ISEGRIM X AG
Ittenhauser Str. 10 | D-88048 Friedrichshafen

Inhaber: Alexander Fürst
Rudel@isegrim-x.com | +49 7541 39739 61

In 9 Schritten zum ISMS

1. Erstellen Sie ein Projekt

Starten Sie das Implementierungsprojekt mit der Ernennung eines Projektleiters, der gemeinsam mit anderen Mitarbeitern ein Projekt erstellt. Dieses Team sollte sich folgende Fragen stellen:

- Was wollen wir erreichen?
- Wie lange wird es dauern?
- Was wird es kosten?
- Hat es die Unterstützung des Managements?

Aus der Praxis wissen wir, dass es sehr nützlich sein kann, einen ausgebildeten **Information Security Officer (ISO)** mit an Bord zu haben, der die Anforderungen der Norm besser versteht. Dadurch können sie leichter umgesetzt werden und Sie sparen Zeit und Geld.

2. Bereiten Sie das Projekt vor

In dieser Phase beschließen Sie

- die Informationssicherheitsziele,
- wer dem Projektteam angehört,

ISEGRIM X AG
Ittenhauser Str. 10 | D-88048 Friedrichshafen

Inhaber: Alexander Fürst
Rudel@isegrim-x.com | +49 7541 39739 61

- den Projektplan und

- das Risikoregister.

3. Legen Sie die Vorgehensweise für das ISMS fest

Im nächsten Schritt vereinbaren Sie**, wie bei der Implementierung des ISMS vorgegangen wird.**

Die ISO 27001 erkennt an, dass sich Prozesse in einem Unternehmen nicht in Stein meißeln lassen, sondern sich verändernden Umständen und Datenlagen anpassen lassen müssen. Daher schreibt die Norm auch keine festen Prozesse vor. Im Gegenteil. Als wirkungsvollstes Vorgehen beim Informationssicherheits-Management sieht sie einen „Prozessansatz“ vor.

Die Norm verordnet Ihnen auch keine bestimmte Methodik. Sie erlaubt es Ihnen stattdessen, Vorgehensweisen zu verwenden, die für Ihr Unternehmen am besten funktionieren. Sie können auch ein bereits bestehendes Modell fortsetzen, wenn es sich bewährt hat.

Vorgehen:

4. Erstellen Sie ein Management Framework

Jetzt **legen Sie den Geltungsbereich Ihres ISMS fest**. Definieren Sie also, welche Teile Ihres Unternehmens durch das ISMS abgedeckt werden sollen. Bei KMU ist es in der Regel das gesamte Unternehmen, für größere Unternehmen können nur bestimmte Abteilungen oder Geschäftsprozesse relevant sein.

Stellen Sie sicher, dass jeder Teil Ihres Unternehmens, der mit sensiblen Informationen zu tun hat, durch das System abgedeckt ist.

ISEGRIM X AG
Ittenhauser Str. 10 | D-88048 Friedrichshafen

Inhaber: Alexander Fürst
Rudel@isegrim-x.com | +49 7541 39739 61

So skalieren Sie Ihr ISMS in drei Schritten fachgemäß:

- Identifizieren Sie jede Stelle, an der sensible Informationen gespeichert sind.

- Bestimmen Sie die Wege, auf denen auf diese Informationen zugegriffen werden kann.

- Definieren Sie, welche Teile Ihres Unternehmens außerhalb des Geltungsbereichs liegen.

5. Identifizieren Sie grundlegende Sicherheitskriterien

In dieser **Phase identifizieren Sie Ihre grundlegenden Sicherheitsanforderungen**. Das sind die Anforderungen und Maßnahmen oder Kontrollen, die für den Geschäftsbetrieb notwendig sind.

