

Risikoorientierte SiKu

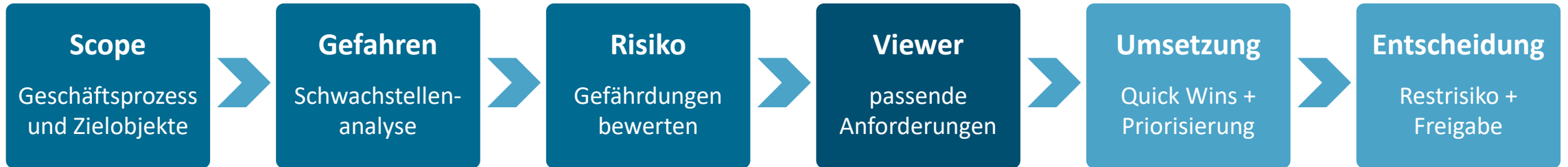
Sicherheitstechnische Kurzbetrachtung

Vom Geschäftsprozess zur Managemententscheidung

Kurzfassung · risikoorientiert · Viewer-gestützt ·
entscheidungsorientiert

Die Sicherheitstechnische Kurzbetrachtung auf einen Blick

Wenige Kernelemente verbinden Risikoanalyse, Viewer-Anforderungen und Managemententscheidung.



Leitfrage

Welche wesentlichen Risiken gefährden den Geschäftsprozess – und welche Anforderungen reduzieren diese Risiken wirksam?

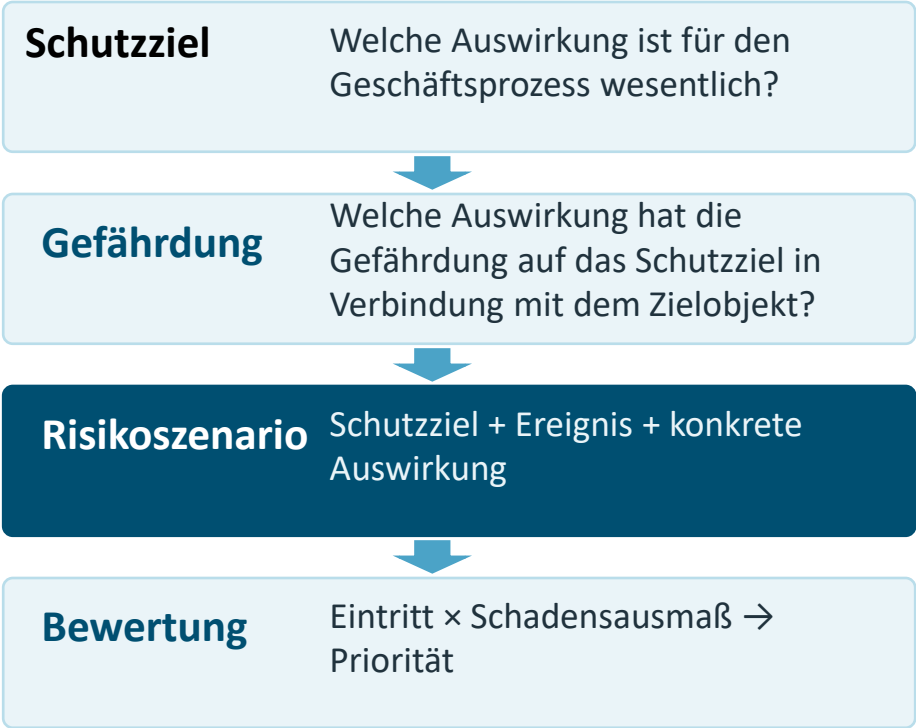
Hilfsmittel

Kurze Prozessbeschreibung · Betriebsdokumentation - logischer/technischer Netzplan · Risikomatrix · Stand-der-Technik-Viewer · kompaktes Risikoregister

