Telconis – Benutzerhandbuch

Die ISMS-Plattform für ISO 27001, NIS2 / NISG 2026, Cyber Trust Austria und Business Continuity Management

Version 1.0 · Stand: Juli 2026

Inhaltsverzeichnis

---

1. Willkommen bei Telconis

Telconis ist eine cloudbasierte Compliance-Plattform. Sie bauen darin Ihr Informationssicherheits-Managementsystem (ISMS) auf, dokumentieren es und behalten den Überblick, ohne zwischen Excel-Tabellen, Word-Dokumenten und mehreren Einzeltools hin- und herzuspringen. Asset-Inventar,

Maßnahmen und Berichte teilen sich alle Module gemeinsam.

Für wen ist Telconis gedacht?

Telconis richtet sich an österreichische und europäische Unternehmen, die

- eine ISO-27001-Zertifizierung vorbereiten oder aufrechterhalten wollen,
- ihre NIS2- bzw. NISG-2026-Pflichten strukturiert erfüllen müssen,
- das Cyber-Trust-Austria-Gütesiegel anstreben,
- oder ihre Betriebskontinuität (BCM) planen und testen.

In den meisten Unternehmen arbeiten zwei Arten von Nutzern mit der Plattform: Administratoren, die Firmenprofil und Benutzerverwaltung im Blick haben, und Benutzer, die inhaltlich an den Compliance-Daten arbeiten. Was genau den Unterschied ausmacht, steht in Kapitel 8.

Die sechs Module im Überblick

Modul	Wofür	Farbe im Menü
ISO 27001	Statement of Applicability (93 Controls), Maßnahmen, Projektplan	Hellblau
NIS2 / NISG 2026	Betroffenheitsprüfung, § 32-Maßnahmen (a–j), Risiko, Lieferkette	Orange
BCM	Business Impact Analyse, Continuity-Pläne, Tests, SPOF-Analyse	Grün
Cyber Trust Austria	Selbstbewertung (B/A/G/P), Assessments, Label-Status	Dunkelblau
Risikomanagement	Asset-Inventar (CIA), Risikoregister, Behandlungspläne	Rot
Personal	Personalverzeichnis, ISMS-Rollen, rollenbasierte Sichtbarkeit	–

Dazu kommen ein KI-Assistent, ein zentraler Dokumentenbereich (Upload, 18 Vorlagen, 8 PDF-Berichte) und die Einstellungen.

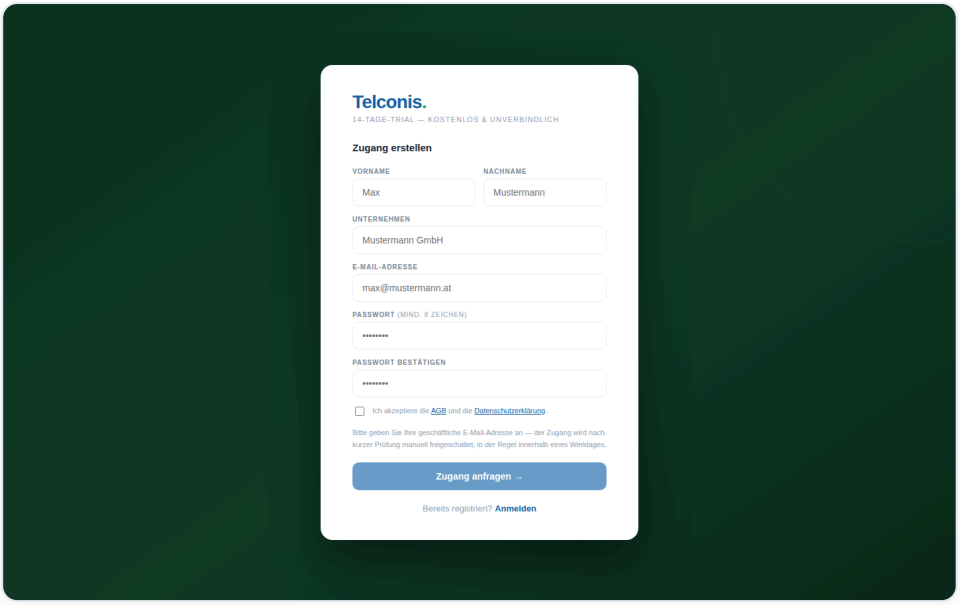
Ein Punkt vorab, der uns wichtig ist: Telconis strukturiert, dokumentiert und verfolgt Ihre Compliance-Maßnahmen – es ersetzt keine Rechtsberatung, ist keine Zertifizierungsstelle und führt kein externes Audit durch. Die Nutzung der Plattform garantiert also weder eine erfolgreiche Zertifizierung noch NIS2-Konformität noch den Ausschluss behördlicher Sanktionen. Für die inhaltliche Richtigkeit Ihrer Daten und die rechtliche Bewertung Ihrer eigenen Betroffenheit sind Sie selbst verantwortlich (siehe § 2 der AGB).

---

2. Erste Schritte

2.1 Trial-Registrierung

Telconis lässt sich 14 Tage kostenlos und unverbindlich testen, ohne Kreditkarte und ohne Zahlungsdaten. Rufen Sie dazu die Registrierungsseite auf und füllen Sie das Formular aus.



Registrierungsformular für den 14-Tage-Trial

Gefragt werden Vorname, Nachname, Unternehmen, geschäftliche E-Mail-Adresse und ein Passwort mit mindestens 8 Zeichen. Danach bestätigen Sie AGB und Datenschutzerklärung – ohne dieses Häkchen lässt sich das Formular nicht absenden.

Zwei Dinge lohnt es sich zu wissen, bevor Sie loslegen: Erstens braucht es eine geschäftliche E-Mail-Adresse. Freemail-Adressen wie Gmail, GMX, Web.de oder Outlook werden direkt am Formular abgelehnt, verwenden Sie also die Adresse Ihrer Unternehmensdomain. Zweitens ist die Zustimmung zu AGB und Datenschutz keine Formsache, sondern Voraussetzung für die Anmeldung.

2.2 Die Freischaltungs-Wartezeit

Anders als bei vielen anderen Diensten bekommen Sie nicht sofort Zugang. Nach dem Absenden des Formulars sehen Sie einen Hinweis, dass Ihre Anfrage geprüft wird, und eine Bestätigungs-E-Mail folgt. Der Trial-Zugang wird anschließend manuell freigeschaltet, in der Regel innerhalb eines Werktages. Erst danach können Sie sich anmelden.

Das ist bewusst so gestaltet und dient der Missbrauchsvermeidung. Solange Ihr Zugang noch nicht freigeschaltet ist und Sie sich anzumelden versuchen, sehen Sie die Meldung:

> „Ihr Zugang wird noch geprüft. Wir melden uns per E-Mail, sobald er freigeschaltet ist.“

Sobald die Freischaltung erfolgt ist, informieren wir Sie per E-Mail. Ab diesem Zeitpunkt läuft Ihre 14-tägige Testphase.

