www.xiting.com

Thomas Tiede

Access Governance in SAP wirksam und compliancekonform

SAP Security Group Vienna Edition · 5. November 2026



Thomas Tiede

Strategic Advisor

E-Mail: ttiede@xiting.com

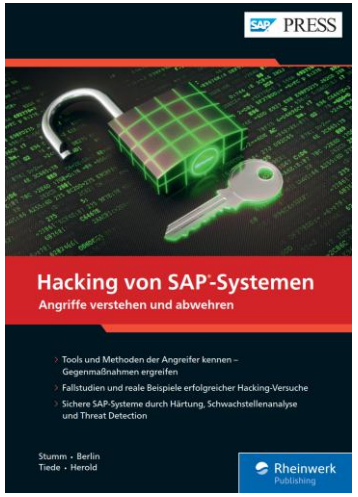
Xiting GmbH

Obere Ringstraße 17
79859 Schluchsee

E-Mail: info@xiting.com
Web: www.xiting.com







Welche Pflichten gelten für Ihr Unternehmen?

Warum SoD-Kontrollen ins Leere laufen

Veraltete Regelwerke

Einmal eingeführt, selten fachlich überarbeitet. Neue Prozesse, Systeme und Vorgaben kommen hinzu, das Regelwerk bleibt.

Fehlende Governance

Niemand ist für den Inhalt verantwortlich. Änderungen passieren technisch, ohne fachliche Freigabe.

Inkonsistenzen zwischen Systemen

Dasselbe Risiko wird in jedem System anders abgebildet. Ergebnisse lassen sich nicht vergleichen.

Das Symptom: viele Befunde, wenige Maßnahmen.

© 2026 Xiting AG. All rights reserved

Prüfregeln aus Listen

Standardkataloge
Für den Durchschnitt gebaut, nicht für Ihr Unternehmen.

Gewachsene Regelsets
Über Jahre ergänzt, selten fachlich überarbeitet.

Inhalte aus Werkzeugen
Mitgeliefert und übernommen, ohne eigene Herleitung.

DSAG-Prüfleitfaden SAP S/4HANA

Die Zuordnung der Prüfungsschwerpunkte zu ISO-Normen, Rahmenwerken wie COBIT und Prüfungsstandards liegt bewusst in der Verantwortung des Prüfenden.

Einleitung, S. 10

In keinem der drei Fälle ist dokumentiert, warum eine Regel gilt und welche fehlt.

© 2026 Xiting AG. All rights reserved

Die Ursache dahinter

Ein Regelwerk ist eine Behauptung darüber, welche Risiken für Ihr Unternehmen relevant sind.

© 2026 Xiting AG. All rights reserved

Geltende Regularien herleiten

Unternehmensprofil

- Sitz und Tätigkeitsländer
- Branche
- Größe
- Kapitalmarktorientierung
- Rolle in Lieferketten
- …

→

Auslöser

Welche Merkmale lösen welche Regularien aus?

Jede Entscheidung muss begründet und dokumentiert werden.

→

Anwendbar
gilt unmittelbar

Begründet nicht anwendbar
geprüft, trifft nicht zu

Indirekt wirksam
über Kunden oder Verträge

Eine weggelassene Vorgabe sieht genauso aus wie eine, die nie jemand geprüft hat.

© 2026 Xiting AG. All rights reserved

Gleiches SAP-System, andere Pflichten

Industrieunternehmen

Automobilzulieferer, exportorientiert

DSGVO anwendbar

Exportkontrolle und Sanktionen anwendbar

TISAX indirekt wirksam

DORA begründet nicht anwendbar

Finanzdienstleister

Beaufsichtigt, Kunden in der EU

DSGVO anwendbar

DORA anwendbar

Geldwäscheprävention anwendbar

TISAX begründet nicht anwendbar

Vereinfachtes Beispiel

Die SAP-Funktionen sind dieselben. Welche Risiken zählen, ist es nicht.

© 2026 Xiting AG. All rights reserved

Ein Risiko, viele Systeme

Risiko, einmal fachlich definiert

„Dieselbe Person legt Lieferanten an und gibt Zahlungen frei."

↓ ↓ ↓ ↓

SAP S/4HANA
eigene technische Ausprägung

SAP ECC
eigene technische Ausprägung

SAP-Cloud-Anwendungen
eigene technische Ausprägung

Weitere Systeme
eigene technische Ausprägung

Fachlich einheitlich, technisch je System.

So werden Ergebnisse über alle Systeme vergleichbar.

© 2026 Xiting AG. All rights reserved

Das Regelwerk als Führungsaufgabe

Herleiten

Geltende Regularien und Risiken bestimmen

→

Freigeben

Fachlich verantworteter Inhalt, nicht nur technisch

→

Betreiben

Befunde bearbeiten, Maßnahmen nachhalten

→

Überarbeiten

Bei festgelegten Anlässen wie neuen Vorgaben oder Systemen

Ein benannter Eigentümer verantwortet den ganzen Kreislauf.

KI kann Pflege und Weiterentwicklung deutlich beschleunigen. Die Verantwortung für den Inhalt bleibt beim Menschen.

