DataGuard

LEITFADEN

ISO 27001-ZERTIFIZIERUNG: IHR ULTIMATIVER LEITFADEN

EINLEITUNG ZUR ISO 27001-ZERTIFIZIERUNG

Eine ISO 27001-Zertifizierung ist für Lieferanten, Kunden und Interessengruppen ein wichtiger Indikator dafür, dass Ihr Unternehmen Informationssicherheit ernst nimmt. Ebenso ist die Zertifizierung ein guter Ausgangspunkt für die Entwicklung einer soliden Cyber-Strategie.

In diesem ultimativen Leitfaden werden wir das Thema von Anfang bis Ende abdecken, um Sie bestmöglich über den Umfang Ihrer (potenziellen) ISO 27001-Zertifizierung zu informieren und Ihre Fragen zu beantworten.

→ **Laden Sie sich Ihren persönlichen Leitfaden zur ISO 27001-Zertifizierung kostenlos herunter.**

Ganz gleich, ob KMU oder Großunternehmen: In diesem Leitfaden finden Sie die wichtigsten Informationen an einem Ort.

WAS IST ISO 27001?

Die ISO 27001 setzt den weltweiten Standard für ein Informationssicherheits-Managementsystem (ISMS), das das Ziel verfolgt, einen Rahmen für die Sicherheit von Informationen zu schaffen. Im Jahr 2022 wurde die Version der ISO 27001:2013 auf die neueste Version, die ISO 27001:2022, aktualisiert.

Ein ISMS schafft eine Reihe von Regeln und Verfahren, die dazu beitragen, den Schaden eines Cyber- oder Ransomware-Angriffs sowie einer Sicherheitsverletzung zu mindern, was heutzutage auf der Tagesordnung jedes Unternehmens stehen sollte. Die Statistiken sprechen für sich selbst: Im dritten Quartal 2022 wurden 108,9 Millionen Konten Opfer von Sicherheitsverletzungen, was einen deutlichen Anstieg von 70 % im Vergleich zum vorangegangenen Quartal bedeutet. Den vollständigen Bericht zu den Trends und Prognosen zur Informationssicherheit finden Sie hier.

Mit einem ISO 27001-konformen ISMS können Sie die Sicherheit der Daten Ihres Unternehmens einfach und kostengünstig verwalten. Außerdem können sich Ihre Kunden, Investoren und andere wichtige Interessengruppen darauf verlassen, dass Sie die weltweit besten Praktiken für den Schutz von Informationen anwenden.

→ **Lernen "What is ISO 27001"**

WAS IST DIE ISO 27001-ZERTIFIZIERUNG?

Die ISO 27001-Zertifizierung wird erteilt, wenn Sie die Anforderungen der ISO 27001-Norm erfüllen. Sobald Sie Ihr ISMS eingerichtet haben, führt eine unabhängige, akkreditierte Zertifizierungsstelle ein Audit durch und stellt nach erfolgreichem Abschluss ein Zertifikat aus.

Eine Zertifizierungsstelle ist im Grunde eine unabhängige Institution, die Unternehmen nach erfolgreichem Bestehen eines externen Audits mit dem ISO 27001-Zertifikat auszeichnen kann.

Die Zertifizierung beweist im Wesentlichen, dass Sie die **geeigneten Schritte zum Schutz Ihrer Informationen (Informationswerte)** unternommen haben. Dazu gehören unter anderem geistiges Eigentum, Geschäftsgeheimnisse, geschützte Daten.

Auch wenn der Begriff "geistiges Eigentum" nicht verwendet wird, sind die Grundsätze der Informationssicherheit in den Normen der Reihe ISO 27000 so ausgelegt, dass sie verschiedene Formen wertvoller und sensibler Informationen, einschließlich geistigen Eigentums, umfassen.

WAS IST DIE NORM ISO 27001:2022?

Die Ausgabe ISO 27001:2022 ist die jüngste Version von ISO 27001, dem weltweiten Maßstab für Informationssicherheits-Managementsysteme, den Sie einhalten müssen, um Ihre Zertifizierung zu erhalten.

WAS IST EIN ISMS?

Ein Informationssicherheits-Managementsystem (ISMS) bietet einen Rahmen von dokumentierten Richtlinien, Verfahren und Kontrollen, um die Risiken für die Informationssicherheit zu verringern. Sobald Sie Ihr ISMS aufgebaut haben, empfiehlt es sich dies nach einer internationalen Norm wie der ISO 27001 zertifizieren zu lassen.

Sehen Sie sich dieses Video über die Beziehung zwischen ISO 27001 und einem ISMS an:

⟶ Lernen "How is the ISO 27001 standard related to an ISMS"

WIE WIRD EIN ISMS AUFGEBAUT UND UMGESETZT?

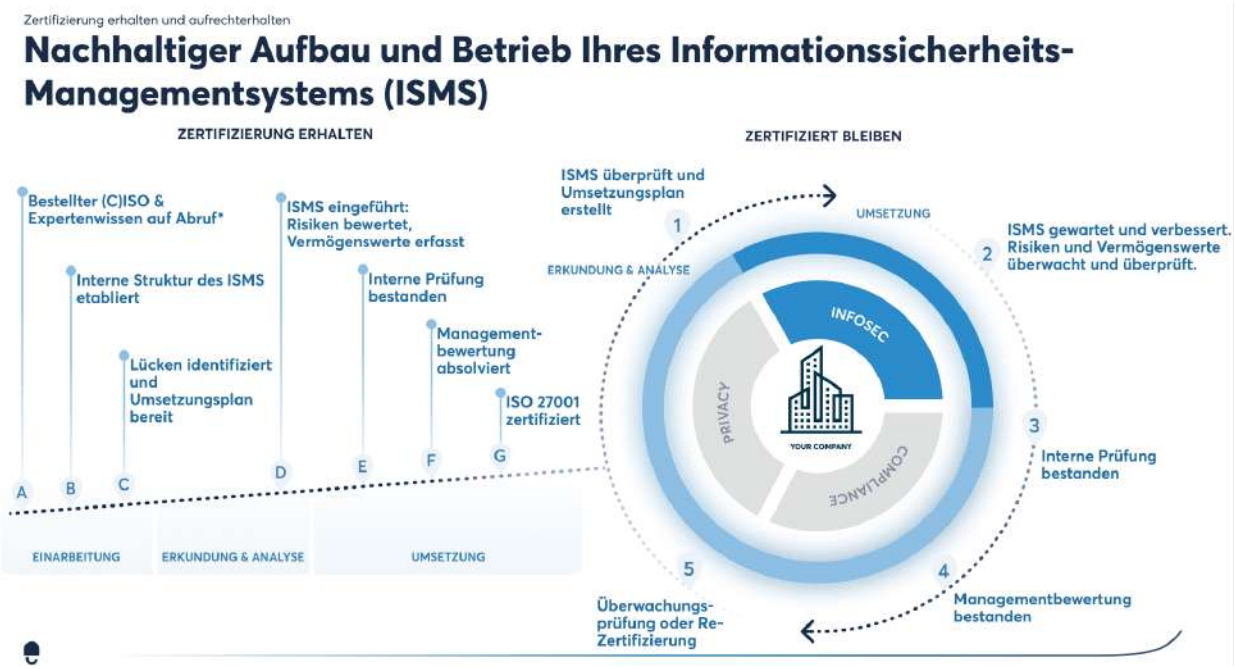
Der Aufbau und die Umsetzung eines ISMS kann in seiner einfachsten Form in 4 Phasen unterteilt werden, die auch als PDCA-Zyklus bekannt sind:

1. **Plan** (Planen): Dies ist die Phase, in der Sie das ISMS einrichten, d. h. Ihre Dokumentation für die ISO 27001-Zertifizierung auf Vordermann bringen.

2. **Do** (Ausführen): Die Prozesse und Verfahren, die Sie in der Planungsphase festgelegt haben, müssen auch umgesetzt und betrieben werden - dies geschieht in der „Do-Phase" des PDCA-Zyklus.

3. **Check** (Prüfen): Im Anschluss überprüfen Sie, ob Ihr ISMS mit der ISO 27001-Norm übereinstimmt, und ermitteln, ob noch Lücken vorhanden sind. Dies geschieht bei internen und externen Audits.

4. **Act** (Handeln): In dieser Phase verbessern Sie das ISMS und schließen vorhandene Lücken in der Informationssicherheit, um sicherzustellen, dass Sie Ihre ISO 27001-Zertifizierung erhalten und behalten können.



Wichtig ist es zu verstehen, dass diese Phasen nicht linear verlaufen, sondern ein Zyklus sind, der sich wiederholt und sicherstellt, dass Ihr ISMS stets mit der ISO 27001 konform ist. Dieser PDCA-Prozess spiegelt sich auch in den Klauseln der ISO 27001-Norm wider und ist als Rahmen für die Einrichtung und Umsetzung eines ISMS empfehlenswert.

WARUM IST ISO 27001 WICHTIG? WARUM SOLLTE ICH EINE ZERTIFIZIERUNG NACH ISO 27001 IN BETRACHT ZIEHEN?

Die Zertifizierung ist aus einer Reihe von Gründen vorteilhaft, dies sind die wichtigsten:

Schafft Vertrauen bei den Beteiligten:

Der Besitz eines ISO 27001-Zertifikats zeigt Ihr Engagement für den Schutz von Informationen und unterstreicht die Glaubwürdigkeit Ihres Unternehmens in den Augen Ihrer Partner und Kunden. Dies kann Ihnen einen Wettbewerbsvorteil verschaffen und den Ruf Ihrer Marke verbessern.

