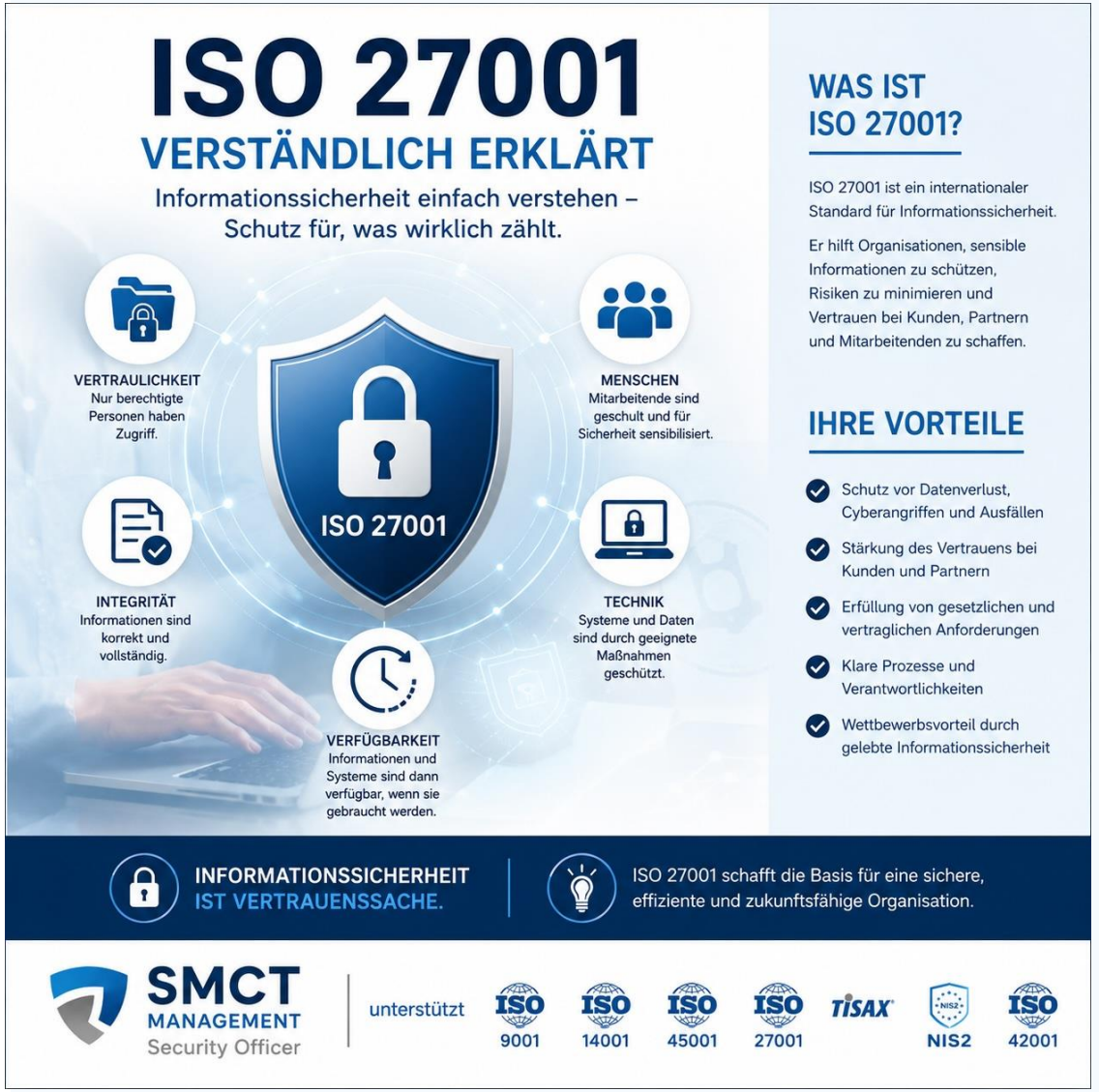
ISO 27001

Verständlich erklärt

Für Menschen ohne Normen- und IT-Sicherheitsvorkenntnisse. Ziel ist ein klares Verständnis: Was wird geschützt? Wie werden Risiken bewertet? Welche Nachweise braucht das Audit?

