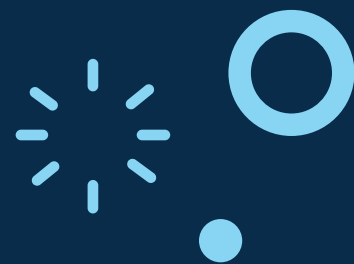




In 8 Schritten ein ISMS aufbauen

Inhalt

1. Anforderungskatalog für Ihr Managementsystem anlegen	6
2. Geltungsbereich festlegen	8
3. Risiken erkennen und minimieren	12
4. Richtlinien aufsetzen und verteilen	13
5. Mitarbeitende schulen und sensibilisieren	14
6. Sicherheitsvorfälle managen	15
7. Bewerten, auditieren & kontinuierlich verbessern	16
8. Lieferanten dokumentieren und bewerten	20

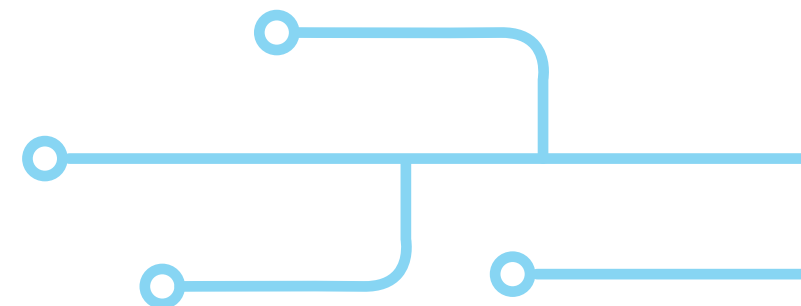


Alle Bilder wurden mittels KI generiert.

Stand: Oktober 2026



**„Entdecken Sie, wie Sie mit moderner
Software Schritt für Schritt ein
Managementsystem für Ihre
Informationssicherheit aufbauen.“**



In 8 Schritten ein ISMS aufbauen

Mit unserer Compliance-Software geben wir Ihnen ein praxisbewährtes Werkzeug an die Hand, mit dem Sie ein Managementsystem für Ihre Informations- und Cybersicherheit aufbauen und pflegen.

Die Software unterstützt Sie dabei, sowohl Ihren Dokumentationspflichten nachzukommen als auch funktionierende Prozesse zu implementieren.

Was ist ein ISMS?

Ein ISMS ist ein strukturiertes System, mit der Organisationen sämtliche Informationen, die sie verarbeiten, wirksam schützen. Ziel ist es, Risiken frühzeitig zu erkennen, Sicherheitsmaßnahmen gezielt umzusetzen und insbesondere auch die IT-Sicherheit laufend zu verbessern. Typischerweise orientiert sich der Aufbau eines ISMS an anerkannten Standards wie der ISO/IEC 27001.

Ein ISMS besteht aber nicht nur aus technischen Maßnahmen. Es berücksichtigt auch organisatorische Fragen:

- Wer hat Zugriff auf welche Daten?
- Was passiert im Notfall?
- Welche IT-Systeme sind besonders schützenswert?

Ein ISMS betrifft demnach die gesamte Organisation und verbessert die Zusammenarbeit zwischen Geschäftsleitung, IT, Datenschutz, Personal und weiteren Fachabteilungen.

Wir geben Ihnen im Folgenden einen Überblick, wie Sie Schritt für Schritt ein ISMS aufbauen.



1. Anforderungskatalog für Ihr Managementsystem anlegen

Im ersten Schritt legen Sie einen strukturierten Anforderungskatalog an, der sämtliche Anforderungen bzw. Controls des gewünschten Managementsystems enthält – zum Beispiel gemäß ISO/IEC 27001. Dafür stehen zwei verschiedene Möglichkeiten zur Verfügung:

- Eigene Kataloge anlegen bzw. importieren (z. B. aus einer Excel-Vorlage)
- Vorkonfigurierte Kataloge aus einer Vorlage (sofern vorhanden) nutzen

Der Katalog dient als zentrale Arbeitsgrundlage zur Umsetzung der entsprechenden Norm. Er ermöglicht es Ihnen, den Umsetzungsstand systematisch zu erfassen und den Reifegrad zu bewerten. Ausstehende Umsetzungsschritte können Sie direkt als Maßnahme anlegen und einem Verantwortlichen zuteilen.



