

ISO/IEC 27001 in a nutshell

Agenda

1. Was darf IT-Sicherheit kosten ?
2. Der Aufbau eines Information Security Management Systems nach ISO/IEC 27001
3. Zusammenfassung

Was Sicherheit kosten? - ROSI

$$ROSI = \frac{(RS \times \%RV) - AK}{AK}$$

**Formel für Return on Security
Investment**

**RS = Risikosumme (potenziell
erwartete Schadensumme)**

RV = Risikoverminderung in Prozent

**AK = Anschaffungskosten einer
Sicherheitslösung**

Implementierung eines ISMS nach ISO 27001

Der Standard beschreibt nur

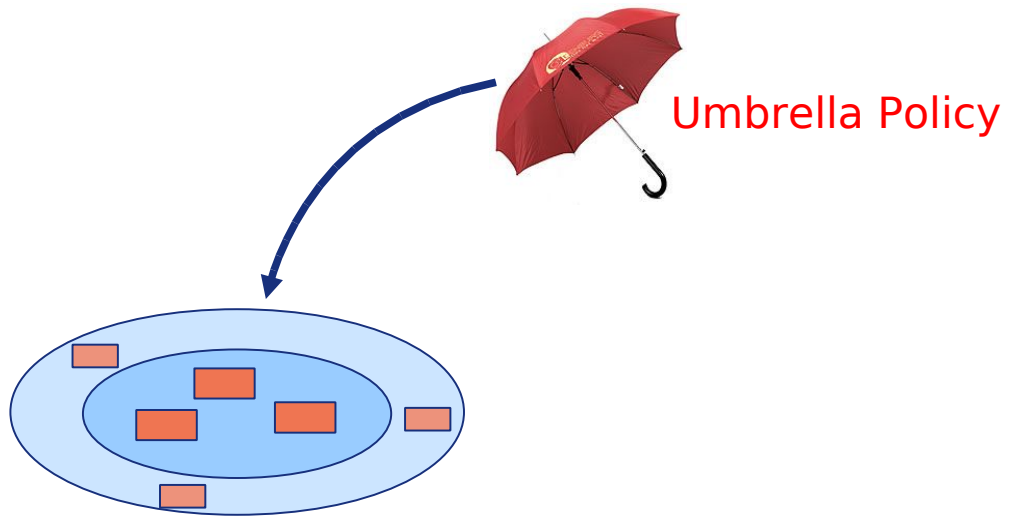
die Vorgehensweise

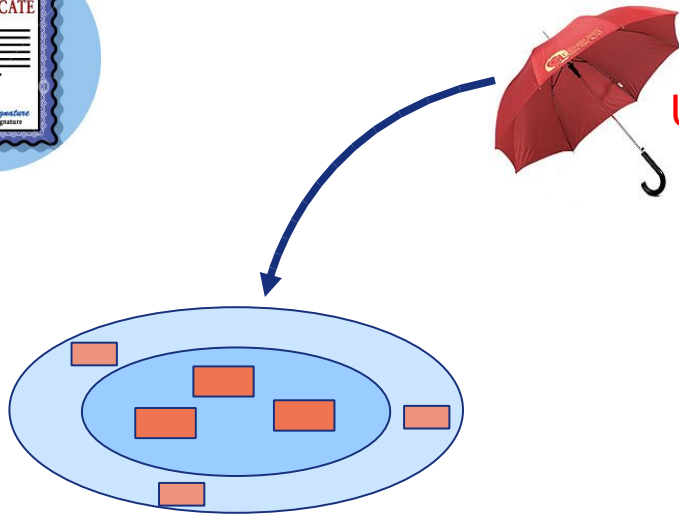
beim Aufbau eines Information Security
Management Systems