Unterstützt die Einhaltung von Rechtsvorschriften:

Die ISO 27001-Zertifizierung hilft Ihnen bei der Erfüllung Ihrer verschiedenen geschäftlichen, rechtlichen, finanziellen und regulatorischen Verpflichtungen.

Indem Sie die gesetzlichen und behördlichen Anforderungen ermitteln, können Sie die Wahrscheinlichkeit kostspieliger Verstöße verringern und so das Risiko teurer rechtlicher Konsequenzen und Geldstrafen reduzieren.

Sichert persönliche Daten und geistiges Eigentum:

Der Zertifizierungsprozess nach ISO 27001 bietet eine unparteiische Bewertung Ihrer Informationssicherheitsstrategie. Er kann auch bei der Verwaltung Ihres geistigen Eigentums und Ihrer Datenquellen helfen und gleichzeitig einen greifbaren Nachweis für die Umsetzung erbringen.

Verringert kostspielige Datenschutzverletzungen im Internet:

Datenschutzverletzungen sind mit einem hohen Preis verbunden. Im Jahr 2023 wurden die durchschnittlichen Kosten einer Datenschutzverletzung auf etwa 4,45 Millionen Dollar geschätzt (IBM, 2023). Die ISO 27001-Zertifizierung schützt Ihre Daten durch festgelegte Verfahren und Prozesse und hilft Ihnen, solche finanziellen Belastungen zu vermeiden.

Legt den Grundstein für die Risikominderung:

Das Risikomanagement ist wichtig für die Aufrechterhaltung Ihrer Geschäftsabläufe und sollte kontinuierlich durchgeführt werden. Der Aufbau einer Risikomanagementstruktur von Grund auf kann jedoch sehr zeitaufwendig sein - ISO 27001 bietet Ihnen einen Rahmen, um die Kriterien für das Risikomanagement in Ihrem Unternehmen zu definieren.

Möchten Sie einen detaillierteren Einblick erhalten, warum eine Zertifizierung nach ISO 27001 sinnvoll ist? Laden Sie hier unser kostenloses E-Book mit den Vorteilen einer ISO 27001-Zertifizierung herunter.

WER BRAUCHT EINE ISO 27001-ZERTIFIZIERUNG?

Die ISO 27001 ist für so ziemlich jedes Unternehmen relevant, das mit Informationen und Daten zu tun hat. Sie ist zwar nicht verpflichtend, aber dennoch gängige Praxis und oft eine Voraussetzung für viele Geschäftsinteressenten, denn eine Geschäftsbeziehung mit Ihnen ohne einschlägige Richtlinien und Verfahren zur Risikobewältigung könnte deren Informationen und Daten gefährden.

Zu den Branchen, die besonders von Ransomware und Cyberangriffen betroffen sind und in denen die Zertifizierung nach ISO 27001 zur Norm wird, gehören:

- Bildung/Forschung
- Regierung/Militär alias der öffentliche Sektor
- Medizintechnik/Gesundheitswesen
- Kommunikation

Doch angesichts des derzeitigen Aufwärtstrends der Cyberkriminalität müssen sich alle Unternehmen - vom KMU bis zum Großkonzern - Gedanken über die Informationssicherheit machen.

Die Zertifizierung nach ISO 27001 ist ein klarer Fahrplan, um diesem Thema Priorität einzuräumen.

WIE SCHWER IST ES, SICH NACH ISO 27001 ZERTIFIZIEREN ZU LASSEN?

Die Zertifizierung nach ISO 27001 ist standardmäßig nicht einfach. tatsächlich ist der Prozess sehr komplex, vor allem, wenn viele Interessengruppen und komplizierte Prozesse beteiligt sind.

Außerdem ist die Zertifizierung nach ISO 27001 in der Regel eine Entscheidung von oben nach unten, was bedeutet, dass die oberste Führungsebene früher oder später in den Prozess einbezogen werden muss.

Als Unternehmen sollten Sie sicherstellen, dass Sie die richtige Erfahrung im Team haben, um die Entscheidungsträger von der Zertifizierung zu überzeugen und den gesamten Prozess zu steuern.

Hier sind vier Tipps für eine erfolgreiche ISO 27001-Zertifizierung:

→ **Lernen "4 Tipps für eine erfolgreiche Zertifizierung nach ISO 27001 und TISAX®"**

HÄUFIGE FALLSTRICKE, DIE BEI DER ISO 27001-ZERTIFIZIERUNG ZU VERMEIDEN SIND

Die Umsetzung von ISO 27001 bietet Ihnen als Organisation mehrere Vorteile, darunter die **leichtere Einhaltung rechtlicher Anforderungen**, eine **bessere Datensicherheit** und ein **größeres Vertrauen** der Interessengruppen.

Der Haken: Die erfolgreiche Umsetzung der Norm kann für Organisationen, die dies zum ersten Mal tun, eine große Herausforderung darstellen.

Da die ISO 27001-Norm so konzipiert ist, dass sie an jede Organisation angepasst werden kann, gibt es mehrere Fälle, in denen Unternehmen bei der Umsetzung Fehler machen können.

Auf der Grundlage unserer umfangreichen Erfahrung in der Zusammenarbeit mit verschiedenen Kunden unterschiedlicher Branchen haben wir eine Liste der häufigsten Fallstricke zusammengestellt, denen Unternehmen bei der Umsetzung der Norm begegnen, und geben Tipps, wie Sie diese vermeiden können.

Falsche Definition des Anwendungsbereichs

Es kann schwierig sein, den richtigen Umfang für die Einführung des ISMS in Ihrem Unternehmen zu finden. Organisationen setzen sich oft zu ehrgeizige Ziele für die Umsetzung ihres ISMS, was dazu führt, dass mehrere überflüssige und nicht benötigte Kontrollen und Prozesse eingeführt werden. Dies kann zu Ressourcenverschwendung, erhöhten Kosten für die Informationssicherheit und demotivierten Mitarbeitenden führen, die unerreichbaren Zielen hinterherjagen.

Andererseits kann es vorkommen, dass eine Organisation ihren Geltungsbereich zu eng definiert und die erforderlichen Kontrollen nicht eingeführt werden. Dies kann zur Nichteinhaltung der ISO 27001-Norm führen und den Anschein erwecken, dass Ihre Organisation ihr ISMS während des Zertifizierungsaudits nicht im Griff hat.

Geringes Engagement der Führungsebene

Engagement In vielen Organisationen wird die Umsetzung der ISO 27001 als eine IT-Übung betrachtet, für die die IT-Abteilung des Unternehmens zuständig ist.

In Wirklichkeit handelt es sich um eine Managementnorm für die Informationssicherheit. Die oberste Führungsebene einer Organisation sieht möglicherweise nicht den Wert, den die Umsetzung von ISO 27001 für das Unternehmen hat, und zögert, sich voll und ganz für die Umsetzung einzusetzen.

Zu wenige Ressourcen

Oft wird die Umsetzung der ISO 27001 von einer bestimmten Person oder einem Team innerhalb der Organisation übernommen. Diese Art von Ansatz kann zu Informationssicherheitssilos führen, in denen nur sehr wenige Personen die Kontrollen und Verfahren rund um das ISMS und andere Aspekte der Norm kennen. Der Verlust dieser Personen könnte den Zusammenbruch des gesamten ISMS zur Folge haben.

Erfahren Sie in unserem kostenlosen Leitfaden über die häufigsten Fallstricke bei der ISO 27001-Zertifizierung, welche zwei weiteren Fallstricke für alle Unternehmen typisch sind und wie Sie diese Fallstricke vermeiden können.

WIE LANGE DAUERT ES, SICH NACH ISO 27001 ZERTIFIZIEREN ZU LASSEN?

In der Regel kann der Prozess je nach Größe und Komplexität des Unternehmens **6 bis 12 Monate** dauern. Durch den Einsatz geeigneter Lösungen wie der DataGuard-Plattform kann der Prozess **auf bis zu 3 Monate verkürzt werden** (ebenfalls abhängig von den Eigenschaften des Unternehmens).

Diese Phase wird als "**Ramp-Up-Phase**" bezeichnet, in der der Hauptteil der Arbeit geleistet wird. Sie führen eine Gap-Analyse durch, die darauf abzielt, bis zu 50 % der wichtigsten Risiken Ihres Unternehmens in bis zu 8 Wochen zu schließen.

Um den Prozess zu durchlaufen, müssen Sie Folgendes tun:

- Festlegung des Anwendungsbereichs
- Aufbau eines Informationssicherheits-Managementsystems
- Identifizierung und Management von Risiken
- Aufbau eines Schutzes Ihrer Informationswerte
- Bestehen Sie Ihr ISO 27001-Audit
- Aufrechterhaltung Ihres ISMS, Erhalt Ihres Zertifikats

Und wenn Sie eine Skalierung anstreben, sollten Sie lieber früher als später damit beginnen. Es ist einfacher, Ihr ISMS parallel zum Wachstum Ihres Unternehmens zu skalieren.

WIE LÄUFT DIE ISO 27001-ZERTIFIZIERUNG AB?

Die Zertifizierung nach ISO 27001 bietet Unternehmen zahlreiche Vorteile, stellt sie aber auch vor große Herausforderung. Beispielsweise ist die Implementierung eines ISMS kein einfacher Prozess.

Das Resultat ist den Aufwand jedoch allemal wert, da ein ISMS effektiv zur Risikominderung in der Informationssicherheit, zum Beispiel bei Cyber- oder Hackerangriffen, beiträgt.

