ISO 27001:2013 Implementierung

Schritt für Schritt

Dieser Weg führt Sie schnell ins Ziel

ProQVis®
THE ENTERPRISE TAILORS

von Eduard Weber

ProQVis®
THE ENTERPRISE TAILORS

ISO 27001 Implementierung Schritt für Schritt - In 12 Schritten schnell ins Ziel - Ein Leitfaden

ISO 27001 Implementierung Schritt für Schritt

In 12 Schritten schnell ins Ziel

Was zeige ich in diesem Artikel?

Dieser Artikel zeigt, die grundsätzliche Vorgehensweise zur Implementierung eines Informationssicherheitsmanagementsystems (ISMS) nach der Norm ISO 27001.

Hallo, ich bin Eduard Weber

Wenn Sie vorhaben ISO 27001 schnell und einfach zu implementieren, dann muss ich Sie fast schon enttäuschen. Diese zwei Begriffe sind relativ. Ich werde Ihnen jedoch helfen die Vorgehensweise leicht zu überblicken. Sie werden hier erfahren, welche 12 Schritte und 4 Phasen Sie gehen können, um relativ leicht an das Zertifikat zu gelangen.

Wir sind spezialisiert auf Kleinunternehmen und mittelständische Unternehmen, diese Schritte sind jedoch gleich bei jeder Unternehmensgröße. Den Unterschied macht es die Detaillierung und die Menge der Fälle die vom Unternehmen zu Unternehmen betrachtet werden müssen, Anzahl der Assets, die Tiefe der Betrachtung, usw.

Mein Name ist Eduard Weber. Ich bin ein passionierter Prozess- und Prozesseffizienz-Berater, ISO-Berater, Qualitätsmanager und Auditor. Wir bieten mit meinem Unternehmen ProQVis GmbH Lösungen im Bereich Unternehmensorganisation, -Optimierung und Geschäftsprozessgestaltung und Vorbereitung auf ISO-Zertifizierungen an. Ich möchte Ihnen mit diesem Dokument einen Leitfaden an die Hand geben, mit dem Sie sich ein gutes Bild über die

Aktivitäten machen können, die bei der Implementierung eines ISMS nach ISO 27001 nötig sind.

Vorteile eines ISMS

Sicherlich habe Sie schon mal davon gehört, das ISO 27001 bzw. ein entsprechendes Managementsystem viele Vorteile bezüglich der Sicherheit von Informationen und Daten bietet. Das sind aber nur sehr vage Aussagen, die zwar gänzlich stimmen, aber nicht detailliert genug sind um die Vorteile tatsächlich auch zu begreifen. Lassen Sie mich hier nur einige mehr aufzuführen.

1 Million Schaden abwehren

Es gibt Statistiken die zeigen, daß eine Sicherheitslücke Organisationen im Durchschnitte 1 Million Dollar kosten. Sicherlich ist das abhängig von den Informationen und Daten, die die Organisation besitzt und schützen müsste. Auch Faktoren wie Eintrittswahrscheinlichkeit, mildern die Schärfe dieser Möglichkeit. Nichtsdestotrotz ist eine angemessene Absicherung immer von Vorteil. ISO 27001 ermöglicht diesen Schutz sehr effektiv.

80% mehr Vertrauen

Ein etabliertes Informationssicherheitsmanagementsystem schafft, wie jedes Managementsystem, ein höheres Vertrauen der Kunden, dass ihre Daten vertraulich und geschützt gehandelt werden.

75% niedrigeres Geschäftsrisiko

Sie können einfach nicht vorsichtig genug sein, wenn es um den Schutz persönlicher Aufzeichnungen und sensibler Informationen geht. ISO / IEC 27001 hilft Ihnen, einen robusten und systematischen Ansatz für die Verwaltung von Informationen zu implementieren und den Ruf Ihrer Organisation zu schützen.

71% besserer Schutz für Ihr Unternehmen (Reputation)

Durch das Identifizieren und Steuern von Risiken unter Bewertung der Wirksamkeit ihres Systems können Sie plötzlich auftretende neue Bedrohungen besser begegnen und abwehren. Durch passende Kontrollen schützen Sie ihr Unternehmen von Angriffen und potenziellen Auswirkungen auf Ihr Unternehmen. Dies wird helfen, Ihre Organisation belastbar zu halten und Ihre Reputation zu behalten.