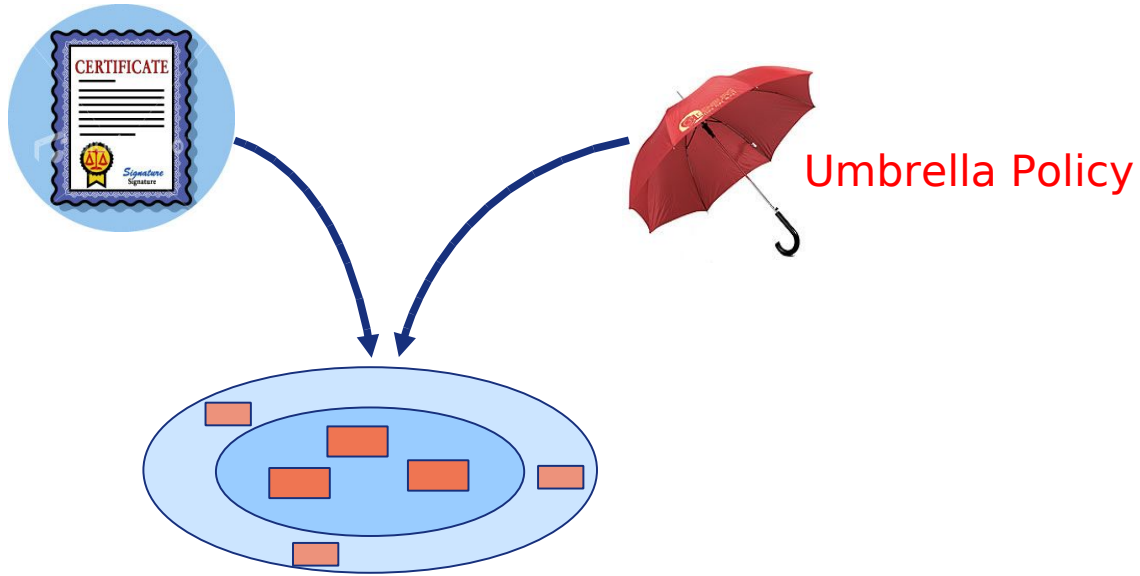
Umbrella Policy

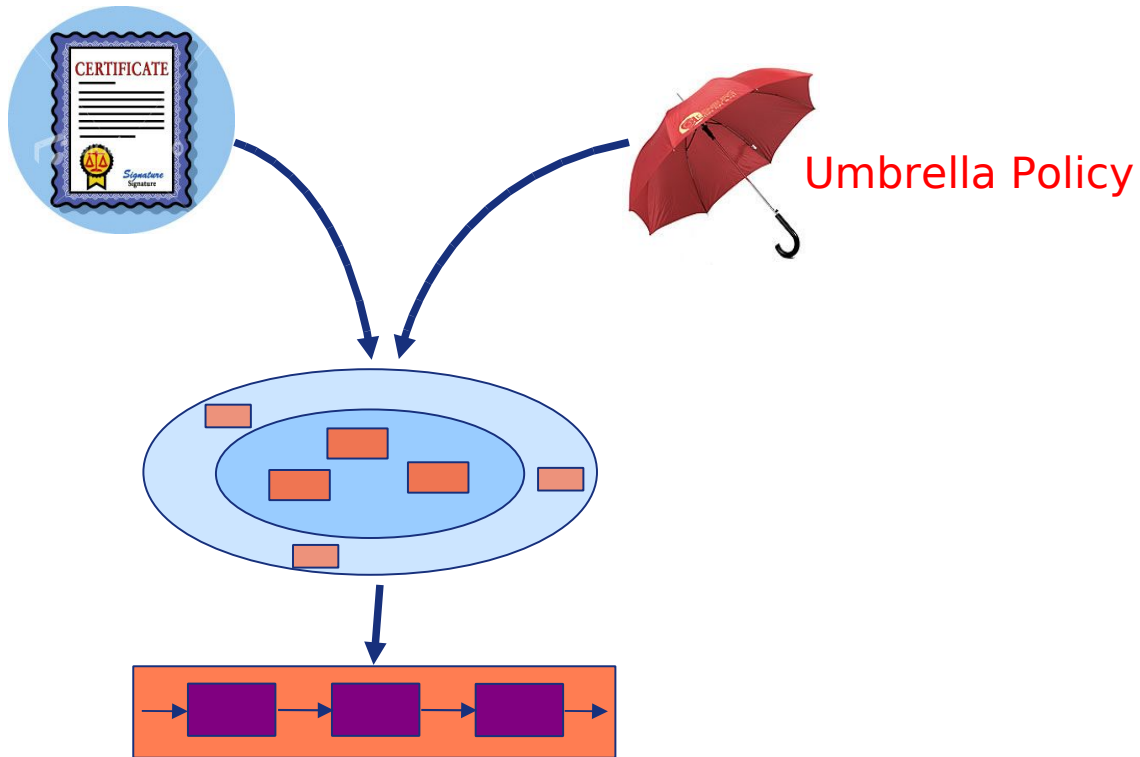


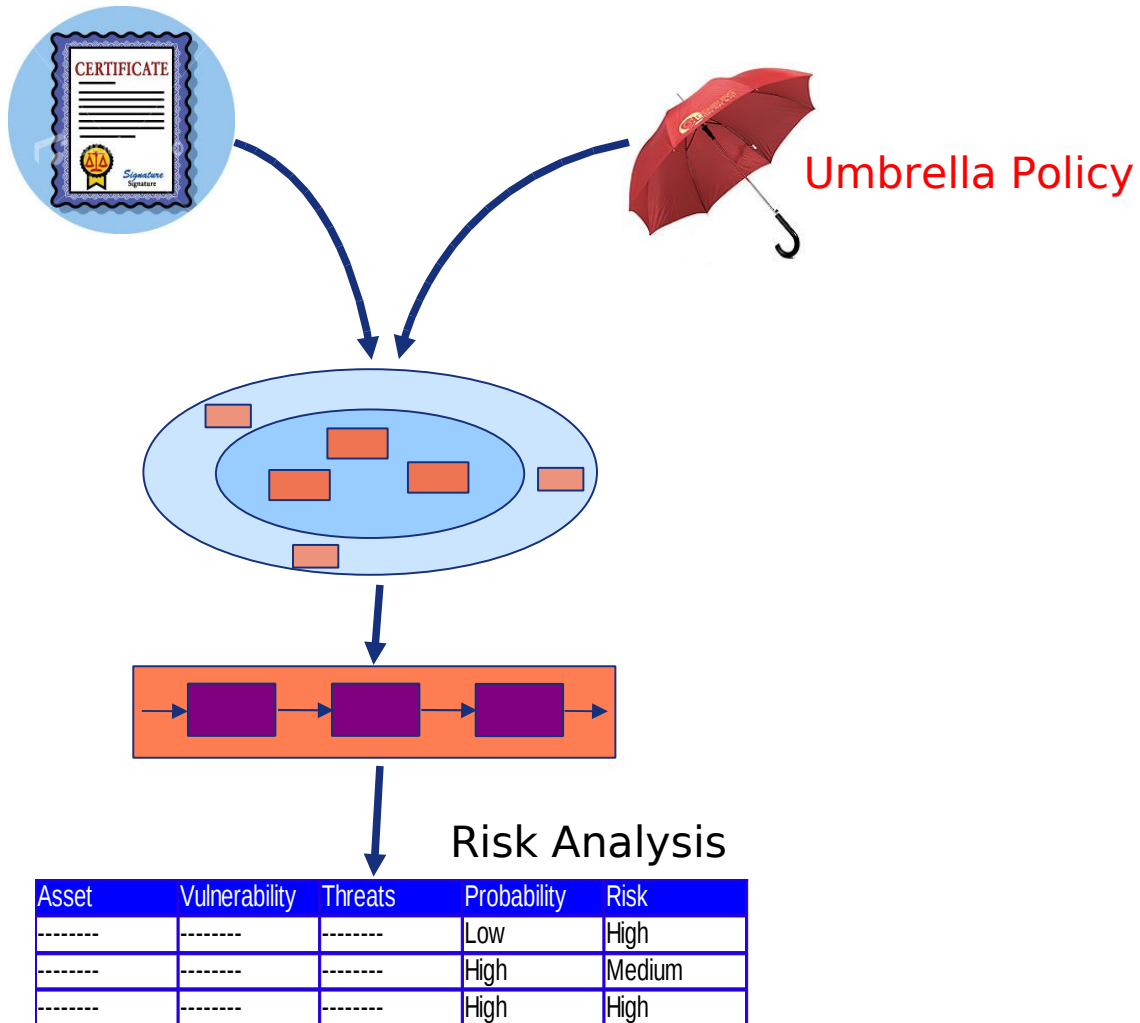




Umbrella Policy





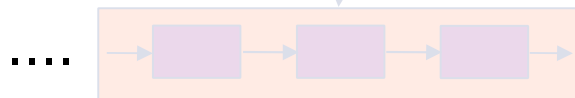


4.2.1 Festlegen des ISMS



Die Organisation muss die folgenden Schritte durchführen.

b) **Definition der ISMS-Leitlinie** unter Berücksichtigung der Eigenschaften des Geschäfts, der Organisation, ihres Standorts, ihrer Werte und ihrer Technologie, die:



3) mit dem **strategischen Risikomanagementkontext** der Organisation abgestimmt ist, in dem die Einrichtung und Instandhaltung des ISMS erfolgen wird;

4) **Kriterien festlegt, nach denen Risiken bewertet werden**

Risk Analysis			
Asset	Vulnerability	Threats	Probability
-----	-----	-----	High
-----	-----	-----	Medium
-----	-----	-----	High

4.2.1 Festlegen des ISMS

c) Definition der Vorgehensweise der Organisation für Risikoeinschätzung.

1) Identifizierung einer Methode für die Risikoeinschätzung, die für das ISMS und die festgelegten Geschäftsanforderungen an Informationssicherheit sowie die gesetzlichen und amtlichen Anforderungen geeignet ist.