2.3 Von der Registrierung zum ersten Login

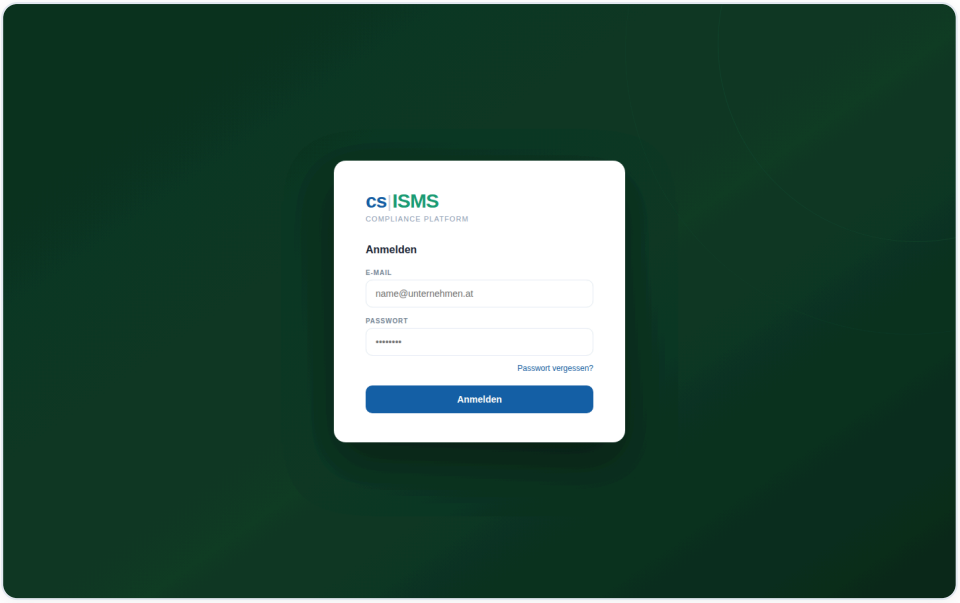
Der Weg von der Anfrage bis zur ersten Anmeldung läuft so ab:

1. Sie füllen das Trial-Formular aus: Vorname, Nachname, Unternehmen, geschäftliche E-Mail-Adresse, Passwort, dazu die Zustimmung zu AGB und Datenschutz.
2. Telconis prüft automatisch, ob die E-Mail-Adresse geschäftlich ist und ob sie bereits registriert wurde. Ist sie bereits vorhanden, bekommen Sie den Hinweis, stattdessen „Passwort vergessen“ zu nutzen.
3. Der Zugang wird angelegt, Status „In Prüfung“. Sie erhalten sofort eine Bestätigungs-E-Mail, intern geht gleichzeitig eine Benachrichtigung an Telconis.
4. Telconis schaltet den Zugang manuell frei, üblicherweise innerhalb eines Werktages (siehe 2.2), und schickt Ihnen eine Freischaltungs-E-Mail.
5. Sie melden sich mit E-Mail-Adresse und Passwort an. Ist 2FA aktiviert, fragt Telconis zusätzlich den sechsstelligen Code aus Ihrer Authenticator-App ab.

6. Sie landen im Dashboard und können loslegen.

2.4 Anmelden (Login)

Nach der Freischaltung melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort an.



Anmeldemaske von Telconis

Passwort vergessen? Ein Klick auf „Passwort vergessen?“ genügt, und Sie erhalten – sofern die Adresse bei uns hinterlegt ist – einen Link zum Zurücksetzen, der eine Stunde gültig ist. Wurden Sie stattdessen von Ihrem Administrator eingeladen, bekommen Sie eine E-Mail mit einem Einmal-Passwort. Beim ersten Login vergeben Sie dann ein neues, sicheres Passwort (mindestens 8 Zeichen, ein Großbuchstabe, eine Zahl) und bestätigen dabei ebenfalls AGB und Datenschutzerklärung.

2.5 Zwei-Faktor-Authentifizierung (2FA) einrichten

Wir empfehlen, die Zwei-Faktor-Authentifizierung zu aktivieren, um Ihr Konto zusätzlich abzusichern. Dafür brauchen Sie eine Authenticator-App auf dem Smartphone, etwa Google Authenticator, Microsoft Authenticator, Authy oder FreeOTP.

So richten Sie sie ein:

1. Öffnen Sie Einstellungen → 2FA (siehe Kapitel 7).
2. Klicken Sie auf „2FA einrichten“ – Telconis zeigt Ihnen einen QR-Code.
3. Scannen Sie ihn mit der Authenticator-App. Ab sofort erzeugt sie alle 30 Sekunden einen sechsstelligen Code.
4. Geben Sie den aktuellen Code zur Bestätigung ein, und 2FA ist aktiv.

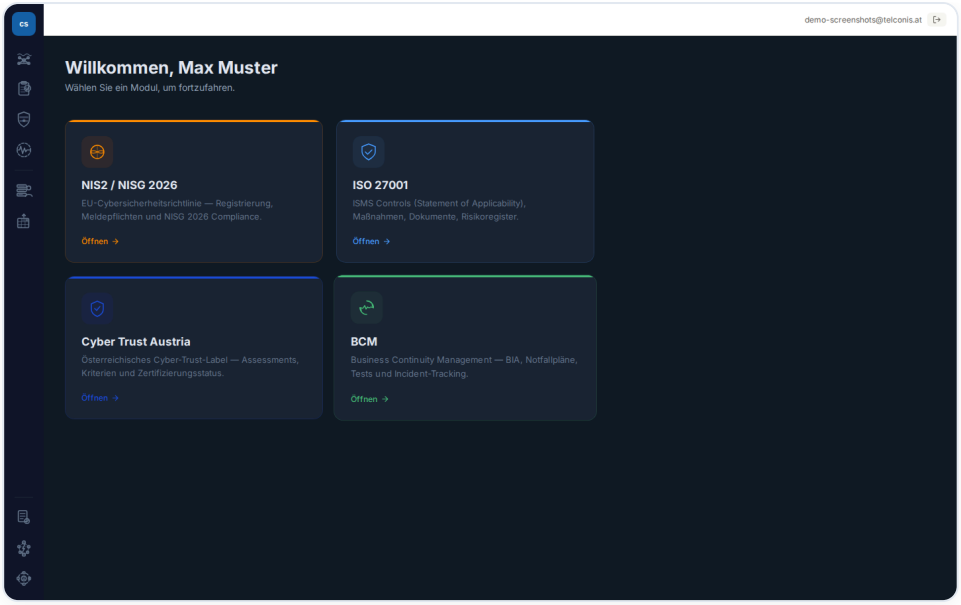
Bei jeder künftigen Anmeldung geben Sie nach E-Mail und Passwort zusätzlich den aktuellen Code aus der App ein. Zum Deaktivieren brauchen Sie Ihr Passwort und einen gültigen Code.

Ein Tipp dazu: Bewahren Sie den Zugriff auf Ihre Authenticator-App sicher auf. Geht das Gerät verloren, hilft Ihnen Ihr Administrator oder unser Support weiter, um wieder Zugang zu bekommen.

---

3. Die Oberfläche verstehen

Die Telconis-Oberfläche gliedert sich in drei Bereiche, die immer sichtbar bleiben und die Navigation einfach halten.



Das Dashboard mit Iconbar, Kontext-Seitenleiste und Übersicht

3.1 Die Iconbar (Modulauswahl)

Ganz links sitzt eine schmale Leiste mit Symbolen, die Iconbar. Über sie wechseln Sie zwischen den Modulen – ISO 27001, NIS2, BCM, Cyber Trust Austria, Risiken, Personal – sowie zu Dokumenten, dem KI-Assistenten und den Einstellungen. Jedes Modul hat seine eigene Farbe, damit Sie sich schnell orientieren können.

