DataGuard POWERS ISO 27001

ISO 27001-Implementierungs-Roadmap

Ihr Leitfaden für die Einführung von ISO 27001:
Die Zertifizierung erhalten und behalten

DataGuard

Leitfaden für die Einführung von ISO 27001: Die Zertifizierung erhalten und behalten

Ein **klarer und gut strukturierter Plan** macht den Weg zur **ISO-27001-Zertifizierung** weniger holprig. Der Implementierungsfahrplan von DataGuard dient als Kompass, der Sie bei Ihrer Zertifizierung leitet und Ihnen zeigt, wie Sie diese **beibehalten** können.

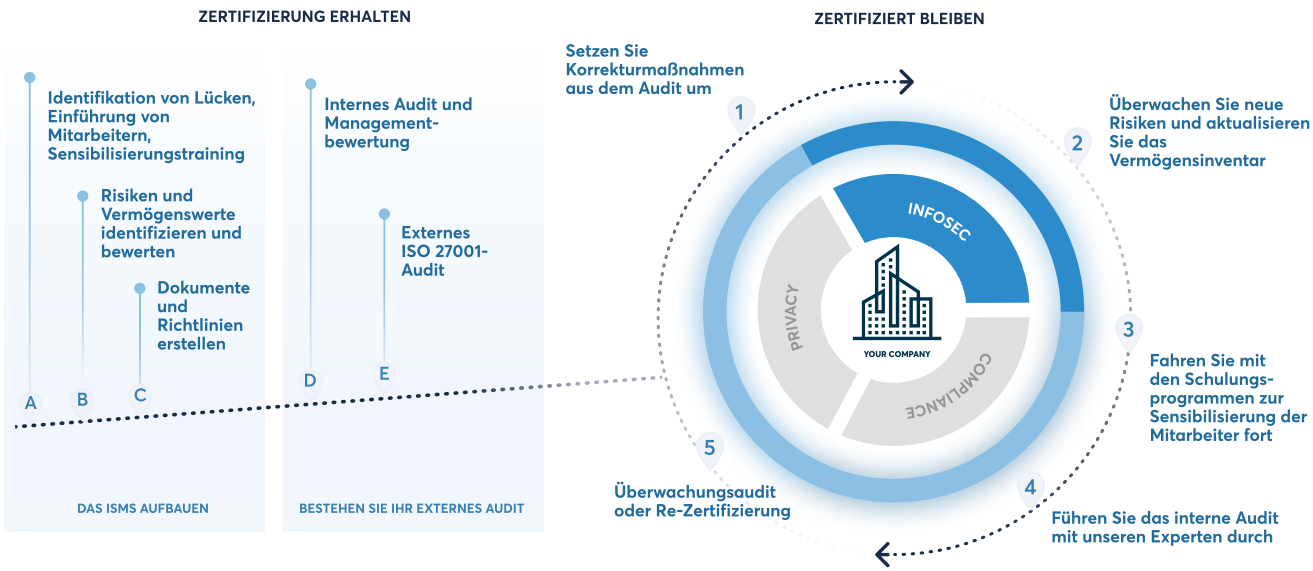
Betrachten Sie die ISO 27001-Zertifizierung als einen kontinuierlichen Prozess

Wir erwähnen immer wieder, wie wichtig es ist, die ISO 27001-Zertifizierung nach Erhalt auch weiterhin aufrechtzuerhalten – und das hat durchaus seine Gründe. Betrachten Sie diesen Prozess als fortlaufend, **die ISO 27001-Zertifizierung ist auf dem Weg zur Informationssicherheit lediglich eine Kontrollinstanz.**

Ihr Unternehmen funktioniert wie ein lebender Organismus; Strategien und Prozesse entwickeln sich kontinuierlich weiter. Sie fügen neue Anlagen hinzu, erwerben innovative Software oder gehen neue Partnerschaften ein. Somit verändert sich auch der Stand Ihrer Informationssicherheit, da neue Bedrohungen entstehen und auftreten können.

Wir raten daher dazu, auch nach einer erfolgreichen Zertifizierung regelmäßig Ihr Informationssicherheits-managementsystem (ISMS) zu überprüfen. Überwachen Sie Ihre Vermögenswerte und Risiken und stellen Sie sicher, dass entsprechende Kontrollinstanzen eingerichtet sind. So sind Ihre Informationen nicht nur gesichert, sondern auch gegen etwaige Cyberangriffe gewappnet. **Auf eine erneute Zertifizierung sind Sie somit bestens vorbereitet** (siehe Abbildung nächste Seite).

→



Ihr Weg zur ISO 27001-Zertifizierung: Was & Wie

Auf dem Weg zu Ihrem ISO 27001-Zertifikat ist jede Station wichtig – von der Gap-Analyse bis hin zum internen Audit als Probe für die externe Prüfung. Jeder Teil spielt eine Rolle bei der Vorbereitung und Aufrechterhaltung Ihres ISMS, damit es den ISO 27001-Richtlinien entspricht.