2) Entwicklung von Kriterien für Risikoakzeptanz und Identifizierung von akzeptablen Risikoniveaus (siehe 5.1 f)).

Die ausgewählte Methode für die Risikoeinschätzung muss sicherstellen, dass die Risikoeinschätzung vergleichbare und reproduzierbare Resultate liefert.

4.2.1 Festlegen des ISMS

d) Identifizierung der Risiken.

2) Identifizierung der **Bedrohungen** für diese organisations-eigenen Werte (Assets).

3) Identifizierung der **Schwachstellen**, die durch diese Bedrohungen ausgenutzt werden könnten.

4) Identifizierung der **Auswirkungen**, die der Verlust von **Vertraulichkeit, Integrität** und **Verfügbarkeit** auf die organisationseigenen Werte (Assets) haben darf.

Asset	Vulnerability	Threats	Probability	Risk
-----	-----	-----	Low	High
-----	-----	-----	High	Medium
-----	-----	-----	High	High

4.2.1 Festlegen des ISMS



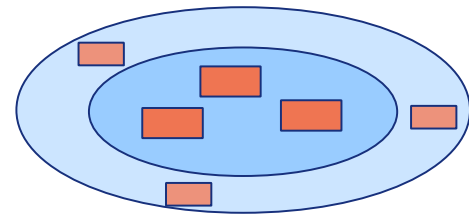
Einschätzung der realistischen Wahrscheinlichkeit, dass Sicherheitsprobleme auftreten, angesichts der existierenden Bedrohungen und Schwachstellen, der mit den organisationseigenen Werten (Assets) verbundenen Auswirkungen, und der momentan umgesetzten Maßnahmen.