55% bessere Erfüllung von Gesetze u. Normen (Compliance)

ISO 27001 gibt Ihnen einen Rahmen, der Ihnen hilft, Ihre gesetzlichen und regulatorischen Anforderungen zu verwalten. Er fordert das Überprüfen und Kommunizieren ihrer regulatorischen Anforderungen an ihre interessierten Parteien. Das verringert die Wahrscheinlichkeit von Geldstrafen oder Strafverfolgung und hilft Ihnen, die relevanten Gesetze einzuhalten und sicherzustellen, dass Sie immer auf dem Laufenden bleiben.

53% Verbesserung Ihrer Wettbewerbsposition

Wie jeder implementierte Standard, erlaubt es ISO 27001 durch die Gesamtheit der Vorteile Ihr Unternehmen besser am Markt zu positionieren. Das bewirkt nicht nur die Präsentation des ISMS bzw. des Zertifikates nach draußen, sondern die durch die Anforderungen der Norm getroffenen Maßnahmen im Unternehmen.

50% niedrigere Fehler-Wahrscheinlichkeit

ISO / IEC 27001 hilft, ein besseres Risikomanagement zu etablieren, damit die Unternehmen sicherer und belastbarer zu machen und auf Bedrohungen der Informationssicherheit besser zu reagieren. Es hilft also, Ihr Unternehmen sicher zu halten, damit Sie sich auf das Alltagsgeschäft konzentrieren, während Sie den Kunden und Lieferanten Ihr Engagement für den Schutz ihrer Informationen deutlich zeigen.

In der heutigen stark vernetzten Welt ist **Effizienz und Sicherheit eine Muss-Anforderung**. Mit jedem neuen Tag ist Schutz der Daten immer wichtiger, denn:

- **75% der Organisationen glauben nicht, dass ihre Geschäftsdaten vollständig sicher sind**
  (NTT Com Security 2016, Bericht über Risikobewertung)
- **90% der Organisationen hatten einen Sicherheitsvorfall im Jahr 2014**
  (PWC 2015, Bericht über Verletzungen der Informationssicherheit)
- **$ 400 Mrd. geschätzten Kosten für Cybercrime**
  (McAfee Schadensbericht, Juni 2014)

Einführungsphasen

Wenn Sie ein Managementsystem für Informationssicherheit implementieren und zertifizieren wollen, sind im Grunde 3 große Phasen zu durchlaufen:

Information

In dieser Phase wird Information beschafft um sich ein Bild zu machen und dann das Management zu überzeugen bzw. zu Informieren und das Commitment zu sichern. ISO / IEC 27001 ist ein international anerkannter Best Practice Rahmen für ein Informationssicherheitsmanagementsystem (ISMS). Es hilft Ihnen, Risiken zu identifizieren und stellt Sicherheitsmaßnahmen, die für Ihr Unternehmen richtig sind, so dass Sie verwalten oder zu reduzieren Risiken für Ihre Informationen. Wie holen Sie sich die ersten Informationen:

- Sie kaufen den Standard, lesen es und versuchen den Inhalt und die Vorteile zu verstehen.

- Klären Sie den Bedarf und sichern Sie das Einverständnis der Unternehmensführung

✓ **Für beide Punkte können Sie uns fragen und sich Unterstützung holen.**

Implementierung

In dieser Phase wird das System definiert, implementiert und etabliert.

- Laden Sie unsere Checkliste zur GAP-Analyse aus dem Internet herunter und versuchen Sie zu prüfen, was Sie noch zu tun haben, oder rufen Sie uns dazu.
- Stellen Sie sicher, daß alle Mitarbeiter den Sinn und die Prinzipien der Informationssicherheit und der Norm, wie auch ihre Rolle im System verstehen. Schulen sie ihre Mitarbeiter oder lassen Sie sie durch uns schulen.
- Führen Sie die Implementierung schrittweise durch.