Im Laufe der Jahre haben wir Unternehmen aus verschiedenen Branchen bei ihrer ISO 27001-Zertifizierung begleitet. **Unsere Reise beginnt mit einer Gap-Analyse.** →

DataGuard

1. Identifizieren Sie sorgfältig mögliche Schwachstellen

Um Ihr Vermögen zu schützen, müssen Sie Ihre Schwachstellen kennen.

Betrachten Sie die Gap-Analyse als ein unverzichtbares Werkzeug, mit dem Sie den Stand der Informationssicherheit in Ihrem Unternehmen bewerten können – ähnlich zu einem Lackmustest. Sie hilft Ihnen dabei, Ihr Unternehmen zu bewerten und festzustellen, welche essentiellen Prozesse und Sicherheitsvorkehrungen bereits umgesetzt werden und welche eventuell noch ergänzt werden sollten.

Die Gap-Analyse bietet einen umfassenden Überblick darüber, inwieweit Ihr Unternehmen den Sicherheitsstandards der ISO-27001 entspricht und was Sie für eine optimale Vorbereitung auf das externe Audit noch anpassen müssen (mehr dazu später).

Diese Punkte machen eine Gap-Analyse so bedeutsam:

- **Es werden Schwachstellen aufgedeckt:** Die Gap-Analyse gleicht einem Sicherheitsaudit. Sie hilft Ihnen dabei, Schwachstellen in Ihrer aktuellen Sicherheitsstruktur aufzudecken.
- **Regeln werden eingehalten:** Verschiedene Branchen haben ihre eigenen Sicherheitsregeln. Die Gap-Analyse dient als Leitfaden, um sicherzustellen, dass Sie alle Anforderungen erfüllen und auf dem neuesten Stand bleiben.
- **Bessere Ressourcen- und Budgetplanung:** Die Gap-Analyse unterstützt Sie dabei, Ihre Ressourcen effektiv zu nutzen. Durch frühzeitige Identifizierung von Schwachstellen können Sie Ihr Budget besser planen.
- **Sie bleiben auf dem Laufenden:** Die Gap-Analyse ist keine einmalige Angelegenheit. Sie ist ein regelmäßiger Check-up, der sicherstellt, dass Ihr Unternehmen in puncto Sicherheit stets auf dem neuesten Stand ist.

So machen wir es Ihnen leichter:

Die Gap-Analyse in Ihrem Unternehmen beginnen wir mit einfachen Fragebögen, die von Ihnen selbst ausgefüllt werden können. Nachdem Sie die Fragen beantwortet haben, erstellen Sie gemeinsam mit Ihrem persönlichen DataGuard-Experten einen Projektplan zur Verbesserung des Reifegrads Ihrer Informationssicherheit.

2. Haben Sie Ihre Informationsbestände im Blick

Organisieren Sie sich von Beginn an. Welche digitalen Informationen in Ihrer Organisation müssen geschützt werden?

Oder anders ausgedrückt: Was steht auf dem Spiel? In dieser Phase der ISO 27001-Zertifizierung überprüfen und organisieren Sie alle Ihre Informationsbestände, vor allem solche, die besonders geschützt werden müssen.

Sie kontrollieren und verwalten alle Ihre digitalen Daten, einschließlich der Zugriffsrechte der Benutzer, wodurch Sie einen umfassenden Überblick gewinnen. So können Sie leichter feststellen, welche Sicherheitsvorkehrungen notwendig sind, um diese Ressourcen sicher und zuverlässig schützen zu können.

Genau deshalb ist das Asset Management von entscheidender Bedeutung:

- **Es schützt Ihre Wertsachen:** Betrachten Sie die Vermögensverwaltung als Schutz Ihrer digitalen Schätze, wie z. B. Kundendateien, um sie privat und korrekt zu halten.
- **Es gewährleistet die Einhaltung von Gesetzen:** Unternehmen müssen verschiedene Vorschriften zur Informationssicherheit einhalten. Die Verwaltung von Informationsbeständen hilft Ihnen dabei, diese Vorschriften einzuhalten.
- **Sie finden jederzeit genau das, was sie gerade brauchen:** Eine gute Verwaltung von Informationsbeständen ermöglicht es Ihrem Team, Daten leichter zu finden und zu nutzen. Dadurch wird Ihre Arbeit schneller und sinnvoller macht.
- **Planung des Lebenszyklus:** Das Asset Management entrümpelt Ihren digitalen Raum. Zu wissen, wann digitale Informationen erstellt, gespeichert oder gelöscht werden sollen, schafft Klarheit und verringert das Risiko.
- **Sie bleiben auf dem Laufenden:** Digitale Informationen und Bedrohungen verändern sich ständig. Regelmäßiges Asset Management hilft Ihnen dabei, mit den neuesten Trends und Gefahren Schritt zu halten.