Umsetzung mit dem Modul „Managementsysteme“

Behalten Sie den aktuellen Fortschritt der Normerfüllung immer im Blick:

- Erstellen Sie einen Managementkatalog mit all Ihren Anforderungen und Controls.
- Verknüpfen Sie Ihre Controls mit Bedrohungen.
- Dokumentieren Sie Ihren Umsetzungsstand.
- Report: Generieren Sie mit einem Klick die Erklärung zur Anwendbarkeit (Statement of Applicability – SoA).



2. Geltungsbereich festlegen

Definieren Sie, welche Organisationseinheiten Ihr ISMS abdecken soll und halten Sie dies in einem Leitdokument fest (Definition des Anwendungsbereichs bzw. Scope). Im Anschluss dokumentieren Sie alle für diesen Anwendungsbereich relevanten Standorte, Systeme, Geräte, Prozesse und weitere Werte Ihrer Organisation – die Assets.



Systemlandschaft und Applikationen dokumentieren

In der Compliance-Software können Sie Ihre gesamte Systemlandschaft abbilden. Legen Sie zunächst Standorte an. Anschließend fügen Sie Geräte und Systeme hinzu. Zudem können Sie Software-Anwendungen dokumentieren.

Auf dieser Basis können Sie im weiteren Verlauf die Ausgabe von Geräten, das Verteilen von Zugangsberechtigungen und die Freigabe von Applikationen managen.

Falls Ihre Organisation häufig Besucher empfängt, können Sie zu Ihren Standorten auch eine Besucherregistrierung aktivieren.

Umsetzung mit dem Modul „Systemlandschaft“

- Verwalten Sie sämtliche Geräte – inkl. digitalem Übergabeprotokoll bei der Ausgabe an Ihre Beschäftigten.
- Definieren Sie Sicherheitsbereiche im Kontext eines Zonenplans.

Umsetzung mit dem Modul „Applikationen“

- Dokumentieren Sie den aktuellen Softwarebestand.
- Definieren Sie, welche Abteilungen auf welche Software zugreifen dürfen.
- Halten Sie fest, inwiefern die Abteilungen Zugang zur Software benötigen (Zugangsanforderung).





Prozesse definieren

Es bietet sich insbesondere für das betriebliche Kontinuitätsmanagement an, die Kern- und Unterstützungsprozesse Ihrer Organisation zu modellieren. Die hierbei eingesetzten IT-Systeme und Geräte sind besonders wichtig für das Tagesgeschäft. Auf dieser Basis fällt die spätere Betrachtung in Bezug auf tolerierbare Ausfallzeiten und Schutzbedarf leichter. Zusätzlich sollten Sie wichtige Verfahrensschritte als Prozesse anlegen, um beispielsweise Vorfälle zu melden und zu behandeln (Notfallprozesse).

Umsetzung mit dem Modul „Prozesse“

- Modellieren Sie Ihre relevanten Geschäftsprozesse (BPMN-Format).
- Definieren Sie IT- & Notfallprozesse.

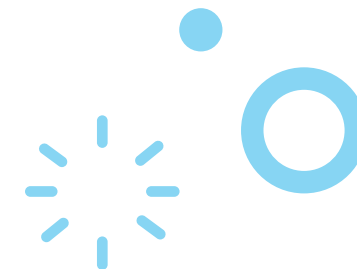
Asset-Register anlegen und pflegen

Parallel zu Ihrer Dokumentation der Standorte, Prozesse, Geräte und Applikationen erstellen Sie Ihr Asset-Register. Es umfasst sämtliche Werte Ihrer Organisation und enthält Informationen zum Schutzbedarf. Damit bildet es die Grundlage für Ihre Risikoanalyse und die Beurteilung, welche Maßnahmen in Ihrem Fall erforderlich sind.

Umsetzung mit dem Modul „Asset-Register“

Verwalten Sie alle Assets zentral auf einer Oberfläche:

- Stellen Sie Beziehungen bzw. Abhängigkeiten zu anderen Assets her (unterstützte und unterstützende Assets).
- Wählen Sie aus, wer von Ihren Beschäftigten oder welcher Rolleninhaber für das Asset zuständig ist (Eigentümer / Asset Owner).
- Legen Sie den Schutzbedarf fest.
- Nutzen Sie die voreingestellten Risikomatrizen oder erstellen Sie Ihre eigenen.
- Dokumentieren Sie maximale Ausfallzeiten und Wiederanlaufzeiten im Zuge des betrieblichen Kontinuitätsmanagements.
- Hinterlegen Sie Notfallpläne in Form von Checklisten.