3.2 Die Kontext-Seitenleiste (ContextSidebar)

Sobald Sie ein Modul auswählen, erscheint daneben die Kontext-Seitenleiste mit der Unternavigation genau dieses Moduls. Im NIS2-Modul sind das zum Beispiel Betroffenheit, Maßnahmen, Risikobewertung, Lieferkette und Dokumente. Über den Zurück-Button gelangen Sie jederzeit zur Modulübersicht.

3.3 Das Dashboard / die Übersicht

Der zentrale Arbeitsbereich zeigt Ihnen je nach Modul eine Übersicht mit Kennzahlen, Fortschrittsbalken und den wichtigsten Aufgaben. Das Haupt-Dashboard bündelt den Gesamtstatus Ihres ISMS – etwa den Umsetzungsgrad der ISO-Controls oder den NIS2-Readiness-Score – und ist der Einstiegspunkt für Ihre tägliche Arbeit.

---

4. Die Module im Detail

Die Reihenfolge in diesem Kapitel folgt der empfohlenen Vorgehensweise. Sie müssen aber nicht alles auf einmal erledigen – Telconis speichert Ihren Fortschritt fortlaufend, Sie können jederzeit unterbrechen und später weitermachen.

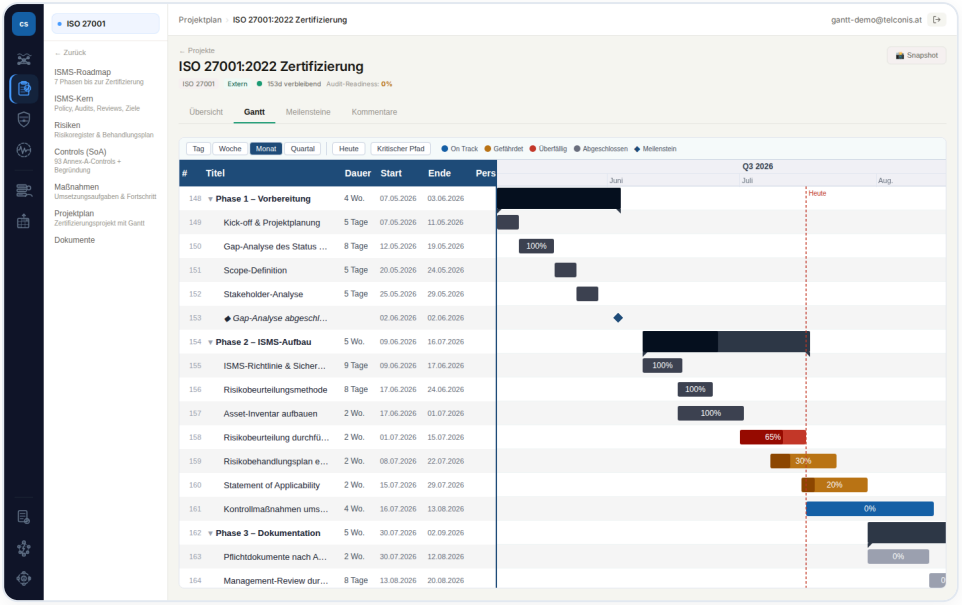
4.1 ISO 27001

Das ISO-27001-Modul bildet den Kern eines ISMS ab: das Statement of Applicability (SoA) mit allen 93 Controls aus Annex A der ISO 27001:2022, den Maßnahmen-Tracker und den Projektplan mit Gantt-Ansicht.

Beim Ausfüllen des SoA öffnen Sie zunächst das Modul und wechseln zu den Controls. Klicken Sie ein Control an, sehen Sie den Anforderungstext direkt hinterlegt – die Norm müssen Sie nicht separat nachschlagen. Setzen Sie den Status (umgesetzt, teilweise umgesetzt, nicht umgesetzt oder nicht anwendbar) und tragen Sie bei „nicht anwendbar“ eine Begründung ein, das ist für ein prüfsicheres SoA Pflicht. Dazu kommen Verantwortlichkeit und bei Bedarf eine Notiz, und Sie können Nachweise hochladen oder vorhandene Dokumente verknüpfen, die die Umsetzung belegen.

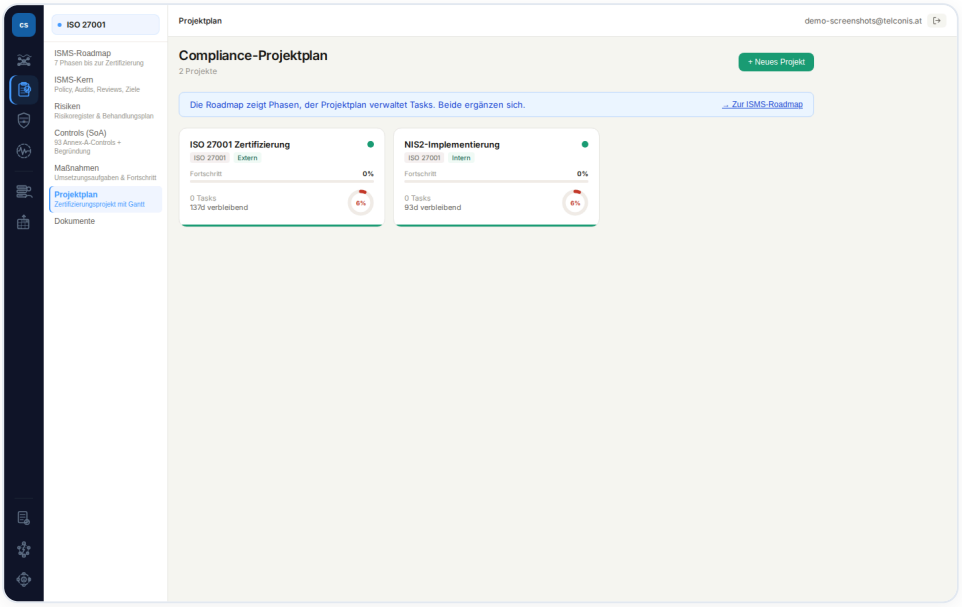
Im Control-Detail sehen Sie außerdem Framework-Mapping-Badges: Sie zeigen, welchem NIST-CSF-2.0-, NIS2-, Cyber-Trust-Austria- oder ISO-22301-Punkt das jeweilige Control entspricht. So arbeiten Sie ein Control einmal aus und sehen sofort, wo es in anderen Rahmenwerken ebenfalls zählt.

Ergänzend zum SoA erfassen Sie im Maßnahmen-Tracker konkrete Verbesserungsmaßnahmen mit Verantwortlichem, Fälligkeit und Status, damit klar bleibt, welche Aufgaben zur Schließung von Lücken noch offen sind.