✓ **Hier können Sie sich jetzt ebenfalls unser Rat und Unterstützung sehr günstig sichern.**

Zertifizierung

Mit der ISO 27001-Zertifizierung, können Sie Kunden, Partnern und andern interessierten Parteien Ihr Engagement für die sichere Verwaltung von Informationen beweisen. Es ist eine große Gelegenheit, Ihre Leistung zu bewerben, Ihr Geschäft zu fördern und zu zeigen, dass Sie eine vertrauenswürdige Organisation sind, was neue Geschäftsmöglichkeiten eröffnet.

Nach einer ersten Untersuchung, einer sogenannten GAP-Analyse, ob das implementierte System zertifizierungsfähig ist und was noch zur Ergänzung getan werden muss um eine Zertifizierung nach ISO 27001 zu bestehen. Wenn alles bereit steht erfolgt ein Zertifizierungsaudit einer akkreditierten Gesellschaft Ihrer Wahl und Ihr Unternehmen wird nach einem

erfolgreichen Audit zertifiziert.

Nach der Zertifizierung sind Sie aber nicht am Ende der Sicherheitsmaßnahmen. Die Sicherheit müssen Sie regelmäßig intern begutachten, bewerten und bei Bedarf Verbesserungsmaßnahmen ergreifen. Das Zertifikat selbst gilt 3 Jahre lang. In dieser Zeit finden jährlich Überwachungsaudits und am Ende der Periode eine Re-Zertifizierung statt.

✓ **Wir beraten Sie gerne bei der Suche nach der passenden Zertifizierungsgesellschaft.**

Fair QMS für KMU

Wussten Sie, dass 2012 laut der IfM in Bonn 99,6% der Unternehmen in Deutschland zu KMU gehören?

Ich habe die Initiative FairQMS ins Leben gerufen um kleineren und mittelgroßen Unternehmen duch ISO-Standards und günstigen Lösungen eine bessere Marktpositionierung zu ermöglichen.

Ihre nächsten Schritte

Egal ob Sie eine Implementierung oder eine Verbesserung Ihres Managementsystems anstreben, wenden Sie sich bei Fragen an unser Expertenteam. Sie erhalten Rat und Orientierungshilfen, mit denen Sie Ihre Ziele erreichen. Planen Sie zum Beispiel mit uns Ihr erstes unabhängiges Assessment zur Erörterung Ihres Status.

Schreiben Sie uns
Kundenservice@proqvis.com
oder rufen Sie uns gleich
an: **08139/2042-600**

Implementierungsschritte

VORBEREITUNG

1. Leadership und Planung

Vorausgesetzt, Sie haben das gesamte obere Management für das Projekt der Implementierung gewonnen, können Sie zur Implementierung schreiten. Sie können um das Management auszurichten die Informationen aus dem Kapitel „Vorteile“ nützen und ggf. auch das Ergebnis einer Selbstuntersuchung mittels der GAP-Analyse.

Sobald Sie die Entscheidung getroffen/erhalten haben dieses Managementsystem zu implementieren können Sie ein Projektplan aufsetzen. Die einzelnen Schritte können Sie aus der Abbildung der Implementierungsschritte entnehmen. Nehmen Sie sich genügend Zeit für die Implementierung, planen Sie die Ressourcen und ihre Einbindung und stellen Sie ihre Verfügbarkeit für dieses Projekt sicher.

Definieren Sie genau, was zu tun ist und in welchem Zeitrahmen. Tun sie das nicht, so wird

Ihr Projekt verzögert aufgrund der höheren Priorität der Alltagsaktivitäten der Teilnehmer. Sorgen Sie dafür, dass alle Teilnehmer zusammenwirken und keine Insel-Projekte entstehen. Planen Sie konkret und setzen sie die Priorität hoch. Dieser Plan kann später als Risikobehandlungsplan weitergeführt werden.