„Um zu einer Applikation oder einem Gerät schnell ein neues Asset anzulegen, klicken Sie im Kontextmenü oben rechts auf den Diamanten.“

3. Risiken erkennen und minimieren

Egal ob Ransomware, Ausfälle oder interne Fehler: Informationssicherheitsrisiken können enorme Auswirkungen auf Ihre Organisation haben – sowohl operativ als auch rechtlich. Analysieren Sie diese Risiken systematisch in Bezug auf Vertraulichkeit, Verfügbarkeit und Integrität Ihrer Daten.



Umsetzung mit den Modulen „Risikoanalysen“ & „Bedrohungen“

- Definieren Sie den Anwendungsbereich, indem Sie die zu betrachtenden Assets hinzufügen.
- Ordnen Sie den Assets Bedrohungen und Schwachstellen zu.
- Leiten Sie Maßnahmen zur Reduzierung des Risikos ab (Risikobehandlungsplan).
- Betrachten Sie die aktuellen Risikowerte nach der Risikobehandlung.
- Formulieren Sie eine Stellungnahme, in der Sie zum Beispiel darlegen, inwiefern Restrisiken akzeptiert werden können.

„Mit dem Intranet richten Sie sich eine zentrale Informationsplattform für alle Beschäftigten ein.“

4. Richtlinien aufsetzen und verteilen

Viele Maßnahmen müssen Sie nicht nur technisch, sondern auch organisatorisch umsetzen. Es werden daher auch einige Konzepte, Richtlinien und Verfahrensanweisungen Teil Ihres ISMS sein. Diese müssen Sie freigeben (lassen) und an die Mitarbeitenden verteilen.



Umsetzung mit den Modulen „Dokumente“ und „Intranet“

- Erstellen Sie mit dem Dokumentengenerator schnell neue Richtlinien (Vorlagenpaket).
- Lenken und versionieren Sie Ihre Dokumente digital und automatisiert.
- Klassifizieren Sie Ihre Dokumente, z. B. nach „öffentlich“, „intern“, „vertraulich“.
- Veröffentlichen Sie Ihre Dokumente im Intranet und lassen Sie die Kenntnisnahme durch die Mitarbeitenden digital bestätigen.

5. Mitarbeitende schulen und sensibilisieren

Technische Schutzmaßnahmen allein reichen nicht aus. Die Wirksamkeit ist abhängig von den Mitarbeitenden, die täglich mit den IT-Systemen arbeiten. Studien zeigen: Über 90 % der Sicherheitsvorfälle lassen sich auf menschliches Fehlverhalten zurückführen – etwa durch Phishing, unsichere Passwörter oder versehentlich gelöschte Daten. Deshalb müssen Organisationen ihre

Mitarbeitenden regelmäßig schulen und sensibilisieren – und nachweisen, dass sie dies auch tun.

Aber auch die Geschäftsleitung selbst muss sich weiterbilden: Eine neue Anforderung, die das BSI mitbringt, ist die Schulungspflicht für Geschäftsleitungen. Das bedeutet, sie müssen ebenfalls regelmäßig an Schulungen teilnehmen, um Kenntnisse im Bereich des Risikomanagements und in der IT-Sicherheit zu erlangen. Mit dem integrierten Schulungsmodul bauen Sie ein strukturiertes Awareness-Programm auf.

Umsetzung mit dem Modul „Schulungen“

- Erstellen Sie Online-Mitarbeiterschulungen inkl. Abschlusstest (z. B. zur Informationssicherheit oder für die Phishing-Sensibilisierung).
- Verschicken Sie automatisiert die Einladungen und Erinnerungen.
- Verfolgen Sie den Fortschritt der Teilnehmenden.
- Versenden Sie nach Abschluss automatisiert Teilnahmezertifikate.

6. Sicherheitsvorfälle managen

Da es trotz etablierter Sicherheitsmaßnahmen und regelmäßiger Mitarbeitersensibilisierung zu Informationssicherheitsvorfällen kommen kann, müssen Sie einen Prozess zur Meldung und Bewältigung von Vorfällen einführen.

Den Beschäftigten muss klar sein, was ein Vorfall ist, wer in diesem Fall informiert werden muss und über welchen Kanal. Es sind konkrete verantwortliche Personen zu benennen, die zuständig sind, den Vorfall zu bearbeiten und zu eskalieren.