Risk Analysis

Asset	Vulnerability	Threats	Probability	Risk
-----	-----	-----	Low	High
-----	-----	-----	High	Medium
-----	-----	-----	High	High



Umbrella Policy

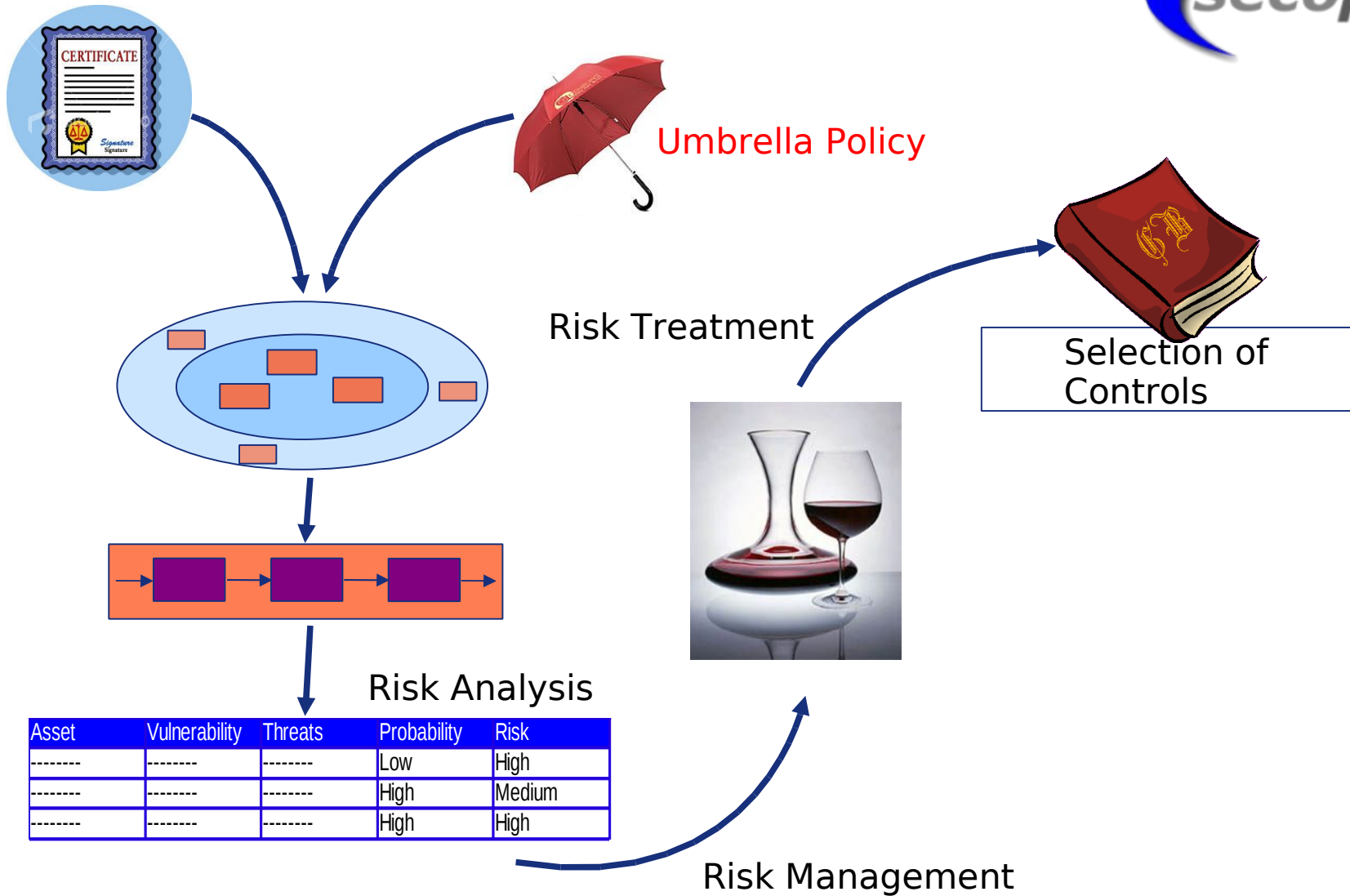


Risk Analysis

Asset	Vulnerability	Threats	Probability	Risk
-----	-----	-----	Low	High
-----	-----	-----	High	Medium
-----	-----	-----	High	High



