Whitepaper

ISO 27001 & ISMS (Informationssicherheits-Managementsysteme) im **Überblick**

- ISO 27001 erklärt
- Alle ISMS-Implementierungsschritte auf einen Blick
- Umfangreiche Checklisten
- Wie EWERK dabei unterstützt

EWERK

Management Summary

Vom IT-SiG2.0 und IT-Sicherheitskatalog zum ISMS: Die Vorteile von Information-Security-Management-Systemen

Angesichts immer kürzerer Innovationszyklen und zunehmender Digitalisierung rüsten auch Cyber-Kriminelle auf. Deswegen reagiert auch der Gesetzgeber: mit einem novellierten IT-Sicherheitsgesetz, einem geänderten BSI-Gesetz, einer überarbeiteten KRITIS-Verordnung und ergänzten IT-Sicherheitskatalogen der Bundesnetzagentur sowie der Datenschutzgrundverordnung. Sie alle haben ein gemeinsames Ziel: Ihr Unternehmen noch cybersicherer zu machen – und gegen unbeabsichtigte Fehler genauso wie absichtliche Manipulation von Daten oder Prozessen zu wappnen. Ein etabliertes Werkzeug dafür: ein Informationssicherheits-Managementsystem (ISMS), zertifiziert nach ISO/IEC 27001. Neben KRITIS-Unternehmen ist ein solches System mittlerweile auch für andere Unternehmen der systemrelevanten Branchen wie kleinere Netzbetreiber Pflicht, selbst wenn sie die Netzführung an Dritte ausgelagert haben.

Was sich zunächst nach einem unüberwindbaren Berg aus teuren Tools und kostenintensiver externer Beratung anhört – ist in Wahrheit beherrschbar. Mit diesem Whitepaper zeigen wir, wie: mit einem roten Faden für ein angemessenes ISMS, das mit vertretbarem Aufwand das Kerngeschäft dabei unterstützt, so sicher wie möglich zu sein.

Die Vorteile von zertifizierten ISMS

1. Bislang verborgene Sicherheitslücken kommen ans Licht und können direkt behoben werden.
2. Alle Prozesse sind transparent. So bleibt Wissen im Unternehmen und nötige Prozessänderungen sind leicht umzusetzen.
3. Dank Kennzahlen zur Prozesskontrolle können Risiken, Prozessfehler, Datenverluste oder Manipulationsversuche schneller erkannt und Gegenmaßnahmen ergriffen werden.
4. Die Zertifizierung ist ein anerkannter Nachweis zur Sicherstellung der Informationssicherheit. Bei Versicherungen führt das zu geringeren Kosten dank günstigerer Policen, etwa bei Haftpflichtversicherern.
5. Die Zertifizierung ist wie ein Gütesiegel – und damit ein weiteres Verkaufsargument für das Unternehmen.

» Für eine erfolgreiche und effiziente Einführung eines Informationssicherheits-Managementsystems gilt: Augenmaß bei der Integration, Nutzung schon vorhandener Prozesse und Dokumente und der Wille, sich ständig zu verbessern. Dann steht einer Zertifizierung nach ISO 27001 nichts im Weg. Dieses Whitepaper zeigt, wie's geht. «

Michael Stach,
Geschäftsführer der
EWERK Consulting GmbH

Inhaltsverzeichnis

2. Grundlagen ISO 27001: Was ist das – und was bedeutet das für mich und mein Unternehmen?

Die ISO 27001 beschreibt als internationale Norm die Anforderungen an Einrichtung, Umsetzung, Aufrechterhaltung und stetige Verbesserung von Informationssicherheits-Managementsystemen (ISMS). Mit einer ISO 27001-Zertifizierung können Sie für Ihr Unternehmen den Nachweis erbringen, dass unabhängige Dritte die Erfüllung von Compliance-Anforderungen nach festgelegten Kriterien geprüft und bestätigt haben. Die Norm liefert genau diese – ist also vergleichbar mit einem Kriterienkatalog für die Zertifizierung eines ISMS.

Die Norm ist in zwei Bereiche gegliedert: einen Management-Rahmen und den Anhang A. Teile der Regeln sind verpflichtend (Kapitel 4-10), Teile sind im Rahmen einer Anwendbarkeitserklärung begründet abwählbar. Der ISO-Standard 27001 wird durch eine Reihe weiterer Standards ergänzt – alleine ist er gar nicht anwendbar. Daher spricht man auch von der ISO 27000-Familie oder ISO 270xx. Konkret umfasst sie fachspezifische Subnormen, etwa für Energieversorger die ISO 20719, oder für Unternehmen aus dem Telekommunikationssektor die ISO 27011.

2.1 Kapitel 4-10

Während in den Kapiteln 1-3 eher Grundlegendes erklärt wird, drehen sich die Kapitel 4-10 um verpflichtende Maßnahmen, die zwingend umgesetzt werden müssen.

Dazu haben wir für Sie einen kleinen Fragenkatalog pro Kapitel erstellt, der all diese Maßnahmen umfasst.