So machen wir es Ihnen leichter:

Wir bieten Ihnen eine Plattform für Ihr Asset Management. Alle Ihre schützenswerten Informationsbestände befinden sich unter einem Dach und wir helfen Ihnen, diese zu verwalten. Sie können bereits bestehende Bestände importieren oder neue Bestände an einem zentralen Ort erstellen.

3. Risiken identifizieren und managen

Risikomanagement ist ein systematischer Ansatz zum Schutz der Daten und der digitalen Infrastruktur Ihres Unternehmens.

In diesem Schritt ermitteln und verfolgen Sie alle Risiken, die die Informationssicherheit Ihres Unternehmens beeinträchtigen.

Darum ist das Risikomanagement so wichtig:

- **Sie haben alle Risiken im Überblick:** Sie wissen, was Sie erwarten könnte. Ähnlich wie die Gap-Analyse hilft das Risikomanagement, potenzielle Bedrohungen und Schwachstellen zu erkennen.
- **Sie gehen Schwierigkeiten aus dem Weg:** Indem Sie die Risiken im Auge behalten, minimieren Sie rechtliche Probleme und Bußgelder. Es ist zudem wahrscheinlicher, dass Sie sich an die Branchenvorschriften halten.
- **Ihr Ruf bleibt intakt:** Effektives Risikomanagement ermöglicht es Ihnen, Bedrohungen im Keim zu ersticken. Sie schützen Ihren guten Ruf, indem Sie potenziellen Problemen vorbeugen.

So machen wir es Ihnen leichter:

Das Identifizieren von Risiken kann gerade dann knifflig werden, wenn man es zum ersten Mal angeht oder noch nicht viel über den Prozess weiß. Wir unterstützen Sie dabei, sämtliche Risiken, die sich auf die Informationssicherheitsziele Ihres Unternehmens auswirken, auf einer einzigen Plattform zu identifizieren und nachvollziehbar zu machen. Vorkenntnisse im Risikomanagement sind hierfür nicht erforderlich – unsere Experten, sowie Videos und Leitfäden begleiten Sie durch den gesamten Prozess. Zusätzlich haben Sie die Möglichkeit, Ihre bestehenden Risiken in Echtzeit auf Dashboards zu überprüfen.

4. Erstellen Sie eine Dokumentation Ihrer Sicherheitsrichtlinien

Auf dem Weg zur ISO 27001-Zertifizierung benötigen Sie eine angemessene Dokumentation zur Unterstützung Ihrer Sicherheitsrichtlinien und -verfahren. Sie hilft Ihnen auch dabei, organisiert zu bleiben.

Hier erfahren Sie, warum eine Dokumentation wichtig ist:

- **Sie legt Sicherheitsregeln fest:** In der Dokumentation zur Informationssicherheit werden die wesentlichen Regeln für den Schutz von Daten und digitalen Systemen festgelegt.
- **Sie setzt Pläne in die Tat um:** Sobald die Regeln festgelegt sind, leitet die Dokumentation Unternehmen bei der Implementierung von Sicherheitskontrollen wie Firewalls und Zugangsbeschränkungen an.
- **Sie ist Wesentlich für die Einhaltung der Vorschriften:** Sie benötigen spezifische Richtlinien und Dokumente, um die Einhaltung der Vorschriften nachweisen zu können und sich auf die Prüfung vorzubereiten.

So machen wir es Ihnen leichter:

Auf unserer Plattform können Sie auf gebrauchsfertige Vorlagen und Richtlinien zurückgreifen. Somit müssen Sie nicht von Grund auf alles neu erstellen. Unsere Experten unterstützen Sie bei der Überprüfung Ihrer Dokumente und stellen sicher, dass sie für die Audits geeignet sind.

5. Schulen Sie Ihr Team zum Thema Sicherheit

Informieren Sie Mitarbeiter und Stakeholder kontinuierlich über Sicherheitsrichtlinien und bewährte Verfahren, um das Bewusstsein für die Informationssicherheit zu schärfen.

Darum ist dies im Zusammenhang mit der ISO 27001-Zertifizierung wichtig:

- **Alle ziehen am selben Strang:** Jeder versteht und befolgt die standardisierten Informationssicherheitspraktiken, die durch die Zertifizierung vorgeschrieben sind.
- **Weniger Risiken:** Gut informierte Personen sind besser in der Lage, potenzielle Sicherheitsrisiken zu erkennen und Ihnen entgegenzuwirken.

