WIE SIE SICHERHEIT einfach umsetzen

Die 5 entscheidenden Sicherheitsmassnahmen, die jedes Unternehmen braucht

VON DIETER HUBER

INHALTSVERZEICHNIS

1 PRAXISNAHER LEITFADEN

- Einleitung 1
- Ihr professionelles Sicherheitssystem 2
- Für wen ist dieser Leitfaden gedacht 3
- Was passiert, wenn Sie nichts tun 4
- Die 5 Massnahmen Ihrer Sicherheit 5
  - Nr. 1: Rollen und Verantwortlichkeiten festlegen 6
  - Nr. 2: Vermögenswerte und Risiken erfassen 7
  - Nr. 3: Sicherheitsdokumente erstellen 8
  - Nr. 4: Sicherheitsbewusstsein nachweisbar machen 9-10
  - Nr. 5: Interne Sicherheitsübungen durchführen 11
- Selbsttest: Ist Ihr Unternehmen vorbereitet? 12

2 UMSETZUNG UND STRUKTUR

- Automatisieren & Delegieren von Sicherheitsaufgaben 13
- Ihre ISMS-Dokumentation strukturieren 14
- Sichtbare Sicherheit auch ohne ISO-Zertifizierung 15
- Professionelle Präsentation Ihrer Sicherheitsdokimentation 16
- Häufige Fallstricke vermeiden 17

3 VOM KONZEPT ZUR UMSETZUNG

- Ihr Schnellstart-Sicherheitskit 18
- Die 90-Tage-Roadmap zur Umsetzung 19
- Erfolgsfaktoren für die Umsetzung 20
- Vorteile des pragmatischen Sicherheitsansatzes 21
- Mit oder ohne Unterstützung: Der Unterschied, der entscheidet 22
- Fallstudie: Sicherheitsaufbau in der Praxis 23
- Ihre nächsten Schritte 24
- Starten Sie jetzt Ihre 90-Tage-Implementierung 25
- Bonus: Die 6 Prinzipien nachhaltiger Sicherheit 26

BEREITS 50+ UNTERNEHMEN SICHERTEN SICH SO IHREN UMSATZ.
SCANNEN SIE DEN QR-CODE FÜR IHR KOSTENLOSES GESPRÄCH!

Dieter Huber

Der Sicherheits-Experte

Nach 27 Jahren in der IT–Security und der Prüfung von über 1000 IT–Dienstleistern habe ich etwas Schockierendes entdeckt: Die meisten Unternehmen sind nicht unsicher – sie können ihre Sicherheit nur nicht richtig zeigen.

Die Folgen sind verheerend: Jeden Monat verlieren gute IT-Dienstleister Aufträge in 6-stelliger Höhe oder mehr. Langjährige Kunden wechseln zur Konkurrenz. Bei Ausschreibungen fliegen sie schon in der Vorqualifikation raus. Und das alles nur, weil sie ihre Sicherheit nicht richtig nachweisen können.

Wer versucht, Sicherheit ohne Erfahrung aufzubauen, zahlt doppelt: mit verlorener Zeit, teuren Fehlern und verpassten Aufträgen.
Mit meiner geführten 90-Tage-Umsetzung sparen Sie Monate – und vermeiden teure Umwege.

Das Ergebnis: Sie gewinnen wieder Ausschreibungen, halten ihre Bestandskunden und wachsen kontinuierlich.

Ihr professionelles Sicherheitssystem

Ein professionelles Sicherheitssystem ist mehr als ein internes Projekt – es ist Ihr Schutzschild gegen Auftragsverluste, teure Sicherheitsvorfälle und beschädigtes Kundenvertrauen.

Wer jetzt keinen strukturierten Ansatz verfolgt, läuft Gefahr, im Ernstfall unvorbereitet zu sein – mit allen finanziellen und reputativen Folgen.

In 90 Tagen statt endloser Projekte

... weil jeder Monat Verzögerung bares Geld kostet.

Die 5 wirksamsten Massnahmen

... reagieren Sie sofort und überzeugend auf Kunden-, Partner- oder Behördenanfragen.

Effizient & kostengünstig

... vermeiden Sie hohe Beraterkosten und interne Ressourcenverschwendung

Strukturierte ISMS-Grundlagen

... damit Sie jederzeit auditbereit sind und keine Anfragen mehr ins Stocken geraten.

ISO 27001 CERTIFIED

Für wen ist dieser Leitfaden wirklich gedacht?

Der Unterschied zwischen Unternehmen, die wachsen, und denen, die Aufträge verlieren, liegt oft in einem unsichtbaren Faktor:

Der Fähigkeit, Sicherheitsanforderungen jederzeit überzeugend nachzuweisen.