Kapitel 4: Kontext der Organisation

- ☐ Wer sind die Stakeholder des ISMS?
- ☐ Für welche Bereiche gilt das ISMS?
- ☐ Haben Sie die gesetzlichen Anforderungen im Zusammenhang mit dem ISMS identifiziert?

Kapitel 5: Führung

- ☐ Wird die Unternehmensleitung ihrer IT-Sicherheits-Verpflichtung gerecht – etwa dank:
  - einer Informationssicherheitsstrategie,
  - der Integration des ISMS in alle relevanten Geschäftsprozesse,
  - der Bereitstellung der benötigten Ressourcen,
  - der Messung, wie wirksam das ISMS ist und des Willens der kontinuierlichen Verbesserung,
  - die Sensibilisierung der Mitarbeitenden aller Ebenen?
- ☐ Hat die Geschäftsführung eine Leitlinie zur Informationssicherheit erarbeitet und kommuniziert?
- ☐ Hat die Unternehmensleitung die Rollen, Verantwortlichkeiten und Befugnisse im Rahmen des ISMS definiert und erhält sie von ebendiesen Reports?

Kapitel 6: Planung

- ☐ Wurde festgelegt, wie mit identifizierten Risiken und Chancen umgegangen wird?
- ☐ Gibt es einen Prozess, wie Informationssicherheitsrisiken identifiziert, bewertet und behandelt werden?
- ☐ Ist eine Anwendbarkeitserklärung zum Anhang A verfasst?
- ☐ Sind die Ziele des ISMS bestimmt und ein Plan erarbeitet, wie, wann und von wem sie erreicht werden?

Kapitel 7: Unterstützung

- [ ] Werden die notwendigen Ressourcen für das ISMS bereitgestellt?
- [ ] Haben die verantwortlichen Mitarbeitenden die erforderlichen Kompetenzen, um ihre Aufgaben im Rahmen des ISMS zu erfüllen?
- [ ] Sind alle Mitarbeiter sensibilisiert auf die ISMS-Leitlinie, ihre Mitwirkungspflicht und die Konsequenzen bei Nichterfüllung?
- [ ] Ist die interne und externe Kommunikation zum ISMS abgestimmt?
- [ ] Werden die von der Norm geforderten Dokumentationen geführt?

Kapitel 8: Betrieb

- [ ] Gibt es einen Prozess
  - zur Erfüllung der Anforderungen an die Informationssicherheit,
  - zur Steuerung von Maßnahmen,
  - zur Aufgabensteuerung, die an Dritte ausgelagert wurden und
  - zur Berücksichtigung der Informationssicherheit bei geplanten Änderungen?
- [ ] Führt das Unternehmen in regelmäßigen Abständen und bei wichtigen Anpassungen eine Risikobeurteilung durch?
- [ ] Erfolgt eine Risikobehandlung?

Kapitel 9: Bewertung der Leistung

- [ ] Gibt es einen Prozess, der die Wirksamkeit des ISMS überwacht?
- [ ] Finden regelmäßige interne Audits statt?
- [ ] Ist ein Auditprogramm erarbeitet?
- [ ] Gibt es eine regelmäßige Managementbewertung?

Kapitel 10: Verbesserung

- [ ] Wird auf nichtkonforme Ereignisse mit adäquaten Maßnahmen reagiert?
- [ ] Werden diese Maßnahmen auf deren Notwendigkeit hin überprüft, eingeleitet und auf Wirksamkeit geprüft?
- [ ] Wird dank des ISMS eine kontinuierliche Verbesserung sichergestellt?

2.2 Anhang A

Neben den beschriebenen zehn Kapiteln sind im Anhang A 114 spezifische Maßnahmen definiert. Sie sind nicht obligatorisch alle zu erfüllen – aber: Es muss zu jedem der 114 Punkte in einer Anwendbarkeitserklärung dargestellt werden, welche Punkte umgesetzt werden, welche nicht, und warum. Für einen groben Überblick haben wir die 114 Maßnahmen für Sie kategorisiert und innerhalb dieser Kategorien gezählt. Damit bekommen Sie ein Gefühl, wie viele Maßnahmen für Sie zu erfüllen sein dürften:

- Informationssicherheitsrichtlinien: 2
- Organisation der Informationssicherheit: 7
- Personalsicherheit: 6
- Verwaltung der Werte: 6
- Zugangssteuerung: 10
- Kryptografie: 2
- Physische und umgebungsbezogene Sicherheit: 15
- Betriebssicherheit: 14
- Kommunikationssicherheit: 7
- Anschaffung, Entwicklung und Instandhaltung von Systemen: 13
- Handhabung von Informationssicherheitsvorfällen: 7
- Informationssicherheitsaspekte im Rahmen des Business Continuity Managements: 4
- Compliance: 8

2.3 Warum bei dieser Norm ein branchenspezifisches Vorgehen sinnvoll ist

Grundsätzlich sind ISO-Normen branchenunabhängig verfasst. Es geht dabei also um eine Art Vogelperspektive: Welche Prozesse, Kennzahlen, Kontrollzahlen und Co. sollen oder können herangezogen werden, um Informationssicherheit zu garantieren?