Grundsätzlich läuft jeder Zertifizierungsprozess folgendermaßen ab:

1. **Vorbereitung:** Das Unternehmen muss ein Informationssicherheits-Managementsystem einrichten, das den Anforderungen der ISO 27001 entspricht. Dazu gehört die Erstellung einer Informationssicherheitspolitik, die Festlegung von Zielen und Maßnahmen sowie die Implementierung dieser Maßnahmen in den IT- und Geschäftsprozessen.

2. **Voraudit/internes Audit:** Ein von Ihnen ausgewählter Auditor (Informationssicherheitsbeauftragter, Beratungsagentur, oder externer CISO) führt ein internes Voraudit durch, um die Umsetzung des ISMS zu bewerten. Dabei werden die Dokumentation des ISMS, die Umsetzung der Maßnahmen und die Wirksamkeit des ISMS überprüft.

3. **Zertifizierungsaudit:** Ein unabhängiger Auditor führt ein Zertifizierungsaudit durch, um die Einhaltung der Anforderungen der ISO 27001 zu bestätigen. Dabei werden alle Bereiche des ISMS, einschließlich der technischen und organisatorischen Maßnahmen, überprüft.

4. **Zertifikatserteilung:** Wenn das Zertifizierungsaudit erfolgreich ist, wird dem Unternehmen ein Zertifikat für das ISMS nach ISO 27001 ausgestellt.

Doch nun beginnt die eigentliche Arbeit, da die **ISO 27001-Zertifizierung alle 3 Jahre erneuert werden muss.** Daher empfiehlt es sich, die Zertifizierung stets aufrechtzuerhalten, um die Vermögenswerte Ihres Unternehmens dauerhaft zu schützen und die Sicherheit Ihrer Informationen fortlaufend zu gewährleisten.

Darüber hinaus müssen die Unternehmen das jährliche Überwachungsaudit bestehen, um die Einhaltung der Vorschriften zu überprüfen und zu verhindern, dass die Zertifizierung vor Ablauf des Dreijahreszyklus erlischt.

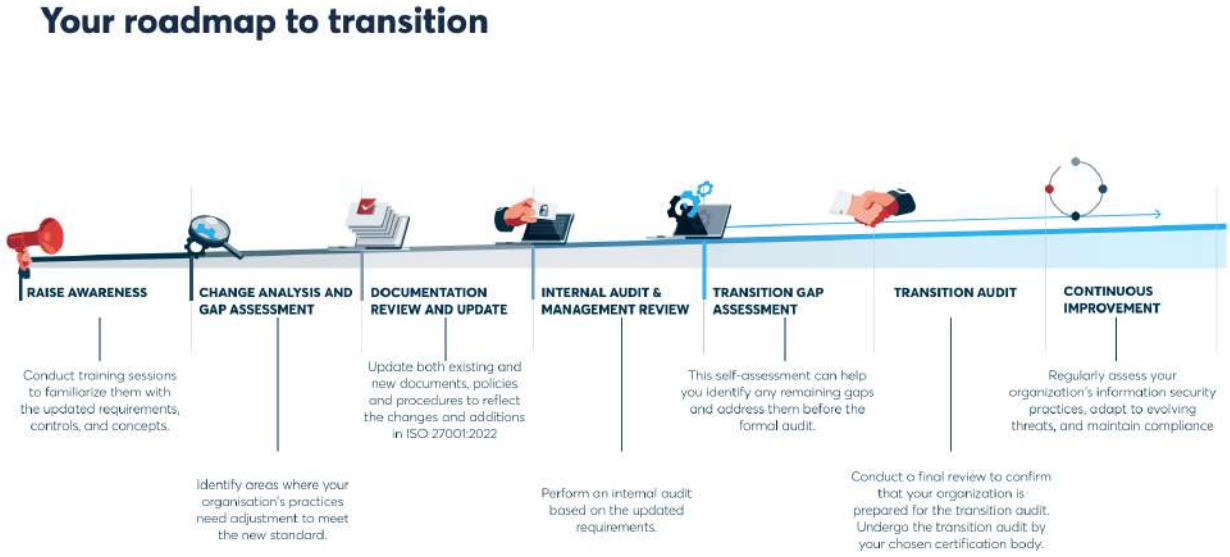
"Wenn eine Organisation, die vom externen Prüfer durchgeführte Überwachungsprüfung nicht besteht, kann ihre ISO 27001-Zertifizierung möglicherweise auslaufen, bevor die volle Dreijahresfrist abgelaufen ist. Die Überwachungsaudits werden in der Regel jährlich durchgeführt, um die laufende Einhaltung der ISO 27001-Norm zu gewährleisten. Wird die Konformität nicht aufrechterhalten, wird die Zertifizierung möglicherweise nicht für den gesamten 3-Jahres-Zeitraum erneuert."

Larissa Bruns, Associate Consultant Tech Practice Professional Services

WIE KANN ICH AUF ISO 27001:2022 UMSTELLEN?

Wenn Sie bereits nach ISO 27001:2013 zertifiziert sind, benötigen Sie nicht unbedingt ein separates Audit für den Übergang zur neuen Revision. Sie können sich entweder einem **eigenständigen Umstellungsaudit unterziehen oder sich für ein Umstellungsaudit zum Zeitpunkt der jährlichen Überwachung oder Rezertifizierung entscheiden**. Dies hängt davon ab, in welcher Phase Sie sich in Ihrem Zertifizierungszyklus befinden.

Hier finden Sie einen Überblick über einen typischen Übergangsplan:



Mit der Veröffentlichung der ISO 27001:2022 am 25. Oktober 2022 begann gleichzeitig auch die Übergangsphase von der alten 2013er-Version. Diese Übergangsfrist wurde auf insgesamt drei Jahre, also **36 Monate festgelegt**. Daher ergeben sich für Normanwender nun folgende Fristen:

- Abhängig von der deutschen Akkreditierungsstelle GmbH konnte eine Zertifizierung nach ISO 27001:2022 zwischen Februar und April 2023 begonnen werden.

- Der letztmögliche Termin für eine Erst- und Rezertifizierung nach ISO 27001:2013 ist bis maximal 30.04.2024 möglich.

- Alle bestehenden Zertifikate müssen bis spätestens Oktober 2025 (3 Jahre nach Veröffentlichung) auf die neue ISO 27001 Version umgestellt werden.

Die Einhaltung der neuen Norm 2022 wird Ihrem Unternehmen mit Sicherheit Ressourcen und Frustrationen ersparen. Deshalb empfehlen wir, die Umstellung lieber früher als später vorzunehmen. Detaillierte Einblicke in die Umstellung erhalten Sie in in unserem Experteneinblick in die neue ISO 27001-Version.

WAS SIND DIE VORTEILE EINER ISO 27001-ZERTIFIZIERUNG?

Die Vorteile der Einführung von ISO 27001 sind zahlreich - sowohl für Ihr Unternehmen als auch für externe Parteien und Interessengruppen.

Hier finden Sie einen Überblick über die wichtigsten:

- **Risikomanagement**: Die Aufrechterhaltung der ISO 27001-Zertifizierung impliziert effektives Risikomanagement. Dadurch stellen Sie sich, dass Risiken rechtzeitig identifiziert, bewertt und behandelt werden.

- **Eindämmung finanzieller Verluste**: Ihr Unternehmen oder Ihre Organisation kann erhebliche finanzielle Verluste, z.B. verursacht durch Ransomware-Angriffe, effektiver verhindern.

- **Gewinn neuer Aufträge**: Mit einem zertifizierten ISMS können Sie sich von der Konkurrenz abheben und das Vertrauen potenzieller Kunden gewinnen.

- **Vertrauenssteigerung**: Möglicherweise können Sie Ihre Investitionen leichter sichern; die Investoren werden sich der Bedrohung durch Ransomware-Angriffe immer mehr bewusst. Durch eine Zertifizierung können Sie nicht nur das Vertrauen von Investoren, sondern auch das Ihrer gewinnen, denn insbesondere technikaffine Kunden wollen wissen, wie Sie sicher mit Daten umgehen.

- **Etablierung von Prozessen**: Die Einrichtung von Prozessen und Verfahren für den Umgang mit Daten kann auch eine Steigerung der betrieblichen Effizienz bedeuten. Denn jetzt haben Sie einen Standardprozess anstelle unterschiedlicher Methoden.

- **Verbesserter Ruf der Marke**: Die Kunden wollen wissen, wie Sie mit ihren Informationen umgehen, und die Zertifizierung nach ISO 27001 ist das ultimative Versprechen, dass Sie die Informationssicherheit ernst nehmen.

IST ES AUSREICHEND DIE ISO 27001 EINZUHALTEN?

Wenn Sie ein Managementsystem für die Informationssicherheit einrichten möchten, ist ISO 27001 die ultimative Grundlage, die die Anforderungen der meisten Unternehmen an die Einhaltung von Vorschriften und die Informationssicherheit erfüllt.

Was Ihre Kunden und Lieferanten verlangen, hängt davon ab, wo Ihr Unternehmen tätig ist. ISO 27001 ist ein international anerkannter Standard, der als Goldstandard bekannt ist, unabhängig vom geografischen Standort oder der Branche. Sie sollte für jeden Anwendungsfall ausreichen, aber wenn Sie sich unsicher sind, ist eine erste Beratung durch einen Experten für Informationssicherheit sinnvoll.

