

Jacqueline Naumann

# Die ganze Härte der ISO 27001

Ihre Berufung zum  
Informationssicherheitsbeauftragten  
(ISB)



Versorgungseinrichtungen Informationssicherheitsvorfälle Lieferantenbewertung  
Softwareentwicklung Überwachung SoA Backup Kennwörter Registrierung Tresor  
Entsorgung Administrator Verkabelung Stromversorgung Zutrittssteuerung  
Protokollierung Bildschirmsperre Privatsphäre



# Kurzüberblick

1. **Einleitung**
2. **Berufung zum ISB**
3. **Erwartungen interessierter Parteien**
4. **Verwaltung der Werte**
5. **Risikoanalyse**
6. **SoA**
7. **Personalsicherheit**
8. **Informationssicherheitsvorfälle**
9. **Lieferantenbeziehung**
10. **Schadsoftware**
11. **Protokollierung**
12. **Backup**
13. **Bildschirmsperre**
14. **Zutrittssteuerung**
15. **Entsorgung**
16. **Softwareentwicklung**
17. **Dokumentierte Betriebsabläufe**
18. **Kontakt mit Behörden**
19. **Sichere Entwicklung**
20. **Benutzeregistrierung und Deregistrierung**

21. **Privatsphäre**
22. **Versorgungseinrichtungen**
23. **Unterbrechungsfreie Stromversorgung**
24. **Kennwörter**
25. **Geräte und Betriebsmittel**
26. **Physische u. umgebungsgebundene Sicherheit**
27. **Überwachung**
28. **Internes Audit**
29. **Managementbewertung**
30. **Schlusswort**

## **Liebe Leserin, lieber Leser,**

vielen Dank, dass Sie sich für dieses Buch entschieden haben.

Informationssicherheit ist derzeit ein brennendes Thema, das vor allem durch das neue IT-Sicherheitsgesetz noch einmal an Fahrt aufgenommen hat.

Ich hoffe, ich kann Ihnen, liebe Informationssicherheitsbeauftragte und lieber Informationssicherheitsbeauftragter mit diesem Buch Unterstützung bieten, damit Sie Ihre neuen Aufgaben mit Eifer und Begeisterung angehen können.

**Herzlichst, Ihre Jacqueline Naumann**

Trainerin, Beraterin, Auditorin der iXactly IT- und Systemberatung



iXactly ist Ihr Dienstleister für Seminare, Beratung und Audits für Ihr ISMS.

Gostritzer Straße 61, 01217 Dresden

[jacqueline.naumann@ixactly.com](mailto:jacqueline.naumann@ixactly.com), [www.ixactly.com](http://www.ixactly.com)

**Vielen Dank**

an Florentine Naumann für die Illustrationen im Buch!