Jede Branche hat aber ihre eigenen kritischen Prozesse und Kennzahlen. So kann ein Prozess, der nicht so läuft wie geplant, in einem Unternehmen einer Branche ein winziges Problem sein, wohingegen er in einer Firma einer anderen Branche Schäden in sechsstelliger Höhe bedeutet. Das hat zwei Konsequenzen:

a) Es gibt branchenspezifische Subnormen in der ISO 27000-Familie, wie etwa für Unternehmen aus der Finanz- und Versicherungsbranche, dem Abwasserbereich, der Energieversorgung, etc.

b) Für ein effektives und wirksames ISMS sind Branchenkenntnisse unabdingbar.

Ein unter diesen Voraussetzungen implementiertes ISMS führt nachweislich zu Kosteneinsparungen – etwa bei Versicherungspolicen, denn: Die Wahrscheinlichkeit von Schadensfällen sinkt.

2.4 ISO 270xx-Standards und deren Zusammenhang

Die ISO 27001 definiert Grundanforderungen an ein ISMS. Näher spezifiziert sind diese in weiteren Standards – derzeit sind 7 relevant:

- ISO 27000 definiert Begriffe der Normenreihe.
- ISO 27001 bestimmt die Zertifizierungsanforderungen an ein ISMS.
- ISO 27002 ist ein Implementierungsleitfaden.
- ISO 27003 beschäftigt sich mit der Einführung eines ISMS.
- ISO 27004 legt Kennzahlen für das ISMS fest.
- ISO 27005 beschreibt Details zum Risikomanagement.
- ISO 27006 gibt vor, nach welchen Kriterien ISMS auditiert und zertifiziert werden.
- ISO 27011 ist eine branchenspezifische Subnorm für Telekommunikationsunternehmen.
- ISO 27015 ist eine branchenspezifische Subnorm für Finanzdienstleistungen.
- ISO 27017/18 ist eine branchenspezifische Subnorm für Cloud Computing Services.
- ISO 27019 ist eine branchenspezifische Subnorm für Energieversorgungsunternehmen.
- ISO 27799 ist eine branchenspezifische Subnorm für das Gesundheitswesen.

3. ISMS: Was ist das?

Ein zentrales System, das alle Prozesse und Regeln festschreibt, die zur dauerhaften Definition, Steuerung, Kontrolle, Aufrechterhaltung und Verbesserung der Informationssicherheit dienen: Das ist ein Informationssicherheits-Managementsystem (ISMS). Es klärt also in einem Unternehmen die Frage, wie Informationssicherheit geplant, bewertet und umgesetzt wird. Ziel ist es, kritische Werte und Informationen vor Verlust, Manipulation oder Kompromittierung zu schützen. Konkret sollen damit Schäden vermieden werden, die durch Cyberangriffe oder Fehler im Datenhandling entstehen und als solche gut messbar sind – genauso wie Schäden immaterieller Art, wie Imageverlust durch Datenpanne.

Ein ISMS zielt darauf ab, sämtliche Prozesse in einem Unternehmen kritisch zu untersuchen und mit Qualitätskriterien in Bezug auf Informationssicherheit zu versehen, die mit sensiblen Daten zu tun haben – und zwar so, dass sie kontinuierlich kontrolliert und verbessert werden können. Das Ziel: Sollte ein unternehmenskritischer Prozess außerhalb der definierten Kontrollziele laufen, kann sofort korrigierend eingegriffen werden – um eventuelle Schäden möglichst früh abzuwenden.

Ein ISMS ist dabei nicht „ein Stück Software“. Es handelt sich vielmehr um eine Sammlung von Management-Instrumenten zur Steuerung und Lenkung von informationssicherheitsrelevanten Prozessen – und noch nicht um konkrete Maßnahmen selbst. Diese werden im zweiten Schritt anhand der Vorgaben aus dem Informationssicherheits-Managementsystem abgeleitet und umgesetzt. Weil nahezu jeder Prozess erst dank der Interaktion von und mit Mitarbeitenden läuft, sind diese bei einem ISMS immer sehr eng einzubinden. Heißt: Neben den IT-Systemen selbst spielen die Mitarbeitenden, ihre Handlungen und ihr Bewusstsein für IT-Sicherheit die entscheidende Rolle. Die Implementierung eines ISMS ist also mehr als eine Einführung von Tools und Reports: Sie ist ein Change-Prozess, meist einhergehend mit einem Kulturwandel. Sehr große Worte – die aber mit kleinen Maßnahmen Schritt für Schritt umsetzbar sind.

3.1 Implementierungsschritte (inkl. Infokästen zu Ressourcenbedarf und Dauer)

Grundvoraussetzung für die erfolgreiche ISMS-Implementierung ist die klare Kommunikation der spürbaren Mehrwerte eines ISMS an die Mitarbeitenden – eine Awareness für IT-Sicherheit zu schaffen. Nur so kann Akzeptanz entstehen, die für den Change-Prozess unabdingbar ist, den eine ISMS-Implementierung mit sich bringt. Denn: Ein ISMS ist die Grundlage für eine Zertifizierung nach ISO 27001. Eine ISMS-Einführung setzt sich aus unterschiedlichen Teilprojekten zusammen und unterschiedlich umfangreich – je nach Unternehmensgröße, Branche, bereits vorhandenen Dokumentationen, Handlungsanweisungen, KPIs sowie dem Grad des bereits gelebten IT-Sicherheitsbewusstseins. Der erste von sechs Schritten, wenn EWERK Sie bei der Zertifizierung begleitet: ein Normverständnis schaffen.