→ **Lernen "ISO 27001: 2 minutes quick guide to certification"**

ZERTIFIZIERUNG NACH ISO 27001 ERHALTEN

Akkreditierte vs. nicht-akkreditierte Zertifizierung

Wie wir bisher erfahren haben, ist die Zertifizierung nach ISO 27001 für Unternehmen nicht zwingend erforderlich. Es wird jedoch empfohlen, die Norm zumindest einzuhalten. Aber was ist der Unterschied zwischen einer ISO 27001-Zertifizierung und ISO 27001 Konformität? Im Allgemeinen müssen Sie die drei Arten der Kommunikation über die Umsetzung von ISO 27001 verstehen:

- ISO 27001-konform
- ISO 27001 zertifiziert
- Zertifizierung nach ISO 27001 durch eine amtlich zugelassene (akkreditierte) Zertifizierungsstelle

Der Unterschied besteht darin, dass eine unabhängige dritte Zertifizierungsstelle eine akkreditierte Zertifizierung validiert. Eine nicht akkreditierte Zertifizierung bedeutet, dass Sie die ISO-Normen umgesetzt haben, sich aber weder einem externen Audit unterzogen haben noch ein Zertifikat einer externen Zertifizierungsstelle erhalten haben.

In Deutschland gibt es eine ganze Reihe unabhängiger und akkreditierter Zertifizierungsstellen. Diese werden von der deutschen Akkreditierungsstelle GmbH (DAkkS) akkreditiert. m Bereich ISO 27001 sind derzeit folgende Zertifizierungsstellen in Deutschland akkreditiert:

- DQS BIT GmbH
- PwC Certification Services GmbH
- TÜV Rheinland
- TÜV Nord
- TÜV SÜD
- BSI Group
- DEKRA
- VDE
- IHK

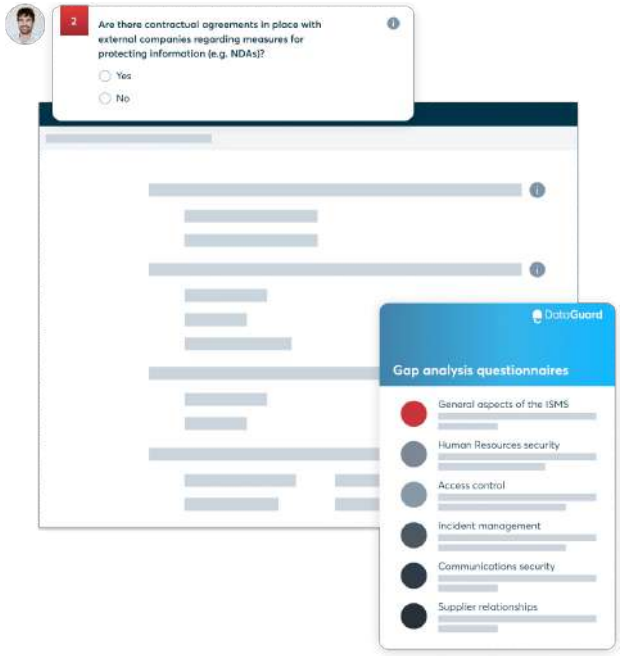
Oft verlangen bestimmte vertragliche Vereinbarungen eine offizielle akkreditierte Zertifizierung. Abgesehen davon ist es sehr empfehlenswert, eine akkreditierte Zertifizierung zu erlangen - Sie können sie in Ihrer Kommunikation mit Kunden verwenden und eine externe Bewertung Ihrer Informationssicherheit vornehmen lassen, um sicherzustellen, dass Ihr ISMS in Ordnung ist.

Wir empfehlen Ihnen, sich ausschließlich von akkreditierten Stellen zertifizieren zu lassen. Geschäftspartner erkennen Zertifizierungen oft nicht an, wenn sie nicht von einer internationalen Akkreditierungsstelle bestätigt wurden.

Tatsächlich beziehen sich die meisten Verträge, die eine ISO 27001-Zertifizierung vorschreiben, implizit auf die Zertifizierung durch eine akkreditierte Stelle. Einen vollständigen Artikel über die akkreditierte vs. nicht akkreditierte ISO 27001-Zertifizierung können Sie hier lesen.

WAS SIND DIE ZERTIFIZIERUNGSSCHRITTE? WIE GENAU LASSE ICH MICH MACH ISO 27001 ZERTIFIZIEREN?

Das Verfahren zur Erlangung der Zertifizierung besteht aus folgenden Schritten:



IDENTIFIZIERUNG VON LÜCKEN UND BEGINN DER IMPLEMENTIERUNG VON ISO 27001

Machen Sie sich zunächst mit dem Rahmenwerk der ISO 27001 vertraut. Führen Sie eine Gap-Analysis durch, um festzustellen, in welchen Bereichen Verbesserungen erforderlich sind, um die Anforderungen zu erfüllen. Arbeiten Sie mit unseren zertifizierten Experten für Informationssicherheit zusammen, um einen maßgeschneiderten ISO 27001-Implementierungsplan zu erstellen. Dieser Plan legt auch den Umfang Ihres Informationssicherheits-Managementsystems fest.

AUFBAU DES ISMS

Das ISMS ist ein umfassender Satz von Richtlinien, Prozessen, Verfahren und Kontrollen, die dazu dienen, die Informationssicherheitspraktiken Ihres Unternehmens zu verbessern.

IDENTIFIZIERUNG UND MANAGEMENT VON RISIKEN

Risiken für die Informationssicherheit ergeben sich aus verschiedenen organisatorischen Quellen, darunter Menschen, Infrastruktur, physische Sicherheit und Beziehungen zu Dritten.

Beginnen Sie also mit einem Brainstorming zu hypothetischen Szenarien, um die verschiedenen Informationssicherheitsrisiken zu ermitteln, denen Ihr Unternehmen ausgesetzt ist. Bewerten Sie deren Auswirkungen aus finanzieller, rufschädigender, rechtlicher und betrieblicher Sicht. Anschließend können Sie technische oder verfahrenstechnische Maßnahmen einführen, um die ermittelten Risiken zu mindern und zu verwalten.

SCHUTZ VON INFORMATIONSWERTEN

Identifizieren und dokumentieren Sie alle Informationswerte in Ihrem Unternehmen wie Hardware, Daten und Personal. Kategorisieren Sie sie nach Kritikalität und Wert, um geeignete Sicherheitskontrollen festzulegen. Legen Sie die Eigentumsverhältnisse fest und weisen Sie die Verantwortlichkeiten für die Verwaltung und den Schutz der Ressourcen zu.

ABSOLVIEREN UND BESTEHEN SIE IHR ISO 27001-AUDIT

Bei der externen Prüfung bewertet ein akkreditierter Prüfer alle Aspekte des ISMS Ihrer Organisation, um die Einhaltung der Norm ISO 27001 zu überprüfen. Führen Sie vorab ein internes Audit durch, u bestmöglich auf die externe Prüfung vorbereitet zu sein und eventuelle Schwachstellen noch rechtzeitig zu beseitigen. Bei der Durchführung eines internen Audits helfen Ihnen gerne die Experten von DataGuard weiter.

DIE EIGENTLICHE REISE BEGINNT: AUFRECHTERHALTUNG IHRES ISMS

Sich entwickelnde Sicherheitsbedrohungen und Änderungen an der organisatorischen Infrastruktur schaffen ständig neue Risiken. Um die kontinuierliche Einhaltung der ISO 27001 zu gewährleisten, müssen Sie Ihr ISMS regelmäßig überprüfen und aktualisieren. Dazu gehören Risikobewertungen, interne Audits und Mitarbeiterschulungen. Um zertifiziert zu bleiben, muss Ihre Organisation jährliche Überwachungsaudits und alle 3 Jahre ein Re-Audit bestehen. Verbessern Sie Ihr ISMS laufend, wenn Ihr Unternehmen wächst und reift. Zeigen Sie mit der ISO 27001-Zertifizierung Ihr Engagement für die Informationssicherheit und gewinnen Sie mehr Aufträge.

DURCHFÜHREN EINER RISIKOBEWERTUNG

Die Durchführung einer Risikobewertung ist nicht so einfach, wie man vielleicht denkt. Zunächst einmal gibt es viele verschiedene Ansätze für Risikobewertungen. Es ist zwar nicht unbedingt üblich, aber die effektivste Methode, um Risiken zu erfassen, ist die szenariobasierte. Das bedeutet, dass frühere Ereignisse berücksichtigt und riskante Szenarien analysiert werden, die ein Problem verursachen könnten.

Die Risikobewertung umfasst folgende Punkte:

1. Identifizieren und bewerten Sie potenzielle Risiken.
2. Risiken behandeln - hier entscheiden Sie, wie Sie mit den Risiken umgehen wollen. Z.B. Akzeptieren, Vermeiden, Übertragen, Abschwächen.
3. Überprüfen Sie die Restrisiken.

Eine Plattform wie DataGuard kann Ihnen dabei helfen, die Risikobewertung auf effiziente Weise mit einem getesteten und bewährten Verfahren durchzuführen. Lesen Sie den vollständigen Artikel über die Durchführung der ISO 27001-Risikobewertung in 7 Schritten hier.

UMSETZUNG VON KONTROLLEN UND EINES RISIKOBEHANDLUNGSPLANS ZUR BEWÄLTIGUNG VON RISIKEN

Ein wesentlicher Bestandteil Ihres Informationssicherheitsprogramms ist der Risikobehandlungsplan. Dieser Plan ist allumfassend und dient der Durchführung von Maßnahmen, um die Möglichkeit oder die Folgen von Risiken entweder zu akzeptieren, zu vermeiden, zu übertragen oder abzuschwächen.

Von größter Bedeutung im Rahmen eines Risikobehandlungsplans ist der Aspekt der Umsetzung. Seine Bedeutung liegt in der Gewährleistung der tatsächlichen Durchführung der Risikobehandlungsverfahren.