Umsetzung mit dem Modul „Intranet“

- Stellen Sie Ihren Beschäftigten eine zentrale Weboberfläche für die Meldung von Vorfällen zur Verfügung.
- Definieren Sie Verantwortliche, die per E-Mail über Vorfälle informiert werden sollen.
- Legen Sie fest, ob automatisch ein Datensatz für ein Sicherheitsereignis angelegt werden soll, sobald das Meldeformular von Beschäftigten genutzt wird.

Umsetzung mit dem Modul „Sicherheitsereignisse“

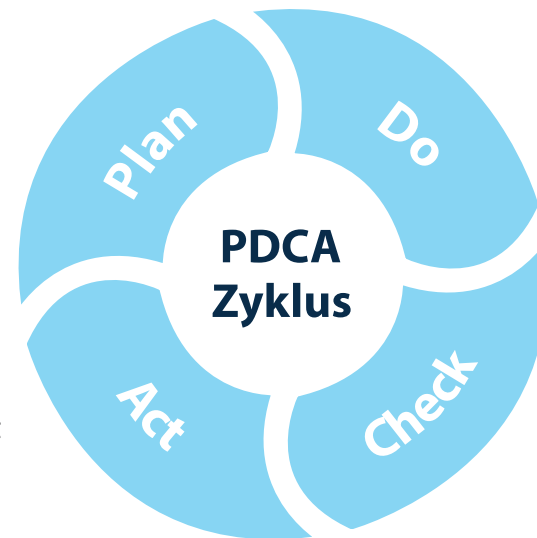
- Hinterlegen Sie bei den Ereignistypen ein Notfallteam und involvieren Sie es bei einem Vorfall automatisch oder mit einem Klick.
- Erfassen Sie Sicherheitsereignisse bzw. -vorfälle manuell und automatisiert mittels Meldeformular oder Schnittstelle (REST-API).
- Bewerten Sie das Ereignis und nutzen Sie, sofern angelegt, Notfall-Checklisten für eine schnelle Reaktion.
- Laden Sie parallel relevantes Beweismaterial hoch.
- Behalten Sie mögliche Meldefristen – z. B. an Behörden – mit dem systemseitigen Timer im Blick.



7. Bewerten, auditieren & kontinuierlich verbessern

Ein einmal aufgebautes ISMS reicht nicht aus – Informationssicherheit ist ein fortlaufender Prozess. Sie müssen Ihr Sicherheitsniveau regelmäßig prüfen und verbessern.

Im Zentrum steht dabei der sogenannte PDCA-Zyklus (Plan – Do – Check – Act): Ein kontinuierlicher Verbesserungsprozess, mit dem Sie Schwachstellen aufdecken, Maßnahmen nachsteuern und Compliance dauerhaft sichern.



Um die Leistung Ihres ISMS bewerten zu können, müssen Sie zunächst Ziele definieren (Teil der Plan-Phase). Klassisch erfolgt dies mit Hilfe von Leistungskennzahlen (KPI). Mit Kennzahlen können Sie zum Beispiel die Kenntnisnahme Ihrer Richtlinien messen. Betrachten Sie hierbei den Anteil der Mitarbeitenden, die die Richtlinien gelesen und akzeptiert haben. Oder Sie erfassen, für wie viele Risikoanalysen, Dienstleister oder Dokumente eine Revision vorliegt.

Umsetzung mit dem Modul „Kennzahlen“

- Nutzen Sie systemseitige Metriken als Grundlage für eine Bewertung Ihres ISMS anhand von Kennzahlen.
- Definieren Sie Ziele und lesen Sie an Ihren Kennzahlen ab, wo Sie stehen.
- Verknüpfen Sie Kennzahlen mit Anforderungen aus Ihrem Managementkatalog.
- Binden Sie ggf. via API oder HTTP-Schnittstelle Fremdsysteme an, um weitere relevante Daten einfließen zu lassen.



„Definieren und dokumentieren Sie Ihre Messmethode, um stets vergleichbare Ergebnisse zu erhalten.“



Führen Sie Audits nicht nur „von oben“ durch – binden Sie Fachabteilungen aktiv ein. So steigern Sie das Sicherheitsbewusstsein und verbessern zugleich die Akzeptanz Ihres ISMS.





„In der Act-Phase reagieren Sie auf die Bewertungsergebnisse. So verbessern Sie Ihr Managementsystem kontinuierlich.“

Nachdem Sie Ihre Ziele definiert haben, ist es womöglich erforderlich, weitere Maßnahmen umzusetzen, um Ihre Ziele zu erreichen (Teil der Do-Phase). Prüfen Sie nach der Umsetzung immer auch die Wirksamkeit (Teil der Check-Phase).