Projektplan als Gantt-Diagramm

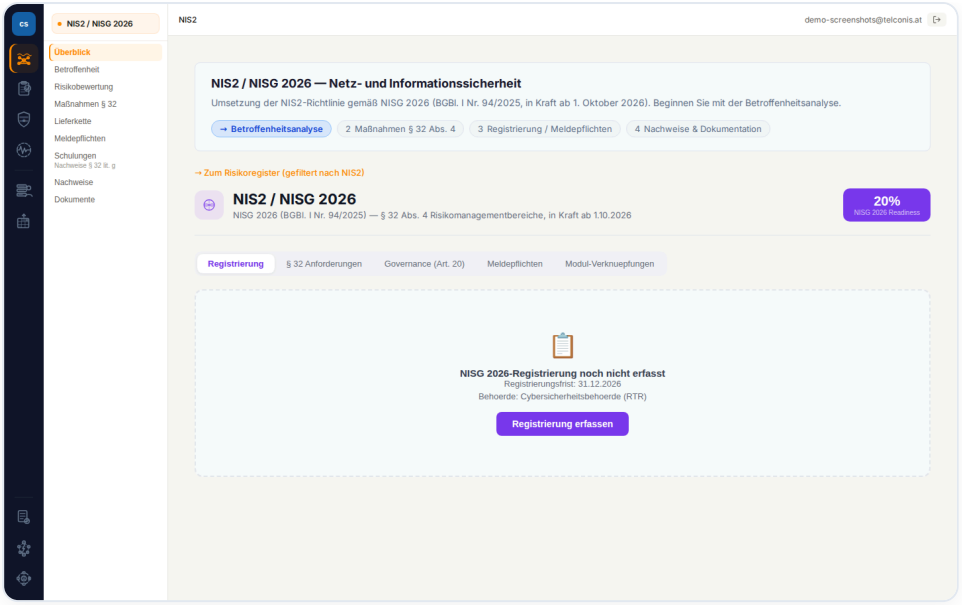
Im Projektplan planen Sie Ihre ISMS-Einführung als Projekt mit Aufgaben, Terminen und Abhängigkeiten. Die Gantt-Ansicht stellt den Zeitverlauf grafisch dar und hilft, Meilensteine wie den Zertifizierungstermin realistisch zu planen.



Projektübersicht

4.2 NIS2 / NISG 2026

Das NIS2-Modul begleitet Sie von der Frage „Sind wir überhaupt betroffen?“ bis zur laufenden Erfüllung der gesetzlichen Pflichten nach dem NISG 2026.



NIS2-Modul mit Maßnahmen und Readiness-Verlauf

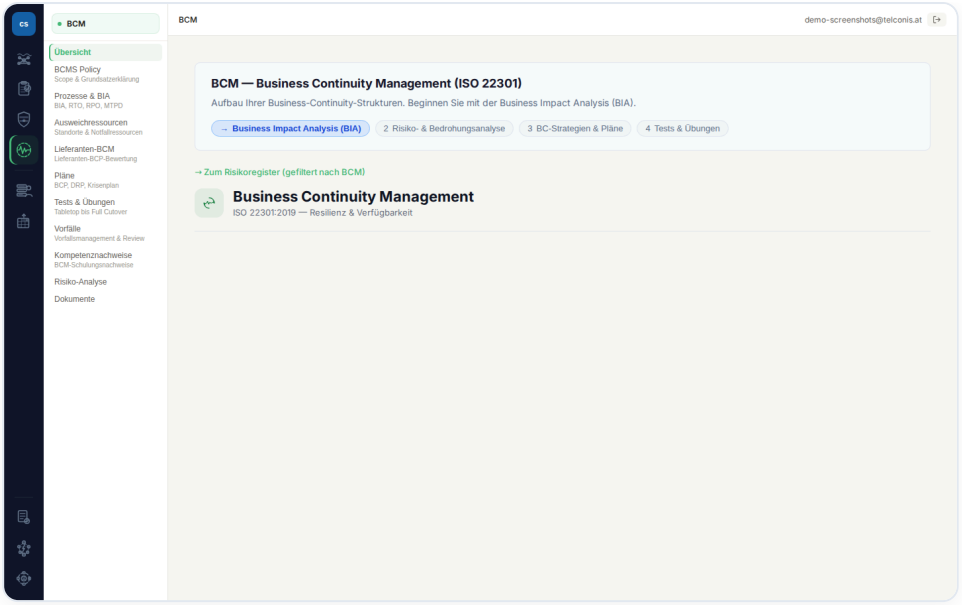
Starten Sie mit der Betroffenheitsprüfung: Sie beantworten Fragen zu Sektor, Unternehmensgröße und Tätigkeit, und das Ergebnis zeigt eine Einschätzung, ob und als welche Kategorie – wesentliche oder wichtige Einrichtung – Sie voraussichtlich betroffen sind. Wichtig dabei: Diese Prüfung ist eine Strukturierungshilfe, die rechtsverbindliche Bewertung Ihrer Betroffenheit bleibt Ihre Sache bzw. die Ihrer Rechtsberatung.

Der Maßnahmenkatalog nach § 32 NISG umfasst zehn Bereiche von a bis j – von Risikomanagement über Vorfallbehandlung, Business Continuity und Lieferkettensicherheit bis zu Verschlüsselung und Zugriffskontrolle. Für jede Maßnahme lesen Sie den hinterlegten Anforderungstext, setzen Status, Verantwortlichen und Fälligkeitsdatum, hinterlegen eine Notiz zur Umsetzung und verknüpfen Nachweis-Dokumente. Pro Maßnahmenzeile sehen Sie außerdem, welche ISO-27001-Controls dazu passen – praktisch, wenn Sie parallel eine ISO-Zertifizierung verfolgen.

Daneben deckt das Modul weitere Bereiche ab: die Risikobewertung Ihrer NIS2-relevanten Risiken, die Lieferkette mit kritischen Lieferanten und Dienstleistern, die Meldepflichten samt Prozessen zur fristgerechten Meldung von Sicherheitsvorfällen, sowie Schulungsnachweise für Sensibilisierungs- und Schulungsmaßnahmen. Der Readiness-Verlauf hält Momentaufnahmen Ihres NIS2-Reifegrads fest und zeigt die Entwicklung als Diagramm.

4.3 Business Continuity Management (BCM)

Das BCM-Modul orientiert sich an ISO 22301 und hilft, den Betrieb auch bei Störungen aufrechtzuerhalten.



BCM-Modul mit Prozessen, Plänen und Readiness-Score

Für die Business Impact Analyse (BIA) erfassen Sie zunächst Ihre kritischen Prozesse und führen dann je Prozess die BIA durch: Sie bewerten die Auswirkungen über verschiedene Zeithorizonte und legen MTPD (maximal tolerierbare Ausfalldauer) sowie MBCO (minimal akzeptable Betriebsleistung) fest, dazu Abhängigkeiten wie IT-Systeme, Lieferanten und Personen.