Lesen Sie weiter mehr zum Risikomanagement nach ISO 27001.

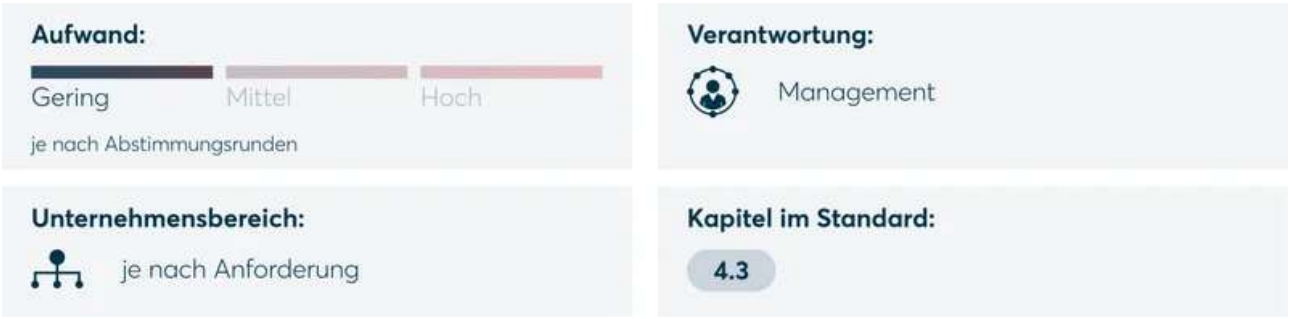
VERVOLLSTÄNDIGEN SIE IHRE ISMS-DOKUMENTATION

Die Dokumentation des Informationssicherheits-Managementsystems ist die Grundlage Ihres ISMS und der wichtigste Bestandteil für die Erlangung und Aufrechterhaltung Ihrer Zertifizierung. Wenn es nicht dokumentiert ist, ist es nicht relevant.

Bei der Dokumentation gibt es viele Dinge zu beachten. Um Ihnen einen vollständigen Überblick über die für die ISO 27001-Zertifizierung erforderliche Dokumentation sowie Informationen zur Erstellung dieser Dokumentation zu geben, haben wir eine detaillierte Liste für die Dokumentation erstellt, aus der Sie auch die Verantwortlichkeit und den Aufwand entnehmen können:

Definition des Anwendungsbereichs des ISMS (Informationssicherheits-Managementsystem)

Der Geltungsbereich des ISMS wird im so genannten "Scope Document" festgelegt. Darin wird definiert, für welche Bereiche Ihres Unternehmens das ISMS gilt.
Ihr ISMS muss nicht zwangsläufig im gesamten Unternehmen ausgerollt werden, sondern nur in den relevanten Abteilungen und Bereichen. Bei kleineren Unternehmen wird es jedoch in der Regel alle Abteilungen abdecken.

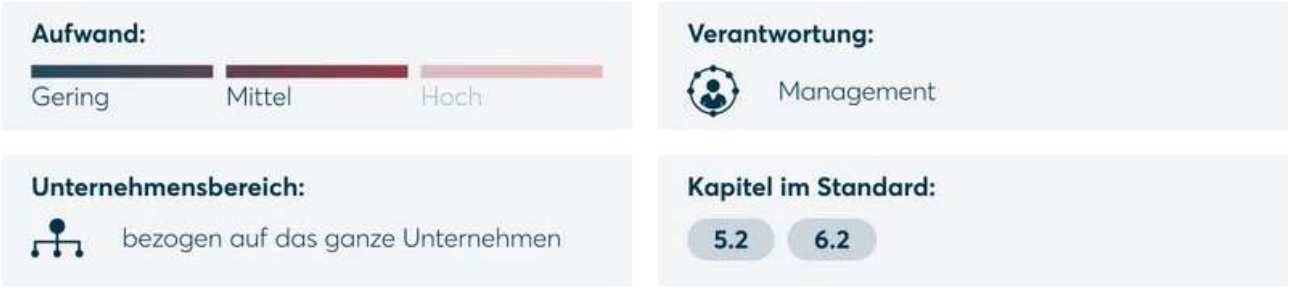


Koordination und Dokumentation der Leitlinie zur Informationssicherheit

Die Ziele, die Ihr Unternehmen mit Ihrem ISMS erreichen will, sollten in der Leitlinie zur Informationssicherheit klar definiert werden. Aus diesem Dokument sollte auch hervorgehen, warum die Informationssicherheit in Ihrem Unternehmen oberste Priorität hat und dass die Geschäftsleitung für die Leitlinie verantwortlich ist. Dies muss nicht von der Geschäftsleitung selbst formuliert werden, sondern muss immer von den notwendigen Interessengruppen genehmigt werden. In der ISO-Norm sind bereits die folgenden Ziele für die Informationssicherheit festgelegt:

This does not have to be formulated by management themselves but must always be approved the necessary stakeholders. The ISO standard already specifies the following information security objectives:

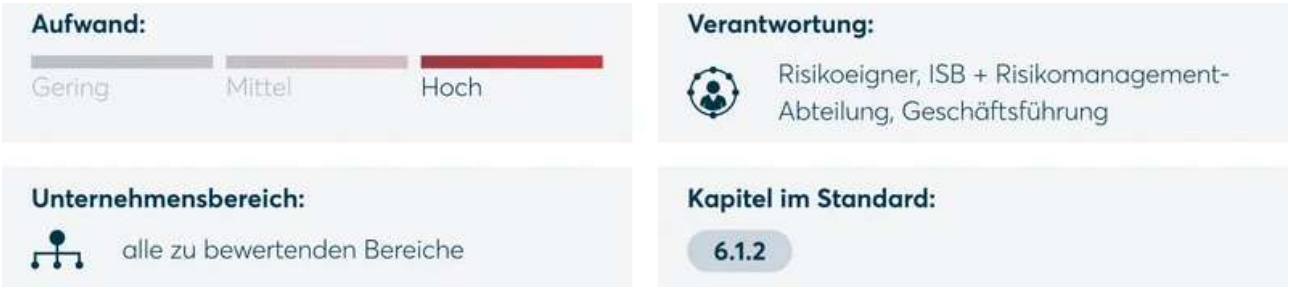
- Vertraulichkeit der Daten
- Verfügbarkeit von Daten
- Integrität der Daten



Definition der Methoden zur Risikobewertung und zum Risikomanagement

Sie müssen die Risiken Ihres Unternehmens ermitteln, sie einzeln bewerten und eine geeignete Methodik für das Risikomanagement festlegen. Die Bewertung sollte immer vom jeweiligen Risikoverantwortlichen durchgeführt und letztlich von der Geschäftsleitung genehmigt werden.

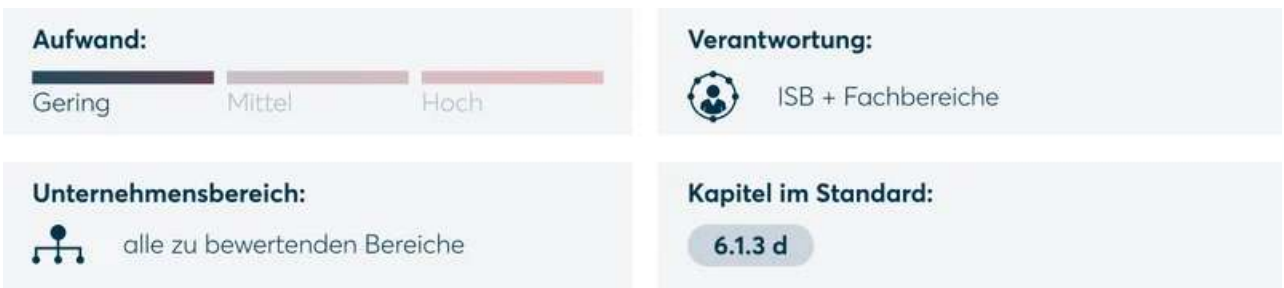
Darüber hinaus sollte dieser Bereich innerhalb des Unternehmens koordiniert werden, idealerweise mit Ihrer ISO-, CISO- oder Risikomanagementabteilung. Da dieser Prozess regelmäßig wiederholt werden muss, kann er vor allem für kleine und mittlere Unternehmen, die über keine internen Sicherheits- und Risikoexperten verfügen, einen hohen Aufwand bedeuten. Wiederholungen finden statt, wenn neue Vermögenswerte im Unternehmen vorhanden sind, die eine Risikobewertung erfordern.



Vorbereitung einer Erklärung zur Anwendbarkeit

Im Rahmen dieses Schrittes sollte sich Ihr interner Informationssicherheitsbeauftragter oder CISO mit den jeweiligen Fachabteilungen abstimmen, welche der 93 in Anhang A der ISO 27001:2022 genannten Controls durchgeführt werden müssen bzw. für das Unternehmen relevant sind.

Die ISO 27001 hat verschiedene Bereiche wie Kryptographie, Personalsicherheit oder Betriebssicherheit festgelegt. Unternehmen können einige dieser Bereiche mit einer entsprechenden Begründung ausschließen. Wenn ein Unternehmen zum Beispiel keine Ladezone hat, ist es einfach nicht notwendig, Regeln für Ladezonen aufzustellen.



→ **Laden Sie unser kostenloses E-Book herunter, um sich über alle 22 Dokumentationsanforderungen zu informieren.**

Wenn Sie sich für die Zusammenarbeit mit Experten wie DataGuard oder einem externen Berater entscheiden, können Sie Dokumentationsvorlagen erhalten, die Ihre manuelle Arbeit im Vergleich zur Erstellung von Grund auf erheblich reduzieren.