# Inhalt

## 1. **Einleitung**

1.1 Bekanntmachung mit unserem Buch-ISBN

1.2 Anonymität

## 2. **Berufung zum ISB**

2.1 Praxisbeispiel: Schwarzer Peter

2.2 Ihre Aufgabe als ISB

2.3 Praxisbeispiel: Neuer Job mit ISB-Rolle

2.4 Praxisbeispiel: ISB ohne Berufung

2.5 Ihre Aufgabe als ISB

## 3. **Erwartungen interessierter Parteien**

3.1 Praxisbeispiel: Kleingedrucktes im Vertrag

3.2 Ihre Aufgabe als ISB

## 4. **Verwaltung der Werte**

4.1 Praxisbeispiel: Multifunktionsgerät

4.2 Ihre Aufgabe als ISB

4.3 Praxisbeispiel: Nummerierte Tabellen

4.4 Ihre Aufgabe als ISB

## 5. **Risikoanalyse**

5.1 Praxisbeispiel: Compliance-Anwalt

5.2 Ihre Aufgabe als ISB

5.3 Praxisbeispiel: Risiko lokale Admin-Accounts

5.4 Ihre Aufgabe als ISB

## 6. **SoA**

6.1 Praxisbeispiel: Keine SoA für den Auditor

6.2 Ihre Aufgabe als ISB

## 7. **Personalsicherheit**

7.1 Praxisbeispiel: Stellenbeschreibungen

7.2 Ihre Aufgabe als ISB

7.3 Praxisbeispiel: Video-Streaming

7.4 Ihre Aufgabe als ISB

## 8. **Informationssicherheitsvorfälle**

8.1 Praxisbeispiel: Verschollene Laptops

8.2 Ihre Aufgabe als ISB

8.3 Das Protokoll zum Informationssicherheitsvorfall

## 9. **Lieferantenbeziehung**

9.1 Praxisbeispiel: Vertrauen ist gut

9.2 Ihre Aufgabe als ISB

## 10. **Schadsoftware**

10.1 Praxisbeispiel: Bewerbermails

10.2 Ihre Aufgabe als ISB

10.3 Praxisbeispiel: E-Mails vom BSI

10.4 Praxisbeispiel: Fake-Mails vom Kollegen

10.5 Ihre Aufgabe als ISB

## 11. **Protokollierung**

11.1 Praxisbeispiel: Protokollierung

11.2 Ihre Aufgabe als ISB

11.3 Praxisbeispiel: Logfiles

11.4 Ihre Aufgabe als ISB

## 12. **Backup**

12.1 Praxisbeispiel: Sicherungskopie

12.2 Ihre Aufgabe als ISB

12.3 Praxisbeispiel: Sicherungstresor

12.4 Ihre Aufgabe als ISB

12.5 Praxisbeispiel: Administratoren Vertretung

12.6 Ihre Aufgabe als ISB

## 13. **Bildschirmsperre**

13.1 Praxisbeispiel: Bildschirmsperre

13.2 Ihre Aufgabe als ISB

## 14. **Zutrittssteuerung**

14.1 Praxisbeispiel: Naschender Vermieter

14.2 Ihre Aufgabe als ISB

14.3 Praxisbeispiel: Sparsame Lizenzvergabe

14.4 Ihre Aufgabe als ISB

14.5 Praxisbeispiel: Vertrauen in Dienstleister

14.6 Ihre Aufgabe als ISB

14.7 Praxisbeispiel: Umfangreicher Schlüsselbund

14.8 Ihre Aufgabe als ISB

14.9 Praxisbeispiel: Offene Schranken

14.10 Ihre Aufgabe als ISB

14.11 Praxisbeispiel: Nicht arbeitender Beamer

14.12 Ihre Aufgabe als ISB

## 15. **Entsorgung**

15.1 Praxisbeispiel: Serververkauf auf IT-Verkaufsplattform

15.2 Praxisbeispiel: Kostenlose Server-Entsorgung

15.3 Ihre Aufgabe als ISB

15.4 Praxisbeispiel: Personalakte im blauen Sack

15.5 Ihre Aufgabe als ISB

## 16. **Softwareentwicklung**

16.1 Praxisbeispiel: Verbot von TRY-CATCH

16.2 Ihre Aufgabe als ISB

16.3 Praxisbeispiel: Tool extra kompliziert

16.4 Ihre Aufgabe als ISB

16.5 Praxisbeispiel: Software kaputt getestet

16.6 Ihre Aufgabe als ISB

16.7 Praxisbeispiel: Qualifizierte Testerin

16.8 Ihre Aufgabe als ISB

## 17. **Dokumentierte Betriebsabläufe**

17.1 Praxisbeispiel: Datenbank zu komplex

17.2 Ihre Aufgabe als ISB

## 18. **Kontakt mit Behörden**

18.1 Praxisbeispiel: Nervender Datenschutzbeauftragter

18.2 Ihre Aufgabe als ISB

18.3 Praxisbeispiel: E-Mail-Weiterleitung

18.4 Ihre Aufgabe als ISB

## 19. **Sichere Entwicklung**

19.1 Praxisbeispiel: Produktivstart ohne Test

19.2 Ihre Aufgabe als ISB

19.3 Praxisbeispiel: Produktivstart im Testsystem

19.4 Ihre Aufgabe als ISB

## 20. **Benutzeregistrierung und Deregistrierung**

20.1 Praxisbeispiel: Wer kennt T34M-ADMIN2

20.2 Ihre Aufgabe als ISB

## 21. **Privatsphäre**

21.1 Praxisbeispiel: Keine User-Laufwerke

21.2 Ihre Aufgabe als ISB

21.3 Praxisbeispiel: Chat-Monitoring

21.4 Ihre Aufgabe als ISB

21.5 Praxisbeispiel: Blindcopy-Mails

21.6 Ihre Aufgabe als ISB

## 22. **Versorgungseinrichtungen**

22.1 Praxisbeispiel: Tropfende Klimaanlage

22.2 Ihre Aufgabe als ISB

22.3 Praxisbeispiel: Gut gefüllter Kabelschacht

22.4 Ihre Aufgabe als ISB

## 23. **Unterbrechungsfreie Stromversorgung**

23.1 Praxisbeispiel: Diesel-Vorräte

23.2 Ihre Aufgabe als ISB

## 24. **Kennwörter**

24.1 Praxisbeispiel: 3-stelliges Kennwort

24.2 Ihre Aufgabe als ISB

24.3 Praxisbeispiel: Zwei Kennwort-Richtlinien

24.4 Ihre Aufgabe als ISB

24.5 Praxisbeispiel: Aufgabenteilung bei Kennwörtern

24.6 Ihre Aufgabe als ISB

## 25. **Geräte und Betriebsmittel**

25.1 Praxisbeispiel: Rollcontainer

25.2 Ihre Aufgabe als ISB

25.3 Praxisbeispiel: Verwitterter Brief

25.4 Ihre Aufgabe als ISB

25.5 Praxisbeispiel: Geschenkte Privat-PCs

25.6 Ihre Aufgabe als ISB

## 26. **Physische u. umgebungsgebundene Sicherheit**

26.1 Praxisbeispiel: Irreführende Kennzeichnung

26.2 Ihre Aufgabe als ISB

## 27. **Überwachung**

27.1 Praxisbeispiel: Videoüberwachung

27.2 Ihre Aufgabe als ISB

27.3 Praxisbeispiel: Büroschlüssel mit Stechuhrfunktion

27.4 Ihre Aufgabe als ISB

28. **Internes Audit**

28.1 Praxisbeispiel: Entwendetes Zertifikat

28.2 Ihre Aufgabe als ISB

28.3 Praxisbeispiel: Port-Scan

28.4 Ihre Aufgabe als ISB

29. **Managementbewertung**

29.1 Praxisbeispiel: Managementbericht vom ISB

29.2 Ihre Aufgabe als ISB

30. **Schlusswort**