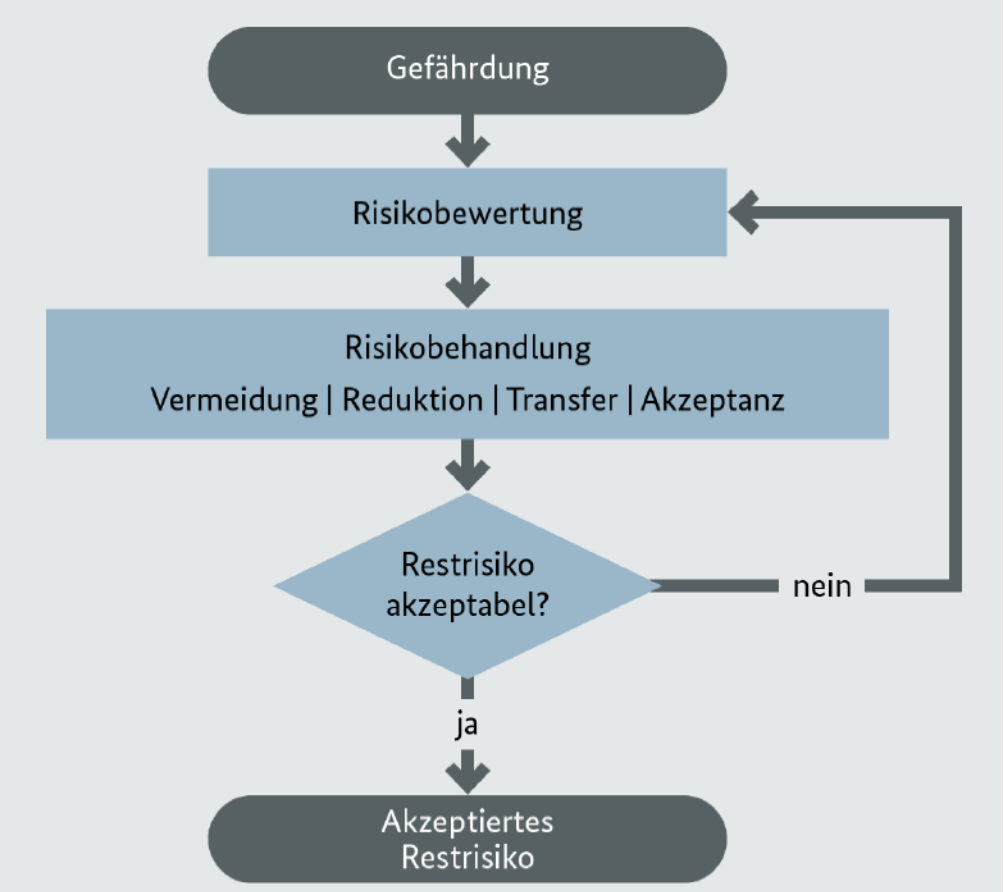
Risiken behandeln

In der Regel wird die Gefährdungsbewertung aufzeigen, dass nicht alle Gefährdungen durch das vorhandene Sicherheitskonzept ausreichend abgedeckt sind. In diesem Fall müssen Sie überlegen, wie angemessen mit den verbleibenden Gefährdungen umgegangen werden kann, und eine begründete Entscheidung hierzu treffen. Folgender Prozess hilft Ihnen bei der Entscheidungsfindung:



Grundsätzlich können vier Möglichkeiten (Risikooptionen) unterschieden werden, mit Risiken umzugehen:

- **A: Risikovermeidung durch Umstrukturierung der Geschäftsprozesse**
  Die Risiken können vermieden werden, indem der Informationsverbund so umstrukturiert wird, dass die Gefährdung nicht mehr wirksam werden kann. Dies bietet sich beispielsweise für an, wenn Gegenmaßnahmen zwar möglich sind, aber einen zu hohen Aufwand bedeuten und gleichzeitig das Risiko nicht akzeptiert werden kann.

- **B: Risikoreduktion (Risikomodifikation) durch weitere Sicherheitsmaßnahmen**

  Die Risiken können durch zusätzliche, höherwertige Sicherheitsmaßnahmen verringert werden. Sofern es für das Zielobjekt, das Sie in der Risikoanalyse betrachtet haben, bereits einen Baustein im IT-Grundschutz-Kompendium gibt, finden Sie in den dort genannten Anforderungen für den erhöhten Schutzbedarf und den zugehörigen Umsetzungsempfehlungen erste Hinweise auf geeignete Maßnahmen. Weitere Quellen sind beispielsweise Produktdokumentationen, Standards zur Informationssicherheit oder in Fachveröffentlichungen.

- **C: Risikotransfer**

  Die Risiken werden verlagert. Durch Abschluss von Versicherungen oder durch Auslagerung der risikobehafteten Aufgabe an einen externen Dienstleister kann zum Beispiel ein möglicher finanzieller Schaden (zumindest teilweise) auf Dritte abgewälzt werden. Achten Sie bei dieser Lösung auf eine sachgerechte, eindeutige Vertragsgestaltung!

- **D: Risikoakzeptanz**

  Die Risiken können akzeptiert werden, sei es, weil die Gefährdung nur unter äußerst speziellen Bedingungen zu einem Schaden führen könnte, sei es, weil keine hinreichend wirksamen Gegenmaßnahmen bekannt sind oder aber weil der Aufwand für mögliche Schutzmaßnahmen unangemessen hoch ist.

Ein Risiko kann nur dann akzeptiert werden, wenn das (z. B. nach Umsetzung von Schutzmaßnahmen verbleibende) **Restrisiko** von der Institution getragen werden kann, sich also im Einklang mit den festgelegten Risikoakzeptanzkriterien befindet.

Aufgabenstellung:

- **Erstellen** Sie eine **Risikobehandlung** für den Virtualisierungsserver S001!
  - **Nutzen** Sie dazu die Vorlage „**Vorlage_Risiko_behandeln_ServerS001**“!
  - **Kopieren** Sie sich diese Vorlage und **benennen** Sie das Dokument entsprechend um!
  - **Informieren** Sie sich mithilfe des **Interviews** (Dokument: **Auszug_Interviews**) über die Situation im Krankenhaus!
  - **Vervollständigen** Sie anschließend die Tabelle mit Inhalten in den Spalten **Risikobewertung** und **Risikohandlungsoption**!