» Ein ISMS zu implementieren ist mehr, als ein Stück Software einzuführen. Es ist ein Change-Prozess. Solche Veränderungen sind so individuell wie die Unternehmen selbst. Dennoch haben wir dank unserer Erfahrung eine grobe Schätzung in Sachen Projekt-Umfang: Je nach Reifegrad und Größe des Unternehmens können Sie mit 100-150 Personentagen rechnen. «

Michael Stach,
Geschäftsführer der
EWERK Consulting GmbH

3.1.1 Einführung und Normverständnis

Ein solides Verständnis von Inhalten der Normen, der geforderten Policies, Prozesse und Dokumentationen ist das A und O bei der ISMS-Implementierung. In einem Workshop vermitteln wir ein generelles Verständnis und schaffen einen Normüberblick: Wir zeigen, welche Auswirkungen ein ISMS hat, was wichtige Einflussfaktoren sind, welche Anforderungen die Norm(en) mit sich bringen und in welche konkret umzusetzenden Maßnahmen das mündet. Unser Ziel: Awareness für das Thema IT-Sicherheit zu schaffen und die Unterstützung des Top-Managements zu sichern. Das ist die Voraussetzung für den erfolgreichen Change-Prozess der ISMS-Einführung.

3.1.2 Umsetzungsumfang bestimmen

Eine Auditierung zur initialen Bestandsaufnahme mit einer Gap-Analyse hilft, den Gesamtaufwand abzuschätzen. Dazu empfiehlt es sich anhand des Code of Practice (ISO 27002) die Bedeutung der einzelnen Controls zu prüfen und existierende Regelungen und Arbeitsweisen zu dokumentieren. Dabei ist entscheidend, die zunächst branchenneutrale Norm auf die jeweilige Branche herunterzubrechen, Subnormen einzubeziehen und die wirklich entscheidenden, kritischen Prozesse zu identifizieren. EWERK stellt das sicher: Wir haben für viele Branchen ausgewiesene Zertifizierungs-Experten im Team.

Diese Grundlagenarbeit ist entscheidend: Daraus ergeben sich der grobe Fahrplan und die von der Norm betroffenen Bereiche. Es entscheidet sich also zum Beispiel, ob der Fokus auf dem Gesamtunternehmen liegt (selten) oder ob nur einzelne Teilbereiche betroffen sind (meistens der Fall).

So ist es nicht nur in größeren Unternehmen sinnvoll, nur einzelne Geschäftsbereiche zu zertifizieren. Auch in kleineren Firmen ist es möglich, Bereiche auszuschließen – etwa, wenn ein Standort oder eine Abteilung nur den Vertrieb abdeckt und als solches für den funktionierenden Betrieb der Software nicht kritisch ist. Genau das muss dann im Anwendungsbereich beschrieben werden. Die Beschreibung des Geltungsbereiches ist also wichtig, damit nachvollzogen werden kann, welche Bereiche und Themen durch das ISMS abgedeckt sind und welche nicht.

In diesem Rahmen ist es sinnvoll, sich spätestens jetzt Gedanken zu Zielen der Informationssicherheit zu machen. Denn: Auch sie entscheiden den Umfang des ISMS mit. Sie sollten im Verhältnis von Umsetzungsaufwand und Nutzen ausgewogen und möglichst messbar sein.

Beispiele für Informationssicherheitsziele

- Alle Beschäftigten für Informationssicherheit sensibilisieren, etwa in Workshops, mit Aushängen, Mailings, etc.
- Zutrittssicherheit zum Rechenzentrum sicherstellen
- 99,9%ige verfügbare Datenanbindungen
- Sicherheitsvorfälle möglichst früh erkennen
- Kundenanforderung an die Vertraulichkeit der Daten sicherstellen
- Den Reifegrad des ISMS stetig steigern
- Kontinuität in den Arbeitsabläufen sicherstellen
- Risiken für die Informationssicherheit regelmäßig identifizieren, bewerten und behandeln

3.1.3 Einarbeitung eines Registers für Unternehmenswerte

Um zu vermeidende Schäden quantitativ bewerten zu können, müssen alle Unternehmenswerte erfasst werden, die an der Übertragung, Speicherung und Verarbeitung von Informationen beteiligt sind. Diese erarbeitet EWERK zusammen mit Ihnen: Wir identifizieren alle relevanten internen wie externen Assets sowie Schnittstellen zu Dritten. Unser Ziel: ein Asset-Register samt Organisationschart mit Schnittstellen. Dazu führen wir Dokumenten-Reviews durch, führen Interviews mit allen Stakeholdern und erstellen alle erforderlichen Templates, Vorlagen und Dokumente gemäß Normvorschrift.