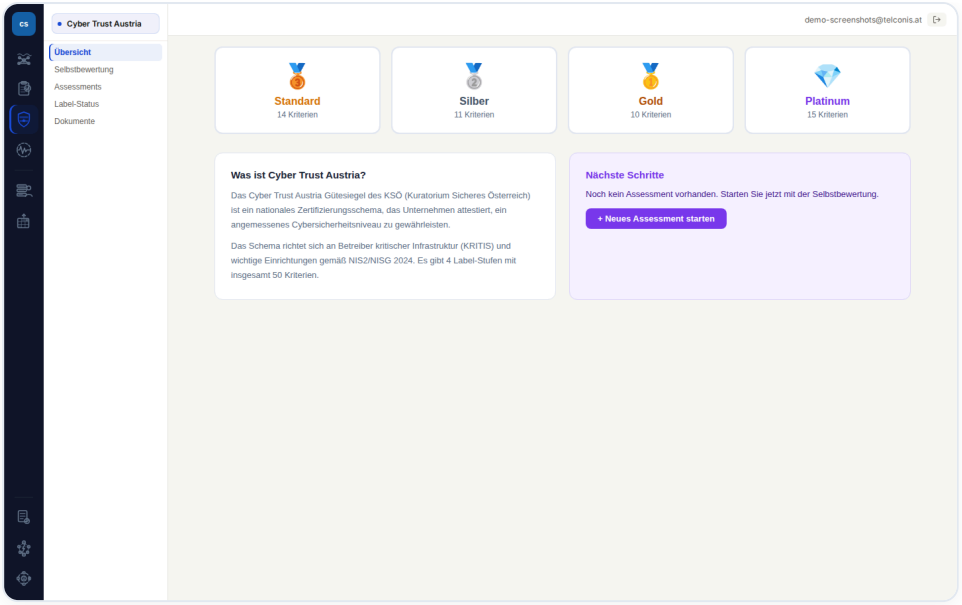
Notfall- und Wiederanlaufpläne (BCP/DRP) legen Sie mit konkreten Aktionen, Kontakten und einem Freigabe-Workflow an – ein Plan durchläuft also einen dokumentierten Genehmigungsschritt, bevor er als verbindlich gilt. Tests und Übungen dieser Pläne sowie reale Vorfälle mit anschließender Nachbetrachtung planen und protokollieren Sie ebenfalls im Modul; regelmäßige Tests sind schließlich ein zentraler Bestandteil eines glaubwürdigen BCM.

Die SPOF-Analyse (Single Point of Failure) identifiziert automatisch Schlüsselpersonen ohne Stellvertreter, also Personen, deren Ausfall den Betrieb gefährden würde. Sie greift dafür auf die im Personal-Modul erfassten ISMS-Rollen zurück.

Aus fünf Komponenten – BIA-Abdeckung, Plan-Abdeckung, Genehmigungsstatus, Testabdeckung und SPOF-Freiheit – berechnet Telconis einen BCM-Readiness-Score, dessen Verlauf über die Zeit dargestellt wird.

4.4 Cyber Trust Austria

Das Cyber-Trust-Austria-Modul (CTA) unterstützt Sie beim Erlangen des freiwilligen österreichischen Gütesiegels des Kuratoriums Sicheres Österreich (KSÖ) mit seinen vier Stufen: B-Kriterien (B1–B14, Standard), A-Kriterien (A1–A11, Silber), G-Kriterien (G1–G10, Gold) und P-Kriterien (P1–P15, Platinum).



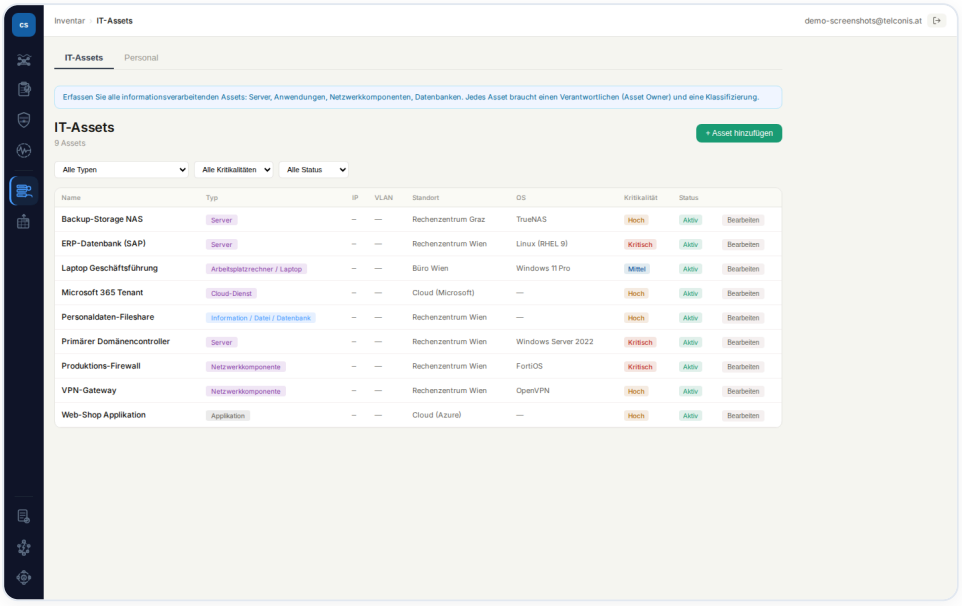
Cyber-Trust-Austria-Modul mit Selbstbewertung und Label-Status

Für die Selbstbewertung wählen Sie im entsprechenden Bereich die passende Stufe (Tab B, A, G oder P) und öffnen ein Kriterium. Über die Status-Buttons setzen Sie den Status, beschreiben im Feld „Umsetzung“, wie Sie das Kriterium erfüllen, ergänzen Fälligkeit und Notiz und verknüpfen Nachweis-Dokumente.

Unter Assessments erstellen Sie eine Bewertungsrunde mit Titel und Ziel-Label und verfolgen den Fortschritt; unter Label-Status hinterlegen Sie Ihr aktuelles CTA-Label mit Gültigkeit und Zertifikatsnummer.

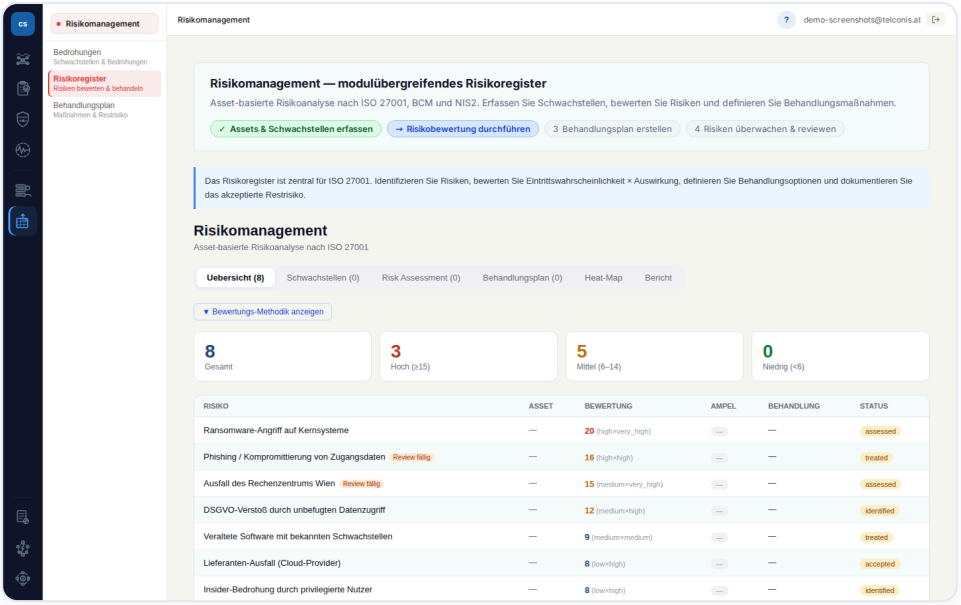
4.5 Risikomanagement

Das Risikomanagement-Modul umfasst zwei eng verbundene Bereiche, das Asset-Inventar und das Risikoregister, und bildet die gemeinsame Grundlage für alle anderen Module.



