CONSULTING

AWARE7

ISO 27001:2022

Whitepaper 2023

Inhaltsangabe

Was ist die ISO 27001:2022?

In der heutigen digitalen Welt ist der Schutz von Informationen und Daten ein entscheidender Aspekt für jedes Unternehmen. Die ISO 27001 bietet einen umfassenden Ansatz für Informationssicherheitsmanagement, um Unternehmen dabei zu helfen, ihre Daten, IT-Systeme und anderweitige Werte zu schützen.

In diesem Whitepaper erhalten Sie einen Überblick über die ISO 27001, die Schritte zur Implmentierung und die Vorteile für Ihr Unternehmen. Darüber hinaus wird die neue Version aus 2022 vorgestellt, inklusive der Chancen und Herausforderungen die sich aus dieser ergeben.

Die ISO 27001 ist eine international anerkannte Norm für Informations- sicherheitsmanagementsysteme (ISMS) und wurde von der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC) entwickelt.

Sie wurde ursprünglich als BS-7799- 2:2002 von der British Standards Institution in den 1990er Jahren veröffentlicht. 2005 wurde durch die ISO die Version ISO/IEC 27001:2005 veröffentlicht, 2013 auf die Version ISO/IEC 27001:2013, und schlussendlich 2017 auf die ISO/IEC 27001:2017 aktualisiert.

Bedeutung eines Informationssicherheits-managmentsystems (ISMS)

Die Implementierung eines Informations- sicherheitsmanagementsystems (ISMS) gemäß ISO 27001 ermöglicht es Unternehmen, Sicherheitsrisiken auf systematische Weise zu erkennen und zu bewerten. Auf Grundlage dieser Einschätzungen können anschließend passende Sicherheits-strategien angewendet werden, um die Auswirkungen der ermittelten Risiken zu mindern oder auf ein akzeptables Maß zu senken. Dies resultiert in einer generellen Stärkung der Sicherheit und schützt das Unternehmen vor möglichen Gefahren und deren Folgen. Zudem hilft die Einhaltung der ISO 27001 Unternehmen, gesetzliche und regulatorische Anforderungen in Bezug auf Infor-mationssicherheit und Datenschutz zu erfüllen.

Durch die Implementierung eines ISMS können Unternehmen nachweisen, dass sie angemessene Sicherheits- maßnahmen getroffen haben, um die Vertraulichkeit, Integrität und Verfügbarkeit ih-rer Informationen zu schützen. Eine Zertifizierung nach ISO 27001 signalisiert Kunden, Partnern und Stakeholdern außerdem, dass ein Unternehmen die Informationssicherheit ernst nimmt und nach international anerkannten Standards handelt. Dies erhöht das Vertrauen in das Unternehmen und seine Fähigkeit, Informationen sicher zu verwalten und zu schützen.

Insbesondere vor dem Hintergrund der Einführung von NIS-2 im Oktober 2024 für in der EU ansässige Unternehmen sollte die Implementierung eines ISMS und somit eine ISO 27001 Zertifizierung in Betracht gezogen werden. Das Ziel der NIS-2 Richtlinie ist die bessere Vorbereitung von Unternehmen auf digitale Bedrohungen, um Sicherheitsvorfälle transparenter zu gestalten und effektiver vermeiden zu können. So sollen Reaktionszeiten gegenüber Cyberangriffen reduziert und ein Überblick über die aktuelle Sicherheitslage in den Mitgliedsstaaten geschaffen werden.

Diese Richtlinie fordert von Unternehmen, dass sie unter anderem die folgenden Maßnahmen umsetzen:

- Vorfallsmanagement
- Aufrechterhaltung des Betriebs (Business Continuity Management)
- Sicherheit der Lieferkette (Suppy Chain Security)
- Schulung und Training
- Management von Werten (Asset Management)
- Dokumentationspflichten

Bei Nichtbeachtung drohen Sanktionen in Form von Geldbußen in Höhe von bis zu 20 Millionen Euro bzw. 4 % des Vorjahresumsatzes.
Auch Sicherheitsvorfälle selbst können die Geschäftsfähigkeit eines Unternehmens ernsthaft gefährden und langfristige Auswirkungen haben. In jedem Fall ist die Stärkung der eigenen Informationssicherheit ein nicht zu vernachlässigender Bestandteil des Unternehmenserfolges.

Übersicht ISO 27001:2022

Die ISO 27001, entwickelt von der ISO und IEC, legt die Anforderungen für ein Informationssicherheitsmanagement- system (ISMS) fest. Dieses ist ein systematischer Ansatz für das Management von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen durch die Anwendung eines Risikomanagementprozesses und der Festlegung von entsprechenden Sicherheitsrichtlinien.

Die Norm ist auf alle Organisationsarten anwendbar, unabhängig von Größe oder Art des Geschäfts. Sie umfasst alle Aspekte der Informationssicherheit, von digitalen Daten bis hin zu physischen Sicherheitsmaßnahmen und betrieb- lichen Prozessen.