Ohne klaren Fahrplan und Erfahrung verschwenden Sie Wochen – während Ihre Mitbewerber längst den Auftrag in der Tasche haben.

Nachweisbare Sicherheit

Sie benötigen nachvollziehbare Informationssicherheit, die Vertrauen bei Kunden und Partnern schafft – ohne unnötigen Aufwand.

Effektive Reaktion auf Anfragen

Sie benötigen einen strukturierten Ansatz und präzise Dokumente, um Sicherheitsanfragen und Compliance (z.B. DSGVO) proaktiv zu begegnen.

Strukturierte Sicherheitsrichtlinien

Ihre Organisation braucht klare, umsetzbare Sicherheitsregeln, um das Sicherheitsniveau nachhaltig zu erhöhen und den Dokumentationsaufwand zu minimieren.

WAS PASSIERT, WENN SIE NICHTS TUN?

Buchen Sie jetzt Ihren Termin – und vermeiden Sie weitere Risiken!

KOSTENLOSE ISO 27001 BERATUNG

Informationssicherheit ist entscheidend für Geschäftsbeziehungen. Unternehmen müssen ihre Sicherheitslage transparent und nachweisbar darlegen:

Kundenanfragen

Kunden fordern detaillierte Sicherheitsnachweise.
Fehlen diese, verzögern sich Vertragsabschlüsse.

Versicherungsanforderungen

Cyberversicherungen verlangen detaillierte Nachweise, z.B. für MFA oder Incident-Response-Pläne.

Lieferanten-Audits

Geschäftspartner auditieren, um Lieferkettenrisiken zu minimieren. Nichterfüllung kann zum Ausschluss führen.

Regulatorische Auflagen

Neue Regulierungen wie NIS2 oder DORA erfordern dokumentierte Prozesse, um Bussgelder und Reputationsschäden zu vermeiden.

> Fehlende Sicherheitsdokumente können Umsatz verlangsamen, Cyberversicherungskosten erhöhen und Geschäftsunterbrechungen verursachen.
>
> Die Lösung liegt in der strategischen Strukturierung und pragmatischen Optimierung Ihrer bestehenden Sicherheitsmassnahmen.

Wer diese Punkte ignoriert, zahlt später doppelt: mit verlorenen Deals, erhöhten Prämien, Bussgeldern und beschädigtem Ruf. Präventives Handeln spart nicht nur Geld, sondern auch Nerven

Die 5 Massnahmen

In der Praxis scheitern viele Unternehmen nicht am Willen, sondern an fehlender Erfahrung, Priorisierung und Dokumentationslogik.

Genau hier bringt externe Unterstützung Klarheit und Geschwindigkeit.

Diese fünf Massnahmen bilden das Fundament für Ihr Sicherheitssystem, das externen Überprüfungen standhält – auch ohne formale Zertifizierung.

Massnahme Nr. 1:
Rollen und Verantwortlichkeiten festlegen

Definieren Sie klare Verantwortlichkeiten für Sicherheitsaufgaben.

Massnahme Nr. 2:
Vermögenswerte und Risiken erfassen

Identifizieren Sie kritische Vermögenswerte und Daten zum Schutz.

Massnahme Nr. 3:
Sicherheitsdokumente erstellen

Erstellen Sie prägnante, nachweisbare Sicherheitsrichtlinien.

Massnahme Nr. 4:
Sicherheitsbewusstsein nachweisbar machen

Schulen Sie Mitarbeiter und dokumentieren Sie deren Teilnahme.

Massnahme Nr. 5:
Interne Sicherheitsübungen durchführen

Führen Sie jährliche Simulationen zur Überprüfung der Reaktionsfähigkeit durch.

Dieser Ansatz deckt relevante Sicherheitsbereiche ab. Er ermöglicht gezielte Massnahmen mit maximalem Sicherheitsvorteil und minimalem Aufwand, um externe Anforderungen zu erfüllen.

Keine ISO-Zertifizierung nötig? Diese fünf Elemente bieten die Struktur, um Ihre Sicherheitskompetenz überzeugend zu demonstrieren.

Massnahme Nr. 1: Rollen und Verantwortlichkeiten

Buchen Sie jetzt Ihren Termin – und klären Sie Ihre Sicherheitsrollen in einem strukturierten Gespräch.

KOSTENLOSE ISO 27001 BERATUNG

Klare Verantwortlichkeiten sind entscheidend für nachweisbare Sicherheit und ein solides Sicherheitsfundament.

> Fehlende Rollen mindern das Vertrauen bei externen Sicherheitsanfragen.

Sicherheitsbeauftragten ernennen

Benennen Sie eine verantwortliche Person für Informationssicherheit und dokumentieren Sie deren Rolle.