Asset-Inventar mit CIA-Bewertung

Im Asset-Inventar erfassen Sie Ihre Werte – Systeme, Anwendungen, Daten, Standorte – und bewerten jedes Asset nach den drei Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit (CIA).



Risikoregister mit Bewertung und Status

Im Risikoregister legen Sie Bedrohungen an, die Ihre Assets betreffen, bewerten jedes Risiko typischerweise nach Eintrittswahrscheinlichkeit und Schadensausmaß und legen einen Behandlungsplan fest: vermeiden, vermindern, übertragen oder akzeptieren, mit Maßnahmen, Verantwortlichen und Status.

Asset-Inventar und Risiken sind mit den anderen Modulen – ISO 27001, NIS2, BCM – verknüpft, sodass Sie Werte und Bedrohungen nur einmal pflegen müssen.

4.6 Personal

Das Personal-Modul führt ein Personalverzeichnis und ordnet Personen ihre ISMS-Rollen zu, etwa Informationssicherheitsbeauftragter, Notfallkoordinator oder Datenschutzbeauftragter.

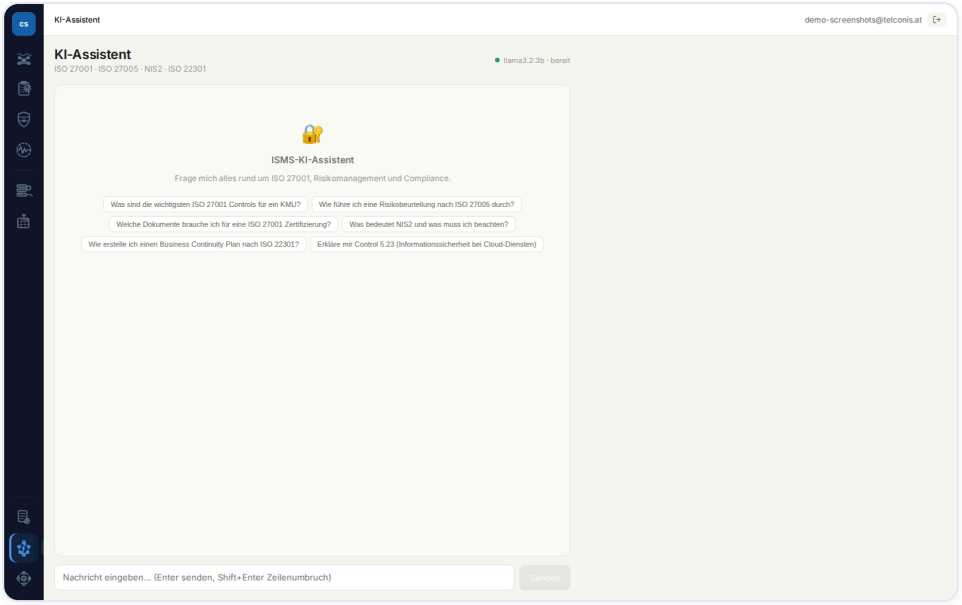
Sie legen Personen mit Name, Kontaktdaten, Position, Abteilung und Standort an und weisen ihnen ISMS-Rollen zu. Diese Zuordnung speist unter anderem die SPOF-Analyse im BCM-Modul.

Nicht jede Rolle sieht dabei alle Personaldaten, das schützt sensible Angaben, ohne sie zu anonymisieren: Administratoren sehen alle Felder inklusive Mobilnummer, Anstellungsart und Verfügbarkeit, Benutzer sehen Name, E-Mail, Telefon, Position, Abteilung, Standort und die ISMS-Rollen. Ein DSGVO-konformer Export der Personaldaten ist ebenfalls möglich.

---

5. Der KI-Assistent

Telconis enthält einen KI-gestützten Assistenten, der Sie bei Compliance-Fragen unterstützt: Er erklärt Fachbegriffe und Normanforderungen aus ISO 27001, NIS2, Cyber Trust Austria und BCM verständlich, hilft bei Formulierungen für Maßnahmenbeschreibungen und Dokumentation und unterstützt Sie bei der Strukturierung Ihrer Compliance-Arbeit.



Der KI-Assistent

Ein Punkt, der uns besonders wichtig ist: Der KI-Assistent läuft vollständig offline auf unserer eigenen Infrastruktur, über ein selbst gehostetes Sprachmodell (Ollama). Ihre Anfragen und Mandantendaten gehen zu keinem Zeitpunkt an einen externen Cloud-KI-Anbieter – es findet keine Datenübertragung ins Internet an Dritte statt. Die Verarbeitung bleibt vollständig innerhalb unserer Systeme, dort, wo auch der Rest Ihrer Telconis-Daten liegt.

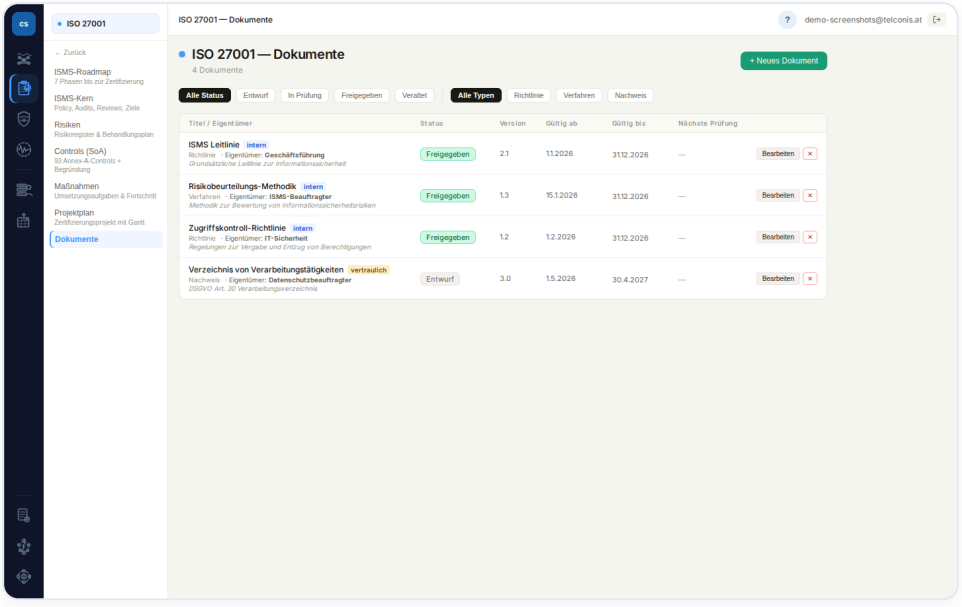
Was er nicht ist: eine Rechtsberatung oder ein Ersatz für ein externes Audit oder eine Zertifizierungsstelle. Seine Antworten können Fehler enthalten und müssen von Ihnen fachlich geprüft werden. Verlassen Sie sich bei rechtlich verbindlichen Entscheidungen – etwa zur eigenen NIS2-Betroffenheit – nicht allein auf die KI, sondern ziehen Sie qualifizierte Beratung hinzu (siehe § 2 der AGB).

Wie viele Anfragen Sie pro Tag stellen können, hängt von Ihrem Plan ab (im Trial zum Beispiel 5 pro Tag). Ist das Tageskontingent erreicht, steht der Assistent am Folgetag wieder zur Verfügung.

---

6. Dokumente, Vorlagen und Berichte

Der Dokumentenbereich ist Ihre zentrale Ablage für alle Nachweise und generierten Unterlagen.