Risk Management

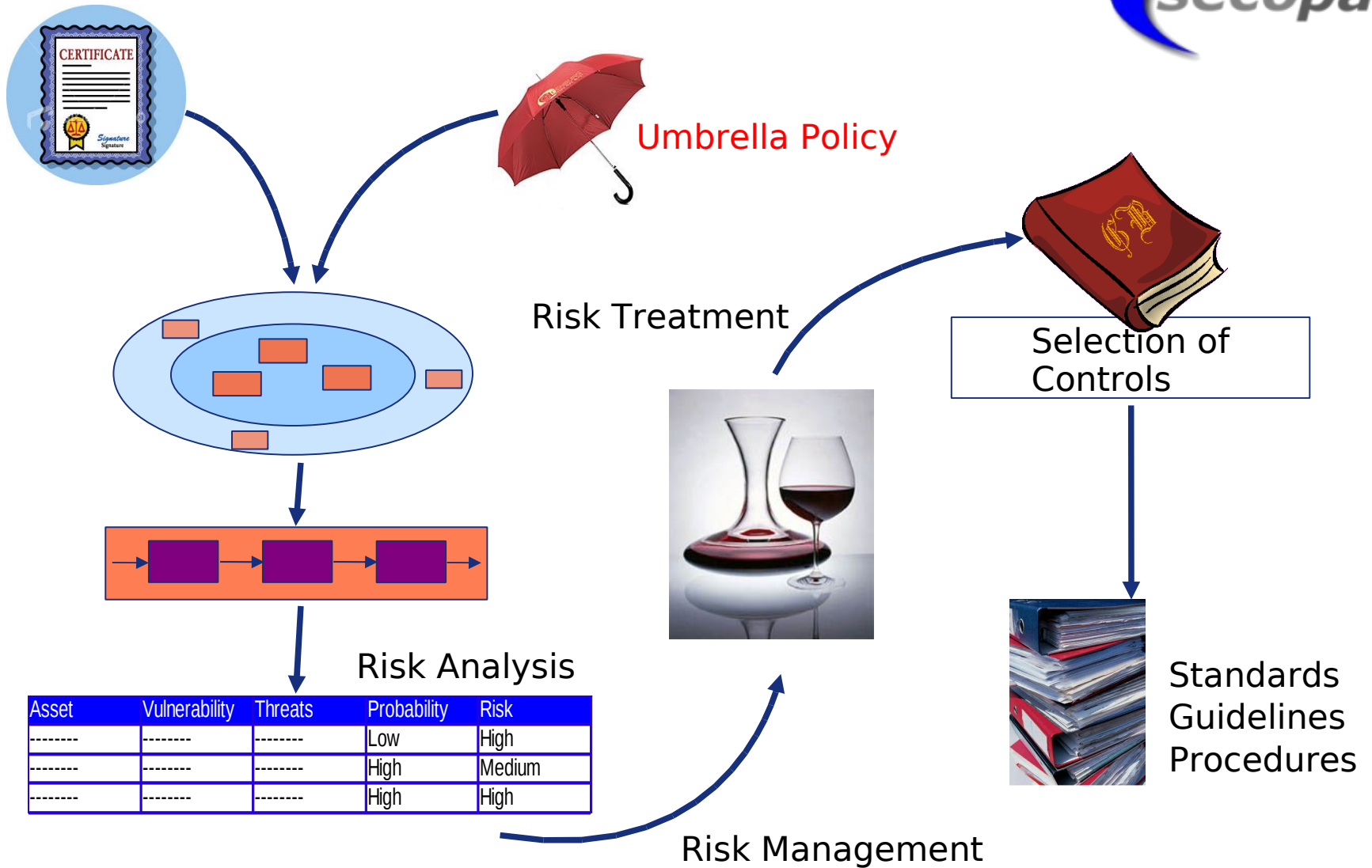


