

ISMS

aufbauen

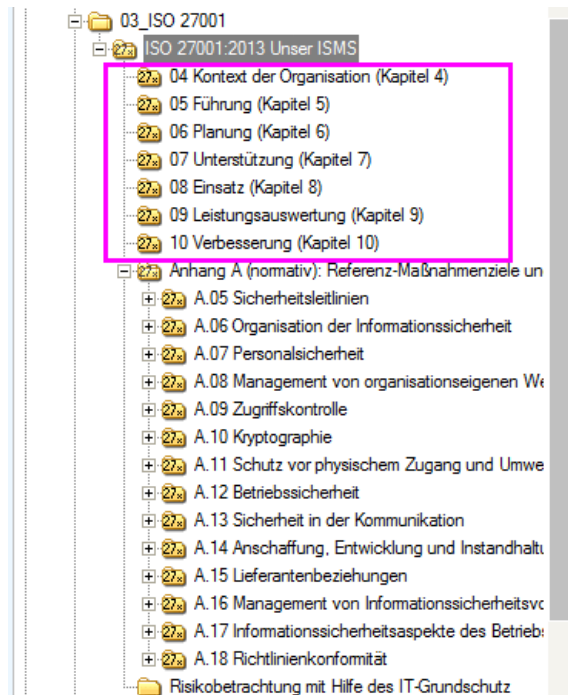
und zertifizieren

Wir hören oder lesen oft, dass die Zertifizierung eines Informationssicherheitsmanagementsystems (ISMS) für manche zu aufwändig und zu teuer sei.

**Nun, es ist eine Frage des Verzichtens!**

Wir als Softwarehersteller leben nicht von Beratungsleistungen und ermöglichen es Ihnen zu einem günstigen Preis Software zu erwerben, die es Ihnen ermöglicht auf "zuviel und unnötige Beratungsleistung", also auf einen der wesentlichen Kostentreiber, zu verzichten.

## 1. Die Zertifizierung des ISMS

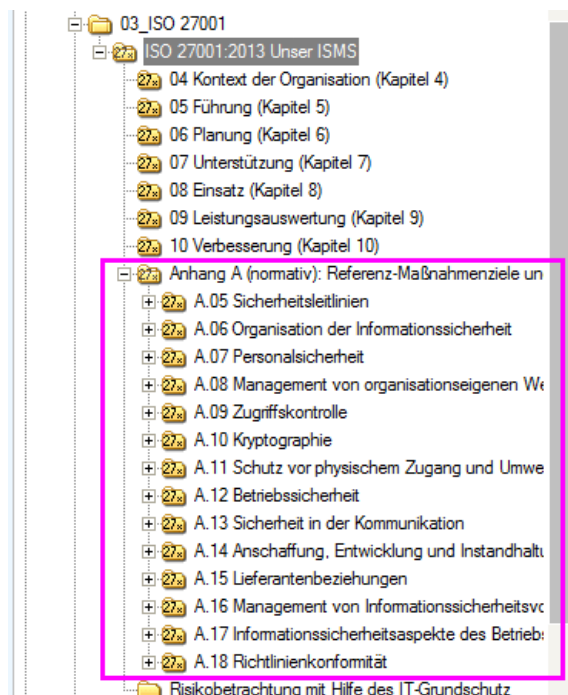


Das Zertifizieren *eines* ISMS ist das Zertifizieren des Managementsystems, der ISO 27001.

Möglicherweise kennen Sie das Prozedere bereits von der ISO 9000 her:

- ca. 30 - 40 Vorschriften\* einführen und bei den betroffenen Mitarbeitern schulen
- eine Istaufnahme der technischen und organisatorischen Maßnahmen, die bereits jetzt realisiert sind

## 2. Überwachungsaudits und Re-Zertifizierung des ISMS



Die Überwachungsaudits und die Re-Zertifizierung *des* Managementsystems erfolgen auf Basis *der* ISO 27002.

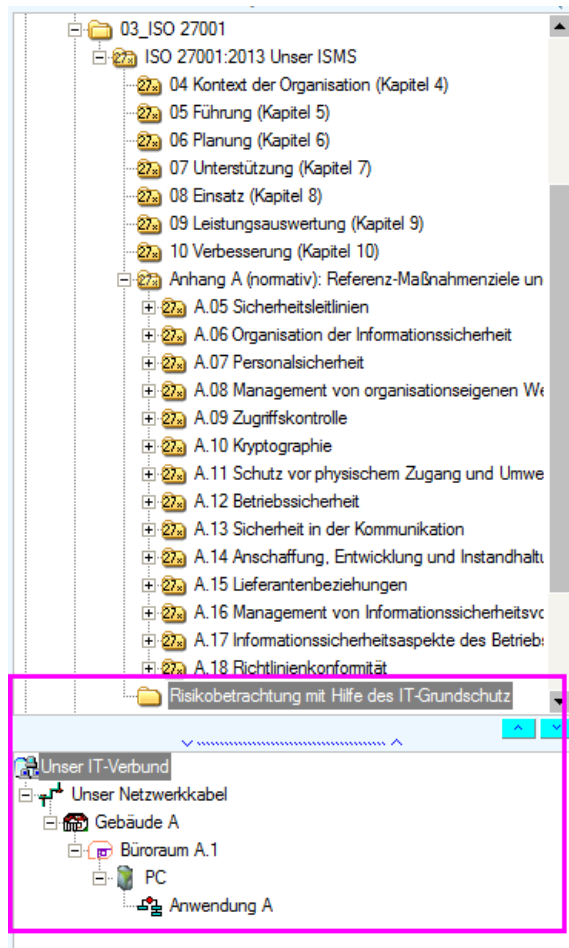
- um diese Anforderung geschickt und kostengünstig zu bewerkstelligen nutzen wir den BSI IT-Grundschutz unter dem Gesichtspunkt:

**Risikobetrachtung!**

Insgesamt gesehen erwartet man von Ihnen über die Jahre eine stetige Verbesserung des Managementsystems.

