WAS IST EIN MANAGEMENTSYSTEM FÜR INFORMATIONSSICHERHEIT (ISMS)?

Die Erfüllung der Anforderungen in Bezug auf die Informationssicherheit und den Datenschutz ist anspruchsvoll. Um dies belegen zu können, muss eine Vielzahl von organisatorischen Aspekten erfasst, aufgezeichnet und beschrieben werden.

Dabei handelt es sich z. B. um die Strategie, verschiedene Rahmenwerke und Grundlagen, Vereinbarungen und Prozesse. Außerdem muss festgelegt werden, auf welche Weise Ihre Organisation sicherstellt, dass die Vereinbarungen eingehalten und Prozesse umgesetzt wurden. Die damit verbundenen Risiken müssen transparent sein und Sie müssen nachweisen, dass Sie angemessene Maßnahmen ergreifen und diese regelmäßig kontrollieren.

Diese Vereinbarungen, Prozesse und Dokumente bilden ein Managementsystem. Alle Aspekte der Informationssicherheit werden in einem „Informationssicherheitsmanagementsystem" zusammengefasst – kurz ISMS.

WAS BEINHALTET EIN ISMS?

Ein ISMS umfasst die drei folgenden wesentlichen Bestandteile:

1. das Handbuch,
2. die Dokumentation (detaillierte Beschreibung, Verfahren, Arbeitsanweisungen usw.) und
3. die Anwendbarkeitserklärung (eine Übersicht über die für die Organisation zutreffenden Anforderungen in Bezug auf die Norm)

Das ISMS-Handbuch besteht aus den folgenden vier Kapiteln:

- **Führung:** Grundlagen, Strategie und Rahmenwerke.
- **Primäre Prozesse:** die Kernaufgaben der Organisation.
- **Sekundäre Prozesse:** die Prozesse der Organisation.
- **Management:** Sicherstellung der Arbeitsabläufe und deren Kontrolle

Der Abschnitt „Dokumentation" enthält die zugrunde liegenden Beschreibungen und zusätzlichen Dokumente, wie die Strategie, den Strategieplan und den Verhaltenskodex.

WAS IST BEI DER EINRICHTUNG EINES ISMS ZU BERÜCKSICHTIGEN?

Es gibt verschiedene Möglichkeiten, ein ISMS einzurichten. In der Regel umfasst die Einrichtung des Systems die folgenden drei Schritte:

1. Konzeption
2. Ausarbeitung
3. Praxisgerechte Gestaltung und fortlaufende Umsetzung

STRATEGIE UND ZIELE
Umfassender Strategieplan und Verhaltenskodex

ERGEBNISSE
Messung, Meldung und Bewertung der Ergebnisse

RISIKOANALYSE
Strukturierte Identifizierung der relevanten Risiken

MANAGEMENT-BEWERTUNG
Bewertung der Leistung und des Managementsystems

1. RICHTUNG - KONZEPTION

Dieser Schritt betrifft strategische Aspekte wie die Bestimmung der Grundlagen. Dies umfasst u. a. den Anwendungsbereich des Managementsystems, die Strategie, den Verhaltenskodex und eine Stakeholder-Analyse. Außerdem ist eine Risikoanalyse durchzuführen. Die erste Sensibilisierung und das Teilen einer Vision zum Thema Informationssicherheit innerhalb der Organisation ist ebenfalls Teil dieses Schrittes.

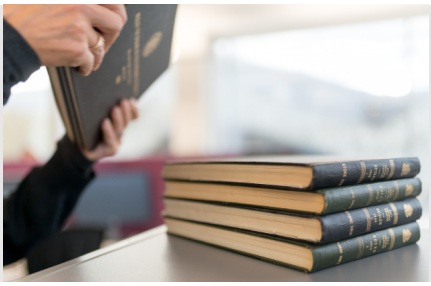
Das ISMS enthält das Rahmenwerk, die Grundlagen und die (strategischen) Entscheidungen für die gesamte Gestaltung der Informationssicherheit. In dieser Phase wird gewissermaßen das „Rahmenwerk des Managementsystems" festgelegt; d. h. die Grundlagen für diesen Themenbereich. Mitarbeiterinnen und Mitarbeiter aus dem Bereich der Informationssicherheit werden einbezogen.

2. EINRICHTUNG - AUSARBEITUNG

In dieser Phase erarbeitet die Organisation Schritt für Schritt alle Prozesse und Unterlagen. Die Arbeitsabläufe der Organisation werden in primären und unterstützenden Prozessen dokumentiert. Die Mitarbeiterinnen und Mitarbeiter, die bestimmte Prozesse lenken oder ausführen, werden daran beteiligt. Die Informationssicherheit wird für jeden Prozess eindeutig definiert.