3.1.4 Vorbereitung und Durchführung eines Risiko-Assessments

Die ISO-Norm 27001 fordert, grundsätzlich Prozesse zu schaffen, in dessen Rahmen die Informationssicherheitsrisiken identifiziert und bewertet werden. Nur so lassen sich die Risiken analysieren und vor allem priorisieren. Dafür der erste Schritt: einen Risikomanagementprozess inklusive Risikokategorien und -kriterien festzulegen, der auch bei Wiederholung zu konsistenten, gültigen und vergleichbaren Ergebnissen führt. Dieser besteht mindestens aus den drei grundlegenden Schritten:

1. Risiken identifizieren: Fragen Sie sich, welche Informationen, Geschäftsprozess oder IT-Systeme sind für Ihren Betrieb besonders kritisch.

   Challengen Sie Ihre Auswahl mit internen und ggf. externen Experten. Sie können dazu beispielsweise Gefährdungskataloge hinzuziehen, etwa vom Bundesamt für Sicherheit in der Informationstechnik (BSI).

2. Risiken bewerten: Im zweiten Schritt bewerten Sie die identifizierten Risiken – je nach Schadenshöhe und Eintrittswahrscheinlichkeit. Das BSI nutzt dazu jeweils vier Kategorien:

   - Eintrittshäufigkeit:
     - Selten: könnte maximal alle fünf Jahre eintreten
     - Mittel: tritt einmal alle fünf oder bis einmal im Jahr ein
     - Häufig: tritt einmal im Jahr bis einmal im Monat ein
     - Sehr häufig: tritt mehrmals im Monat ein
   - Schadenshöhe:
     - Vernachlässigbar
     - Begrenzt und überschaubar
     - Beträchtlich
     - existenzbedrohend

3. Risiken behandeln: Für die am höchsten bewerteten Risiken (häufig, sehr häufig, beträchtlich und existenzbedrohend) legen Sie eine Handlungsstrategie fest, etwa:

   - Risikovermeidung dank Einstellen bzw. Anpassen einer Tätigkeit oder eines Prozesses
   - Risikoreduktion durch Einführung geeigneter Sicherungsmaßnahmen
   - Risikotransfer dank Versicherung oder
   - Risikoakzeptanz.

EWERK kann Sie dabei unterstützen

- Wir führen mit Ihren Fachexperten das gesamte Risiko-Assessment inklusive der erforderlichen Dokumentation und Steuerung interner Zuarbeiten durch.
- Wir erarbeiten ein vollständiges Verfahrensmodell für die jährliche Risikoanalyse.
- Wir führen die Risikoanalyse durch und werten sie aus.
- Wir erstellen einen Risikobehandlungsplan.

3.1.5 Vorbereitung und Prüfung erforderlicher Dokumente & Umsetzung der Maßnahmenpläne

Im nächsten Schritt geht es darum, Verfahren und Maßnahmen festzulegen, die die Informationssicherheit definieren, steuern, kontrollieren und kontinuierlich verbessern – also die Etablierung eines Informationssicherheitsmanagement-Systems (ISMS). Dieser Schritt untergliedert sich in Teilprojekte: etwa die Erstellung der erforderlichen Rahmendokumente auf Basis der Norm, die Umsetzung aller identifizierten Maßnahmen sowie deren Implementierung.

Die Norm hat zahlreiche Anforderungen – aber davon sollte sich niemand abschrecken lassen, denn: Viele Sicherheitsmaßnahmen existieren in Unternehmen bereits und müssen nur noch dokumentiert werden. Oftmals können auch existierende Prozesse genutzt werden, um Maßnahmen zu steuern oder Vorfälle zu melden. Insbesondere bei der ersten Zertifizierung geht es darum, die notwendige Dokumentation sowie die Prozesse nachzuweisen und danach zu „leben“. Alle Sicherheitsmaßnahmen aus dem Anhang A müssen noch nicht lückenlos umgesetzt sein. Allerdings muss ein Weg aufzeigt werden, wie und wann sie umgesetzt werden.

Obligatorische ISMS-Dokumente:

- Definition des Anwendungsbereichs – auch Geltungsbereich oder Scope genannt
- Anwendbarkeitserklärung: Welche der Maßnahmen im Anhang A sind (nicht) relevant oder werden (nicht) umgesetzt und warum
- Definition der interessierten Parteien (Stakeholder) und deren Anforderungen an die Informationssicherheit
- Ziele der Informationssicherheit
- Planung der ISMS-Ressourcen
- ISMS-Rollen und Verantwortlichkeiten
- Gesetzliche und regulatorische Anforderungen
- Interne und externe Kommunikation im ISMS
- Auditprogramm
- Managementbericht
- Risikobehandlungsplan

Obligatorische Richtlinien:

- Leitlinien zur Informationssicherheit
- Richtlinie zum Risikomanagement
- Richtlinie zum Umgang mit Sicherheitsvorfällen
- Richtlinie für Lieferanten, Dienstleister und Fremdfirmen
- Richtlinie zur Klassifizierung und zum Umgang mit Informationen
- Richtlinie zum sicheren IT-Betrieb
- Richtlinie für Personal- und Berechtigungsmanagement
- Allgemeine Regeln zur Informationssicherheit für alle Mitarbeitenden

Bei der Erstellung der erforderlichen Dokumentation, der Rahmendokumente und des kontinuierlichen Verbesserungsprozesses hilft EWERK gern mit Planung, Erarbeitung von Vorschlägen und inhaltlichen Ausarbeitungen. Die erforderlichen Templates, Vorlagen und Dokumente haben wir im Portfolio und schneiden sie passgenau auf Ihr Unternehmen zu. Oder wir reviewen „nur“ Ihre erstellten Dokumente auf inhaltliche und formelle Anforderungen hinsichtlich der Norm-Erfordernisse.