ISMS | Risiken steuern | Nachweise liefern | Auditfähig werden

SMCT MANAGEMENT unterstützt ISO 9001 · ISO 14001 · ISO 45001 · ISO 27001 · TISAX® · NIS2 · ISO 42001



Was diese Präsentation leistet

ISO 27001 ohne Fachchinesisch: verständlich, praxisnah und mit Blick auf das Audit.

1. Orientierung geben

- ISO 27001 wird häufig als reine IT-Norm missverstanden.
- Die Präsentation zeigt, dass es um Management, Verantwortung, Risiken und Nachweise geht.
- Der Einstieg wird in einfachen Begriffen und mit konkreten Beispielen erklärt.

2. Auditlogik erklären

- Auditoren suchen nicht nur Dokumente, sondern gelebte Umsetzung.
- Kundinnen und Kunden verstehen, warum Scope, Assets, Risiken und SoA zusammengehören.
- Das vermeidet reinen Papieraufwand ohne Nutzen.

3. Nächste Schritte ableiten

- Welche Informationen werden benötigt?
- Welche Personen müssen beteiligt werden?
- Welche Nachweise sind vor dem Zertifizierungsaudit aufzubauen?
- Welche Unterstützung kann SMCT MANAGEMENT leisten?

Merksatz: ISO 27001 wird leichter verständlich, wenn man es als systematischen Schutz wichtiger Unternehmensinformationen betrachtet.

Was ist ISO 27001 eigentlich?

Eine Norm für ein Informationssicherheits-Managementsystem – kein einzelnes IT-Tool und keine reine Checkliste.

Einfach gesagt

ISO 27001 hilft, wichtige Informationen systematisch zu schützen: mit klaren Regeln, Verantwortlichkeiten, Maßnahmen, Nachweisen und regelmäßiger Verbesserung.

Managementsystem

- legt Verantwortlichkeiten fest
- steuert Risiken und Maßnahmen
- ordert regelmäßige Prüfung und Verbesserung

Auditfähig

- Nachweise zeigen Umsetzung
- Interviews prüfen das Verständnis
- Abweichungen werden behandelt

Nicht nur Technik

- auch Menschen, Prozesse und Dienstleister zählen
- Dokumentation muss zur Praxis passen
- Leitung und Fachbereiche sind beteiligt

Drei Leitfragen

- Was kann schiefgehen?
- Wie verhindern oder begrenzen wir das?
- Wie belegen wir, dass es funktioniert?

Warum ist ISO 27001 für Unternehmen wichtig?

Informationssicherheit schützt Vertrauen, Lieferfähigkeit, Kundenbeziehungen und die Handlungsfähigkeit der Organisation.

Kunden & Ausschreibungen

- Kunden fragen nach Nachweisen zur Informationssicherheit.
- Sicherheitsanforderungen werden zunehmend Teil von Verträgen und Lieferantenbewertungen.
- Ein ISMS zeigt, dass Schutzmaßnahmen systematisch gesteuert werden.

Cyberrisiken & Ausfälle

- Ransomware, Phishing und Fehlkonfigurationen können Prozesse stoppen.
- Backups, Wiederanlaufpläne und klare Meldewege senken die Auswirkungen.
- ISO 27001 macht Risiken transparent und behandelbar.

Regulatorik & Compliance

- Datenschutz, NIS2 und Branchenanforderungen erhöhen den Nachweisdruck.
- ISO 27001 schafft eine nachvollziehbare Struktur für Sicherheitsmaßnahmen.
- Die Norm hilft, Pflichten geordnet zu steuern.

Führung & Steuerung

- Informationssicherheit wird zur Managementaufgabe.
- Die Geschäftsführung entscheidet über Ziele, Ressourcen und Restrisiken.
- Ein ISMS verhindert ungeplanten Aktionismus.

Laienbild: ISO 27001 ist der Sicherheitsgurt für wichtige Unternehmensinformationen – nicht sichtbar im Alltag, aber entscheidend, wenn etwas passiert.

Das ISMS einfach erklärt: Planen · Umsetzen · Prüfen · Verbessern

ISO 27001 folgt einem bewährten Kreislauf, damit Sicherheit nicht einmalig bleibt.

