

Jacqueline Naumann

The full force of ISO 27001

Your appointment as
Information Security
Officer (ISO)



Utilities Information Security incidents Supplier relationships Software
Development Monitoring User registration Backup vault Disposal
Administrator Wiring Power supply Access control Logging Screen lock
Privacy Passwords SoA Backup



Kurzüberblick

1. **Introduction**
2. **Appointment as ISO**
3. **Expectations of interested parties**
4. **Verwaltung der Werte**
5. **Risk analysis**
6. **SoA**
7. **Human Resources Security**
8. **Information security incidents**
9. **Supplier relationships**
10. **Malware**
11. **Logging**
12. **Backup**
13. **Screen lock**
14. **Entry control**
15. **Disposal**
16. **Software Development**
17. **Documented business processes**
18. **Contact with public authorities**
19. **Safe development**
20. **User registration and deregistration**

21. **Privacy**
22. **Utilities**
23. **Uninterruptible power supply**
24. **Passwords**
25. **Devices and operational means**
26. **Physical and environmental security**
27. **Monitoring**
28. **Internal audit**
29. **Management evaluation**
30. **Closing statement**

Dear reader,

Thank you for selecting this book.

Information security is currently a hot topic that has picked up speed, in particular due to the new IT Security Act.

Dear Information Security Officer, I hope that this book can offer you the succour you need to tackle your new tasks diligently and enthusiastically.

Yours sincerely, Jacqueline Naumann

Trainer, Consultant, Auditor of iXactly IT and System Consulting



iXactly is your service provider for seminars, consultancy and audits for your ISMS.

Gostritzer Straße 61, 01217 Dresden, Germany

Many thanks

to Florentine Naumann for the illustrations in the book!

Inhalt

1. **Introduction**

- 1.1 Get acquainted with the ISO in the book at hand
- 1.2 Anonymity
- 1.3 Symbolism of the sword

2. **Appointment as ISO**

- 2.1 Real life example: Black Peter - the blame-the-other one game
- 2.2 Your remit as ISO
- 2.3 Real life example: New job with ISO role
- 2.4 Real life example: ISO without being appointed
- 2.5 Your remit as ISO

3. **Expectations of interested parties**

- 3.1 Real life example: Small print in the contract
- 3.2 Your remit as ISO

4. **Verwaltung der Werte**

- 4.1 Real life example: Multifunctional device
- 4.2 Your remit as ISO
- 4.3 Real life example: Numbered tables
- 4.4 Your remit as ISO

5. **Risk analysis**

5.1 Real life example: Compliance lawyer

5.2 Your remit as ISO

5.3 Real life example: Risk: Local admin accounts

5.4 Your remit as ISO

6. **SoA**

6.1 Real life example: No SoA for the Auditor

6.2 Ihre Aufgabe als ISB

7. **Human Resources Security**

7.1 Real life example: Job specifications

7.2 Your remit as ISO

7.3 Real life example: Video Streaming

7.4 Your remit as ISO

8. **Information security incidents**

8.1 Real life example: Missing Laptops

8.2 Your remit as ISO

8.3 The information security incident log

9. **Supplier relationships**

9.1 Real life example: Trust is good

9.2 Your remit as ISO

10. **Malware**

10.1 Real life example: Job applicant mails

10.2 Your remit as ISO

10.3 Praxisbeispiel: Real life example: E-mails from the police Office

10.4 Praxisbeispiel: Real life example: Fake e-mails from colleagues

10.5 Your remit as ISO

11. **Logging**

11.1 Real life example: Logging

11.2 Ihre Aufgabe als ISB

11.3 Real life example: Log files

11.4 Your remit as ISO

12. **Backup**

12.1 Real life example: Backup copies

12.2 Your remit as ISO

12.3 Real life example: Backup vault

12.4 Your remit as ISO

12.5 Real life example: Administrator proxy

12.6 Your remit as ISO

13. **Screen lock**

13.1 Real life example: Screen lock

13.2 Your remit as ISO

14. **Entry control**

14.1 Real life example: Nibbling landlord

14.2 Your remit as ISO

14.3 Real life example: Skimpy licensing

14.4 Your remit as ISO

14.5 Real life example: Trust in service providers

14.6 Your remit as ISO

14.7 Real life example: Comprehensive bunch of keys

14.8 Your remit as ISO

14.9 Real life example: Open barriers

14.10 Your remit as ISO

14.11 Real life example: Data projector not working

14.12 Your remit as ISO

15. **Disposal**

15.1 Real life example: Sale of servers on IT sales platforms

15.2 Real life example: Free of charge disposal of servers

15.3 Your remit as ISO

15.4 Praxisbeispiel: Personalakte im blauen Sack

15.5 Your remit as ISO

16. **Software Development**

16.1 Real life example: Ban on TRY-CATCH

16.2 Your remit as ISO

16.3 Real life example: Tool particularly complicated

16.4 Your remit as ISO

16.5 Real life example: Software tested until corrupt

16.6 Your remit as ISO

16.7 Real life example: Qualified tester

16.8 Your remit as ISO

17. **Documented business processes**

17.1 Real life example: Database too complex

17.2 Your remit as ISO

18. **Contact with public authorities**

18.1 Real life example: Annoying Data Protection Officer

18.2 Your remit as ISO

18.3 Real life example: E-mail forwarding

18.4 Your remit as ISO

19. **Safe development**

19.1 Real life example: Go-Live without testing

19.2 Your remit as ISO

19.3 Real life example: Go-Live in the test system

19.4 Your remit as ISO

20. **User registration and deregistration**

20.1 Real life example: Who knows T34M-ADMIN2

20.2 Your remit as ISO

21. **Privacy**

21.1 Real life example: No user drives

21.2 Your remit as ISO

21.3 Real life example: Chat monitoring

21.4 Your remit as ISO

21.5 Real life example: Blind Copy mails

21.6 Your remit as ISO

22. **Utilities**

22.1 Real life example: Dripping air conditioning

22.2 Your remit as ISO

22.3 Real life example: Well filled cable duct

22.4 Your remit as ISO

23. **Uninterruptible power supply**

23.1 Real life example: Diesel supplies

23.2 Your remit as ISO

24. **Passwords**

24.1 Real life example: 3-digit password

24.2 Your remit as ISO

24.3 Real life example: Two password policies

24.4 Your remit as ISO

24.5 Real life example: Task sharing for passwords

24.6 Your remit as ISO

25. **Devices and operational means**

25.1 Real life example: Rolling cabinets

25.2 Your remit as ISO

25.3 Real life example: Weathered letter

25.4 Your remit as ISO

25.5 Real life example: Private PCs as a gift

25.6 Your remit as ISO

26. **Physical and environmental security**

26.1 Real life example: Misleading designation

26.2 Your remit as ISO

27. **Monitoring**

27.1 Real life example: Video surveillance

27.2 Your remit as ISO

27.3 Real life example: Office key with time clock function

27.4 Your remit as ISO

28. **Internal audit**

28.1 Real life example: Stolen certificate

28.2 Your remit as ISO

28.3 Real life example: Port scan

28.4 Your remit as ISO

29. **Management evaluation**

29.1 Real life example: Management report prepared by the ISO

29.2 Your remit as ISO

30. **Closing statement**