Verantwortlichkeiten beschreiben

Erstellen Sie präzise Zuständigkeitsbeschreibungen und klare Berichtslinien.

Externen Ansprechpartner benennen

Bestimmen Sie eine zentrale Person für alle externen Sicherheitsanfragen.

Massnahme Nr. 2: Vermögenswerte und Risiken erfassen

**Buchen Sie jetzt Ihren Termin –
und erfassen Sie gemeinsam mit mir alle Risiken.**

KOSTENLOSE ISO 27001 BERATUNG

Effektiver Schutz basiert auf umfassendem Wissen. Erfassen Sie Vermögenswerte und Risiken detailliert, um gezielte Schutzmassnahmen zu entwickeln und Ihr Systemverständnis zu demonstrieren.

Vermögenswerte auflisten

Erstellen Sie eine umfassende Liste aller Technologien und Informationen (z.B. Software, Hardware, Cloud-Dienste, sensible Daten). Erfassen Sie Name, Zweck, Eigentümer und Wichtigkeit jedes Assets als Grundlage für Risikobewertungen.

Risiken analysieren

Identifizieren und dokumentieren Sie spezifische Risiken (z.B. Zugriffs-, Datenschutz-, Betriebsrisiken) basierend auf Ihrer Vermögensliste.
Bewerten Sie Auswirkung und Eintrittswahrscheinlichkeit, um Massnahmen zu priorisieren.

Bonus:
Erstellen Sie eine Risiko-Heatmap zur visuellen Darstellung.
Ideal, um Ihr Risikoverständnis extern zu zeigen.

Mit einer klaren Übersicht über Vermögenswerte und Risiken schaffen Sie Transparenz, Prioritäten – und Sicherheit, die Sie belegen können.

Massnahme Nr. 3: Sicherheitsdokumente erstellen

Buchen Sie jetzt Ihren Termin –
und erhalten Sie alle nötigen Dokumente direkt einsatzbereit.

KOSTENLOSE ISO 27001 BERATUNG

Ihre Sicherheitsdokumente sind das Rückgrat Ihres Systems. Sie transformieren informelle Praktiken in klare, nachvollziehbare Schritte und belegen Ihre Sicherheitsreife intern und extern. Konzentrieren Sie sich auf Pragmatismus.

Tipp: Der Wert liegt in Praktikabilität und Anwendbarkeit. Prägnante, gut gepflegte Dokumente, die gelebte Praktiken widerspiegeln, sind effektiver als umfangreiche, ungenutzte Richtlinien.

Sicherheitsrichtlinie

Ein prägnantes, 1-2 Seiten umfassendes Dokument mit Zielen, Geltungsbereich, Rollen und wesentlichen Regeln (z.B. Passwortsicherheit, Meldepflichten).

Kontrollbeschreibungen

Beschreiben Sie die wichtigsten Sicherheitskontrollen (z.B. Datensicherung, Zugriffskontrolle, Incident Response):
Was, wie, wer, wann.

Verantwortlichkeitsdiagramm

Ein übersichtliches Diagramm (z.B. RACI-Matrix), das Verantwortlichkeiten für Sicherheitsaufgaben klar zuweist.

Diese Dokumente sind professioneller Nachweis Ihrer Sicherheitsreife bei Audits und Partnern. Sie ermöglichen fundierte Antworten auf Anfragen zu Ihren Richtlinien und Verfahren.

Massnahme Nr. 4: Nachweisbares Sicherheitsbewusstsein

Buchen Sie jetzt Ihren Termin –
und sichern Sie sich den einfachsten Weg zum Awareness-Nachweis.

KOSTENLOSE ISO 27001 BERATUNG

Schluss mit langweiligen PowerPoints!

Traditionelle Sicherheitsschulungen sind ineffektiv, führen selten zu Verhaltensänderungen oder belastbaren Nachweisen. Ein Paradigmenwechsel ist nötig.

Eine moderne und wirksame Schulung sollte folgende Kriterien erfüllen:

Kurz

Module von 5-10 Minuten, fokussiert auf ein Thema.

Nützlich

Fokus auf reale, unternehmensrelevante Bedrohungen (z.B. Phishing).

Unterhaltsam

Ansprechende Inhalte durch Szenarien, Animationen oder interaktive Fragen.

Klar

Konkrete, umsetzbare Anweisungen (z.B. "So melden Sie eine verdächtige E-Mail").

Nachweisbar

Aufzeichnungen über Abschluss und Verständnis der Kernbotschaften (z.B. via Quizzes).

