Innovative Lösungen
nicht nur für den Mittelstand

ProQVis GmbH
Unteranger 24a
D-85244 Röhrmoos

+49 (0)8139-20 42 600
+49 (0)8139-20 42 681
+49 (0)176-11 39 32 37
Kundenservice@proqvis.com

DOKUMENTATION ZU ISO 27001:2013

Obligatorische dokumentierte Information für ISO 27001:2013

Einer der ersten Fragen, die Kunden stellen, wenn es um die Implementierung eines ISO 27001-Managementsystems geht, ist, wie viele Dokumente erstellt werden müssen um die Zertifizierung zu bestehen. Wenn die Beratung so anfängt, muss dem Kunden zuerst die Illusion genommen werden, dass er mehr spart, wenn nur die Zertifizierung beabsichtigt wird. Es ist fast unmöglich die Zertifizierung zu erlangen und über die Jahre zu behalten, wenn die Sache so betrachtet wird. Ein korrekt implementiertes ISMS wird Ihnen viel mehr (er)sparen, als es kostet. Andere vermuten, dass der Aufwand anhand der zu erstellenden Dokumente gemessen werden kann. Bitte berücksichtigen Sie, dass die zu erstellende Information in unterschiedlichen oder in gleichen Dokumenten abgelegt werden kann, oder sogar in einem CMS (Content Management System). Weiterhin ist die Risikobedarfsanalyse und die Implementierung von Maßnahmen die Umfangreicheren Anteile und nicht die Dokumentinformation. Also ist es schwierig die Mange an Aufwand anhand der Menge an generierten Dokumente zu messen. Nichtsdestotrotz können Sie davon ausgehen, welche Information Sie unbedingt betrachten sollten. Ich stelle hier eine Liste dar anhand der Normabschnitte. Ich liste nicht nur die obligatorischen, sondern auch die am häufigsten verwendeten für die Implementierung dar.

Obligatorische Unterlagen gemäß ISO 27001: 2013

Hier sind die Dokumente, die Sie erstellen müssen, wenn Sie mit ISO 27001 konform sein möchten:

*(*Bitte beachten Sie, dass Dokumente aus Anhang A nur dann zwingend vorgeschrieben sind, wenn Risiken vorliegen, die ihre Umsetzung erfordern würden).*

1. Geltungsbereich des ISMS (Abschnitt 4.3)
2. Grundsätze und Ziele der Informationssicherheit (Ziffern 5.2 und 6.2)

Geschäftsführer: Eduard Weber Handelsregister: Amtsgericht München, HRB 216091, Sitz Röhrmoos
USt-IdNr.: DE298119044 St.-Nr.: 115/135/41459
Bankverbindung: Deutsche Bank Privat- und Geschäftskunden AG, München
IBAN: DE33700700240056030000 BIC/SWIFT: DEUTDEDBMUC

3. Risikobewertung und Methoden der Risikobetrachtung (Abschnitt 6.1.2)
4. Geltungsbereich (Ziffer 6.1.3 d)
5. Risikoplan (Ziffern 6.1.3 e und 6.2)
6. Risikobewertungsbericht (Abschnitt 8.2)
7. Definition der Sicherheitsrollen und Zuständigkeiten (Klauseln A.7.1.2 und A.13.2.4)
8. Vermögensbestand (Abschnitt A.8.1.1)
9. Angemessene Verwendung von Vermögenswerten (Abschnitt A.8.1.3)
10. Zugangskontrollrichtlinie (Abschnitt A.9.1.1)
11. Betriebsverfahren für das IT-Management (Abschnitt A.12.1.1)
12. Sichere systemtechnische Grundsätze (Abschnitt A.14.2.5)
13. Lieferanten-Sicherheitspolitik (Abschnitt A.15.1.1)
14. Verfahren der Störungsbehebung (Abschnitt A.16.1.5)
15. Geschäftskontinuitätsverfahren (Abschnitt A.17.1.2)
16. Gesetzliche, regulatorische und vertragliche Anforderungen (Klausel A.18.1.1)