Dokumentenbereich mit Vorlagen und Berichten

6.1 Dokumente hochladen und verwalten

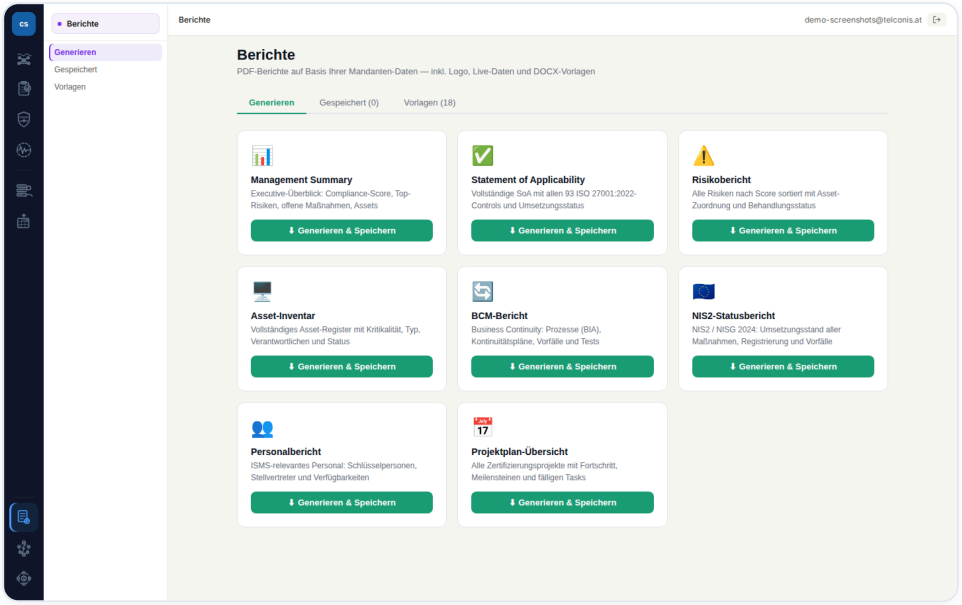
Dateien laden Sie einfach hoch, etwa PDF, DOCX oder XLSX, bis zu 25 MB pro Datei. Zu jedem Dokument hinterlegen Sie Eigentümer, Prüfer, Klassifizierung und das zugehörige Modul. Der Download ist sicher, PDFund Bilddateien lassen sich zudem direkt im Browser ansehen. In den Modulen – ISO, NIS2, CTA – verknüpfen Sie vorhandene Dokumente als Evidence, um die Umsetzung einer Anforderung nachvollziehbar zu belegen.

6.2 Die 18 Dokumentvorlagen (DOCX)

Telconis enthält 18 vorgefertigte DOCX-Vorlagen, bereits mit Ihren Mandantendaten wie Firmenname und Datum vorausgefüllt:

Rahmenwerk	Vorlagen
ISO 27001 (10)	Anwendungsbereich, Sicherheitsziele, Risikobeurteilungsmethodik, Risikobehandlungsplan, Statement of Applicability, Asset-Inventar, Auditprogramm, Auditbericht, Management-Review-Protokoll, Korrekturmaßnahmen
Business Continuity (4)	Business-Impact-Analyse, BCM-Strategie, Business-Continuity-Plan, Testbericht
NIS2 / NISG 2026 (3)	Maßnahmenübersicht § 32, Sicherheitsvorfallmeldung, Registrierungsdokumentation
Cyber Trust Austria (3)	Selbstbewertungs-Checkliste (alle Kriterien), Maßnahmenplan mit Normenreferenzen, Cyber-Trust-Austria-Nachweis

6.3 Die 8 PDF-Berichte



Berichte und Vorlagen

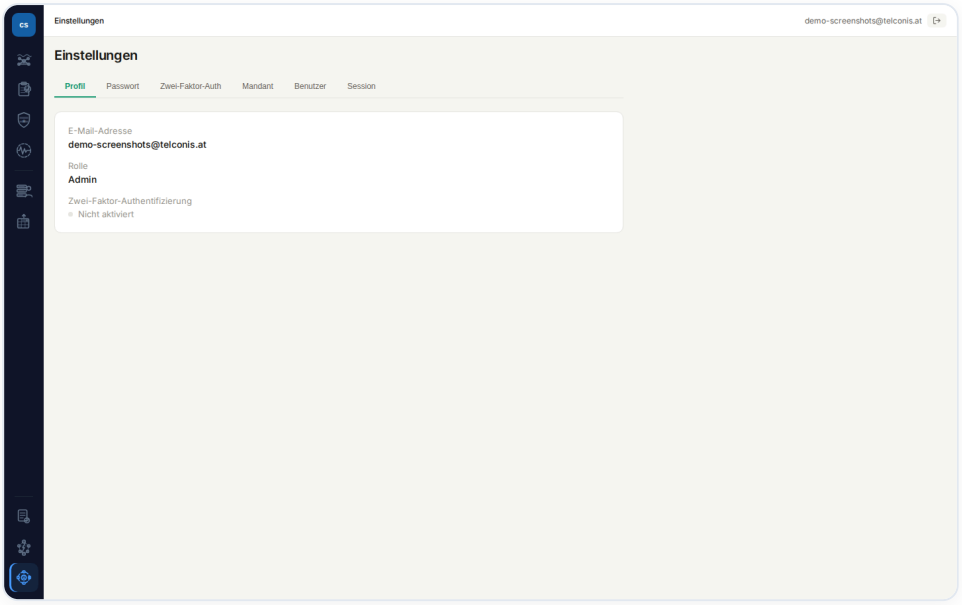
Direkt aus Telconis generieren Sie acht PDF-Berichte auf Basis Ihrer aktuellen Daten: Management Summary, Statement of Applicability (SoA), Risikobericht, Asset-Inventar, BCM, NIS2, Personal und Projektplan.

Zum Trial-Plan noch ein Hinweis: Der Export von PDF-Berichten und DOCX-Vorlagen ist in den kostenpflichtigen Plänen enthalten. Im kostenlosen Trial kann er eingeschränkt sein, ein Upgrade schaltet die volle Export-Funktion frei.

---

7. Einstellungen

Die Einstellungen erreichen Sie über das Zahnrad-Symbol in der Iconbar. Welche Bereiche Sie darin sehen, hängt von Ihrer Rolle ab.



Einstellungen

7.1 Für alle Nutzer

Unter Profil finden Sie Ihre E-Mail-Adresse, Ihre Rolle und den 2FA-Status. Beim Passwort brauchen Sie zum Ändern Ihr aktuelles Passwort, das neue muss mindestens 8 Zeichen haben. Unter 2FA richten Sie die Zwei-Faktor-Authentifizierung per TOTP ein oder deaktivieren sie wieder (siehe Abschnitt 2.5). Und unter Berichte generieren Sie PDF-Berichte wie SoA, Management Summary oder Risikoregister.

7.2 Nur für Administratoren

Unter Mandant pflegen Sie das vollständige Unternehmensprofil: Name, Adresse, PLZ, Ort, Land, Telefon, Fax, Website, E-Mail, UID-Nummer, Firmenbuchnummer, Branche und Unternehmensgröße. Diese Daten fließen direkt in die vorausgefüllten Vorlagen und Berichte ein.