Weitere Informationen zur ISMS-Dokumentation gibts in diesem Video:

→ **Lernen "ISMS-Dokumentation für ISO 27001 und TISAX® - Schritte zum Erfolg®"**

WAS IST EIN AUDIT, UND WARUM IST ES WICHTIG?

Ein Audit ist im Grunde der Prozess der Überprüfung, ob Ihr ISMS die Anforderungen und Kriterien einer Norm erfüllt. Wenn Sie sich nach ISO 27001 zertifizieren lassen, sind es die Anforderungen der Norm ISO 27001.

Audits stellen den Erfolg Ihres ISMS sicher, indem sie Nichtkonformitäten im Bereich der Informationssicherheit aufdecken und können entweder intern oder extern durchgeführt werden.

Interne Audits können mit den eigenen Ressourcen der Organisation durchgeführt werden - sei es durch interne Mitarbeiter des Unternehmens oder durch beauftragte unabhängige Berater (2nd party auditors).

Externe Audits werden von einer unabhängigen Zertifizierungsstelle, externen Partnern oder Kunden durchgeführt, die das ISMS auf eigene Faust bewerten wollen. Letzteres ist eher die Ausnahme als die Regel - wenn von einem externen Audit die Rede ist, ist in den meisten Fällen eine Zertifizierungsstelle gemeint.

Doch auch aus den folgenden Gründen sind Audits besonders wichtig für Ihre Organisation:

- Sie sind eine konkrete Anforderung der ISO 27001.
- Sie sind die einzige Möglichkeit, zu überprüfen, ob Sie die Norm einhalten.
- Sie sind notwendig, um Ihre ISO 27001-Zertifizierung zu erhalten.

DURCHFÜHRUNG DES EXTERNEN AUDITS: WAS SIE ERWARTEN KÖNNEN

Bevor Sie ein externes Audit angehen, sollten Sie sich zunächst mit Ihrem Auditor in Verbindung setzen, um einen Audittermin zu vereinbaren, um Ressourcen und Zeitpläne für das Audit festzulegen.

Im Allgemeinen gibt es vier Arten von externen Audits:

Audit der Stufe 1: Hierbei handelt es sich um ein Audit zur Überprüfung der Dokumentation, bei dem der externe Prüfer analysiert, ob Ihre Organisation über alle erforderlichen Unterlagen für ein voll funktionsfähiges ISMS verfügt.

Ihre Dokumente müssen die in der Norm ISO/IEC 27001 geforderte Dokumentation abdecken. Die Zertifizierungsstelle wird sich die Zeit nehmen, um ein ausreichendes Verständnis des ISMS-Aufbaus im Kontext Ihrer Organisation, der Risikobewertung und -behandlung (einschließlich der festgelegten Kontrollen), der Informationssicherheitspolitik und der Ziele zu gewinnen. Ein großes Augenmerk wird auch auf die Vorbereitung Ihres Unternehmens auf das Audit gelegt. Dies ermöglicht die Planung für Stufe 2.

Audit der Stufe 2: Auf der Grundlage der im Auditbericht der Stufe 1 dokumentierten Feststellungen entwickelt die Zertifizierungsstelle einen Auditplan zur Durchführung von Stufe 2 des Audits. Neben der Bewertung der wirksamen Umsetzung des ISMS besteht das Ziel von Stufe 2 darin, zu bestätigen, dass Ihr Unternehmen seine eigenen Richtlinien, Ziele und Verfahren einhält.

Zu diesem Zweck wird sich das Audit auf folgende Punkte konzentrieren:

- Führung und Engagement des Top-Managements für die **Informationssicherheitspolitik** und die **Informationssicherheitsziele;**
- **Dokumentationsanforderungen** aus der ISO/IEC 27001;
- Bewertung der mit der Informationssicherheit verbundenen **Risiken** und dass die Bewertungen bei Wiederholung konsistente, gültige und vergleichbare Ergebnisse liefern;
- Festlegung von **Kontrollzielen** und **Kontrollen** auf der Grundlage der Risikobewertung der Informationssicherheit.
- **Prozesse zur Risikobehandlung;**

- Informationssicherheitsleistung und die **Wirksamkeit des ISMS**, die anhand der Informationssicherheitsziele bewertet werden;

- Übereinstimmung zwischen den festgelegten Kontrollen, **der Erklärung zur Anwendbarkeit** und den Ergebnissen der Risikobewertung der Informationssicherheit und des Risikobehandlungsprozesses mit der Politik und den Zielen der Informationssicherheit;

- **Umsetzung der Kontrollen (siehe Anhang A)** unter Berücksichtigung des externen und internen Kontextes und die damit verbundenen Risiken, die Überwachung, Messung und Analyse der Informationssicherheit durch die Organisation,

- **Prozesse und Kontrollen**, um festzustellen, ob die Kontrollen implementiert und wirksam sind und die angegebenen Ziele der Informationssicherheit erfüllen;

- **Programme, Prozesse, Verfahren, Aufzeichnungen, interne Audits und Überprüfungen der Wirksamkeit des ISMS**, um sicherzustellen, dass diese auf Entscheidungen der obersten Führungsebene und die Informationssicherheitspolitik und -ziele zurückgeführt werden können.

Wenn Sie die zweite Stufe abgeschlossen und das Audit bestanden haben, erhalten Sie Ihre offizielle Zertifizierung.

- **Überwachungsaudits/periodische Audits**: finden zwischen der Zertifizierung und den Rezertifizierungsaudits statt und konzentrieren sich auf bestimmte Bereiche des ISMS. Dies wird jedes Jahr durchgeführt.

- **Rezertifizierungsaudit**: Dies ist notwendig, um Ihre Zertifizierung aufrechtzuerhalten, deckt alle Aspekte der Norm ab und muss alle 3 Jahre durchgeführt werden.

DURCHFÜHRUNG VON INTERNEN AUDITS: WIE MAN DABEI VORGEHT

Interne Audits sind entscheidend für den langfristigen Erfolg bei der Erlangung und Aufrechterhaltung Ihrer ISO 27001-Zertifizierung. Sie sollten regelmäßig von Mitarbeitern des Unternehmens durchgeführt werden, im Gegensatz zu externen Auditoren, die in Ihr Unternehmen kommen, um Ihr ISMS zu bewerten.

Allerdings sind Unabhängigkeit und Qualifikation ein Muss für die Tätigkeit eines internen Auditors. Eine weitere Möglichkeit ist die Durchführung interner Audits mit externen Beratern, wie den Experten von DataGuard, die ebenfalls regelmäßige Audits anbieten. Interne Audits sind die beste Möglichkeit, Lücken in Ihrer Dokumentation zu finden und diese zu verbessern.

Wenn Sie sich zum ersten Mal zertifizieren lassen, stellt das interne Audit sicher, dass Sie alles haben, was Sie brauchen, um Ihre Zertifizierung auf Anhieb zu bestehen.

Eine Checkliste für interne Audits hilft Ihnen, den Überblick über die notwendigen Schritte in diesem Prozess zu behalten. Hier finden Sie einen Überblick über die Schritte eines internen Audits:

1. **Überprüfung der Dokumentation**

- Die gesamte Dokumentation des Verwaltungs- und Kontrollsystems sollte überprüft werden, um sicherzustellen, dass sie vollständig, korrekt und aktuell ist.
- Ein Team sollte mit dieser Aufgabe betraut werden.
- Das Team sollte klare Anweisungen erhalten, die es bei der Durchführung der Überprüfung zu befolgen hat.
- Die Dokumentation sollte auf Vollständigkeit, Genauigkeit, Konsistenz und Eignung für den vorgesehenen Zweck geprüft werden.
- Der Prüfer kontrolliert dann, ob Sie die erforderlichen Unterlagen haben und ob sie den Normen entsprechen.

2. **Überprüfung der Dokumentation**

- Das Management-Review-Team sollte die Unterlagen noch einmal durchgehen, um sicherzustellen, dass alle relevanten Informationen aufgezeichnet wurden und dass keine Informationen in den Unterlagen fehlen oder ausgelassen wurden.

- Schließlich muss die Leitung den Bericht durchsehen und die Prüfungsergebnisse berücksichtigen. Stellen Sie sicher, dass alle notwendigen Änderungen und Korrekturmaßnahmen umgesetzt werden.

Hier finden Sie eine vollständige Übersicht über die Durchführung eines internen Audits.

WIE LANGE DAUERT ES, SICH AUF EIN EXTERNES ISO 27001-AUDIT VORZUBEREITEN?

Je nach Größe Ihres Unternehmens oder Ihrer Organisation können Sie in bis zu 8 Wochen prüfungsreif sein. Wenn Sie sich für den manuellen Weg entscheiden und Ihre Dokumentation von Grund auf neu erstellen, kann dies mindestens 4 Monate dauern.

Es gibt einige Hauptanforderungen, die Sie erfüllen müssen, um Ihre ISO 27001 zu erhalten. Um Ihnen dabei zu helfen, haben wir eine Reihe von Checklisten zusammengestellt, die Ihnen einen Überblick über alles geben, was Sie für Ihre Zertifizierung benötigen. Hier finden Sie eine Übersicht der groben Vorbereitungsdauer, abhängig von der Unternehmensgröße:

- **1 bis 20 Mitarbeiter - bis zu 3 Monate**
- **20 bis 50 Mitarbeiter - 3 bis 5 Monate**
- **50 bis 200 Mitarbeiter - 5 bis 8 Monate**
- **Mehr als 200 Mitarbeiter - 8 bis 20 Monate**

Weiterhin ist es wichtig, verschiedene andere Variablen zu berücksichtigen, die sich auf die Zeit auswirken können, die Sie für den Erhalt der Zertifizierung benötigen:

- Die Anzahl der Personen, die am ISMS-Implementierungsprojekt beteiligt sind (im Verhältnis zur Größe des Unternehmens).
- Der Zeitaufwand, den der Einzelne bereit ist, für das Projekt aufzuwenden.
- Engagement / Befürwortung / Unterstützung durch die Führung.
- Die Größe des Unternehmens und die Komplexität.
- Verfügbarkeit eines externen Auditors für die Durchführung des externen Audits.