So machen wir es Ihnen leichter:

Sie können Ihre Mitarbeiter in unseren On-demand-Sicherheitsschulungen über die DataGuard Academy einschreiben, ein interaktives E-Learning-Feature auf unserer Plattform. Die Kurse behandeln Grundlegendes zur DSGVO und Informationssicherheit, sowie spezialisierte Themen wie Phishing, Incident Response und Künstliche Intelligenz.

6. Führen Sie ein internes Audit durch

Betrachten Sie Ihr internes Audit als eine Art Generalprobe vor dem externen Audit.

Bei einem externen Audit bewertet ein Prüfer Ihr ISMS (Informationssicherheits-Managementsystem) in Bezug auf den Schutz sensibler Informationen, das Risikomanagement und die Einhaltung der Anforderungen der ISO 27001. Während ein externes Audit von einem akkreditierten Zertifizierungsdienst (CB) durchgeführt wird, führen Sie eine interne Überprüfung unabhängig durch – es sei denn, Sie arbeiten mit einem Partner wie DataGuard zusammen.

Das macht das interne Audit so wichtig:

- **Identifikation von Schwachstellen:** Interne Audits helfen dabei, Schwachstellen in den Praktiken der Informationssicherheit zu identifizieren und ermöglichen präventive Maßnahmen, bevor das externe ISO-27001-Audit stattfindet.
- **Reibungsloses externes Audit:** Durch die frühzeitige Behebung von Problemen ebnet die interne Prüfung den Weg für einen reibungslosen externen ISO-27001-Audit und steigert die Wahrscheinlichkeit einer erfolgreichen Zertifizierung.

Wie wir es Ihnen leichter machen:

Wir nehmen Ihnen den Stress ab, den die Durchführung eines internen Audits mit sich bringt. Unsere Experten unterstützen Sie dabei, ein internes Audit durchzuführen, um sicherzustellen, dass Sie alle Richtlinien, Kontrollen und Prozesse haben, um das externe Audit zu bestehen. Bis heute liegt die Erfolgsquote unserer Kunden, das externe Audit im ersten Anlauf zu bestehen, bei 100 %.

7. Halten Sie Ihre Zertifizierung aufrecht

Die Einhaltung der ISO-27001-Standards endet nicht mit der offiziellen Zertifizierung nach einem erfolgreichen externen Audit.

Wenn neue Risiken auftauchen oder Sie und Ihre Organisation sich weiterentwickeln, müssen auch Ihre Informationssicherheitsmaßnahmen kontinuierlich überprüft und angepasst werden. So halten Sie Ihre Zertifizierung aufrecht.

Wie wir es Ihnen leichter machen:

Wir unterstützen Sie dabei, Ihre Assets zu aktualisieren, Risiken zu minimieren, Schulungen für Mitarbeiter durchzuführen, sicherzustellen, dass Richtlinien und Kontrollen auf dem neuesten Stand sind – und letztendlich dabei, Ihre Organisation auf jährliche Überwachungsaudits vorzubereiten.

Ihre Reise zur ISO 27001-Zertifizierung beginnt jetzt

Es gibt viel zu beachten, das wissen wir.

Dennoch ist die ISO-27001-Zertifizierungsreise viel weniger herausfordernd, wenn Sie eine dedizierte Plattform und einen zuverlässigen Partner an Ihrer Seite haben, der Sie durch jeden Abschnitt des Zertifizierungskreises führt.

Wir hoffen, dass dieser Umsetzungsleitfaden Ihnen einen guten Überblick darüber gegeben hat, was Sie in Ihrem ISO-27001-Zertifizierungsprojekt erwarten wird.

Wenn Sie bereit sind, vereinbaren Sie ein kostenloses 30-minütiges Gespräch mit einem unserer Informationssicherheitsexperten und lassen Sie sich gemeinsam mit uns zertifizieren.

DataGuard

Für Compliance entwickelt.
Für Sie gemacht.

Für weitere Infos besuchen Sie dataguard.de

DataGuard ist ein Software-as-a-Service-Unternehmen (SaaS), spezialisiert auf Datenschutz, Informationssicherheit und Compliance. Die Plattform unterstützt bei der Einhaltung von Datenschutzrichtlinien (z. B. DSGVO, CCPA, NIS2, EU-Whistleblower-Richtlinie) und der umfassenden Verwaltung von Informationssicherheitszertifizierungen (z. B. ISO 27001, TISAX®, SOC 2). DataGuard befähigt mehr als 3.500 Unternehmen jeglicher Größe in mehr als 50 Ländern täglich darin, die Menschen hinter den Daten zu schützen. Zeitsparende Automatisierung, nahtlose Integrationsmöglichkeiten und kompetente Expertenberatung minimieren Risiken, sparen Ressourcen und schaffen gleichzeitig Mehrwert durch erhöhtes Vertrauen und Transparenz. Das Unternehmen beschäftigt mehr als 250 Mitarbeitende weltweit mit Niederlassungen in München, Berlin, London und Wien.

DataGuard