1 PLAN

Risiken erkennen
Ziele und Scope festlegen
Maßnahmen planen

2 DO

Richtlinien einführen
Maßnahmen umsetzen
Mitarbeitende schulen

ISMS

4 ACT

Abweichungen behandeln
Verbesserungen steuern
Ressourcen anpassen

3 CHECK

Audits durchführen
Nachweise prüfen
Kennzahlen bewerten

Wichtig: Ein ISMS ist kein Ordner für das Audit, sondern ein laufender Steuerungs- und Verbesserungsprozess.

Was wird geschützt?

Nicht nur Computer: ISO 27001 betrachtet Informationen, Systeme, Prozesse, Menschen und Dienstleister.

Informationen

- Kunden-, Vertrags-, Finanz-, Personal- und Projektdaten
- Know-how, Kalkulationen, Entwicklungsdaten, Angebote

Systeme

- Server, Cloud, Endgeräte, Anwendungen, Netzwerke
- Backups, Datenbanken, Schnittstellen, Monitoring

Prozesse

- Angebot, Auftrag, Support, Entwicklung, Betrieb
- Beschaffung, Lieferantensteuerung, Incident Management

Menschen

- Mitarbeitende, Führung, Administratoren
- Dienstleister, Prozessverantwortliche , externe Partner

Nachweise

- Protokolle, Schulungen, Audits, Management Review
- Prüfungen, Freigaben, Maßnahmenverfolgung

Merksatz: Erst wenn man weiß, was wichtig ist, kann man es sinnvoll schützen und später im Audit nachvollziehbar erklären.

Der Einstieg: 7 Schritte zum wirksamen ISMS

Ein praxistauglicher Ablauf verhindert Aktionismus und schafft Auditfähigkeit.

1

Ziel & Scope

Was soll geschützt und zertifiziert werden?

2

Rollen

Wer entscheidet, liefert Informationen und setzt Maßnahmen um?

3

Assets

Welche Werte, Systeme, Daten und Prozesse sind relevant?

4

Risiken

Was kann passieren und wie hoch ist das Risiko?

5

SoA

Welche Controls sind anwendbar und warum?

6

Richtlinien

Welche Regeln und Prozesse gelten verbindlich?

7

Nachweise

Was wurde umgesetzt und wie ist es belegbar?

Merksatz: ISO 27001 beginnt mit Managementlogik – nicht mit einer Checkliste. Die Checkliste ist erst stark, wenn Scope, Risiken und Verantwortlichkeiten geklärt sind.

Schritt 1: Ziel, Scope und Verantwortlichkeiten

Der Scope entscheidet über Aufwand, Auditumfang und spätere Nachweisführung.

Scope sauber festlegen

- Standorte, Dienstleistungen und Prozesse abgrenzen.
- Kritische Informationen, Systeme und Dienstleister aufnehmen.
- Zu enger Scope wirkt im Audit schnell konstruiert; zu großer Scope erhöht Aufwand.

Rollen verbindlich klären

- Geschäftsführung bleibt verantwortlich.
- ISB/ISMS-Verantwortliche koordinieren das System.
- IT und Fachbereiche liefern Nachweise und setzen Maßnahmen um.

Entscheidungen dokumentieren

- Ziele, Verantwortlichkeiten und Freigaben schriftlich festhalten.
- Ressourcen, Termine und Projektstruktur definieren.
- Kommunikation an die Mitarbeitenden planen.

Typische Scope-Fragen

- Welche Leistungen sind für Kunden oder Zertifizierung relevant?
- Welche Standorte, Teams und Anwendungen gehören wirklich zum ISMS?
- Welche Daten, Verträge, Cloud-Dienste und Dienstleister tragen hohen Schutzbedarf?
- Welche Schnittstellen dürfen nicht vergessen werden?

Bewährt: Verantwortlichkeiten schriftlich festlegen, bevor operative Maßnahmen starten.

Schritt 2: Assets erfassen und Schutzbedarf verstehen

Ohne Asset Inventar bleibt die Risikoanalyse theoretisch.

Asset Inventar

Das Asset Inventar ist die strukturierte Übersicht über Informationen, Systeme, Prozesse, Standorte, Dienstleister und Verantwortliche.

Was gehört hinein?

- Informationswerte und Datenarten
- Anwendungen, Server, Cloud und Endgeräte
- Netzwerke, Schnittstellen und Backups
- Geschäftsprozesse und Lieferanten

Verantwortung

- Jedes Asset braucht eine verantwortliche Rolle.
- Fachbereiche kennen Bedeutung und Schutzbedarf oft besser als die IT.
- Die IT bewertet technische Abhängigkeiten.