Entscheidend für diese Phase ist die Schaffung von Akzeptanz. Bringen Sie die richtigen Leute zusammen. Bilden Sie einen Lenkungsausschuss und eine Projektgruppe. Außerdem ist es von wesentlicher Bedeutung, das Management und die Beteiligten zu informieren. Informieren Sie die gesamte Organisation über das Projekt und überzeugen Sie diese von dessen Bedeutung. Informationssicherheit liegt in der Verantwortung jedes Einzelnen in der Organisation.

HANDDBUCH
Umfassender Strategieplan und Verhaltenskodex



PROTOKOLLE
Informations-sicherheitsprotokolle mit Management-maßnahmen

GESCHÄFTS-KONTINUITÄTSPLAN
Leitfaden im Notfall oder im Falle von Eskalationen

EINDEUTIGE VERWEISE
Eindeutige Verweise auf Normen und gesetzliche und regulatorische Anforderungen

3. IMPLEMENTIERUNG - PRAXISGERECHTE GESTALTUNG UND FORTLAUFENDE UMSETZUNG

In diesem Schritt geht es um die Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für die Notwendigkeit, sich an die beschriebenen Prozesse und Verfahren tatsächlich zu halten. Es sollte außerdem festgelegt werden, wie die Organisation gewährleisten kann, dass die getroffenen Vereinbarungen auch in Zukunft beachtet werden.

Beispiele:

- Kontinuierliche Informationen an alle Mitarbeiterinnen und Mitarbeiter
- Weiterentwicklung der Fähigkeiten (Kompetenzen) der Prozessverantwortlichen
- Probemäßige Anwendung des Geschäftskontinuitätsplans. Wie stellen wir sicher, dass wir als Unternehmen im Notfall so schnell wie möglich wieder handlungsfähig sind?
- Messung und Rückmeldung: Durchführung von Penetrationstests an IKT-Systemen, Durchführung interner und externer Audits, Durchführung von Clean-Desk- und Clear-Screen-Checks.

Die Informationssicherheit wird verbessert, indem anhand verschiedener Quellen kontinuierlich untersucht wird, wo Verbesserungspotenziale sind. Das Erfassen der Möglichkeiten und Abweichungen ist dabei unerlässlich. Der nächste Schritt ist die Festlegung und Umsetzung der Verbesserungsmaßnahmen.

KOMPETENZ
Durch Training und Coaching

INTERNES AUDIT
Zur Vorbereitung auf das externe Audit

SENSIBILISIERUNG UND VERHALTEN
Mittels Sensibilisierungssitzungen

ÜBERWACHUNG UND MESSUNG
Erfassung der Prozessleistung

FAHRPLAN

Im Einzelnen umfasst der Fahrplan des Projektes folgende Schritte:

- Kick-off – Was ist unser Ziel und wie gehen wir vor?
- Erfassung der Ist-Situation – Wo befindet sich die Organisation?
- Aktionsplan – Welche Maßnahmen sind erforderlich und wer übernimmt was?
- Beschreibung der Prozesse und Erstellung unterstützender Dokumentation
- Erstellung der Konformitätserklärung
- Risikoanalyse
- Sensibilisierungssitzungen
- Internes Audit
- Managementbewertung
- Durchführung zusätzlicher Maßnahmen
- Externes Audit (Zertifizierung)

WEITERE INFORMATIONEN

Wünschen Sie ein unverbindliches Angebot für eine Zertifizierung nach ISO 27001?
Fordern Sie dies auf www.dnv.de/angebot an.

Möchten Sie wissen, wo Ihre Organisation steht und eine Erfassung der Ist-Situation durchführen lassen? Kein Problem! Kontaktieren Sie unsere Experten unter kundenservice@dnv.com oder +49 (0) 201 7296-222.

WEITERE INFOS UND KONTAKT

DNV führt Ihre ISO 27001-Audits gerne für Sie durch. Neben der Zertifizierung nach diesen Normen bietet DNV Ihnen auch die nötige Unterstützung bei der Zertifizierung vieler anderer Normen, z. B.:

- ISO 9001
- ISO 22301
- TISAX®
- ISO 27017
- ISO 20000

Haben Sie Fragen zu unseren Dienstleistungen oder möchten Sie mehr über die Zertifizierung erfahren? Bitte kontaktieren Sie uns.

DNV Business Assurance
Wolbeckstr. 25
45329 Essen

- kundenservice@dnv.com
- +49 (0)201 7296-222

Besuchen Sie unsere Website **www.dnv.de/assurance** oder fordern Sie unter **www.dnv.de/angebot** ein kostenloses Angebot an.