Struktur und Inhalte

Um die Informationssicherheit möglichst umfänglich abzusichern und zu stärken, umfasst die ISO 27001 viele unterschiedliche Bereiche eines Unternehmens. Dadurch ergeben sich die wichtigsten Bestandteile:

- **Kontext der Organisation**
  Verständnis der Organisation, um den Umfang des ISMS festzulegen
- **Führung**
  Rolle des Managements bei der Einrichtung und Aufrechterhaltung des ISMS
- **Planung**
  Festlegung von Anforderungen und Bewertung von Risiken
- **Unterstützung**
  Ressourcen und Kompetenzen, welche für das ISMS notwendig sind
- **Betrieb**
  Bewertung und Behandlung von Risiken sowie Einrichtung entsprechender Sicherheitsmaßnahmen
- **Leistungsbewertung**
  Messung und Evaluierung des ISMS für eine stetige Verbesserung
- **Verbesserung**
  Durchführung von Korrekturmaßnahmen, um die Informationssicherheit stetig zu steigern

Zusätzlich zu den genannten Normkapiteln umfasst die ISO 27001 einen Anhang mit Maßnahmen, die je nach Risikoprofil der Organisation angewendet werden können. Hierbei ist es wichtig darauf zu achten, dass diese nicht als eine Einheitslösung betrachtet werden können. Die Auswahl und Implementierung der Maßnahmen muss auf Grundlage einer gründlichen Risikobewertung erfolgen.

Neuerungen und Änderungen

Die ISO 27001 wurde im Jahr 2022 erneut überarbeitet und einigen wichtigen und längst überfälligen Änderungen unterzogen. Im Oktober 2022 veröffentlichte das Internation Accreditation Forum (IAF) die neue und verbesserte ISO/IEC 27001:2022. Sie löst die bisher geltende ISO 27001:2017 ab. Durch die Namensänderung zu “Informationssicherheit, Cybersicherheit und Datenschutz – Informations- sicherheitsmaßnahmen” rückt der Datenschutz weiter in den Vordergrund, da dieser bei der Benennung hinzugekommen ist. Diese Änderung ist nicht überraschend, da Informations- sicherheit und Datenschutz oft Hand in Hand gehen, obwohl sie unterschiedliche Perspektiven einnehmen.

Der Maßnahmenkatalog wurde aktualisiert und neu strukturiert. Dadurch wurden die Maßnahmen in vier anstatt 14 Abschnitten eingeordnet und die Anzahl von 114 auf 93 reduziert. Dabei sind elf Maßnahmen neu dazu gekommen. Zusätzlich werden die Maß- nahmen nun jeweils in fünf verschiedene Attribute eingestuft: Kontrolltyp, Eigen- schaft der Informationssicherheit, Cyber- sicherheitskonzepte, Operative Fähigkeit und Sicherheitsdomänen.

Die Änderungen erfordern zwar keinen komplett neuen Umgang mit dem Thema Informationssicherheit, fördern aber die kritische Auseinandersetzung mit diesem und somit die Anpassung an aktuelle Sicherheitsvoraussetzungen.

Die Übergangsfrist ist auf drei Jahre festgelegt worden, weswegen bereits zertifizierte Unternehmen die neuen Maßnahmen frühstmöglich anpassen beziehungsweise aktualisieren sollten. Dies gilt insbesondere für das Business Continuity Management, da die Anforderungen an die Dokumentation in diesem Bereich strenger geworden sind. Noch nicht zertifizierte Unternehmen sollten die Auditierung nach der neuen Version anstreben, um ihre Informationssicherheit an neuesten Gegebenheiten auszurichten.

Vorteile eines ISMS

Die Implementierung eines ISMS gemäß ISO 27001 trägt maßgeblich zur Verbesserung der Sicherheit im Unternehmen bei. Ein effektives ISMS ermöglicht es Unternehmen, Risiken im Bereich der Informationssicherheit frühzeitig und systematisch zu identifizieren, zu bewerten und zu behandeln. Auf diese Weise können Bedrohungen rechtzeitig erkannt und angemessene Maßnahmen zur Risikominderung eingeleitet werden. Dies begrenzt oder verhindert einen möglichen Schaden, sei es der Vertrauensverlust gegenüber Kunden und Stakeholdern oder ein rein finanzieller Verlust.

Zusätzlich kann es Unternehmen dabei helfen, gesetzliche und regulatorische Anforderungen im Bereich der Informationssicherheit zu erfüllen. Diese Anforderungen können je nach Branche und Region variieren, aber die ISO 27001 bietet einen umfassenden und international anerkannten Rahmen, der in vielen Fällen als Nachweis der Einhaltung herangezogen werden kann. Gerade Betreiber kritischer Infrastruktur und mittlere wie auch große Unternehmen müssen sich im Rahmen der NIS-2 Gesetzgebung spätestens ab dem Herbst 2024 mit ihrer Informationssicherheit befassen, wenn eine Vielzahl neuer Regularien auf die deutsche Wirtschaft zukommen. Eine frühzeitige Ergreifung von Maßnahmen, beispielsweise durch die Einführung eines ISMS, ist daher allein schon aus Eigeninteresse sinnvoll.