GELTUNGSBEREICH FESTLEGEN

2. Definieren des Geltungsbereiches

Um den Geltungsbereich zu definieren, müssen Sie ein Bild der Organisation besitzen mit Organigramm, Abteilungen, usw. und also alle wichtigen interessierten Parteien kennen. Es stellt sich die Frage, welche Organisationseinheiten, Prozesse, Informationsflüsse (Datenflüsse), welche Anforderungen und welche externe Einflussfaktoren in der Implementierung berücksichtigt werden sollten. Je größer Ihre Organisation, desto eher kann es sein, daß Sie ISO 27001 nur für bestimmte Bereiche implementieren wollen. Dabei kann eine Kapselung nach außen sehr schwierig sein. Sie müssen konkret alle Schnittstellen der Anwendungsbereiche prüfen auf eine nachrangige Verbindung nach Außen und entsprechend Vereinbarungen (SLA, OLA, LOI, etc.) zur Regelung treffen.

3. ISMS Sicherheitsrichtlinie und Ziele definieren

Da ein Managementsystem eine Dokumentation impliziert, sollten Sie sich bereits am Anfang Gedanken darüber machen, welche Form diese haben sollte. Als zentrales Dokument des ISMS beinhaltet die **Leitlinie der Informationssicherheit**:

- die Benennung der Sicherheitsziele bzw. einer Methodik, um diese zu definieren, festzulegen, zu messen und ihre Realisierung zu planen,
- die Selbstverpflichtung zur Informationssicherheit in der Organisation und

- die Selbstverpflichtung zur kontinuierlichen Verbesserung des ISMS

Die ISMS Sicherheitsrichtlinie muss nicht sehr detailliert sein, aber es sollte die wichtigsten grundlegenden Fragen für die Informationssicherheit in Ihrer Organisation definieren. Darin sollte das Management definieren, was es erreichen und wie es das kontrollieren will.

Die Dokumentationsstruktur und das Richtlinienrahmenwerk bauen Sie vom Anfang an mit auf und ergänzen es schrittweise in den kommenden Schritten.

SCHUTZBEDARF FESTSTELLEN

4. Asset-Register erstellen

Das Asset-Register ermöglicht systematisch alle schutzbedürftigen Geschäftsinformationen (primäre Assets) und Unterstützungseinrichtungen (IT-Systeme, Arbeitsmittel, Mitarbeiter) zu erfassen und zu bewerten.

Die sogenannte Wirkungskette zwischen den Assets kann gut mit einer Excel-Datei dokumentiert werden.

5. Schutzbedarfsanalyse definieren

Die Risikobewertung, bzw. eine Gefährdungsanalyse ist einer der komplexesten Aufgaben im ISMS. Hier müssen Sie die Regeln für die Ermittlung der Vermögenswerte, Schwachstellen, Bedrohungen, Auswirkungen und Eintrittswahrscheinlichkeiten definieren und das akzeptable Risiko festzulegen.

Wenn diese Regeln nicht eindeutig definiert wurden, wird es schwierig den erwünschten Schutz zu erhalten.

6. Schutzbedarfsanalyse durchführen

Hier müssen Sie die im vorigen Schritt definierten Methoden anwenden. Bei größeren Organisationen kann das einige Monate Zeit dauern, steuern Sie also diese Aktivitäten mit Bedacht. Es geht darum, ein umfassendes Bild der Gefährdungen für die Informationen Ihrer Organisation zu erhalten. Der Zweck der Schutzbedarfsanalyse besteht darin, die Risiken, die nicht akzeptabel sind, zu verringern. Dies geschieht in der Regel durch die Verwendung der Kontrollen aus Anhang A der Norm.

Die Vorgehensweise ist folgende: man bewertet die primären Assets und Prozesse um bestimmen zu können welches Schutzniveau für betroffene Geschäftsprozesse und verwendeten IT-Systeme angemessen ist. Es hat sich gut bewährt folgenden Kategorien zur Bewertung zu benutzen: finanzielle, Compliance- und operative Auswirkungen wie auch Außen- und Innenauswirkungen. Für Eintrittswahrscheinlichkeiten wählen Sie beispielsweise sehr wahrscheinlich (60-100%), wahrscheinlich (40-60%), möglich (10-40%), unwahrscheinlich (0-10%). An dieser Stelle möchte ich weitere Vertiefungen vermeiden.

Bei Fragen kontaktieren Sie uns.

