



Jacqueline Naumann

Die ganze Härte der ISO 27001

Ihr Kampf als
Informationssicherheits-
beauftragter (ISB)

Kommunikation Dokumentenlenkung Sicherheitsbereiche Ressourcen
Transport Politik Audit ISMS Scope Beweismittel Hochverfügbarkeit Drucker
Kontext Richtlinien Vertraulichkeit Betriebsmittel Monitoring Freigabe



Kurzüberblick

1. Einleitung
2. Kontext der Organisation
3. Anwendungsbereich
4. Führungsaufgaben
5. Ressourcen
6. Informationssicherheits-Richtlinien
7. Dokumentenlenkung
8. Sicherheitsbereiche
9. Softwareentwicklung
10. Unterbrechungsfreie Stromversorgung
11. Privatsphäre
12. Geräte und Betriebsmittel
13. Unbeaufsichtigte Benutzergeräte
14. Vertraulichkeit
15. Sammeln von Beweismitteln
16. Hochverfügbarkeit
17. Kommunikation
18. Sicherheit der Verkabelung
19. Informationssicherheitsereignisse
20. Videoüberwachung
21. Monitoring
22. Entsorgung von Datenträgern
23. Maßregelung

24. Sicherheit von Netzwerkdiensten
25. SoA - Statement of Applicability
26. Sichere Anmeldeverfahren
27. Maßnahmen gegen Schadsoftware
28. Datenschutz
29. Zertifizierungsaudit
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 wertvolle Praxisbeispiele bieten, die Sie für Ihre Aufgaben nutzen 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

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
 - 1.3 Die Schwert-Symbolik
2. Kontext der Organisation
 - 2.1 Praxisbeispiel: PowerPoint-Präsentation
 - 2.2 Ihre Aufgabe als ISB
3. Anwendungsbereich
 - 3.1 Praxisbeispiel: Trägerischer Scope
 - 3.2 Praxisbeispiel: Zertifikats-Scope
 - 3.3 Praxisbeispiel: Empfohlener Übungs-Scope
 - 3.4 Ihre Aufgabe als ISB
4. Führungsaufgaben
 - 4.1 Praxisbeispiel: Keine Freigabe vom BO\$\$
 - 4.2 Ihre Aufgabe als ISB
 - 4.3 Praxisbeispiel: Sorge vor eigener Politik
 - 4.4 Ihre Aufgabe als ISB
5. Ressourcen
 - 5.1 Praxisbeispiel: 10% zeitliche Ressourcen
 - 5.2 Ihre Aufgabe als ISB
 - 5.3 Praxisbeispiel: ISMS-Projektleiter
 - 5.4 Ihre Aufgabe als ISB

6. Informationssicherheits-Richtlinien
 - 6.1 Praxisbeispiel: Dokumente für die Schublade
 - 6.2 Ihre Aufgabe als ISB
 - 6.3 Praxisbeispiel: Dokumente aus dem Internet
 - 6.4 Ihre Aufgabe als ISB
7. Dokumentenlenkung
 - 7.1 Praxisbeispiel: Redundante Datumsangaben
 - 7.2 Praxisbeispiel: Fehlendes Freigabedatum
 - 7.3 Ihre Aufgabe als ISB
 - 7.4 Praxisbeispiel: Unauffindbare Belehrungen
 - 7.5 Ihre Aufgabe als ISB
8. Sicherheitsbereiche
 - 8.1 Praxisbeispiel: Angemietete Räume
 - 8.2 Ihre Aufgabe als ISB
9. Softwareentwicklung
 - 9.1 Praxisbeispiel: Transport von Software
 - 9.2 Ihre Aufgabe als ISB
10. Unterbrechungsfreie Stromversorgung
 - 10.1 Praxisbeispiel: Wöchentliche Stromausfälle
 - 10.2 Ihre Aufgabe als ISB
11. Privatsphäre
 - 11.1 Praxisbeispiel: Veröffentlichte Forenbeiträge
 - 11.2 Ihre Aufgabe als ISB
12. Geräte und Betriebsmittel
 - 12.1 Praxisbeispiel: Brandlast hinter Serverschrank
 - 12.2 Ihre Aufgabe als ISB
 - 12.3 Praxisbeispiel: Inergen-Löschanlage