Ihr 4-Schritte-Ansatz für Sicherheitsbewusstsein

1

Videos erstellen

Produzieren Sie kurze Videos (5-10 Min.) zu wichtigen Sicherheitsregeln. Nutzen Sie einfache Tools. Jedes Video behandelt ein spezifisches, umsetzbares Thema (z.B. Phishing-Erkennung).

2

Mit dem Team teilen

Verteilen Sie die Videos regelmässig (z.B. monatlich oder quartalsweise) über Ihre Kommunikationskanäle. Legen Sie klare Fristen fest.

3

Nachverfolgen

Implementieren Sie Mechanismen zur Bestätigung des Abschlusses, z.B. durch kurze Quizze oder Tracking-Funktionen. Erfassen Sie jeden Abschluss individuell.

4

Aufzeichnungen führen

Führen Sie ein zentrales Register (z.B. in Google Sheets) mit Datum und Punktestand. Diese Aufzeichnungen dienen als Nachweis für Audits.

Diese Vorgehensweise steigert das Sicherheitsbewusstsein effektiv und liefert Nachweise für Audits.

Sicherheitsbewusstsein muss nicht langweilig sein. Gestalten Sie Schulungen kurz, praxisnah und konzentrieren Sie sich auf das Wesentliche für Ihr Unternehmen.

Massnahme Nr. 5: Interne Sicherheitsübungen

Buchen Sie jetzt Ihren Termin –
und planen Sie Ihre nächste Audit-Übung professionell.

KOSTENLOSE ISO 27001 BERATUNG

Regelmässige Sicherheitsübungen bereiten Ihr Team auf unerwartete Anfragen vor. Dies minimiert Verzögerungen, deckt Schwachstellen auf und stärkt Ihre Sicherheitsreife.

1. Vorbereitung

Bilden Sie ein Kernteam (IT, Recht, Betrieb). Wählen Sie eine realistische externe Sicherheitsanfrage (z.B. Kundenfragebogen) und sammeln Sie nötige Dokumente. Klären Sie die Übungsziele.

2. Übung

Führen Sie einen 60-minütigen "Mini-Audit" durch, bei dem das Team die Anfrage in Echtzeit bearbeitet. Identifizieren und stellen Sie Nachweise bereit. Beobachten Sie Zusammenarbeit und Engpässe.

3. Ergebnisse überprüfen

Analysieren Sie Lücken und Herausforderungen: War alles auffindbar, Zuständigkeiten klar, Nachweise aktuell? Identifizieren Sie Verbesserungsbereiche für Prozesse und Dokumentationen.

4. Kontinuierliche Verbesserung

Ergreifen Sie gezielte Massnahmen zur Verbesserung: Aktualisieren Sie Dokumente, klären Sie Rollen (z.B. RACI-Matrix) oder verbessern Sie die Zugänglichkeit von Nachweisen. Sichern Sie die Umsetzung und regelmässige Überprüfung.

Diese Übungen testen und stärken Ihre Sicherheitsstrategie kontinuierlich. Sie minimieren Stress und Verzögerungen bei realen Anfragen und liefern konkrete Belege für Ihre organisatorische Reife.

Wie bereit ist Ihr Unternehmen für echte Sicherheitsanfragen? Finden Sie es mit diesen 7 Fragen heraus.

1	Können Sie Sicherheitsrichtlinien und andere wichtige Dokumente (z.B. Datenschutz, Asset-Inventar) schnell finden und präsentieren?
2	Sind Verantwortlichkeiten für jeden Sicherheitsbereich (z.B. Schwachstellenmanagement, Notfallwiederherstellung) klar definiert und bekannt?
3	Können Sie aktuelle Beweise für Backup-Pläne und die regelmässige Prüfung von Wiederherstellungstests vorlegen?
4	Haben Sie detaillierte Aufzeichnungen über Sicherheitsaktivitäten (z.B. Zugriffsüberprüfungen, Patch-Management, Schulungen)?
5	Können Sie aufzeigen, wie der Zugriff auf kritische Systeme/Daten kontrolliert, protokolliert und regelmässig überprüft wird?
6	Haben Sie einen schriftlichen und erprobten Plan, was im Falle eines Sicherheitsproblems (z.B. Datenpanne, Cyberangriff) zu tun ist?
7	Können Sie anhand konkreter Beispiele erläutern, wie Sie Sicherheitsrisiken identifizieren, bewerten und behandeln?

Wenn Sie mehr als zwei Punkte mit ‚Nein' beantworten mussten, ist es Zeit zu handeln!

Buchen Sie jetzt Ihren Termin –
und sichern Sie sich Ihren klaren Fahrplan

KOSTENLOSE ISO 27001 BERATUNG

Automatisieren & Delegieren

Automatisierung und Delegation von Aufgaben halten Ihre Sicherheitsmassnahmen langfristig aktuell und effizient.