Bei der Implementierung Ihres ISMS kann es zu unvorhergesehenen Herausforderungen kommen, die auch die Zertifizierung verzögern können.

In unserer kostenlosen Roadmap für die Zertifizierung erfahren Sie alles, was Sie über den Weg zur Zertifizierung wissen müssen.

Laden Sie Ihren kostenlosen Leitfaden herunter.

"Unser Zeitplan betrug weniger als 6 Monate, und ohne DataGuard wäre das unmöglich gewesen."

WAS PASSIERT, WENN SIE DAS EXTERNE AUDIT NICHT BESTEHEN?

Der externe Prüfer gibt Ihnen in der Regel bereits während des externen Audits Hinweise darauf, ob Sie das Audit voraussichtlich bestehen oder nicht. Schwerwiegende Mängel können zu einem nicht bestandenen externen Audit führen.

Auch wenn dies wie ein großer Rückschlag erscheinen mag, sollten Sie es viel mehr als Chance zur Verbesserung sehen.

Sie werden einen Auditbericht erhalten, aus dem Sie erschließen können, was Sie ändern müssen, um Ihr nächstes externes Audit zu bestehen. Außerdem empfiehlt es sich, mit den Prüfern zu sprechen, um sich erklären zu lassen, was genau verbessert werden muss. So erhalten Sie nicht nur wertvolle Tipps, sondern demonstrieren auch Ihr Interesse an der Informationssicherheit.

Im Allgemeinen werden Nichtkonformitäten in folgende Kategorien eingeteilt:

- Größere Nichtkonformitäten
- Kleinere Nichtkonformitäten
- Möglichkeiten zur Verbesserung

Es gibt keine direkte Strafe für das Nichtbestehen eines externen Audits, aber das Nichtbestehen der Zertifizierung kann dazu führen, dass Sie kein angemessenes Risikomanagement haben, Rufschädigungen in Kauf nehmen und mit zusätzlichen finanziellen Kosten rechnen müssen.

Eine gründliche Vorbereitung und die Durchführung interner Audits verringern das Risiko eines Scheiterns erheblich. **Wenn Sie in der Vergangenheit bereits ein Audit nicht bestanden haben, empfehlen wir Folgendes:**

- Bewertung Ihres Auditberichts.
- Besprechen Sie das Ergebnis mit dem externen Prüfer.
- Kommunikation des Ergebnisses und der Gründe an alle relevanten Beteiligten und Sicherstellung der internen Abstimmung.
- Erstellung eines Aktionsplans mit nach Prioritäten geordneten Aufgaben, auch nach Fälligkeitsdatum und verantwortlichen Personen.
- Erneutes Einleiten des gesamten Prozesses zur Einrichtung und Verbesserung Ihres ISMS. Außerdem sollten Sie sicherstellen, dass genügend relevant Ressourcen zur Verfügung stehen, insbesondere für interne Audits.

- Sobald der Umfang der Verbesserung Ihres ISMS klar ist, legen Sie einen Termin für Ihr nächstes externes Audit fest.

WAS SIND DIE ANFORDERUNGEN DER ISO 27001-ZERTIFIZIERUNG?

Die wichtigsten Anforderungen für die ISO 27001-Zertifizierung sind: Dokumentation, Durchführung von Audits und Übernahme der Prozesse durch Ihre Mitarbeiter.

Die Dokumentation umfasst die Erstellung und Pflege der erforderlichen Unterlagen für Ihr Informationssicherheits-Managementsystem, wie z. B. Richtlinien, Verfahren, Risikobewertungen und Kontrollen.

Die Durchführung von Audits umfasst sowohl das Audit der Stufe 1, bei der Dokumentation und Bereitschaft geprüft werden, als auch das Audit der Stufe 2, bei der die praktische Umsetzung Ihres ISMS bewertet wird.

Der erfolgreiche Abschluss dieser Audits ist notwendig, um die ISO 27001-Zertifizierung zu erhalten. Außerdem müssen Sie sich internen Audits und Managementprüfungen unterziehen.

Entscheidend ist auch, dass die Prozesse effektiv kommuniziert werden. Damit soll sichergestellt werden, dass die Informationssicherheitspraktiken Ihrer Organisation mit den ISO 27001-Normen übereinstimmen. Sie müssen nicht nur über die Dokumentation verfügen, sondern auch die Prozesse in die Tat umsetzen, indem Sie sicherstellen, dass die Mitarbeiter sie kennen und befolgen.

→ **Lernen "ISMS Documentation Checklist"**

Die obligatorischen Dokumente, die für die ISO 27001-Norm erforderlich sind, haben wir unten für Sie aufgeführt. Alle Kriterien müssen befolgt und entsprechend dokumentiert werden, damit eine Organisation bei externen Audits vorgelegt werden kann.

Die Norm schreibt vor, dass Sie sich vor einem externen Audit einem internen Audit unterziehen müssen. Dadurch werden etwaige Lücken in Ihrem ISMS aufgedeckt.

Sobald Sie die Dokumentation erstellt und ein internes Audit sowie eine Managementbewertung durchgeführt haben, müssen Sie sich einem externen Audit durch eine zertifizierte Stelle unterziehen.

Die obligatorischen Dokumente, die für ISO 27001 erforderlich sind, sind:

- 4.1 Verstehen der Organisation und ihres Kontexts
- 4.2 Verstehen der Bedürfnisse und Erwartungen der interessierten Parteien
- 4.3 Der Anwendungsbereich des ISMS
- 4.4 Der Prozess des Informationssicherheits-Managementsystems
- 5.1 Die Verpflichtung des ISMS
- 5.2 Informationssicherheitsrichtlinien
- 5.3 Rollen und ihre Verantwortlichkeiten (RACI/RASCI)
- 6.1.2 Prozess der Bewertung und Behandlung von Informationssicherheitsrisiken
- 6.1.3 Plan zur Behandlung und Bewertung von Informationssicherheitsrisiken
- 6.1.3 Die Erklärung zur Anwendbarkeit
- 6.2 Ziele der Informationssicherheit
- 6.3 Änderungsmanagement für das ISMS
- 7.1 Ressourcenplanung
- 7.3 Plan zur Sensibilisierung
- 7.4 Kommunikationsplan
- 7.2 Kompetenznachweis
- 7.5 Dokumentenkontrollpolitik
- 5.5.1 Dokumentierte Informationen, die von der Organisation als notwendig für die Wirksamkeit des ISMS erachtet werden
- 8.1 Operative Planung und Kontrolle
- 8.2 Ergebnisse der Risikobewertung der Informationssicherheit
- 8.3 Ergebnisse der Behandlung von Informationssicherheitsrisiken
- 9.1 Nachweise für die Überwachung und Messung der Ergebnisse
- 9.2 Ein dokumentiertes internes Auditverfahren
- 9.2 Nachweis der Auditprogramme und der Auditergebnisse
- 9.3 Nachweis über die Ergebnisse von Managementprüfungen
- 10.1 Nachweis der Art der Nichtkonformitäten und der daraufhin ergriffenen Maßnahmen
- 10.1 g) Nachweis über die Ergebnisse von Korrekturmaßnahmen

Eine vollständige Aufschlüsselung der ISO 27001-Anforderungen finden Sie in diesem Beitrag: ISO 27001 Anforderungen: Vorbereitung auf die Zertifizierung.

WAS SIE BEI EINEM EXTERNEN AUDIT ERWARTEN KÖNNEN

Wenn Sie Ihr internes Audit erfolgreich durchlaufen haben, ändert sich in Sachen Ablauf beim anstehenden externen Audit im Grunde nicht mehr viel für Sie. Ein Auditor kommt in Ihr Unternehmen, überprüft Ihr ISMS und spricht mit Ihren Mitarbeitern.

Der Gesamtprozess sieht folgendermaßen aus:

1. Dokumentenprüfung

Zunächst wird der externe Prüfer Ihre gesamte ISMS-bezogene Dokumentation überprüfen. Es ist inzwischen auch üblich, dass die Prüfer dies aus der Ferne tun können. Wenn Sie sie jedoch in Ihr Unternehmen einladen, damit sie Ihr Team kennenlernen können, schafft dies von Anfang an Vertrauen.

2. Audit vor Ort

In der zweiten Stufe wird ein Vor-Ort-Audit durchgeführt. Einige Ihrer Mitarbeiter werden befragt, und Ihre Systeme werden stichprobenartig überprüft. Neben Mitarbeitern wie Ihrem CISO/ISB, die direkt mit dem ISMS befasst sind, sollte Ihr CFO oder CEO dem Prüfer die Gewissheit geben, dass die finanziellen Mittel für den Betrieb des ISMS fest verankert sind.

Sie werden bereits während der Inspektion wissen, ob Sie das Audit bestehen und die Zertifizierung erhalten werden, da der Auditor kleinere und vielleicht sogar größere Probleme direkt ansprechen wird.

Schwerwiegende Verstöße führen zu einem nicht bestandenen Audit. Das Einzige, was bleibt, ist die gemeinsame Festlegung des Termins und der Bedingungen für ein Folgeaudit.