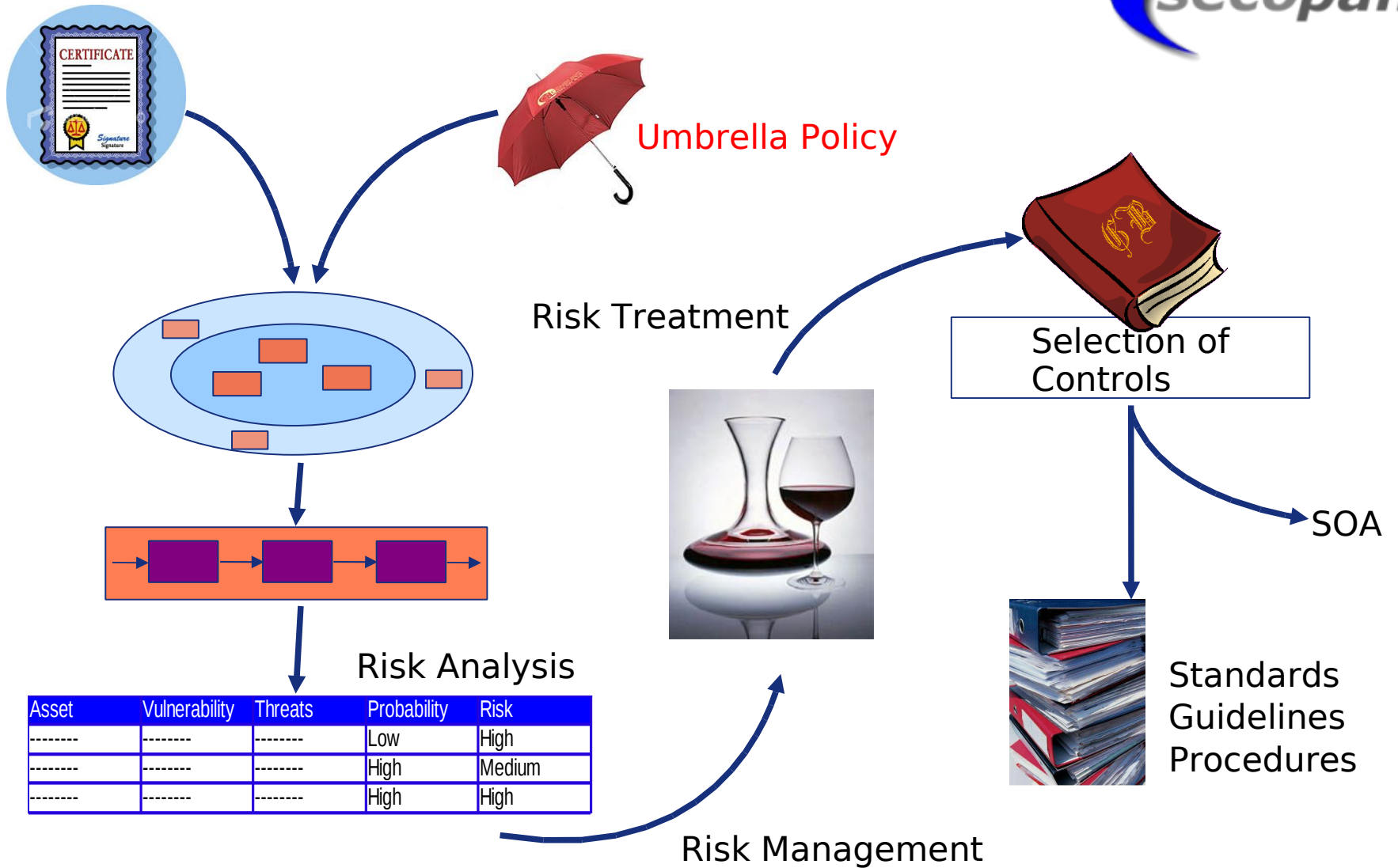


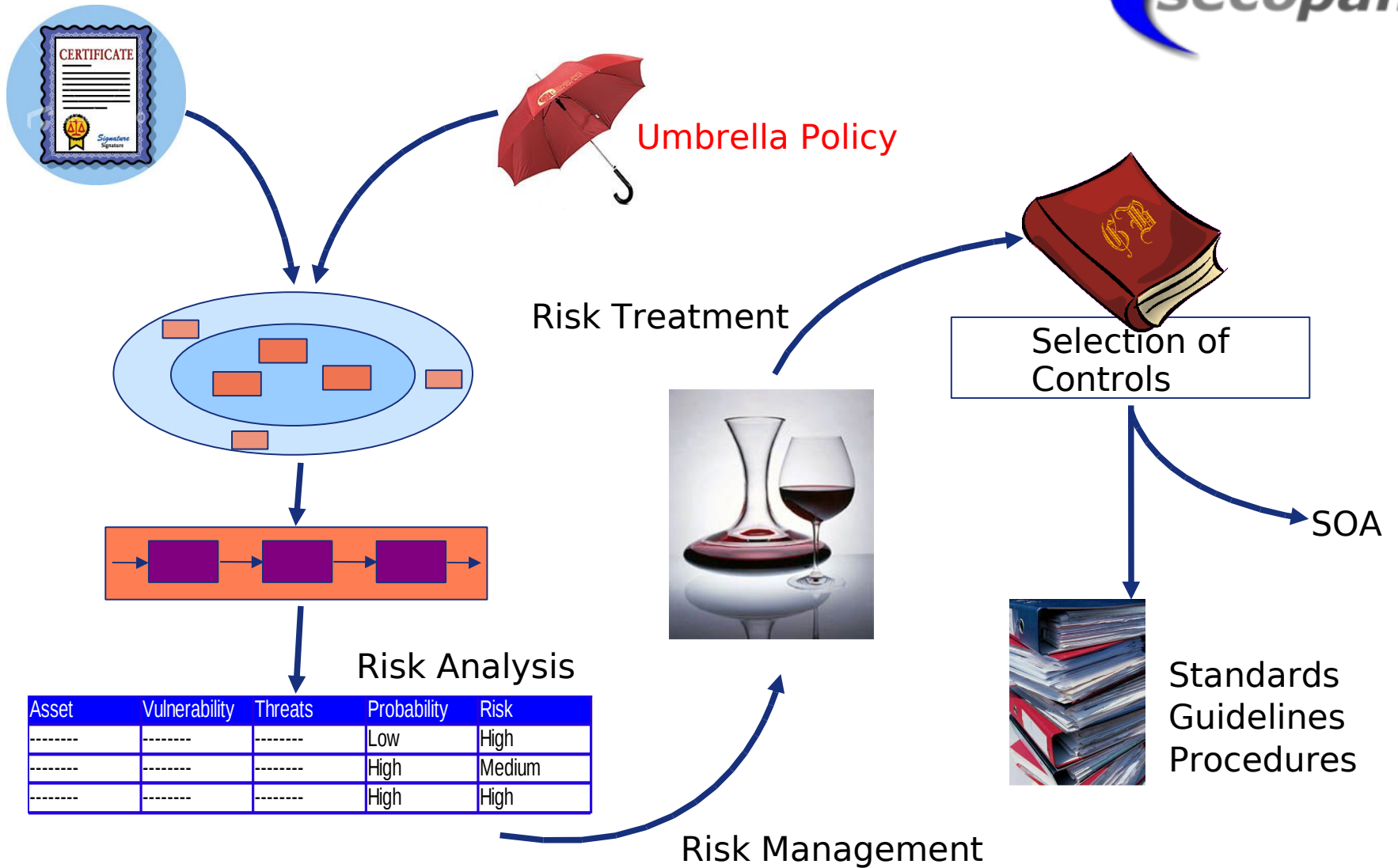