Automatisierungstools nutzen

Nutzen Sie No-Code- oder Low-Code-Automatisierungstools für repetitive Aufgaben. Das minimiert Fehler und entlastet Ihr Team.

Fristen-Erinnerungen

Automatische Benachrichtigungen für Prüfungen und Schulungen.

Dokumentenmanagement

Automatische Verwaltung von Sicherheitsdokumenten.

Statusberichte

Automatische Berichte über Aufgaben und Compliance.

Aufgaben delegieren

Delegieren Sie Routineaufgaben an administrative Mitarbeiter. Dies steigert die Effizienz und entlastet Ihr technisches Team.

1. **Dokumentenaktualisierungen**
   Formatierung, Organisation und Textaktualisierung von Sicherheitsdokumenten delegieren.
2. **Berechtigungsinformationen**
   Administrative Kräfte sammeln Benutzerzugriffe und Berechtigungen aus Systemen.
3. **Datei-Organisation**
   Regelmässige Pflege der digitalen Ablage von Sicherheitsdokumenten beauftragen.
4. **Schulungsnachweise**
   Teilnahme an Sicherheitsschulungen verfolgen und archivieren.

Ihr ISMS strukturieren

Klare ISMS-Dokumentation steigert Effizienz, Glaubwürdigkeit und Compliance – auch ohne ISO-Zertifizierung.

Beispiel: Dokumentationsstruktur

Richtlinien & Leitfäden

- ISMS-Richtlinie IT-Nutzung &
- Passwörter Remote-Arbeit &
- Datenklassifizierung

Risiken & Kontrollen

- Risikobewertung & -behandlung
- Kontrollbeschreibungen

Sensibilisierung & Schulung

- Schulungsmaterialien
- Nachweise jährlicher Schulungen

Bestandsaufnahme

- Asset-Register (Technologie, Software, Daten)
- Verzeichnis Drittanbieter

Management-Übersicht

- Sicherheits-Dashboard & KPIs
- Vorfallprotokoll & Berichte

Diese Struktur erleichtert den Zugang zu Informationen und stärkt das Vertrauen bei Partnern und Kunden.

Ihr Ziel: Eine gut organisierte Dokumentation für reibungslose Zusammenarbeit und schnelle Entscheidungen.

Sichtbare Sicherheit auch ohne ISO-Zertifizierung

Auch ohne ISO-Zertifizierung belegen Sie extern glaubwürdige Sicherheitspraktiken durch gezielte Dokumentation.

Ihr externes Sicherheits-Kit

Ein „Sicherheits-Kit“ bietet externen Stakeholdern Transparenz, ohne interne Details offenzulegen.

Öffentliche Sicherheitsrichtlinie

Eine prägnante externe Version Ihrer ISMS-Richtlinie, die übergeordnete Prinzipien und Datenschutz-Engagement kommuniziert.

Zusammenfassung der Schlüsselkontrollen

Beschreibung Ihrer wichtigsten Sicherheitskontrollen und -praktiken, inkl. Zugriffskontrolle, Datenschutz, Geschäftskontinuität, Vorfallreaktion und Sicherheitsüberwachung.

Nachweis des Sicherheitsbewusstseins

Dokumentation der Effektivität Ihres Sensibilisierungsprogramms: Zusammenfassungen der Schulungsinhalte und Abschlussquoten.

Sicherheitskontakt und Eskalationspfad

Klare Kontaktinformationen für Sicherheitsfragen: Hauptverantwortlicher, Kanal für Vorfallmeldung und kurzer interner Eskalationspfad.

Professionelle Präsentationsansätze

Format und Bereitstellung Ihrer Sicherheitsdokumentation beeinflussen die externe Wahrnehmung. Berücksichtigen Sie folgende Ansätze zur Maximierung Ihrer Glaubwürdigkeit:

Konsistentes Branding - Signalisiert Professionalität und Vertrauenswürdigkeit.

Sicheres PDF-Format - Gewährleistet Integrität und Unveränderlichkeit.

Versionskontrolle - Zeigt aktives Dokumentenmanagement.

Führungskräfte-Zustimmung - Unterstreicht Management-Engagement.

Klare und verständliche Sprache - Macht Inhalte für alle zugänglich.

Visuelle Elemente - Veranschaulichen komplexe Sachverhalte.

> Ein hohes Mass an Vertrauen und Professionalität kann oft das übertreffen, was Konkurrenten mit formalen Zertifizierungen, aber mangelhafter Dokumentation bieten.

Durch die proaktive Bereitstellung dieses kuratierten Pakets demonstrieren Sie umfassende Sicherheitskompetenz durch greifbare Nachweise statt ausschliesslich durch Zertifizierungen. Eine gut vorbereitete Dokumentation schafft oft mehr Vertrauen als Zertifizierungsnamen allein.