Obligatorischen Aufzeichnungen:

17. Aufzeichnungen über Ausbildung, Fertigkeiten, Erfahrung und Qualifikationen (Ziffer 7.2)
18. Überwachungs- und Messergebnisse (Abschnitt 9.1)
19. Interne Audit-Programm (Abschnitt 9.2)
20. Ergebnisse der internen Audits (Ziffer 9.2)
21. Ergebnisse der Managementbewertung (Ziffer 9.3)
22. Ergebnisse von Korrekturmaßnahmen (Abschnitt 10.1)
23. Protokolle von Benutzeraktivitäten, Ausnahmen und Sicherheitsereignissen (Klauseln A.12.4.1 und A.12.4.3)

Unverbindliche Unterlagen

Es gibt viele andere Dokumente, die für die ISO 27001-Implementierung verwendet werden, obwohl sie nicht von der Norm gefordert werden, insbesondere für die Sicherheitskontrollen aus Anhang A:

Geschäftsführer: Eduard Weber Handelsregister: Amtsgericht München, HRB 216091, Sitz Röhrmoos
USt-IdNr.: DE298119044 St.-Nr.: 115/135/41459
Bankverbindung: Deutsche Bank Privat- und Geschäftskunden AG, München
IBAN: DE33700700240056030000 BIC/SWIFT: DEUTDEDBMUC

24. Verfahren zur Dokumentensteuerung (Abschnitt 7.5)
25. Steuerelemente für die Verwaltung von Datensätzen (Abschnitt 7.5)
26. Verfahren für die interne Revision (Ziffer 9.2)
27. Maßnahmen zur Abhilfe (Ziffer 10.1)
28. Bringen Sie Ihr eigenes Gerät (BYOD) Politik (Abschnitt A.6.2.1)
29. Mobilfunk- und Telearbeitspolitik (Abschnitt A.6.2.1)
30. Informationsklassifizierungsrichtlinie (Klauseln A.8.2.1, A.8.2.2 und A.8.2.3)
31. Kennwortrichtlinien (Klauseln A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1 und A.9.4.3)
32. Entsorgungs- und Vernichtungspolitik (Klauseln A.8.3.2 und A.11.2.7)
33. Verfahren zum Arbeiten in sicheren Bereichen (Abschnitt A.11.1.5)
34. Clear Desk und Clear Screen-Politik (Abschnitt A.11.2.9)
35. Änderungsmanagementpolitik (Klauseln A.12.1.2 und A.14.2.4)
36. Sicherungsrichtlinie (Abschnitt A.12.3.1)
37. Informationsaustausch-Politik (Klauseln A.13.2.1, A.13.2.2 und A.13.2.3)
38. Wirtschaftliche Folgenabschätzung (Klausel A.17.1.1)
39. Ausübungs- und Prüfungsplan (Abschnitt A.17.1.3)
40. Wartungs- und Überprüfungsplan (Abschnitt A.17.1.3)
41. Business-Continuity-Strategie (Abschnitt A.17.2.1)

Ob das viel oder wenig ist, überlasse ich jedem einzelnen zu beurteilen. Nutzen Sie diese Liste als Quelle für Ihre Vollständigkeit.

Weitere Fragen beantworten wir Ihnen gerne!
Schreiben Sie uns ✉ Kundenservice@proqvis.com oder
rufen Sie uns gleich an: **08139/2042-600**

Geschäftsführer: Eduard Weber **Handelsregister:** Amtsgericht München, HRB 216091, Sitz Röhrmoos
USt-IdNr.: DE298119044 **St.-Nr.:** 115/135/41459
Bankverbindung: Deutsche Bank Privat- und Geschäftskunden AG, München
IBAN: DE33700700240056030000 **BIC/SWIFT:** DEUTDEDBMUC