Im Anschluss an die Risikoanalyse wird festgelegt, wie diese Risiken behandelt werden sollen. Es erfolgt die Zuordnung der Maßnahmen aus dem Anhang A. Während dieses Schritts wird ein Risikobewertungsbericht erstellt, der alle Schritte der Schutzbedarfsanalyse und des Verfahrens dokumentiert. Ferner muss eine Genehmigung für Restrisiken erfolgen. Das kann entweder als gesondertes Dokument oder als Teil der Geltungsbereichserklärung erfolgen.

MAßNAHMEN ZUR RISIKOBEHANDLUNG ERGREIFEN

7. Statement of Applicability schreiben (Gültigkeitserklärung)

Sobald Sie die Schutzbedarfsanalyse abgeschlossen und die dazugehörige Risikobehandlung festgelegt haben, werden Sie genau wissen, welche Kontrollen aus den insgesamt 133 aus Anhang A Sie benötigen. Das SoA (Statement of Applicability) sollte alle Kontrollen aufzulisten und festlegen, welche anwendbar sind und welche nicht und die Gründe dafür, welche Ziele mit den Kontrollen zu erzielen sind, und eine Beschreibung darüber beinhalten, wie sie Implementiert werden.

> Die Gültigkeitserklärung ist auch das geeignetste Dokument, um eine Managementgenehmigung für die Implementierung eines ISMS zu erhalten.

8. Risikobehandlungsplan erstellen

Im Anschluss an die Risikoanalyse wird festgelegt, wie diese Risiken behandelt werden sollen. Es erfolgt die Zuordnung der Maßnahmen aus dem Anhang A oder aus weiteren Maßnahmenkatalogen für jede Gefährdung. Der Zweck des Risikobehandlungsplans ist es, genau festzulegen, wie die Kontrollen von SoA umgesetzt werden - wer, wann, mit welchem Budget die Maßnahmen ausführen usw.

> Dieses Dokument ist der Implementierungsplan für die Kontrollen und ist nötig, um weitere Schritte im Projekt zu koordinieren.

9. Implementierung und Pflichtdokumente

Sobald der Plan fertig ist, kann es an die Implementierung gehen. Dies ist in der Regel die schwierigste Aufgabe in Ihrem Projekt. Es impliziert in der Regel den Einsatz neuer

Technologien und die Umsetzung neuen Verhaltensweisen. Oft sind neue Leitlinien, Vorgaben und Verfahren erforderlich, was eine starke Veränderung bedeutet. Da der Mensch Änderungen und Wandel nicht leicht mitmacht, ist die Kommunikation, Training und das Schaffen eines entsprechenden Bewusstseins (Awareness) entscheidend.

10. ISMS Betrieb

In diesem Schritt erfolgt das Monitoring und Reporting der Aktivitäten der Organisation im Hinblick auf die Einhaltung von Richtlinien und Sicherheitsmaßnahmen. Es finden verstärkt (zumindest in der Stabilisierungsphase) Audits statt (interne, Lieferanten- und Dienstleister-Audits). Alle Sicherheitsvorfälle werden gemeldet und analysiert. Dabei ist es wichtig Aufzeichnungen zum Nachweis zu führen. Richtlinien, Verfahrensanweisungen müssen ausreichend genau formuliert und bei Bedarf angepasst werden.

STEUERUNG UND VERBESSERUNG

11. Management Review

Ein erstes Management Review (ein Rückblick) sollte nach der Einführung bzw. Implementierung erfolgen. Das Management muss darin erfahren, ob alle nötigen Aufgaben durchgeführt werden und das ISMS die gewünschten Ergebnisse erzielt, um nötige Korrekturmaßnahmen einzuleiten.

12. Verbessern und vorbeugen

Damit kommen wir schon zum kontinuierlichen Verbesserungsprozess. Das ist eigentlich der Sinn des Managementsystems. Nämlich sicherzustellen, dass alles korrekt abläuft und wenn nicht, entsprechende Korrekturen vorzunehmen. Deswegen fordert die ISO 27001, dass Korrektur- und vorbeugende Maßnahmen systematisch durchgeführt werden. Das bedeutet, dass die Hauptursache

für eine Nichtkonformität identifiziert und dann beseitigt und nachträglich die Auswirkung überprüft werden muss.