Häufige Fallstricke vermeiden

Erkennen Sie Fallstricke frühzeitig, um Ihren Plan erfolgreich umzusetzen.

Dokumenten-Chaos

Inkonsistente Dokumente erschweren Audits.

Lösung: Zentrale Ablage, Versionskontrolle.

Unklare Verantwortlichkeiten

Unklare Aufgaben schaffen Lücken.

Lösung: Verantwortlichkeiten klären und kommunizieren.

Richtlinien versus Realität

Unpraktische Richtlinien führen zu Audit-Problemen.

Lösung: Praktiken realitätsnah dokumentieren.

Undokumentierte Sensibilisierung

Fehlende Nachweise für Awareness- Aktivitäten.

Lösung: Teilnahme nachweisbar dokumentieren.

Ungesteste Backups

Ungesteste Backups versagen im Ernstfall.

Lösung: Regelmässige Backup-Tests planen und dokumentieren.

Prinzipien zur Fallstrick-Vermeidung:

- **Einfachheit**

  Pflegbare Dokumentation und Implementierung.

- **Evidenz-Fokus**

  Nachweise (Logs, Berichte) für Audits bereitstellen.

- **Regelmässige Überprüfungen**

  Dokumentation und Praktiken periodisch überprüfen.

Ihr Schnellstart-Sicherheitskit

Strukturierte Sicherheit ist einfach. Dieser Abschnitt zeigt Schlüsselkomponenten für eine solide Sicherheitsgrundlage in 90 Tagen.

1	**Wöchentliche Zeitinvestition** Eine Stunde pro Woche genügt. Konzentrieren Sie sich konsequent auf eine spezifische Aufgabe des 90-Tage-Plans.
2	**Asset- und Risikovorlage** Dokumentieren Sie Assets und Risiken in einer einfachen Tabellenvorlage (z.B. Google Sheets) mit Name, Eigentümer, Kritikalität, Risiken und Kontrollen.
3	**Sensibilisierungsvideo** Erstellen Sie ein kurzes (5-10 Min.) Video zu internen Sicherheitspraktiken als Schulung und Nachweis. Intern hosten mit einfachem Überprüfungsmechanismus (z.B. Quiz).
4	**Richtlinien- und Massnahmen-Dokument** Ein prägnantes PDF (max. 5-10 Seiten) mit Ihrer Sicherheitsrichtlinie und operativen Massnahmen, basierend auf tatsächlichen Praktiken.
5	**Speicherstruktur** Richten Sie eine klare digitale Ordnerstruktur für Sicherheitsdokumente ein. Implementieren Sie konsistente Namenskonventionen und Zugriffskontrollen.

**Buchen Sie jetzt Ihren Termin –
und sichern Sie sich Ihren klaren Fahrplan!**

KOSTENLOSE ISO 27001 BERATUNG

Implementierungszeitplan: 90-Tage-Sicherheits-Roadmap

Diese 90-Tage-Roadmapunterteilt denAufbaueinerglaubwürdigenSicherheitsgrundlage in überschaubarePhasenmitklaren Meilensteinen.

1

Tage 1-15: Grundlagen & Umfang

- Sicherheitsverantwortlichen benennen.
- Digitale Ordnerstruktur anlegen.
- Erste Inventur kritischer Vermögenswerte.

Meilenstein: Verantwortlicher ernannt und Dokumentationsframework für ISMS vorhanden.

2

Tage 16-30: Dokumentation & Analyse

- Umfassende Vermögensinventur abschliessen.
- Gezielte Risikobewertung entwickeln.
- Wichtige Kontrollen & Massnahmen dokumentieren.

Meilenstein: Umfassendes Sicherheitsdokumentationspaket fertiggestellt .

3

Tage 31-60: Implementierung & Sensibilisierung

- Praktische Sensibilisierungsinhalte erstellen.
- Obligatorische Teamschulung durchführen.
- Wirkungsvolle Sicherheitskontrollen implementieren (z.B. MFA).

Meilenstein: Wesentliche Sicherheitsmassnahmen in Betrieb, Mitarbeiterbewusstsein verbessert.

4

Tage 61-90: Verifizierung & Verfeinerung

- Interne Sicherheitsüberprüfung durchführen.
- Dokumentenabruf & Genauigkeit testen.
- Richtlinien basierend auf Testergebnissen verfeinern.

Meilenstein: Auditbereite Sicherheitslage etabliert und für externe Anfragen vorbereitet.

Erfolgsfaktoren für die Implementierung:

90

Tage bis zur Implementierung

Glaubwürdige Sicherheitsgrundlage in 90 Tagen.