Schutzbedarf bewerten

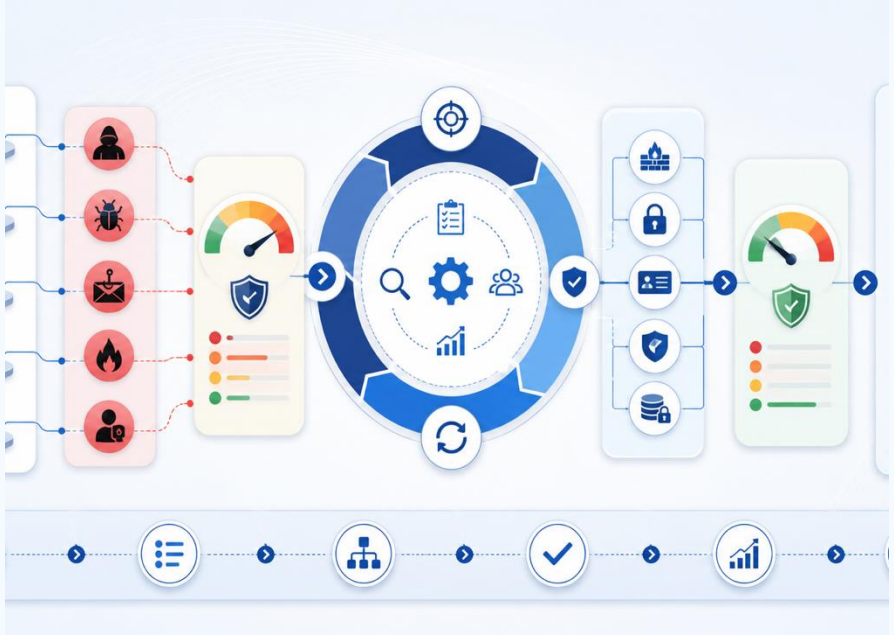
- Vertraulichkeit: Wer darf es sehen?
- Integrität: Wie wichtig ist Korrektheit?
- Verfügbarkeit: Wie kritisch ist Ausfallzeit?
- Bewertung je Asset oder Asset-Gruppe

Auditnutzen

- Assets verbinden Risiken, Controls, Maßnahmen und Nachweise.
- Auditoren können die Logik des ISMS nachvollziehen.
- Lücken werden schneller sichtbar.

Schritt 3: Risikoanalyse ohne Fachchinesisch

Ein Risiko ist: Was könnte passieren – und wie schlimm wäre es für das Unternehmen?



1. Bedrohung

Was kann passieren? Beispiele: Phishing, Ransomware, Ausfall eines Cloud-Dienstes, Verlust eines Laptops oder Fehler bei Berechtigungen.

2. Schwachstelle

Warum kann es passieren? Beispiele: kein MFA, veraltete Software, fehlende Backup-Tests, unklare Zuständigkeiten oder fehlende Schulung.

3. Auswirkung

Was wäre die Folge? Beispiele: Datenverlust, Stillstand, Vertragsverletzung, Reputationsschaden, Bußgeldrisiko oder Lieferverzug.

4. Behandlung

Was tun wir dagegen? Risiken werden gemindert, vermieden, übertragen oder bewusst akzeptiert – mit klarer Begründung.

Formel im Alltag

Risiko = Eintrittswahrscheinlichkeit × Schadensausmaß. Ziel ist nicht, Risiken schönzurechnen, sondern sie transparent und behandelbar zu machen.

Auditfrage

Kann das Unternehmen nachvollziehbar erklären, warum ein Risiko bewertet wurde, welche Maßnahme gewählt wurde, wer verantwortlich ist und wie das Restrisiko akzeptiert wurde?

93 Controls: Werkzeugkasten statt Pflichtliste

Die Controls aus Anhang A sind Sicherheitsmaßnahmen. Sie werden risikobasiert bewertet und in der SoA begründet.

Controls

- Zugriffskontrolle und Identitäten
- Backup und Wiederherstellung
- Logging und Überwachung
- Lieferantenmanagement
- Incident Management
- Awareness und Schulung

SoA

- Ist das Control anwendbar?
- Warum ist es anwendbar oder nicht anwendbar?
- Wie wird es umgesetzt?
- Welche Risiken stehen dahinter?
- Welche Nachweise belegen die Umsetzung?