12.4 Ihre Aufgabe als ISB

13. Unbeaufsichtigte Benutzergeräte

13.1 Praxisbeispiel: Ausdruck im Multifunktionsgerät

13.2 Praxisbeispiel: Kunden-Angebot im Drucker

13.3 Ihre Aufgabe als ISB

14. Vertraulichkeit

14.1 Praxisbeispiel: Rezepte am offenen Fenster

14.2 Ihre Aufgabe als ISB

15. Sammeln von Beweismitteln

15.1 Praxisbeispiel: Unvollständige Störungsprotokolle

15.2 Ihre Aufgabe als ISB

16. Hochverfügbarkeit

16.1 Praxisbeispiel: Hochverfügbares Internetportal

16.2 Ihre Aufgabe als ISB

17. Kommunikation

17.1 Praxisbeispiel: Unzuverlässige Kommunikation

17.2 Ihre Aufgabe als ISB

17.3 Praxisbeispiel: Lieferanten-Forderung

17.4 Ihre Aufgabe als ISB

18. Sicherheit der Verkabelung

18.1 Praxisbeispiel: Rechenzentrum-Neubau

18.2 Ihre Aufgabe als ISB

19. Informationssicherheitsereignisse

19.1 Praxisbeispiel: Gehackter Computer

19.2 Ihre Aufgabe als ISB

19.3 Praxisbeispiel: Herabfallende Deckenplatten

- 19.4 Ihre Aufgabe als ISB
- 20. Videoüberwachung
 - 20.1 Praxisbeispiel: Überwachung rund um die Uhr
 - 20.2 Ihre Aufgabe als ISB
- 21. Monitoring
 - 21.1 Praxisbeispiel: Bitcoin-Mining
 - 21.2 Ihre Aufgabe als ISB
- 22. Entsorgung von Datenträgern
 - 22.1 Praxisbeispiel: Überfüllter Sicherheitscontainer
 - 22.2 Ihre Aufgabe als ISB
- 23. Maßregelung
 - 23.1 Praxisbeispiel: Maßregelungsprozess
 - 23.2 Ihre Aufgabe als ISB
- 24. Sicherheit von Netzwerkdiensten
 - 24.1 Praxisbeispiel: WLAN für Jalousien und Beleuchtung
 - 24.2 Ihre Aufgabe als ISB
- 25. SoA - Statement of Applicability
 - 25.1 Praxisbeispiel: Streng geheime SoA
 - 25.2 Ihre Aufgabe als ISB
- 26. Sichere Anmeldeverfahren
 - 26.1 Praxisbeispiel: 3-Faktor-Authentifizierung
 - 26.2 Ihre Aufgabe als ISB
- 27. Maßnahmen gegen Schadsoftware
 - 27.1 Praxisbeispiel: Angebliche Privataufnahmen
 - 27.2 Ihre Aufgabe als ISB
- 28. Datenschutz

28.1 Praxisbeispiel: Fehlendes Datenschutzrisiko

28.2 Ihre Aufgabe als ISB

29. Zertifizierungsaudit

29.1 Praxisbeispiel: Geschenktes Zertifikat

29.2 Ihre Aufgabe als ISB

29.3 Praxisbeispiel: 11 Zeichen Passwortlänge

29.4 Ihre Aufgabe als ISB

30. Schlusswort

Ihre Aufgaben als ISB sind nicht immer einfach

Ihr Kampf als ISB

1 Einleitung

Nach Ihrer Ernennung oder Berufung zum Informationssicherheitsbeauftragten mussten Sie sicherlich so einige Kämpfe austragen. Alle ISBs, mit denen ich bisher gesprochen habe, bestätigten mir dies.

Einige leiden in ihrer Rolle, andere hingegen sehen die Herausforderungen, die ein ISMS-Aufbau mit sich bringt als Chancen.

Xavier Naidoo fand in seinem Song *Dieser Weg* eine Beschreibung, die auch auf den Weg eines ISBs zutreffen könnte:

„Dieser Weg wird kein leichter sein, dieser Weg wird steinig und schwer.“

ISO/IEC 27001 [Kap. 10.2](#) Fortlaufende Verbesserung

Auch wenn Sie glauben, Ihr ISMS vollständig aufgebaut zu haben, erlaubt Ihnen die ISO 27001 gar keine Fertigstellung. Diese Norm-Anforderung finden Sie im [Kapitel 10.2 Fortlaufende Verbesserung](#). Das heißt, die Norm fordert uns auf, das ISMS in seiner Ausprägung fortlaufend weiter zu verbessern.

Mit diesem Buch will ich Ihnen deshalb wieder eine Reihe Praxisbeispiele vorstellen, anhand derer Sie möglicherweise neuen Input für Ihre Verbesserungen erhalten.

1.1 Bekanntmachung mit unserem Buch-ISBN

Leser des ersten Bandes kennen unseren Buch-ISBN und seine Mitmenschen bereits. Für alle anderen, die mit diesem Band in die Reihe *Die ganze Härte der ISO 27001* einsteigen, werden die Personen des Buches in den folgenden Zeilen kurz erläutert.

Im Buch werden viele Praxisbeispiele aus tatsächlich stattgefundenen Begebenheiten wiedergegeben. Um die Anonymität zu gewährleisten, nutze ich sogenannte schwarze Schafe, denen ich alle Kuriositäten unterschiebe.

Mein schwarzes Schaf für unsere fiktive Organisation T34M heißt im Buch T34M-L34D. Bei T34M handelt es sich um eine fiktive Organisation, die unter anderem Nachrichten produziert sowie zu den KRITIS (kritische Infrastrukturen) im Bereich Medien zählt, von denen das neue IT-Sicherheitsgesetz fordert, ein ISMS aufzubauen.

Bei dem ISB, der im Buch interviewt wird oder einfach Tatsachen erzählt, handelt es sich um T34M-L34D.

Die Organisation hatte bei ihrer Gründung Freude daran, die Buchstaben E durch 3 und A durch 4 zu ersetzen, so wie es einige angehende Hacker in der Sprache Leet tun.

T34M-L34D steht stellvertretend für hunderte Kunden, Kollegen, Mitarbeiter und Seminarteilnehmer, mit denen ich in den mittlerweile über 16 Jahren gesprochen oder denen ich einfach nur zugehört habe.

T34M-L34Ds Erzählungen sind Praxisbeispiele, die Ihnen, in Ihrer Rolle als ISB zeigen sollen, dass sich in allen