5

Fokus auf Kernmassnahmen

5 wirkungsvolle Massnahmen für maximalen Wert.

25

Stunden Gesamtaufwand

Geringer Zeitaufwand (ca. 25 Std.) dank Vorlagen.

90%

Abdeckung von Fragebögen

Deckt ca. 90% typischer Sicherheitsfragebögen ab.

Ihr Ziel:

Sicherheit sichtbar und nachweisbar machen,
ohne Zertifizierungskomplexität:
90 Tage fokussierte Implementierung anstelle von 9 Monaten Frustration.

Vorteile des pragmatischen Sicherheitsansatzes

Wer auf diese Vorteile verzichtet, läuft Gefahr, im Wettbewerb zurückzufallen. Während Ihre Konkurrenz Vertrauen aufbaut, schnell auf Anfragen reagiert und Versicherungskosten senkt, kämpfen Sie noch mit verstreuten Dokumenten und verpassten Chancen.

Operative Vorteile

Beschleunigte Implementierung

Nachweisbare Sicherheit in 90 Tagen statt 9-12 Monaten. Schliesst Sicherheitslücken schneller und beschleunigt die Reife.

Kosteneffizienz

Robuste Sicherheit mit minimalen Beratungs- und Zertifizierungskosten (bis zu 70 % Einsparung). Konzentriert Ressourcen auf wirkungsvolle Verbesserungen.

Praktischer Fokus

Ressourcen auf Massnahmen konzentrieren, die reale Risiken (menschliches Versagen, Phishing) direkt mindern, statt abstrakte Compliance-Anforderungen zu erfüllen.

Geschäftliche Vorteile

Verbessertes Kundenvertrauen

Selbstbewusste Reaktion auf Sicherheitsfragebögen durch vorbereitete Dokumentation und Whitepaper. Schafft Vertrauen bei sicherheitsbewussten Kunden.

Verbesserte Cyberversicherungs-Position

Umfassende Sicherheitsprüfung durch dokumentierte Kontrollen nachweisen. Kann zu 10-20 % Prämienreduktion oder erhöhter Deckung führen.

Greifbarer Wettbewerbsvorteil

Differenzierung durch gut dokumentierte, agile Sicherheitspraktiken als Verkaufsargument, besonders in regulierten Branchen.

Mit oder ohne Unterstützung – der Unterschied, der entscheidet

Ohne Unterstützung laufen viele Unternehmen in dieselben Fallen.
Mit meiner Begleitung gehen Sie den direkten Weg zu auditfähiger Sicherheit.

ALTER WEG	PLANSEC-METHODE
Dokumente from scratch	55+ auditbewährte Vorlagen – sofort einsatzbereit
ISO als Nebenjob des IT-Admins	Geführter Prozess mit Coach & klaren Rollen
Vage Timeline, viele Meetings	90-Tage-Fahrplan mit wöchentlichen Fo[illegible]nritten
Berater-Taxameter ohne Endkontrolle	Fixpreis & Ergebnisverantwortung inklusive
Prüfer kommt, wenn du „hoffst, bereit zu sein“	Generalprobe vor Stage-2 – Null Überraschungen
Keine Garantie – hohes Auditrisiko	**Bestehensgarantie** – sonst übernehmen wir die Kosten

Buchen Sie jetzt Ihren Termin –
und nehmen Sie die Abkürzung zu auditfähiger Sicherheit.

KOSTENLOSE ISO 27001 BERATUNG

Fallstudie: Mittelständisches Softwareunternehmen (50 Mitarbeiter)

Vor der Einführung	Nach 90-tägiger Implementierung
Monatlich 5-10 komplexe Sicherheitsfragebögen, die 20-30 Stunden Bearbeitungszeit erforderten und den Umsatz verzögerten.	Konsolidierte Dokumentation verkürzt Antwortzeit auf unter 3 Stunden pro Fragebogen.
Keine optimierte Kundenansprache, lange Verkaufszyklen.	Verkaufszyklus für sicherheitsbewusste Kunden verkürzt sich um 25-30 %.
Hohe Prämien für Cyberversicherungen ohne Dokumentation.	7-Mio.-€-Police genehmigt, 15 % Prämienreduzierung (ca. 7.500 € Ersparnis / Jahr).

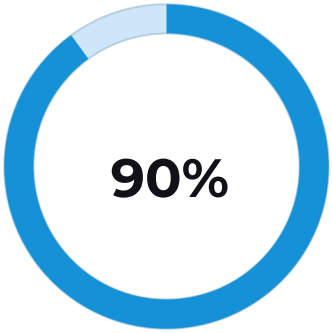
> Struktur und Klarheit statt Tool-Überlastung: Dieser Ansatz priorisiert Substanz, um echte Sicherheitsverbesserungen und Nachweisbarkeit zu erzielen.