3.1.6 Entfaltung der Wirksamkeit, Interne Audits und Management-Bericht

Um das ISMS zu zertifizieren, reichen die bisher genannten Richtlinien, Dokumentationen und Rahmendokumente nicht aus. Beim Aufbau eines Managementsystems für Informationssicherheit handelt es sich nicht um eine einmalige Aufgabe: Das ISMS muss stetig geprüft werden – auf Eignung, Angemessenheit und Wirksamkeit.

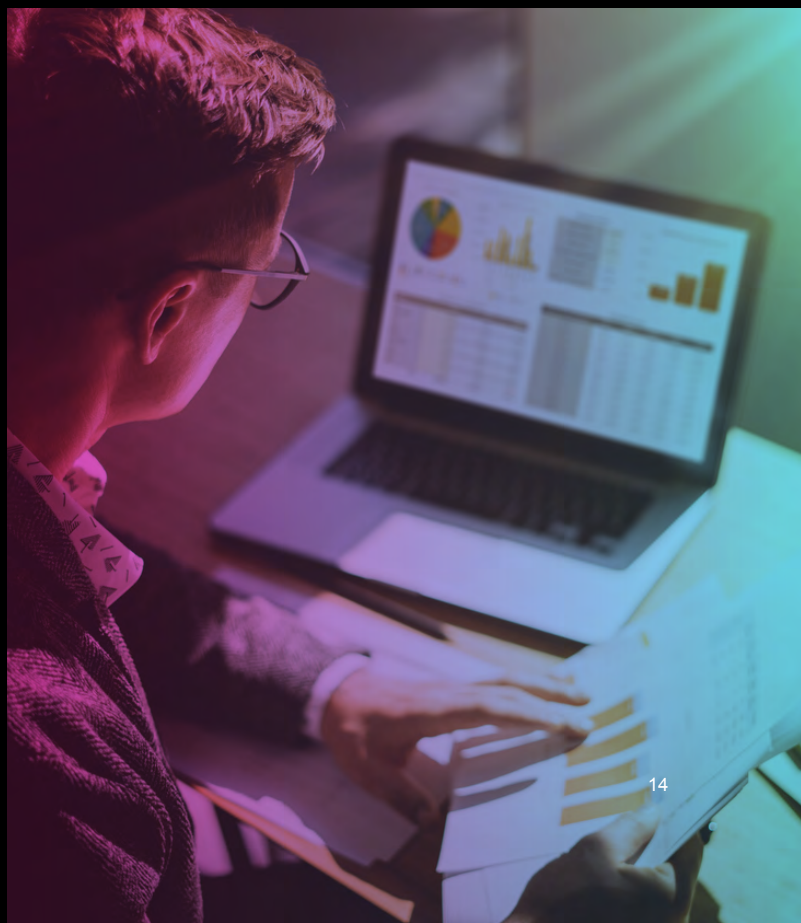
Kontinuierlicher Verbesserungsprozess und die Wirksamkeit des ISMS

Es geht also mehr um ein System, das regelmäßig verbessert wird. Dazu ist kein konkretes Vorgehen vorgeschrieben – allerdings hat sich eines sehr bewährt: ein Zyklus aus Plan, Do, Check und Act – der so genannte PDCA-Kreislauf. Demnach werden die geplanten (plan) und umgesetzten (do) Aktivitäten im ISMS auf Wirksamkeit geprüft (check) und gegebenenfalls überarbeitet (act). Was sich dafür am besten eignet: ein Ticketsystem oder Aufgabenplanungstool mit festgelegten Verantwortlichkeiten,

Zieldaten – das idealerweise sogar unternehmensintern schon existiert und bisher für andere Zwecke genutzt wurde. Tipp: Für das ebenfalls nötige Management-Reporting lohnt es sich, die Maßnahmen aus der Informationssicherheit mit Flags oder Tags auswertbar zu machen. So können sie automatisch in Berichte einfließen.

Management-Berichte

Diese Berichte – auch Managementbewertung genannt – sind entscheidend, damit die Geschäftsführung stets über den Status des ISMS informiert ist. Eine solche Berichterstattung sollte mindestens einmal im Jahr erfolgen – und kann später auf quartalsweise erhöht werden. Die Inhalte des Reportings gibt die Norm vor: Status von Maßnahmen, Ergebnisse aus internen Audits, dem Risikomanagement, Sicherheitsvorfälle, Kennzahlen und Ziele der Informationssicherheit sowie die Rückmeldung von interessierten Parteien, wie Kunden oder Behörden und Themen, die einen signifikanten Einfluss auf das ISMS haben – etwa neue Produkte, Standorte oder Prozesse.