Audit

- Auditoren prüfen die Plausibilität der SoA.
- Nicht anwendbare Controls brauchen eine belastbare Begründung.
- Anwendbare Controls müssen in der Praxis erkennbar umgesetzt sein.
- Kontrollen werden durch Interviews, Dokumente und Nachweise geprüft.

Für Laien: Die SoA ist die begründete Entscheidungsliste für die 93 Controls – nicht einfach eine Ja/Nein-Tabelle.

Welche Dokumente braucht man?

Dokumentation ist kein Selbstzweck. Sie zeigt, was geregelt, umgesetzt und geprüft wurde.

Scope
Was gehört zum ISMS und was nicht?

Asset Inventar
Welche Informationen, Systeme und Prozesse sind wichtig?

Risikoanalyse
Welche Risiken bestehen und wie werden sie bewertet?

Risikobehandlung
Welche Maßnahmen werden umgesetzt und wer ist verantwortlich?

SoA
Welche Controls gelten und wie sind sie begründet?

Richtlinien
Welche Regeln gelten verbindlich im Unternehmen?

Internes Audit
Wurde das ISMS unabhängig geprüft?

Managementbewertung
Hat die Leitung Eignung und Wirksamkeit bewertet?

Die beste Dokumentation ist so einfach wie möglich – aber so vollständig, dass ein Auditor den Ablauf nachvollziehen kann.

Vom Start bis zur Zertifizierung

Eine realistische Reihenfolge hilft, Aufwand und Erwartungen zu steuern.

1

Bestandsaufnahme

Welche Regelungen, Nachweise, Systeme und Prozesse sind bereits vorhanden?

2

ISMS aufbauen

Scope, Assets, Risiken, SoA, Richtlinien und Maßnahmenplan strukturieren.

3

Umsetzen

Maßnahmen real einführen, Mitarbeitende informieren und Nachweise sammeln.

4

Intern prüfen

Internes Audit durchführen, Abweichungen bearbeiten und Managementbewertung erstellen.

5

Zertifizieren

Stage 1 prüft die Dokumentationsreife, Stage 2 prüft die Umsetzung im Alltag.

Stage 1

Dokumentenprüfung: Passt die Grundlage des ISMS? Sind Scope, Risiken, SoA und Auditprogramm plausibel?

Stage 2

Umsetzungsprüfung: Wird das ISMS im Alltag gelebt? Gibt es Nachweise und funktioniert die Steuerung?

Was prüft der Auditor?

Nicht nur, ob Dokumente vorhanden sind – sondern ob das System funktioniert.

Dokumente

Scope und Kontext
Risikoanalyse und Risikobehandlung
SoA und Richtlinien
interne Auditberichte
Managementbewertung
Maßnahmenverfolgung

Interviews

- Geschäftsführung zu Verantwortung und Ressourcen
- ISB/IT zu Risiken und Maßnahmen
- Prozessverantwortliche zu Abläufen
- Mitarbeitende zu Awareness und Meldewegen
- Dienstleister, sofern relevant

Nachweise

- Schulungen und Teilnehmerlisten
- Berechtigungsreviews
- Backup-Tests und Wiederherstellungen
- Patch- und Schwachstellenmanagement
- Vorfälle und Lessons Learned
- Verträge und Lieferantenbewertungen

Kernfrage des Auditors: Ist es geregelt? Ist es umgesetzt? Gibt es Nachweise? Wird regelmäßig verbessert?

Typische Fehler – und wie man sie vermeidet

Ein pragmatischer, sauberer Start ist meist besser als ein perfekter Papierstart.

Typische Fehler

- Scope ist zu groß, zu eng oder unklar abgegrenzt.
- Asset Inventar enthält nur IT-Geräte, aber keine Informationen, Prozesse oder Dienstleister.
- Risikoanalyse ist formal, aber nicht mit der Praxis verbunden.
- SoA enthält Ja/Nein-Angaben ohne nachvollziehbare Begründung.
- Richtlinien werden erstellt, aber nicht kommuniziert oder gelebt.
- Nachweise fehlen, obwohl Maßnahmen angeblich umgesetzt wurden.