Der pragmatische Ansatz bietet Vorteile formeller Sicherheitsprogramme ohne übergrossen Aufwand. Er führt zu greifbaren Sicherheitsverbesserungen und entscheidender Nachweisbarkeit. Für die meisten Unternehmen die optimale Kapitalrendite für Sicherheitsinvestitionen und eine schnelle, robuste Grundlage.

Ihre nächsten Schritte

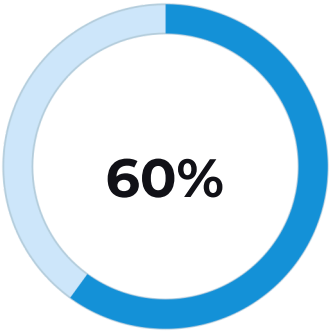
Jeder Monat ohne klare Struktur kostet bares Geld – und Sie merken es oft erst, wenn der Auftrag schon verloren ist. Starten Sie jetzt, bevor der nächste Kundenfragebogen Sie in den roten Bereich bringt.

Ihre Vorteile im Überblick



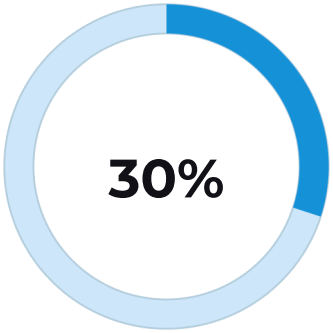
Steigerung der Kundenzufriedenheit

Kunden fordern nachweisbare Sicherheit. Machen Sie Ihre Dokumentation zum Wettbewerbsvorteil.



Reduzierung des Fragebogenaufwands

Standardisierte Dokumentation senkt den Aufwand für Sicherheitsfragebögen um bis zu 60%.



Beschleunigter Verkaufszyklus

Proaktive Sicherheit verkürzt den Verkaufszyklus um 30%.

Starten Sie jetzt Ihre 90-Tage-Implementierung

1	**Dedizierte Sicherheitsstunde planen** Eine Stunde pro Woche für die Roadmap.
2	**Verantwortung zuweisen** Hauptansprechpartner (Massnahme 1) formell festlegen.
3	**Dokumentenstruktur einrichten** Leicht zugängliche Ordnerstruktur (Massnahme 3) erstellen.
4	**Risikobewertung durchführen** Kritische Risiken identifizieren (Massnahme 2).
5	**Asset-Bestandsaufnahme starten** Kritische Tech-Assets listen (Massnahme 2).
6	**Grundlegende Sicherheitsrichtlinie entwerfen** Kurze Richtlinie (Datenschutz, Verantwortlichkeiten) entwerfen.

Expertenunterstützung:

Jetzt **kostenlose** ISO 27001-Beratung vereinbaren!

https://calendly.com/plansec/iso27001-beratung?month=2025-07

Bonus: Die 6 Prinzipien nachhaltiger Sicherheit

Einfachheit vor Komplexität

Setzen Sie auf einfache, wartungsfähige Massnahmen zur Risikominderung, statt komplexer Rahmenwerke.

Praxisnahe Dokumentation zählt

Praxisnahe Dokumentation zählt Ohne formelle Dokumentation sind Sicherheitspraktiken nicht nachweisbar. Setzen Sie auf präzise, umsetzbare Aufzeichnungen.

Konsistenz schafft Vertrauen

Sorgen Sie für Übereinstimmung von Richtlinien, Verfahren und Betriebspraktiken, um Vertrauen aufzubauen.

Fortschritt vor Perfektion

Verfolgen Sie einen iterativen Ansatz: Beginnen Sie grundlegend und erweitern Sie kontinuierlich. Vermeiden Sie Stillstand durch Perfektionismus.

Nachhaltigkeit sichert Erfolg

Nachhaltigkeit sichert Erfolg Gestalten Sie Ihr Sicherheitsprogramm wartungsfähig und anpassungsfähig, um es nahtlos in den Alltag zu integrieren.

Sie können versuchen, diese Punkte allein umzusetzen – riskieren aber Wochen an Mehraufwand und teure Fehler. Mit meiner geführten 90-Tage-Umsetzung gewinnen Sie sofort Klarheit, Tempo und Sicherheit.

Starten Sie jetzt Ihre Umsetzung – mit einer kostenlosen Beratung vom Experten!

ADRESSE
PlanSec AG, Sinserstrasse 67, CH-6330 Cham

EMAIL ADRESSE
dieter.huber@plansec.ch

TELEFON
+41 41 784 2110