Interne Audits

Ebenso für eine Zertifizierung nötig: interne Audits. Weil diese oft nicht zum Tagesgeschäft gehören, sind Grundbegriffe zu definieren – das über allem stehende Auditprogramm, ein Auditplan für die einzelnen Audits und der Auditbericht.

Im Auditprogramm dokumentieren sie alle anstehenden Audits – also nicht nur interne, sondern auch externe und Lieferantenaudits.

Steht das Auditprogramm, geht es um den ersten internen Audit, das mit einem Auditplan vorbereitet wird. In ihm wird nicht nur der auditierte Bereich, das Datum, die Zeit und Räumlichkeiten definiert. Er dient auch zur Koordination und Information aller am Audit teilnehmenden Mitarbeitenden.

Auch wenn es im internen Audit hauptsächlich darum geht, Verbesserungsmöglichkeiten zu identifizieren: Nehmen Sie positive Ergebnisse unbedingt in den Auditbericht mit auf – das motiviert nicht nur die Teilnehmenden, sondern stützt auch die ISMS-Akzeptanz.

Zeitlich sollten Sie sich von Planung bis Überführung der Verbesserungsmaßnahmen ins Ticketsystem etwa 2 Monate Zeit einplanen:

- Auditplan erstellen: 1 Monat vor Audit
- Terminfindung und Verantwortlichkeiten mit zu auditierendem Bereich klären: 3 Wochen vor Audit
- Auditplan bereitstellen: 2 Wochen vor Audit
- Audit: Mindestens einen Tag einplanen, um Dokumente zu sichten, Interviews zu führen und Systeme zu sichten – je nach Komplexität auch mehr.
- Maßnahmen und Termine mit dem auditierten Bereich abstimmen: 2 Wochen nach Audit
- Auditbericht bereitstellen: 3 Wochen nach Audit
- Maßnahmen in Maßnahmenliste (z.B. Ticketsystem) überführen: 1 Monat nach Audit

3.1.7 Zertifizierung

Ist das ISMS implementiert, ist viel dafür getan, mögliche Risiken und Schadensfälle zu minimieren und Transparenz in die Informationssicherheit gebracht. Jetzt schließt sich die ISO-Zertifizierung an – ein Audit durch speziell akkreditierte Gutachter. Mit externen Beratungsunternehmen wie EWERK empfiehlt es sich, vor einer solchen externen Auditierung alles noch einmal auf Herz und Nieren zu prüfen. EWERK prüft dazu alle Punkte der Controls auf ihre Umsetzung und hilft dabei, mögliche Abweichungen vor dem offiziellen Audit zu korrigieren. Ebenso schult EWERK Mitarbeitende und Verantwortliche und unterstützt während des gesamten Zertifizierungsverlaufs – etwa mit der Beantwortung von Audit-Fragen oder in der Argumentation gegenüber dem Auditor.

Mit einer erfolgreichen Zertifizierung setzen Sie ein starkes Zeichen für die Sicherheit von Informationen, Daten und Systemen – auf das sich nicht nur Ihre Mitarbeitenden verlassen können, sondern auch alle anderen Stakeholder. Die Zertifizierung ist ein klarer Wettbewerbsvorteil mit hohem Vermarktungspotenzial und Vertrauensgarantie.

4. Checkliste: Die ISMS-Implementierung optimal vorbereiten

Mit unserer Checkliste erkennen Sie ganz einfach auf einen Blick, in welchen Bereichen Sie und Ihr Unternehmen die Anforderungen der ISO 27001 bereits erfüllen und mit welchen Themen Sie sich noch intensiver beschäftigen müssen. Das Beste daran: Sie brauchen dafür maximal 15 Minuten.

Organisation

- [ ] Sie haben den Aufbau Ihres Unternehmens dargestellt (etwa als Organigramm).
- [ ] Sie haben eine Übersicht aller relevanten gesetzlichen, regulatorischen und vertraglichen Anforderungen erstellt, die einen Einfluss auf Ihre Informationssicherheits-Strategie haben.
- [ ] Für welche Bereiche das ISMS gelten soll, haben Sie definiert.
- [ ] Sie haben Sicherheitsmaßnahmen definiert und dokumentiert – etwa in einer Erklärung zur Anwendbarkeit („Statement of Applicability“) oder einem Handbuch.
- [ ] Sie haben eine Umfeldanalyse durchgeführt und so das ISMS im Unternehmen eingeordnet.
- [ ] Alle relevanten Interessensgruppen, die in irgendeiner Weise mit dem ISMS zu tun haben, sind in das Projekt eingebunden.