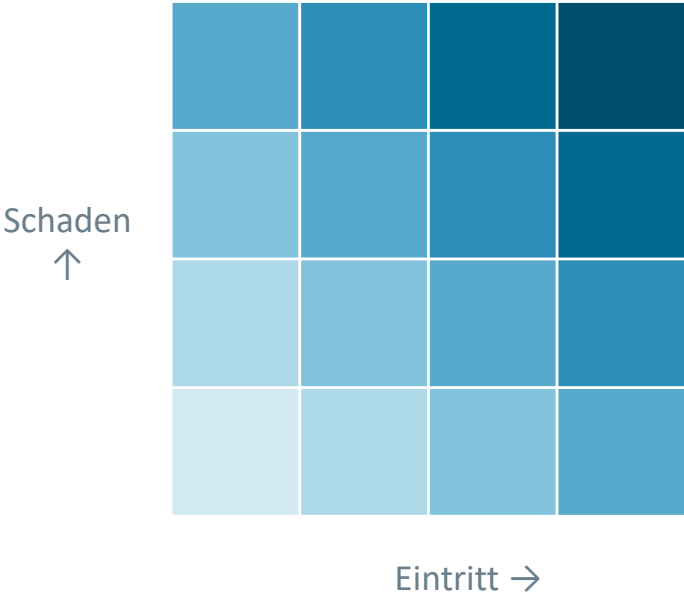
Abstraktes Beispiel: „Zentrale Verbindung fällt aus → Geschäftsprozess ist eingeschränkt → passende Sicherheitsanforderungen und Maßnahmen werden priorisiert.“

Risiko zuerst: vom Schadensszenario zur Bewertung

Die Kurzbetrachtung fokussiert auf die wenigen Risiken, die für den Geschäftsprozess tatsächlich relevant sind.



Einfache Risikomatrix



Abstraktes Beispiel

Gefährdung: Ausfall einer zentralen Verbindung

Ereignis: Kernfunktion nicht erreichbar

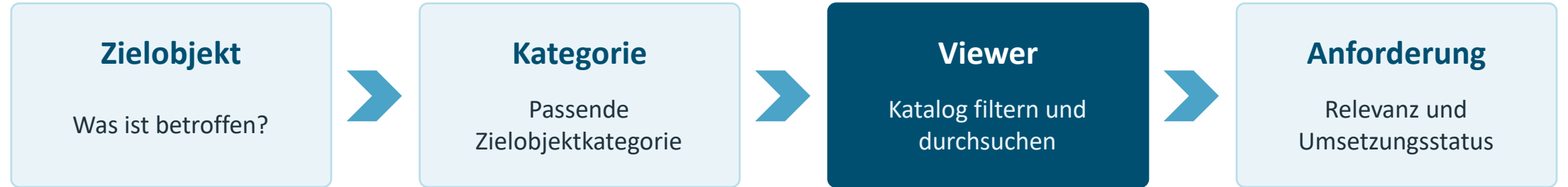
Schaden: Prozessunterbrechung

→ Risiko bewerten und Maßnahmen priorisieren

Optionales Hilfsmittel bei Top-Risiken: vereinfachte Bow-Tie-Sicht „Ursachen → Barrieren → kritisches Ereignis → Folgen“.

Vom Risiko zur passenden Anforderung

Der Viewer unterstützt die strukturierte Auswahl – die fachliche Relevanzbewertung bleibt Teil der Kurzbetrachtung.



Hilfsmittel im Viewer

Zielobjektkategorien · Vererbung · Volltext-/Mehrfachsuche · Filter nach Schutzzielen und Katalogeigenschaften

Abstraktes Beispiel

„Netze“ als Zielobjekt → passende Kategorie wählen → Anforderungen auf Schutzziel Verfügbarkeit prüfen

Ergebnis

Kompaktes Anforderungspaket mit Status: erfüllt · nicht erfüllt · nicht anwendbar

Nützliche Links

[Stand-der-Technik-Viewer](#)

[BSI Bibliothek \(GitHub\)](#)

[Zielobjektkategorien \(CSV\)](#)

Praxisregel: Nicht den gesamten Katalog „abarbeiten“, sondern Anforderungen risikoorientiert und zielobjektbezogen auswählen.

Quick Wins zuerst – danach risikobasiert priorisieren

Schnell wirksame Verbesserungen werden umgesetzt; strukturelle Maßnahmen folgen nach Risiko und Wirkung.



Priorität nach Risiko

- P0** **sofort**
nicht vertretbar
- P1** **kurzfristig**
hohe Wirkung
- P2** **verbindlich planen**
mittlere Priorität
- P3** **beobachten**
geringes Risiko

Quick-Win-Test: „Kann die Maßnahme mit wenig Aufwand kurzfristig eine erkennbare Risikoreduktion erzeugen?“

Managemententscheidung: wenige Informationen, klare Entscheidung

Die Detailarbeit bleibt im Risiko- und Anforderungspaket – die Leitung erhält die entscheidungsrelevante Verdichtung.