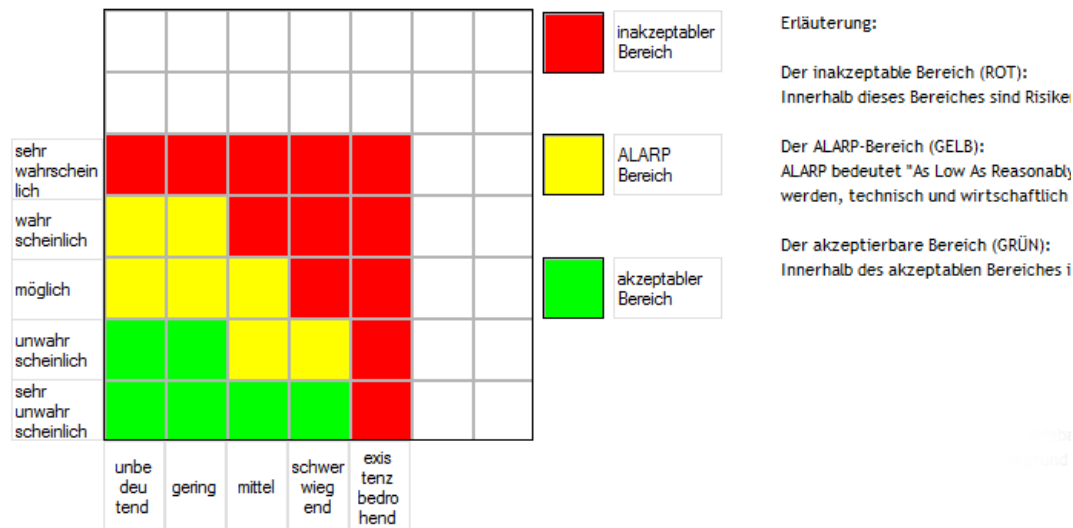
(\* diese Vorschriften sind zu ca. 700 \$ käuflich zu erwerben oder können, als Grundlagentexte, durch opus i erzeugt werden.

### 3. Die Risikobetrachtung mit Hilfe des BSI IT-Grundschatzes



Damit wir die Risiken automatisch zusteuern und selbst betrachten können, bauen wir unsere IT *logisch* als **IT-Verbund** nach und erhalten über den BSI IT-Grundschatz ca. 700 Gefährdungen zugesteuert, die wir zu betrachten und zu bewerten haben.

## 4. Wir betrachten und bewerten die Risiken mit Hilfe einer Risikomatrix



**Das Bewerten der wirkenden Risiken (Bedrohungen), nach den Vorgaben, die Sie in der Risikomatrix festgelegt hatten, dauert**

- wenn Sie es machen ca. 1 Arbeitstag
- wenn Sie es zu zweit machen ca 2 - 3 Arbeitstage (Sie und der (oberste) Entscheider)
- usw.

**Merke:** je risikofreudiger Sie sind, sprich, je mehr Risiken Sie akzeptieren, desto weniger Arbeit haben Sie später!

**Achtung:** Sie müssen Ihre Risikofreudigkeit dem Auditor , der Sie zertifizieren soll, plausibel machen können!

**Diese Risikobewertung legen wir nun auf die Maßnahmen, die für den IT-Verbund automatisch vorgeschlagen wurden...**

und erhalten durch **geschicktes Filtern** für den Beginn unserer Bemühungen **ca. 50 bis 100** (oder mehr) Maßnahmen, die zwingend umzusetzen sind. Das Implementieren der Maßnahmen wird Risikobehandlung genannt!

Für obigen *sehr kleinen* IT-Verbund haben wir durch geschicktes Filtern genau **12** Maßnahmen herausgearbeitet, die zwingend zu implementieren sind.

Objektname	BSI Nr.	BSI Nr. Farbe	Maßnahme	Zertifikats-level	Initiierung durch	Umsetzung durch	Lebenszyklus/Phase	Umsetzungs-Status	Nr./Kapitel
Unser IT-Verbund	2.224	Rot	Vorbeugung gegen Schadprogramme	A Einstieg	Kron	Administrator	04 BT Betrieb	unbearbeitet	ISO27001:2013 > 1
Unser IT-Verbund	2.64	Rot	Kontrolle der Protokolldateien	A Einstieg	Kron	Sebastian	04 BT Betrieb	unbearbeitet	ISO27002:2013 > 1 ISO27002:2013 > 1 ISO27002:2013 > 1 ISO27002:2013 > 1
Unser IT-Verbund	2.199	Rot	Aufrechterhaltung der Informationssicherheit	A Einstieg	Kron	Kron	04 BT Betrieb	unbearbeitet	ISO27001:2013 > 1 ISO27001:2013 > 1

## Wir filterten in den Spaltenköpfen der Tabelle nach

- ROT (Maßnahmen zu rot eingestuften Risiken)
- A Einstieg (die relevantesten Maßnahmen überhaupt)
- 04 BT Betrieb (die Betriebsphase der IT)

## **\*Was meinen Sie?**

**Ist es für Sie zu aufwändig**

**30 - 40 Richtlinien einzuführen und**

**für den Anfang ca. 50 bis 100 Maßnahmen  
zu implementieren, von denen  
möglicherweise heute bereits die Hälfte  
implementiert sind?**

(\*) Wir glauben:  
Wenn Sie **opus i** verstanden haben,  
wird Ihre Antwort "nein" lauten!

Ende des Papers.