Festlegen des ISMS

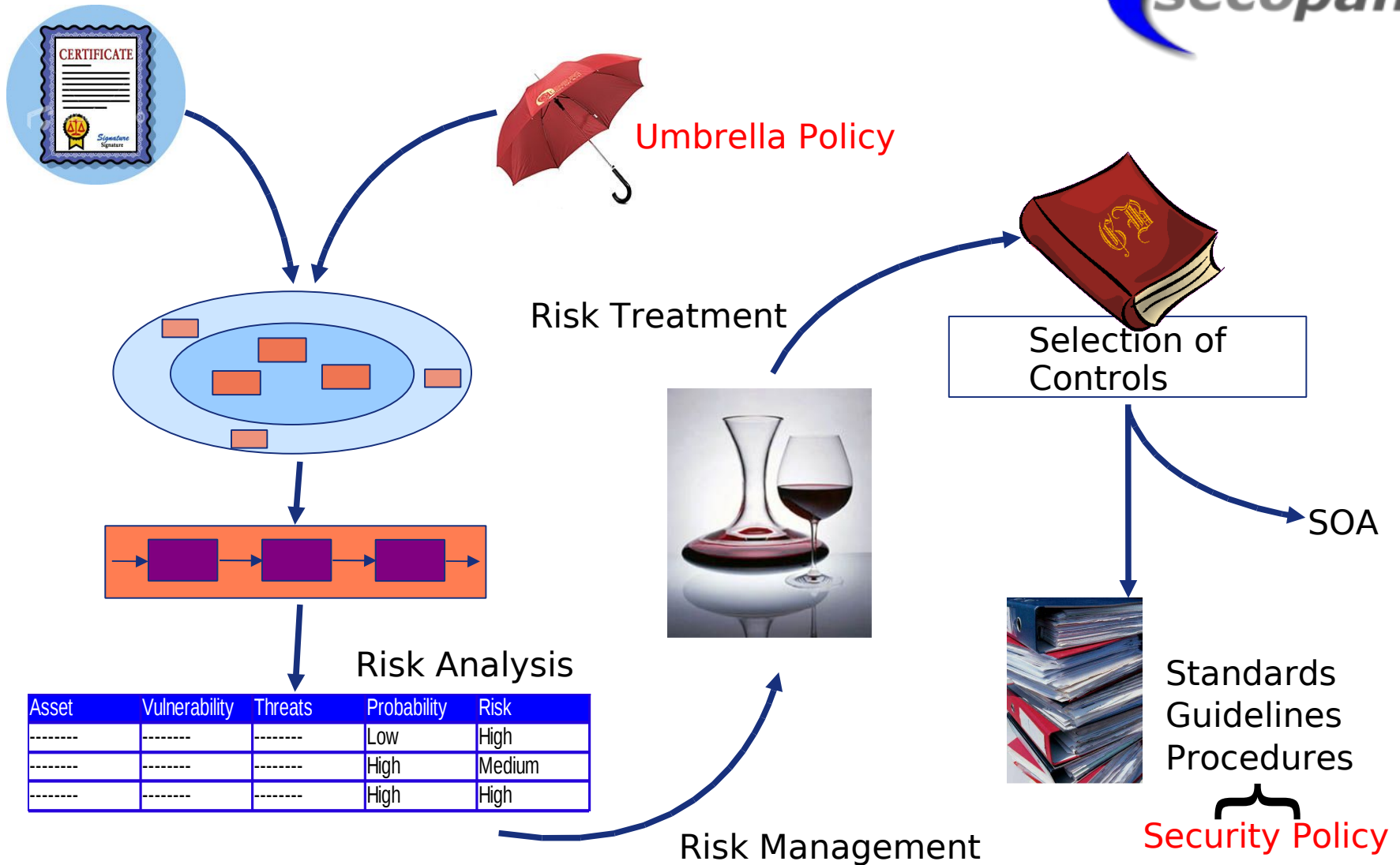
Mögliche Aktionen sind:

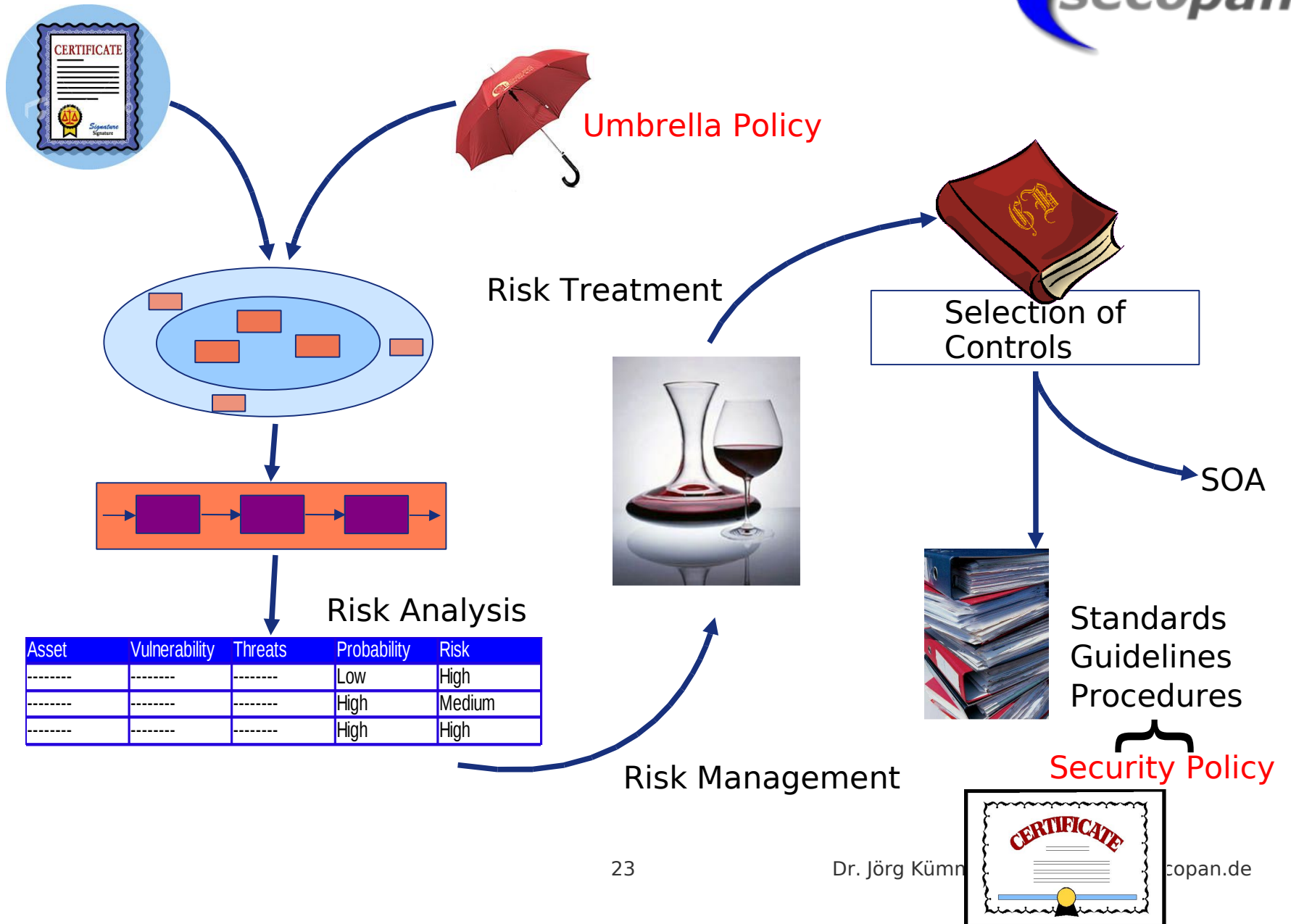
- 1) **Anwendung geeigneter Maßnahmen;**
- 2) **bewusste und objektive Akzeptanz** der Risiken, sofern diese eindeutig den Leitlinien und Kriterien der Organisation für Risikoakzeptanz genügen);
- 3) **Vermeidung der Risiken;** und
- 4) **Übertragung** der zugehörigen Geschäftsrisiken an andere, z. B. Versicherer, Lieferanten.











Zusammenfassung

- ▶ ISO/IEC 27001 unterstützt die Optimierung von IT-Prozessen
- ▶ ISO/IEC 27001 fördert den effizienten Einsatz von Finanz- und Personalressourcen
- ▶ ISO/IEC 27001 erlaubt die Integration in bestehende Qualitätsmanagement-Systeme
- ▶ ISO/IEC 27001 erlaubt die Integration in bestehende Risikomanagement-Systeme
- ▶ ISO/IEC 27001 schafft Vertrauen zwischen Geschäftspartnern