Hilfsmittel: maximal dreiseitige Managementvorlage mit Top-Risiken, offenen Anforderungen, Maßnahmen, Restrisiken und Entscheidung.

Grafiken

Rückverfolgbarkeit der fachlichen Anforderungsauswahl

Jede Anforderung muss fachlich vom konkreten Zielobjekt und Risiko her begründet werden.

Fachliche Begründungskette



Rückverfolgbarkeit Die Referenz-IDs verbinden jede ausgewählte Anforderung mit Zielobjekt, Gefährdung, Risiko und betroffenem Schutzziel. Damit ist jederzeit nachvollziehbar, warum die Anforderung Bestandteil der Sicherheitsbetrachtung ist.

Managementnutzen

- Nachvollziehbar**
Warum wurde die Anforderung ausgewählt?
- Prüfbar**
Welche Referenzen und Nachweise gehören dazu?
- Priorisierbar**
Welches Risiko wird mit welcher Wirkung reduziert?

Fachliche Auswahl der Anforderungen

Die Auswahl entsteht aus der Kombination von vier fachlichen Merkmalen.

AUSWAHLMERKMALE



Der Stand der Technik Viewer des BSI

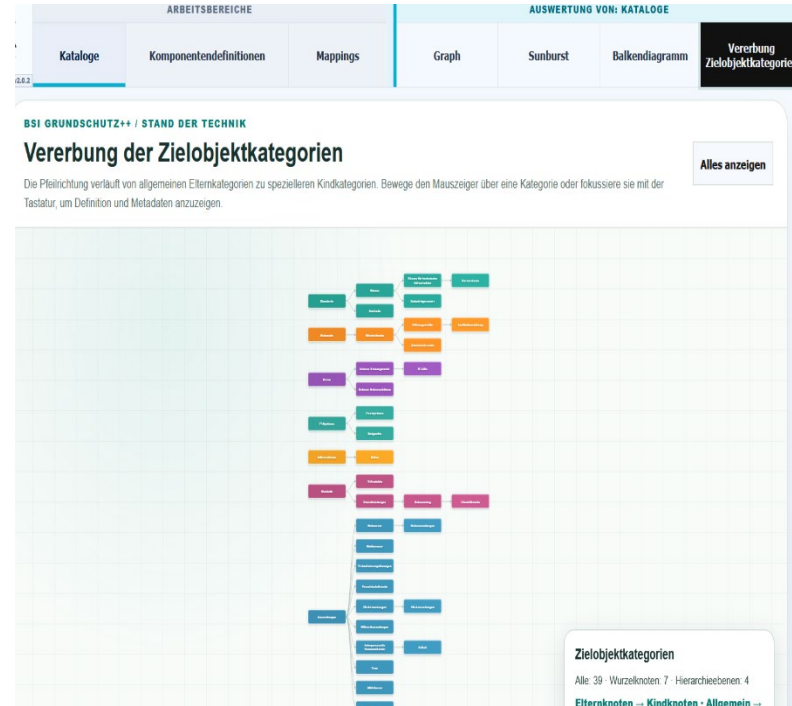
(Stand 14.08.2026)

The screenshot displays the 'Stand der Technik Viewer' web application. The interface is divided into several sections:

- Header:** Includes the logo 'STAND DER TECHNIK VIEWER' and a version number 'v3.0.2'. Navigation tabs are present for 'Kataloge', 'Komponentendefinitionen', and 'Mappings' under the 'ARBEITSBEREICHE' section. Another set of tabs under 'AUSWERTUNG VON: KATALOGE' includes 'Graph', 'Sunburst', 'Balkendiagramm', and 'Vererbung Zielobjektkategorien'.
- Left Sidebar:** Contains two main sections: 'Dateiupload' (with a sub-link 'Katalog laden und Quellen verwalten') and 'Inhalte filtern' (with a sub-link 'Suche und 11 Filter').
- Main Content Area:**
 - Kataloganalyse:** A section with a description: 'Die Übersicht priorisiert sichtbare Treffer, aktive Einschränkungen und Schnellaktionen, damit Navigation und Auswertung ohne Suchaufwand funktionieren.'
 - Summary Cards:** Four cards displaying key statistics:
 - GELADEN:** 1000 (Anforderungen insgesamt)
 - SICHTBAR:** 1000 (Treffer in der aktuellen Ansicht)
 - PRAKTIKEN:** 20 (Erkannte Praktiken)
 - THEMEN:** 140 (Zweite Gruppenebene)
 - AKTUELLER FOKUS:** A section with a button 'Keine aktiven Einschränkungen'.
 - SCHNELLAKTIONEN:** A section with four buttons: 'Filter zurücksetzen', 'Alles aufklappen', 'Alles zuklappen', and 'Als PDF exportieren'.