Leadership

- [ ] Unternehmensziele und Anforderungen, die mit der Informationssicherheitspolitik zusammenhängen, sind klar definiert und dokumentiert.
- [ ] Sie haben eine Informationssicherheitsstrategie erarbeitet.
- [ ] Diejenigen Mitarbeitenden, die für die Steuerung des ISMS der zu schützenden Organisation verantwortlich sind und über den Ressourceneinsatz dazu entscheiden, haben sie klar festgelegt.
- [ ] Sie haben eine Informationssicherheitsleitlinie – etwa in Form eines Handouts, einer Seite im Intranet, eines Wikis oder ähnliches.

Planung

- [ ] Sie haben alle Sicherheitsziele für Ihr Unternehmen und alle Stakeholder definiert.
- [ ] Sie besitzen ein dokumentiertes Risikobewertungsverfahren.
- [ ] Den Risikobeurteilungsprozess haben sie dokumentiert.
- [ ] Es gibt einen Prozessplan für Risikofälle.
- [ ] Alle Ergebnisse und Aufzeichnung von durchgeführten Risiko-Assessments bzw. -analysen haben Sie festgehalten.
- [ ] Alle Daten, Ergebnisse und Aufzeichnungen von Risikobehandlungen haben Sie dokumentiert und abgelegt.

Unterstützung

- [ ] Ein Kommunikationsplan bzw. eine -matrix unterstützt Sie bei der Dokumentation aller Informationen im Unternehmen mit Bezug zu Informationssicherheit.
- [ ] Die erforderlichen Ressourcen für die Infrastruktur, Implementierung und Steuerung des ISMS können Sie bereitstellen.
- [ ] Sie verfügen über eine Strategie zum Umgang mit dokumentierten Informationen.
- [ ] Eine Übersicht über alle relevanten Ressourcen haben Sie aufbereitet (Budget, Personal, etc.).
- [ ] Alle Rollenbeschreibungen relevanter Mitarbeiter im Geltungsbereich des ISMS liegen vor, alle Nachweise über deren Kompetenzen haben Sie dokumentiert.
- [ ] Sie haben ein Schulungskonzept in Bezug auf das ISMS samt Schulungsunterlagen und Nachweise über die Teilnahme Ihrer Mitarbeiter.

Betrieb

- [ ] Die korrekte Ausführung der ISMS-Prozesse zur Kontrolle und Leistungsmessung können Sie nachweisen – dank entsprechender Dokumentation.
- [ ] Interne Audits führen Sie durch.
- [ ] Sie haben einen Incident Response Plan samt Kontaktlisten und Eskalationsplänen.
- [ ] Alle Messstrukturen für sicherheitsrelevante KPIs sind dokumentiert, genauso wie die daraus abgeleiteten Managementberichte zur Eskalation.
- [ ] Ihre Dokumentation umfasst:
- [ ] Verhaltensregeln bei sicherheitsrelevanten Unregelmäßigkeiten.
- [ ] Prozessbeschreibungen und Arbeitsanweisungen für die Sicherung von Beweisen und Berichte von Informationssicherheitsvorfällen.
- [ ] Sie haben Nachweise über die Art von Nichtkonformitäten und sämtliche umgesetzte reaktive und korrigierende Maßnahmen.
- [ ] Sie verfügen über eine Übersicht der Ergebnisse von Risikobewertung und -behandlung (Bewertungsberichte, KPIs, Testberichte, ...).

5. Warum EWERK

Wir sind nach ISO 27001:2013 und 9001:2015 zertifiziert. Mit den Umsetzungsmodellen und Zertifizierungsprozessen der ISO-Standards sind wir bestens vertraut:

- Erfahren: EWERK verfügt über tiefes Verständnis für Informations-sicherheitsmanagement und hat langjährige Erfahrungen bei der Einführung und Beratung der ISO 27001.

- Umfassend: Wir beraten und unterstützen zu allen Aspekten und Dokumentationsanforderungen der ISO 27001. Wir können Unternehmen – angefangen vom Normverständnis und Umfangbestimmung über die unternehmensindividuelle Konzeption bis hin zur Einführung der ISO-Norm – begleiten.

- Flexibel: Alle Beratungsleistungen zur ISO 27001 bieten wir modular oder als Komplettpaket an.

- Clever: Wir verfügen über ein eigenes entwickeltes Einführungsmodell und eine pragmatische Vorgehensmethodik, die eine effiziente und ressourcenschonende Umsetzung und Etablierung der ISO 27001 ermöglicht. Dies betrifft insbesondere Referenzvorlagen für die erforderlichen Normdokumente, Metriken und Leitlinien.

- Transferierend: Wir bieten eine Zertifizierungsvorbereitung und -begleitung sowie das Coaching verantwortlicher Mitarbeitenden an. Wir verfolgen den Ansatz, die verantwortlichen Mitarbeiter im Rahmen der Erstzertifizierung zu schulen und zu befähigen, sodass Folge-Zertifizierungen weitestgehend intern abgebildet werden können.

EWERK Whitepaper

Sind Sie bereit für optimales ISMS?

Wir beraten, führen und unterstützen Sie!

Michael Stach,
Geschäftsführer der EWERK Consulting & IT-Sicherheitsexperte

EWERK Group
Brühl 24, 04109 Leipzig
P +49 341 42649-99
F +49 341 42649-98
marketing@ewerk.com

EWERK