Besonderheiten für unterschiedliche Branchen

Für die Implementierung des Standards hilft die Zusammenfassung der Kontrollen aus dem Anhang A und die detaillierteren Informationen hierzu aus der ISO 27002. Die ISO 27001 ist für Organisationen jeder Art und Größe anwendbar. Trotzdem sollten branchenspezifische Vorgaben immer eingehalten werden, um individuelle Situationen zu berücksichtigen. So sollten Sie zum Beispiel im **Energiesektor** die vorgeschlagenen Empfehlungen und Maßnahmen aus der **DIN SPEC 27019** (DIN SPEC 27019 – Informationstechnik – Sicherheitsverfahren – Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung) im ISMS ergänzend berücksichtigt werden. Die ISO 27019 können Sie mit der ISO 27002 vergleichen, nur mit einem speziellen Fokus auf Energielieferanten. Es gibt noch weitere ISO 270xx-Normen, die unterschiedliche Gegebenheiten der verschiedenen Branchen und vertiefte Themen, wie z.B. Risikomanagement in ISO 27005 berücksichtigen. Ich unterlasse es diese hier aufzuzählen. **Bei Fragen rufen Sie uns einfach an oder schreiben Sie uns.**

Tipps zur Umsetzung von ISO / IEC 27001

- ✓ Sichern Sie sich die Unterstützung durch das oberste Management.
- ✓ Binden Sie das ganze Unternehmen mittels interner Kommunikation ein.
- ✓ Vergleichen Sie die vorhandene Sicherheit bzw. ein vorhandenes

Sicherheitsmanagement mit der ISO 27001.

- ✓ Klären Sie den Bedarf Ihrer Kunden- und Lieferanten an Informationssicherheit. Was wird von Ihnen erwartet? Was haben Sie noch nicht bedacht/erfüllt?
- ✓ Stellen Sie ein Implementierungsteam und einen Verantwortlichen auf, um das Vorhaben zum Erfolg führen zu können.
- ✓ Definieren Sie Rollen, setzen Sie Verantwortlichkeiten und planen Sie die nötige Zeit ein.
- ✓ Passen Sie die Grundsätze der ISO 27001-Norm an Ihr Unternehmen an. Sie tun sicherlich schon vieles um wichtige Informationen zu sichern. Überlegen Sie, was davon bereits in Ihren Aktivitäten abgebildet ist und was sie noch davon benötigen.
- ✓ Motivieren Sie alle Ihre Mitarbeiter sich zu beteiligen und bilden Sie diese entsprechend aus.
- ✓ Machen Sie ISO27001-Wissen verfügbar für alle Mitarbeiter.
- ✓ Überprüfen Sie regelmäßig Ihr ISO 27001-System, und ergreifen Sie bei Bedarf Verbesserungsmaßnahmen.

Was ist jetzt zu tun?

Das wären meine Tipps, die Sie bei der Implementierung von ISO 27001 berücksichtigen sollten. Ich habe in diesem E-Book versucht strukturiert die wichtigsten Schritte der ISO 27001-Implementierung darzustellen und kurz zu erläutern. Organisationen, die sich nach ISO 27001 zertifizieren lassen wollen, empfehle ich die oben aufgeführten Tipps und Hinweise zu nutzen, um erfolgreich die Implementierung zu planen, zu starten und durchzuführen.

Sollten Sie noch Fragen dazu haben, zögern Sie nicht **uns anzurufen oder uns zu schreiben**. Wir werden uns umgehend bei Ihnen melden und versuchen eine erste Meinung zu Ihrem Problem abzugeben. Einfach so.

Sollten Sie mal eine erste Selbsteinschätzung allein durchführen wollen, so laden Sie einfach die kostenlose Checkliste zur „**GAP-Analyse zu ISO 27001**“ hier herunter.

KOSTENLOSE WEBINARE

Ich biete immer wieder Webinare unter anderen zu den Themen:

- Informationssicherheit,
- Qualitätsmanagement,
- Marketing und Werbung im Internet,
- Unternehmensgestaltung,
- Unternehmenspersönlichkeit

und würde mich freuen Sie zur gegeben Zeit in einem meiner Webinare begrüßen zu dürfen. Ich werde Sie gerne dazu rechtzeitig einladen, sofern Sie in unserem Newsletter abonniert bleiben.