3. Auditbericht und ISO 27001-Zertifikat

Schließlich erhalten Sie von Ihrem Auditor einen Auditbericht und das Zertifikat. Viele Zertifizierungsunternehmen sind derzeit sehr beschäftigt, so dass dies einige Monate dauern kann.

WAS SIND ISO 27001-CONTROLS, UND WIE GEHT MAN BEI DER UMSETZUNG VOR?

Eine Control ist eine Maßnahme zum Managen von Risiken.

In der 2022er-Version der ISO 27001 gibt es im Anhang A insgesamte 93 sogenannter Controls, die verschiedene Bereiche einer Organisation abdecken.

Diese Kontrollen sind in 4 verschiedene Kategorien (Domänen) unterteilt. Je nachdem, welche für Ihr Unternehmen, Ihre Risiken, Ihre Branche und Ihre Kunden relevant sind, werden Sie die Anforderungen in den einzelnen Anhängen erfüllen.

Zu den üblichen Controls gehören:

- A.8 Asset Management
- A.14 Entwicklung und Wartung der Systemlandschaft
- A.10 Kryptographie
- A.18 Compliance

Sie möchten mehr über die Kontrollen und ihre Umsetzung erfahren? Hier können Sie tief eintauchen: ISO 27001 Anhang A Controls - Ein detaillierter Leitfaden.

DIE KOSTEN DER ISO 27001-ZERTIFIZIERUNG

Die Kosten für die Zertifizierung lassen sich in drei Phasen unterteilen: Implementierung (Ihres ISMS), interne Prüfung und Zertifizierung.

Interne Kosten

Diese Kosten können umfassen:

- Interne Personalkosten
- Beratungskosten
- Managementressourcen für Überprüfungen und Kommunikation
- Ressourcen für Projektmanagement und Sensibilisierung des Personals
- Software-Tools zur Unterstützung der Einrichtung eines ISMS

Externe Kosten

Hierbei handelt es sich im Allgemeinen um die Kosten für den Auditor; im Durchschnitt belaufen sich die Kosten für ein Audit pro Tag auf 1000 Euro - die Anzahl der Tage und die Frage, ob Sie ein Fern- oder ein Vor-Ort-Audit durchführen werden, wirken sich auf die externen Kosten aus.

Beispielhafte Aufschlüsselung der Kosten für die ISO 27001-Zertifizierung

Nachstehend finden Sie eine beispielhafte Aufschlüsselung der Kosten, die Sie in den einzelnen Phasen erwarten können:

Implementierung

- Vorzertifizierung Phase I (Umfang, Definition, Risikobewertung, Risikobehandlungsplan, Lückenbewertung), Phase II (Sanierungsplan) – 15.000 Euro.
- Vorzertifizierungsphase II (Lückenschluss, Auswahl des Registrators, Entwicklung von ISMS-Artefakten, Risikomanagement Ausschuss, Reaktion auf Vorfälle, internes ISMS-Audit, Unterstützung des Zertifizierungsaudits vor Ort) - 10.000 Euro.
- Durchschnittliches Jahresgehalt eines Compliance-Managers (USA) - 100.000 Euro (Nur wenn Ihre Organisation diese Position besetzt hat).
- Durchschnittliche jährliche Kosten für Compliance-Software und -Tools - 15.000 Euro bis 100.000 Euro.

Interne Rechnungsprüfung

Kosten für Compliance-Berater - 140/Stunde Euro, für etwa 24 bis 160 Beratungsstunden

Certification

Kosten für einen ISO 27001-Auditor - 5.500 Euro bis 18.000 Euro

Kosten für Überwachungsaudits

- Jahresgehalt eines Compliance-Spezialisten - 75.000 Euro bis 90.000 Euro.
- Kosten für das ISO 27001-Audit - 5.500 Euro bis 12.000 Euro

Die Gesamtkosten für die ISO 27001-Zertifizierung liegen zwischen 10.000 Euro und 48.000 Euro. Um die Kosten für Ihre eigene ISO 27001-Zertifizierung zu kalkulieren, empfehlen wir Ihnen, so viel wie möglich zu recherchieren, Angebote von verschiedenen Beteiligten einzuholen und Preise zu vergleichen. Durch den Einsatz von Software-Tools, die den Zertifizierungsprozess rationalisieren, kann Ihr Budget erheblich gesenkt werden.

Hier finden Sie eine vollständige Aufschlüsselung der Kosten für die Erlangung von ISO 27001.

**Bitte beachten Sie, dass es sich bei den Kostenangeben lediglich um Annahmen basierend auf internen Erfahrungen handelt und Kosten jederzeit abweichen können.*

LOHNT SICH DIE INVESTITION?

Die Informationssicherheit wird immer wichtiger und sollte einfach nicht ignoriert werden. Da Ransomware und Cyberangriffe Jahr für Jahr zunehmen, erkennen die Unternehmen, dass ein präventiver Ansatz besser ist, als den Ruf und das finanzielle Chaos zu bereinigen, wenn etwas passiert ist.

Zwei Statistiken, die jede Diskussion um den Wert einer Investition in Cyber- und Informationssicherheit erübrigen und die Frage unmittelbar beantworten, haben wir für Sie im Folgenden herausgearbeitet:

Laut Statista lag die Gesamtschadenssumme für Cyberkriminalität im Jahr 2022 bei insgesamt 202,7 Milliarden Euro. Verursacht wurde die Summe vor allem durch Datendiebstahl, Industriespionage oder Sabotage.

Zudem stiegen die weltweiten Investitionen in Cybersicherheit zwischen 2017 und 2023 von 34 auf 79,5 Milliarden US-Dollar – ein Anstieg um mehr als das doppelte.

Am Ende bleibt es jedem Unternehmen selbst überlassen, über Investitionen in Cyber- und Informationssicherheit zu entscheiden. Eine Zertifizierung nach ISO 27001 ist aber mit Sicherheit eine kostengünstige und zukunftssichere Variante, sich effizient abzusichern.

Natürlich müssen Sie Ihren individuellen ROI für die Zertifizierung nach ISO 27001 berücksichtigen. Ein Gespräch mit einem Experten für Informationssicherheit kann Ihnen eine Vorstellung davon vermitteln, welche Kosten Sie erwarten können und ob sich die Investition lohnt.

Gleichzeitig hat die Art und Weise, wie Sie sich zertifizieren lassen - z. B. mit Hilfe einer prozessgesteuerten Plattform, die von Experten unterstützt wird, oder durch die Einstellung eines internen Compliance-Managers - einen erheblichen Einfluss darauf, wie viel Sie investieren müssen und ob sich dies langfristig lohnt.

WIE MAN MIT DER ISO 27001-ZERTIFIZIERUNG BEGINNT

Wie Sie sehen, gibt es viele Aspekte, über die Sie nachdenken müssen, wenn Sie die ISO 27001-Zertifizierung erreichen wollen. Aber der beste Zeitpunkt, um damit zu beginnen, ist jetzt. Lassen Sie Ihr ISMS mit Ihnen wachsen und skalieren.

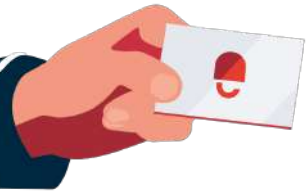
Die empfohlene und gängige Praxis für den Einstieg in die ISO 27001-Norm ist folgende:

- Suchen Sie sich einen **qualifizierten Berater und/oder eine Plattform**, um ein erstes Beratungsgespräch zu führen, damit Sie sich über den Umfang, die Kosten und den Zeitplan, den Sie für Ihr Unternehmen erwarten können, klar werden können.

- Entwickeln Sie einen **Projektplan** und einen **Zeitplan**, in dem alle **wichtigen Beteiligten** genannt werden.

- Sorgen Sie für die **Zustimmung der Geschäftsleitung**. Informationssicherheit muss ganzheitlich angegangen werden, um die Vermögenswerte des gesamten Unternehmens zu schützen. Erstellen Sie also einen Plan, um grünes Licht und die aktive Beteiligung des gesamten Teams zu erhalten.

- Beginnen Sie mit der **Festlegung Ihres Geltungsbereichs** und arbeiten Sie sich durch die Zertifizierungsschritte.



DataGuard ist ein Compliance-Software-Unternehmen mit Fokus auf Datenschutz und Informationssicherheit. Als einer der europäischen Marktführer im Bereich Compliance-SaaS ermöglicht DataGuard Tausenden KMU und Großunternehmen die unkomplizierte Operationalisierung von Datenschutz (Privacy), Informationssicherheit und Compliance (kurz: „PIC"). Mit seiner Komplettlösung reduziert DataGuard für Unternehmen Zeit und Kosten bei der Einhaltung von Datenschutzgesetzen wie der DSGVO, der Einholung und Verwaltung von Einwilligungen und Präferenzen oder beim Erhalten von Zertifizierungen wie der ISO 27001. So können sich Kunden auf ihr Kerngeschäft konzentrieren, Mehrwert durch Vertrauen und Compliance schaffen und gleichzeitig Risiken minimieren. DataGuard hat Standorte in München, Berlin, London und Wien.

Jetzt Termin vereinbaren, um über Ihre Herausforderungen zu sprechen und erste Schritte zu definieren:

Erstgespräch buchen

Weiterführende Ressourcen:

→ **Leitfaden zum Übergang zur ISO 27001:2022**

→ **Die Vorteile einer ISO 27001-Zertifizierung**

→ **4 häufige Fehler bei der ISO 27001 Implementierung**

dataguard.de kontakt@dataguard.de +49 89 452 459-900

DataGuard