Besser machen

- Klein, aber sauber starten: erst Scope, dann Assets, dann Risiken.
- Vorhandene Maßnahmen nutzen und nur echte Lücken schließen.
- Fachbereiche einbinden, weil sie Schutzbedarf und Auswirkungen kennen.
- Nachweise direkt beim Umsetzen mitdenken.
- Internes Audit früh planen, nicht erst kurz vor der Zertifizierung.
- Alle Entscheidungen dokumentieren und regelmäßig überprüfen.

Leitsatz: ISO 27001 muss zur Organisation passen. Ein schlankes, gelebtes ISMS ist stärker als ein großer, ungenutzter Dokumentensatz.

90-Tage-Startplan für ISO 27001

Ein realistischer Einstieg bringt Struktur, ohne das Unternehmen zu überfordern.

Tage 1–15	**Scope & Rollen** Zielbild, Geltungsbereich, Projektteam, Verantwortlichkeiten
Tage 16–35	**Assets & Schutzbedarf** Asset Inventar, Verantwortliche, CIA-Bewertung, Dienstleister
Tage 36–60	**Risiken & SoA** Risikoanalyse, Risikobehandlung, Controls und Begründungen
Tage 61–80	**Richtlinien & Umsetzung** Leitlinie, Kernrichtlinien, Maßnahmen, Schulungen, Nachweise
Tage 81–90	**Auditvorbereitung** Internes Audit, Managementbewertung, Maßnahmenplan, Zertifizierungsreife

Für die Zertifizierung zählt nicht Geschwindigkeit allein. Entscheidend ist, dass das ISMS konsistent, nachvollziehbar und im Alltag anwendbar ist.

Wie SMCT MANAGEMENT unterstützt

Strukturierte Begleitung vom Einstieg bis zur Zertifizierungsvorbereitung.

1. Orientierung & Scope

- Erstgespräch und Zielklärung
- Geltungsbereich abgrenzen
- Rollen und Projektstruktur festlegen

2. Dokumentation

- Asset Inventar & Schutzziele
- Risikoanalyse und Behandlung
- SoA, Richtlinien und Nachweise

3. Umsetzung unterstützen

- Maßnahmenplan priorisieren
- Verantwortliche einbinden
- Nachweise auditfähig strukturieren

4. Internes Audit

- Auditprogramm und Checklisten
- Auditbericht und Abweichungen
- Maßnahmenverfolgung

5. Managementbewertung

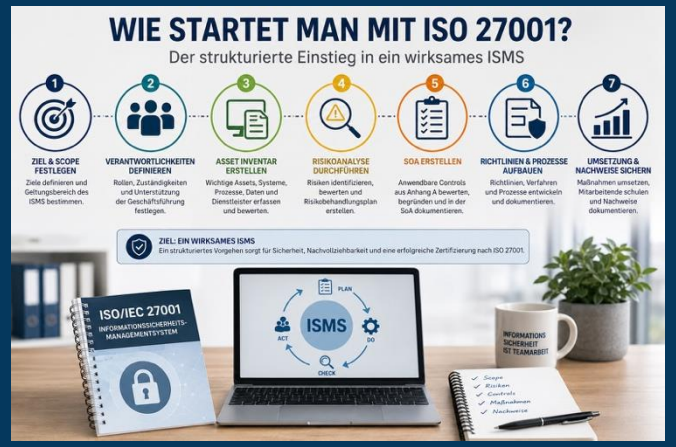
- Inputdaten vorbereiten
- Bewertung der Wirksamkeit
- Entscheidungen dokumentieren

6. Auditvorbereitung

- Stage 1 und Stage 2 vorbereiten
- Nachweise sortieren
- Interviewfähigkeit stärken

ISO 27001 verständlich, strukturiert und auditfähig starten

Der richtige Einstieg verbindet Scope, Assets, Risiken, SoA, Richtlinien und Nachweise. Dadurch entsteht kein Papier-ISMS, sondern ein nachvollziehbares Managementsystem, das Informationssicherheit dauerhaft verbessert.



Nächster Schritt

- Scope-Workshop und Bestandsaufnahme durchführen
- Asset Inventar und Schutzbedarf strukturiert aufbauen
- Risikoanalyse, SoA und Maßnahmenplan erstellen
- Auditfähigkeit mit internem Audit und Managementbewertung prüfen

Kontakt: info@smct-management.de