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

Ich freue mich auf Ihre Rückfragen und wünsche Ihnen bei allen ISO-Vorhaben viel Erfolg.

Eduard Weber

ProQVis GmbH
Unteranger 24a
D-85244 Röhrmoos
info@proqvis.com
08139/2042-600

Wir bieten viele für kleinere und mittelgroße Unternehmen maßgeschneiderte Lösungen zur Implementierung von Standards und IT-Lösungen.

ProQVis® eQMS – ISO 9001 – der e-Coach für KMU

So bietet Ihnen zum Beispiel unsere Implementierungs- und Umstellungslösung **„ProQVis® eQMS“** eine innovative Vorgehensweise für die ISO 9001-Implementierung an dessen Ende das fertig implementierte oder angepasste Qualitätsmanagementsystem einerseits und die/der entsprechend in Qualitätsmanagement-Methoden, Managementsystemimplementierung, Marketing und Strategie weitergebildete Teilnehmer/in stehen.

Wenn Sie mit **minimalen Aufwand und Kosten** ein QM-System erstellen, umstellen oder anpassen wollen, dann ist **ProQVis® eQMS das richtige für Sie!**

Klicken Sie hier und erfahren Sie mehr über ProQVis® eQMS und besuchen unseren kostenlosen online Informations-Seminar zu dieser Lösung. Schreiben Sie sich ein zu einem Termin unter http://eqmswebinar.proqvis.com

Für Kleinunternehmen und Mittelständler in Berufsvereinen, kann eine ähnliche Lösung für mehr Branchenspezifizität gewählt werden, das **ProQVis® Unified QMS**. Diese Lösung basiert auf Synergien dank geichberuflicher Teilnehmer. Die dadurch erzielte Ersparnis geben wir gerne an unsere Kunden weiter.

ProQVis® Cloud QMS – ISO 9001 Prozessportal für verteilte Unternehmen

Mit dieser Lösung wird aus Ihrem Managementsystem ein weltweit zugängliches Prozessportal und Quelle für entsprechen einzusetzenden Formblätter, Vorlagen und Checklisten. Basierend auf ein BPMN-Tool vereint diese Lösung auch Prozessanalyse-Werkzeuge, wie

auch wichtigen Standardisierungsmittel, wie ein Unternehmensglossar.

Das System ist sehr schnell einsatzbereit und kann auch bei Bedarf mittels Test-Zulassung kennengelernt werden. Fordern Sie weitere Informationen unter

ProQVis® Care – Ihr/e externe/r Beauftragte/r für mehr Erfolg!

Damit Sie auch nach der Implementierung Ihres Managementsystems von Unsicherheit und Fehler geschützt sind und Ihr System nutzbringend und optimal einsetzen, stehen wir Ihnen zur Seite. Ob ein Tag, 3 Tage, 10 Tage, 30 Tage oder sogar mehr im Jahr sind, entscheiden Sie. Wir können Ihnen dazu Empfehlungen machen. Ihre ProQVis® Care Lösung hier erfragen.

ISO 27001 Implementierung und Unterstützung

Für den Bereich ISO 27001 werden wir Ihnen ebenfalls ähnliche schnelle Implementierungslösungen anbieten. Bis dahin stehen Ihnen die kostenlosen Info-Dokumente zum Download und unserer direkten Beratung zur Verfügung.

Kostenlose Dokumentation und Tipps

Für ISO 27001

ISO 27001 Implementierung Schritt für Schritt (dieses Dokument)

ISO 27001 – Obligatorische Dokumentation

ISO 27001 GAP-Analyse – Vorbereitende Checkliste

FÜR ISO 9001

ISO 9001:2015 – Implementierung 75% günstiger

Management Review – Unternehmen ausrichten

ISO 9001:2015 Umstellung Schritt für Schritt

ISO 9001:2015 – 7 wichtigste Änderungen

ISO 9001:2015 – Obligatorische Dokumentation

ISO 9001 – vorbereitende GAP-Analyse