Für eine umfassende Bewertung des Umsetzungsstandes Ihrer Anforderungen bzw. Controls ist es zusätzlich erforderlich, dokumentierte interne Audits

durchzuführen. Die Ergebnisse sind ein wichtiger Baustein für die Managementbewertung durch die oberste Leitungsebene.

In der Compliance-Software stehen für interne Audits grundsätzlich zwei Möglichkeiten zur Verfügung, wobei sich die zweite Möglichkeit insbesondere an Audit-Expertinnen und -Experten richtet.

Praxistipp: Falls Sie Ihr ISMS durch eine offizielle Zertifizierungsstelle prüfen lassen möchten, sollten Sie vor dem ersten Zertifizierungsaudit mindestens einmal Ihren PDCA-Zyklus durchlaufen haben. Insbesondere sollten Sie ein internes Audit durchgeführt haben, in dem alle ISMS-Anforderungen und Controls der entsprechenden Norm geprüft wurden.

Möglichkeit 1 für interne Audits: Umsetzung mit dem Modul „Managementsysteme“

- Erstellen Sie Fragenkataloge, um einzelne Prüfbereiche zu auditieren.
- Übernehmen Sie Antworten und Erkenntnisse automatisch in Ihr Managementsystem.
- Leiten Sie Maßnahmen ab, um bei Abweichungen gegenzusteuern.
- Generieren Sie hieraus die Grundlage für Ihre Managementbewertung.
- Aktivieren Sie die Prüfansicht für Auditoren, um den aktuellen Umsetzungsstatus, Ihre SoA und relevante Nachweisdokumente sicher mit internen oder externen Prüfern zu teilen.

Möglichkeit 2 für interne Audits: Umsetzung mit dem optionalen Modul „Interne Audits“

- Legen Sie ein Auditprogramm mit den nächsten geplanten Audits an – fügen Sie ggf. auch Zertifizierungsaudits hinzu, die extern durchgeführt werden.
- Hinterlegen Sie Anforderungskataloge, um die verschiedenen Prüfaspekte strukturiert zu betrachten.
- Führen Sie Audits durch und dokumentieren Sie die Konformität, Abweichungen oder Verbesserungspotenziale.
- Schlagen Sie ggf. Korrekturmaßnahmen vor.
- Nutzen Sie bei Bedarf zusätzlich oder anstelle eines Anforderungskataloges Protokolleinträge, um relevante Aspekte Ihres Audits zu dokumentieren.
- Bereiten Sie das Audit nach, indem Sie weitere Anmerkungen aufnehmen und Maßnahmen in das Modul „Maßnahmen“ übernehmen.
- Erstellen Sie einen Auditbericht mit Ihren Ergebnissen.



8. Lieferanten dokumentieren und bewerten

Auch wenn Ihre Organisation intern alles richtig macht – Sie arbeiten wo möglich mit externen Partnern zusammen, die ebenfalls Zugriff auf IT-Systeme und sensible Daten haben, zum Beispiel durch Wartung, Hosting oder Support. Damit Sicherheitslücken nicht unbemerkt über externe Dienstleister in die eigene Organisation hineinwirken, ist es notwendig, auch die Sicherheits-

vorkehrungen Ihrer Partner im Blick zu behalten. Gesetzliche Rahmenwerke wie das BSIG (bzw. vorher NIS2-Umsetzungsgesetz) sehen vor, dass Unternehmen nachvollziehbar darlegen können, wie mit Risiken aus der Lieferkette umgegangen wird. Es geht darum, mögliche Risiken frühzeitig zu erkennen und angemessene Schutzmaßnahmen gemeinsam zu etablieren.



Umsetzung mit dem Modul „Dienstleister/Lieferanten“

- Verwalten Sie all Ihre Dienstleister in einer übersichtlichen Struktur.
- Dokumentieren Sie die Zulässigkeit von Datenübermittlungen.
- Versenden Sie Fragebögen an Lieferanten, um automatisch einen Risikowert zu erhalten.

Vielen Dank für Ihr Vertrauen!

Sollten Sie Fragen haben oder eine individuelle Beratung wünschen, stehen wir Ihnen jederzeit gerne zur Verfügung.

Kontaktieren Sie uns

LegallInnovate Technologies GmbH
Geschäftsführer: Thomas Niersmann
Adresse: Issumer Tor 45, 47608 Geldern
E-Mail: info@dpms-online.de



Management
System
ISO/IEC
27001:2022

www.tuv.com
ID 9000045316

Noch mehr Infos
finden Sie hier!