Der Zielobjektbaum

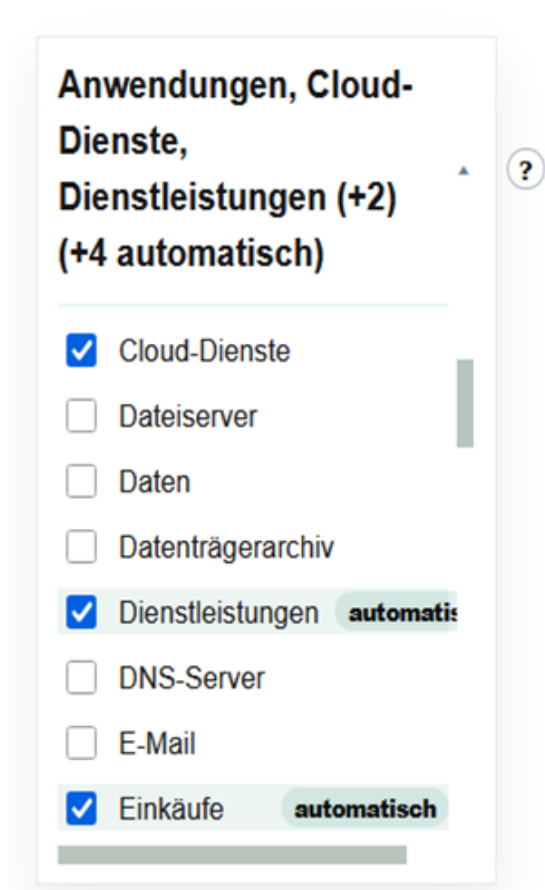
(Stand 14.08.2026)



Filterfunktionen und Vererbung

(Stand 14.08.2026)

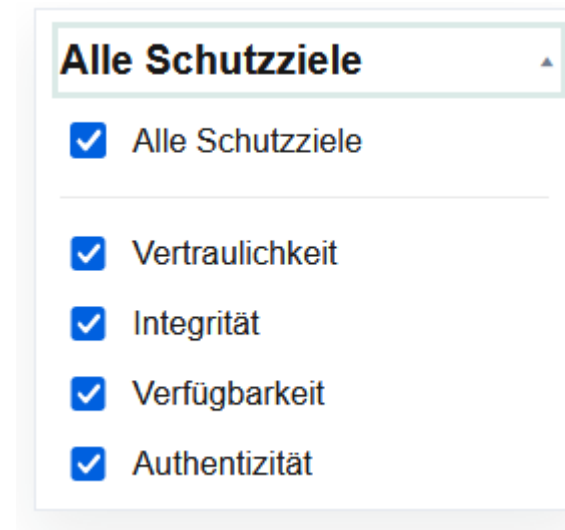
Vererbung: Beispiel Cloud-Dienste



The screenshot shows a filter menu with the title "Anwendungen, Cloud-Dienste, Dienstleistungen (+2) (+4 automatisch)". It contains a list of items with checkboxes and some with additional labels:

- ☒ Cloud-Dienste
- ☐ Dateiserver
- ☐ Daten
- ☐ Datenträgerarchiv
- ☒ Dienstleistungen **automatisch**
- ☐ DNS-Server
- ☐ E-Mail
- ☒ Einkäufe **automatisch**

Filterfunktionen Schutzziele



The screenshot shows a filter menu with the title "Alle Schutzziele". It contains a list of items with checkboxes:

- ☒ Alle Schutzziele
- ☒ Vertraulichkeit
- ☒ Integrität
- ☒ Verfügbarkeit
- ☒ Authentizität