Die Benutzerverwaltung erlaubt es, Benutzer per E-Mail einzuladen, zu bearbeiten, Passwörter zurückzusetzen sowie zu aktivieren oder zu deaktivieren. Eine Platz-Anzeige („X von Y belegt“) zeigt, wie viele Benutzer im Rahmen Ihres Plans noch dazukommen können. Und unter Session konfigurieren Sie das Session-Timeout, nach dem inaktive Nutzer automatisch abgemeldet werden.

Zum Benutzer-Limit: Jeder Plan erlaubt eine bestimmte Anzahl aktiver Benutzer – Standard sind 4 insgesamt, der Trial umfasst bis zu 3, Starter bis zu 5, Professional bis zu 25. Ist das Limit erreicht, müssen Sie entweder einen bestehenden Benutzer deaktivieren oder Ihren Plan erweitern, bevor Sie jemand Neuen einladen können. Das gilt übrigens auch beim Reaktivieren bereits deaktivierter Benutzer, nicht nur beim Neueinladen.

Um jemanden einzuladen, öffnen Sie Einstellungen → Benutzer und klicken auf „Einladen“. Sie geben E-Mail-Adresse und Rolle an (Admin oder Benutzer), und die eingeladene Person erhält eine E-Mail mit einem Einmal-Passwort. Beim ersten Login vergibt sie ihr eigenes Passwort und bestätigt dabei ebenfalls AGB und Datenschutzerklärung.

---

8. Rollen & Rechte

In der Oberfläche unterscheidet Telconis zwei Rollen: Admin und Benutzer. (Intern gibt es feinere Abstufungen, die für die tägliche Arbeit aber keine Rolle spielen.)

Bereich	Admin	Benutzer
Compliance-Daten ansehen und bearbeiten	✓	✓ (je nach interner Berechtigung lesend oder bearbeitend)
Firmenprofil (Mandant) bearbeiten	✓	–
Benutzer einladen / verwalten	✓	–
Session-Timeout konfigurieren	✓	–
Alle Personalfelder sehen	✓	– (eingeschränkte Sicht, siehe 4.6)
Eigenes Profil, Passwort, 2FA verwalten	✓	✓

Administratoren verwalten also das Unternehmenskonto – Firmenprofil, Benutzer, Sitzungseinstellungen – und sehen alle Daten. Benutzer arbeiten inhaltlich an den Compliance-Modulen, sehen bei Personaldaten aber nur die allgemeinen Felder und haben keinen Zugriff auf die Verwaltungsbereiche.

Für Konzerne oder Mehr-Mandanten-Umgebungen gibt es zusätzlich eine übergeordnete Betreiberrolle (Superadmin) bei Telconis selbst, die neue Mandanten anlegt und freischaltet. Als Kunde kommen Sie damit nur bei der erstmaligen Freischaltung in Berührung (siehe Kapitel 2).

---

9. Häufige Fragen (FAQ)

Was ist NIS2 / NISG 2026 und wer ist in Österreich betroffen? NIS2 ist die EU-Richtlinie für Cybersicherheit, in Österreich umgesetzt durch das NISG 2026. Betroffen sind wesentliche und wichtige Einrichtungen aus Sektoren wie Energie, Gesundheit, digitale Infrastruktur, Verkehr oder verarbeitendes Gewerbe, je nach Unternehmensgröße und Branche. Telconis bietet dafür eine Betroffenheitsprüfung sowie den vollständigen § 32-Maßnahmenkatalog (a–j).

Was ist der Unterschied zwischen ISO 27001, NIS2 und Cyber Trust Austria? ISO 27001:2022 ist ein internationaler Zertifizierungsstandard für Informationssicherheits-Managementsysteme mit 93 Controls im Annex A. NIS2 / NISG 2026 ist eine gesetzliche EU-Verpflichtung für bestimmte Sektoren mit Meldepflichten bei Sicherheitsvorfällen. Cyber Trust Austria wiederum ist ein freiwilliges österreichisches Gütesiegel des KSÖ mit vier Stufen (Standard, Silber, Gold, Platinum). Telconis bildet alle drei Rahmenwerke inklusive gegenseitiger Control-Zuordnung in einer Plattform ab.

Kann Telconis mehrere Compliance-Normen gleichzeitig abbilden? Ja. ISO 27001:2022, NIS2 / NISG 2026, Cyber Trust Austria und Business Continuity Management (ISO 22301) laufen zentral, mit gemeinsamem Asset-Inventar, geteilten Maßnahmen, Risikoregister und konsolidierten Berichten statt separater Einzeltools.

Gibt es eine kostenlose Testversion? Ja, 14 Tage kostenlos, ohne Kreditkarte, mit Zugriff auf alle Compliance-Module für bis zu 3 Nutzer. Beachten Sie, dass der Zugang nach der Registrierung zunächst manuell geprüft und freigeschaltet wird, in der Regel innerhalb eines Werktages.

Warum kann ich mich nach der Registrierung nicht sofort anmelden? Zum Schutz vor Missbrauch wird jeder neue Trial-Zugang manuell geprüft und freigeschaltet. Sie bekommen eine E-Mail, sobald er aktiv ist.

Warum wird meine private E-Mail-Adresse abgelehnt? Die Registrierung setzt eine geschäftliche Adresse voraus. Freemail-Adressen wie Gmail, GMX, Web.de oder Outlook werden nicht akzeptiert.

Welche Dokumentvorlagen sind enthalten? 18 vorausgefüllte DOCX-Vorlagen, unter anderem Risikobeurteilungsmethodik, Statement of Applicability, Business-Impact-Analyse und Sicherheitsvorfallmeldung, dazu 8 direkt generierbare PDF-Berichte wie Management Summary, SoA und Risikobericht.

Garantiert Telconis meine Zertifizierung oder NIS2-Konformität? Nein. Telconis dokumentiert und verfolgt – es ersetzt keine Rechtsberatung, keine Zertifizierungsstelle und kein externes Audit. Für die inhaltliche Richtigkeit Ihrer Daten und die Bewertung Ihrer Betroffenheit sind Sie selbst verantwortlich.

Wie sichere ich mein Konto zusätzlich ab? Über die Zwei-Faktor-Authentifizierung unter Einstellungen → 2FA, siehe Abschnitt 2.5.

Wie viele Benutzer kann ich anlegen? Das hängt vom Plan ab: Trial bis zu 3, Starter bis zu 5, Professional bis zu 25. Die Benutzerverwaltung zeigt Ihnen die belegten und freien Plätze.

Ich habe mein Passwort vergessen – was tun? Klicken Sie auf der Anmeldeseite auf „Passwort vergessen?“ und folgen Sie dem Link in der E-Mail, der eine Stunde gültig ist. Alternativ kann Ihr Administrator Ihr Passwort zurücksetzen.

---

10. Support kontaktieren

Wir helfen gern weiter:

- E-Mail-Support: support@telconis.at
- Website: https://telconis.at

Geben Sie bei Support-Anfragen bitte Ihren Firmennamen und, falls vorhanden, eine kurze Beschreibung des Problems inklusive des betroffenen Moduls an – das beschleunigt die Bearbeitung.

Telconis wird betrieben von der Telcon OG. Es gelten die auf telconis.at veröffentlichten AGB und die Datenschutzerklärung. Dieses Handbuch beschreibt den Funktionsumfang zum angegebenen Stand; einzelne Funktionen können je nach Plan und Weiterentwicklung abweichen.