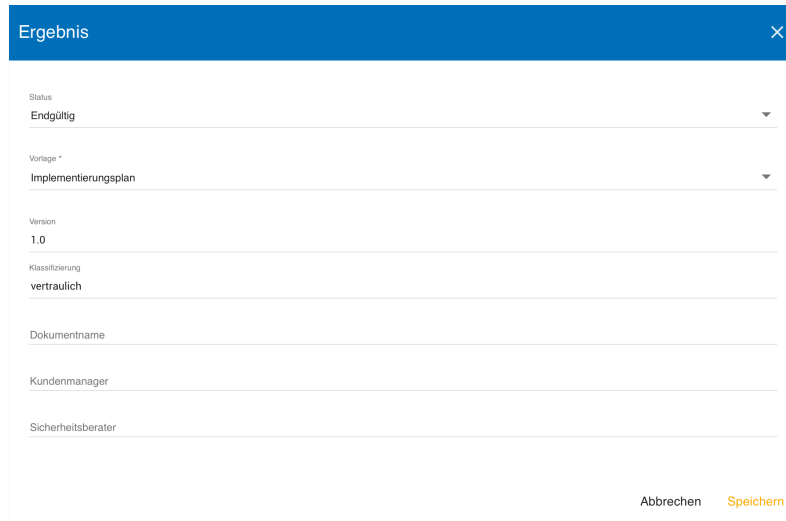
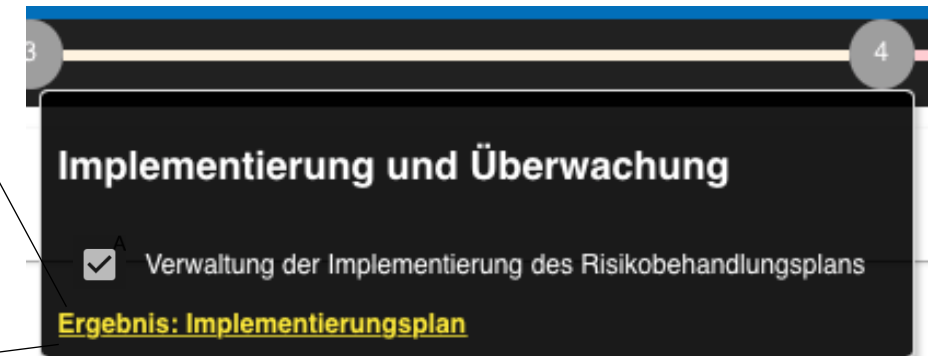
☐ Verwaltung der Implementierung des Risikobehandlungsplans

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



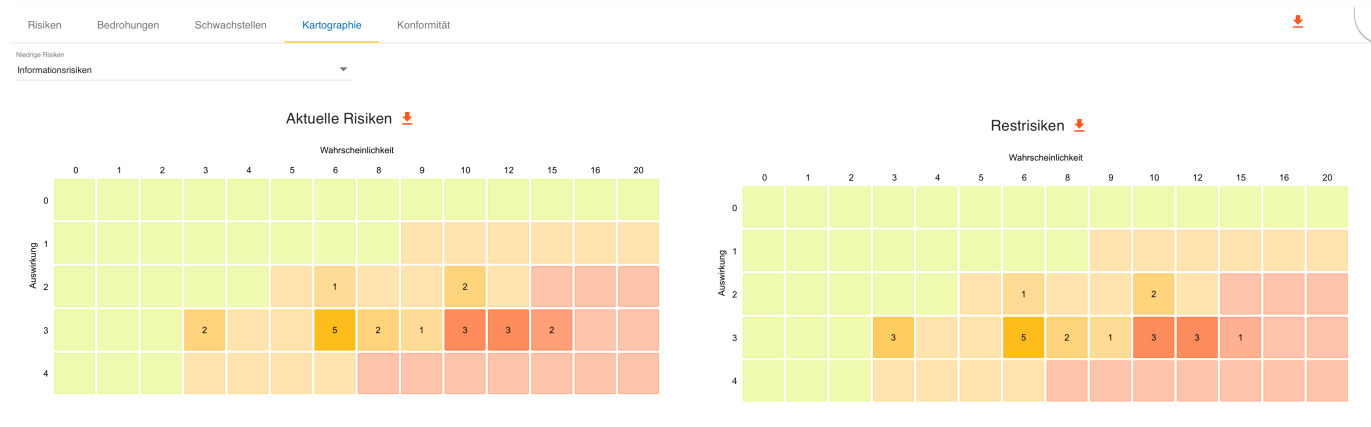
4. Implementierung und Überwachung - Übung

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...					
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 - 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

Suchen...

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

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

- Abbildung von EU-DSGVO Nachweisen

MONARC - Anwendbarkeitserklärung

Home > MyPrintGER > Statement of applicability

Anwendbarkeitserklärung

ISO 27002

Suchen...

Kategorie	Code	Maßnahme	Einbeziehung / Ausschluss	Bemerkungen/Begründung	Nachweise	Aktionen	Grad der Konformität
Informationssicherheitspolitik	5.1.1	Informationssicherheitsrichtlinien	<div>WE RA VV</div> <div>GA BV ERB</div>				
Informationssicherheitspolitik	5.1.2	Überprüfung der Informationssicherheitsrichtlinien	<div>WE RA VV</div> <div>GA BV ERB</div>				
Organisation der Informationssicherheit	6.1.1	Informationssicherheitsrollen und -verantwortlichkeiten	<div>WE RA VV</div> <div>GA BV ERB</div>				
Organisation der Informationssicherheit	6.1.2	Aufgabentrennung	<div>WE RA VV</div> <div>GA BV 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

- Usermanagement und Berechtigungen
- Downloadmöglichkeiten unter 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
 - 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">• 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	<ul style="list-style-type: none">• Interne Audits• Zertifizierungsaudits• §8a (3) BSIG – KRITIS• BSI TR-03109-6• IT-Revisionsprüfungen• Trusted ERP	<ul style="list-style-type: none">• Cyber Security Awareness• K8 macht Schule• Phishing-Kampagnen• Risikomanagement mit MONARC• Inhouse Schulungen	<ul style="list-style-type: none">• Penetrationstests• Sicherheits-Analyse• Prüfung von Sicherheitskonzepten

Ihr Kontakt



 <https://www.konzeptacht.de>

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

 [Thomas Kochanek](https://www.x.com/ThomasKochanek)

 [Thomas Kochanek](https://www.linkedin.com/in/ThomasKochanek)

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>

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

 [Marc Sparwel](https://www.linkedin.com/in/MarcSparwel)