Anforderungen:

6. Entwickeln Sie einen Risikomanagement-Prozess

Die ISO 27001 erlaubt es Unternehmen, die **angewandten Risikomanagement-Prozesse weitgehend selbst zu definieren**. Dazu gibt es gängige Methoden, die sich auf die Betrachtung von Risiken für bestimmte Werte (Assets) oder für bestimmte Szenarien konzentrieren. Jede Methode hat ihre Vor- und Nachteile. Wählen Sie die Methode aus, die zu Ihrer Organisation passt. Im Zentrum einer Risikobewertung nach ISO 27001 stehen aber immer fünf wichtige Aspekte:

1. Festlegung eines Rahmens für die Risikobewertung
2. Identifizierung der Risiken
3. Analysieren der Risiken
4. Bewertung der Risiken
5. Auswahl von Risikobehandlungen

a) Risikominimierung
b) Risikovermeidung
c) Risikoauslagerung
d) Risikoakzeptierung

ISEGRIM X AG
Ittenhauser Str. 10 | D-88048 Friedrichshafen

Inhaber: Alexander Fürst
Rudel@isegrim-x.com | +49 7541 39739 61

7. Erstellen Sie einen Risikobehandlungsplan

Als nächstes **legen Sie die Sicherheitsmaßnahmen fest**, mit denen Sie die Informationswerte Ihres Unternehmens schützen. Am besten definieren Sie einen Prozess, der beschreibt, was Sie zum Erreichen Ihrer ISMS-Ziele benötigen. Dieser Prozess beinhaltet folgende Schritte:

- Ermitteln Sie die erforderlichen Kompetenzen.

- Legen Sie alle notwendigen Schritte fest, um die Kompetenzen zu überprüfen und aufrechtzuerhalten, wie die Durchführung einer Bedarfsanalyse und die Definition eines gewünschten Kompetenzniveaus.

- Schulen Sie Ihre Mitarbeiter in den Pflichten der Informationssicherheit, um die Wirksamkeit der Maßnahmen zu überprüfen. Stellen Sie nach abgeschlossenem Training fest, ob sie die Maßnahmen umsetzen und in Ihren Arbeitsalltag integrieren können.

8. Messen, überwachen und überprüfen Sie die Ergebnisse

Damit ein ISMS funktioniert, müssen die Informationssicherheitsziele auf lange Sicht erfüllt werden. Sie sollten daher **Ihr ISMS regelmäßig überprüfen und überwachen.** Um die Effektivität und Umsetzung der Kontrollen zu messen, sollten Sie Metriken oder andere Methoden identifizieren, die für Ihr Unternehmen funktionieren.

Plan für Überprüfung und Überwachung:

9. Lassen Sie sich ISO 27001 zertifizieren

Mit einer Zertifizierung nach ISO 27001 belegen Sie, dass Ihr ISMS funktioniert und dass Ihr Unternehmen Informationssicherheit auf einem hohen Niveau betreibt und lebt. Deshalb raten wir Ihnen dringend, **eine Zertifizierung durch eine akkreditierte Zertifizierungsstelle einzuleiten, sobald das ISMS eingerichtet ist.**

ISEGRIM X AG
Ittenhauser Str. 10 | D-88048 Friedrichshafen

Inhaber: Alexander Fürst
Rudel@isegrim-x.com | +49 7541 39739 61

Der Zertifizierungsprozess bedeutet eine Überprüfung Ihrer ISMS-Dokumentation, sowie der Prozesse und Kontrollen. Die Zertifizierungsstelle wird auch ein Audit bei Ihnen vor Ort durchführen, um die Verfahren in der Praxis zu überprüfen.

Sie möchten diesen aufwendigen Prozess nicht alleine durchlaufen? ISEGRIM X steht Ihnen gerne als Partner zur Verfügung!

Kontaktieren Sie uns einfach & unverbindlich für weitere Informationen.

Senden Sie eine Mail an: **Rudel@isegrim-x.com**

Rufen Sie unseren Ansprechpartner Alex Fürst an: **+49 7541 39739 61**

Oder vereinbaren Sie bequem einen Kennenlern-Termin über unser Kalender-Tool:

Termin vereinbaren