Schritte zur Implementierung eines ISMS

Im ersten Schritt wird das Unternehmen mitsamt seines gesamten Kontextes erfasst. Dies beinhaltet ein umfassendes Verständnis der organisatorischen Prozesse, der Anforderungen und Erwartungen der beeinflussten Parteien sowie der Sicherheitsrisiken. Es wird eine Risikobewertung und -evaluierung durchgeführt, um Bedrohungen, Schwachstellen und potenzielle Aus- wirkungen auf die Informationssicher- heit zu identifizieren. Auf Basis dieser Erkenntnisse werden im Rahmen einer Risikobewertung Maßnahmen festgelegt, welche technischer oder auch orga- nisatorischer Natur sein können. Zusätzlich wird dokumentiert, inwieweit das Unternehmen die Anforderungen an die verschiedenen Normkapitel lang- fristig erfüllt und sicherstellt.

Die gewählten Sicherheitsmaßnahmen werden schließlich auf Basis der Normen geplant und implementiert. Dazu können beispielsweise Zugangskontrollen, Ver- schlüsselungsmaßnahmen, Richtlinien oder Prozesse und Schulungen gehören.

Zu jedem erfolgreichen ISMS gehört zudem eine regelmäßige Bewertung der eingeführten Maßnahmen, um sicher- zustellen, dass diese den gewünschten Effekt haben und die Informationssicherheit nachweislich dadurch ge- stärkt wird. Interne Audits und Managementbewertungen müssen durchgeführt werden, um Abweichungen und Verbesserungsmöglichkeiten zu identifizieren und Korrekturmaßnahmen durchführen zu können.

Fazit

Die Implementierung von ISO 27001:2022 bietet einem Unternehmen eine Vielzahl an Vorteilen, indem sie einen anerkannten Rahmen für das Informationssicherheitsmanagement bereitstellt. Diese Norm hilft Organisationen, sich auf die wachsenden Herausforderungen der Informationssicherheit vorzubereiten und sie effektiv zu bewältigen.

Die ISO 27001:2022 bietet eine robuste Grundlage für den Aufbau einer umfassenden Informationssicherheits- strategie. Durch die Implementierung der Norm können Organisationen ihre Datenverarbeitung und Datensicherheit effizienter und sicherer gestalten.

Die Zertifizierung nach ISO 27001:2022 stellt sicher, dass Organisationen den besten Sicherheitspraktiken folgen (Best practices) und ständig nach Ver- besserungen suchen. Außerdem erhöht sie das Vertrauen von Kunden, Partner und Aktionären in das Unternehmen und kann zur Geschäftsentwicklung bei- tragen.

Zudem hilft die Implementierung der Norm, gesetzliche und regulatorische Anforderungen zu erfüllen, indem Sie einen klaren Rahmen für die Einhaltung von Datenschutzgesetzen und Vorschriften bietet. Hinsichtlich der kommenden NIS-2 Verordnung ist die Implementierung lohnenswert, um sich rechtzeitig mit der Informations- sicherheit seines Unternehmens aus- einandergesetzt zu haben. Um das Informationsmanagement- system stetig voranzubringen und zu pflegen, müssen im Unternehmen ausreichend Ressourcen zur Verfügung gestellt werden.

Zusammenfassend lässt sich sagen, dass die Implementierung der ISO 27001:2022 trotz der Heraus- forderungen ein wichtiger Schritt zur Gewährleistung der Informations- sicherheit und zur Unterstützung der Geschäftsziele ist. Um die Anforderungen der ISO 27001 komplett umsetzen zu können, bieten wir neben der ausführlichen Beratung auch Vorlagen für die Ausarbeitung sowie Umsetzung der Normen und Maßnahmen an. Diese können auf Anfrage zur Verfügung gestellt werden.

Über die AWARE7

Die AWARE7 GmbH ist ein Cyber Security Unternehmen aus Gelsenkirchen das Technologien und Produkte entwickelt sowie Dienstleistungen anbietet, die zur Förderung, Steigerung und Erhaltung des IT-Sicherheitslevels dienen. Durch die praktische Arbeit und die regelmäßige Veröffentlichung von wissenschaftlichen Artikeln gelingt es uns komplexe Betrugs- und Angriffsmethoden zu erklären und zu entdecken, um Unternehmen und Behörden zu schützen.

IT-Sicherheit funktioniert nur, wenn die Technik sicher und die Menschen sensibilisiert sind. Komplexe Angriffe nutzen menschliche Schwachstellen in Kombination mit technischen Sicher- heitslücken aus. Betrachten Sie das IT- Sicherheitsniveau in ihrem Unternehmen ganzheitlich auf menschlicher und technischer Ebene. Wir sind in Sachen Sicherheit ganzheitlich an Ihrer Seite.

AWARE7

Kontakt

AWARE7 GmbH
Munscheidstraße 14
45886 Gelsenkirchen
info@aware7.de

Chris Wojzechowski
Geschäftsführer
+49 209 88306761
chris@aware7.de