© 2026 Xiting AG. All rights reserved

Vom Unternehmensprofil zum Regelwerk

Profil erfassen

Merkmale des Unternehmens, vorrecherchiert und bestätigt

KI + Mensch

→

Regularien zuordnen

Gegen eine kuratierte Sammlung, jede Entscheidung begründet

KI

→

Auf SAP abbilden

Welche Funktionen im System betrifft die Vorgabe?

KI

→

Regeln erzeugen

Risiko fachlich einmal, technisch je System

KI

→

Fachlich freigeben

Je Regel durch eine benannte Person

Mensch

Jede Regel ist rückverfolgbar, von der Fundstelle bis zur technischen Ausprägung.

Die KI übernimmt Recherche, Zuordnung und Formulierung.
Was sie nicht übernimmt: die Entscheidung, welche Regel gilt.

© 2026 Xiting AG. All rights reserved

Plausibel ist nicht belegt – Fehlerquellen

Erfundene Fundstelle

Paragraf, Ziffer oder Kapitel: korrekt formatiert, inhaltlich passend, aber in der Norm nicht vorhanden.

Erfundener technischer Name

Transaktion oder Berechtigungsobjekt nach SAP-Namenskonvention, das im System nicht existiert.

Stille Auslassung

Eine geltende Vorgabe fehlt, ohne Begründung. Im Ergebnis sieht man sie nicht.

Diese Fehler überstehen die Nachkontrolle, weil sie richtig aussehen.

Je besser die KI formuliert, desto glaubwürdiger wirkt der Fehler.

© 2026 Xiting AG. All rights reserved

Leitplanken gegen Halluzinationen

Quellenhierarchie

Systemdaten vor offiziellen Quellen vor der Bibliothek. Trainingswissen ist keine Quelle für konkrete Namen.

Geschlossene Welt

Was nicht wörtlich in der kuratierten Sammlung steht, existiert nicht.

Prüfung vor der Ausgabe

Geprüft wird, bevor ein Ergebnis entsteht, nicht korrigiert danach.

Sichtbare Unsicherheit

Jeder Wert trägt einen Status: belegt, nicht belegt oder nicht vorhanden.

Die fachliche Freigabe bleibt in jedem Fall beim Menschen.

© 2026 Xiting AG. All rights reserved

Prüfung eines Regelwerks

Wie prüft man, was eine KI erzeugt hat?

Wie prüft man ein Regelwerk, das eine KI erzeugt hat?

Verfahren prüfen

Kuratierte, versionierte Sammlung der Regularien als einzige Quelle

Quellenbindung: Was nicht in der Sammlung steht, existiert nicht

Unsicherheit ist sichtbar gekennzeichnet

Ergebnis prüfen

Stichprobe gegen Primärquellen, nicht gegen die Ausgabe selbst

Stichprobe der technischen Ausprägung gegen das System

Abweichungen dokumentiert und nachverfolgt

Verantwortung prüfen

Fachliche Freigabe je Regel durch eine benannte Person

Freigabe im Gremium aus Fachbereich, IT und Compliance

Die KI ist kein Freigebender

Unabhängigkeit der Revision

Die Revision kann das Verfahren nutzen, um ein bestehendes Regelwerk zu bewerten. Erstellt sie das Regelwerk selbst, prüft sie ihre eigene Arbeit.

DSAG-Prüfleitfaden Kap. 5.4 verweist bei KI-gestütztem Change-Management auf den deutschen Prüfungsstandard IDW PS 861 „Prüfung von KI-Systemen“

© 2026 Xiting AG. All rights reserved

Vier Fragen

01 Wer entscheidet, welche Regularien für Ihr Regelwerk gelten, und wo ist das dokumentiert?

02 Wann wurde Ihr Regelwerk zuletzt fachlich überarbeitet, nicht nur technisch migriert?

03 Woran würden Sie erkennen, dass in Ihrem Regelwerk Risiken fehlen?

04 Wie viele Ihrer Regeln versteht Ihr Fachbereich ohne Übersetzung durch die IT?

© 2026 Xiting AG. All rights reserved

Fragen?

Thomas Tiede · Strategic Advisor · Xiting · ttiede@xiting.com

Anhang

Beispiel aus einem Proof of Concept, anonymisiert

Unternehmensprofil (Auszug; KI-unterstützt)

Anhang · zu Folie 7

Profilmerkmal	Wert	Konfidenz	Beleg
Sitzland	AT	**Belegt**	Impressum (Firmenbuch)
Branche	Energie	**Belegt**	Unternehmenszweck: Erzeugung, Übertragung, Handel, Vertrieb
Börsennotiert	ja	**Belegt**	Streubesitz börsengehandelt
SEC-registriert	nein	**Plausibel**	Nur ADR Level 1 im US-OTC-Handel, keine SEC-Berichtspflicht
NIS2-relevant	ja	**Belegt**	NISG 2026, Sektor Energie, Großunternehmen
KRITIS-relevant	nein · zu klären	**Plausibel**	RKEG in Kraft, Einstufung nicht öffentlich
OT-Bezug (IEC 62443)	nein · zu klären	**Offen**	Kraftwerke und Netz plausibel, kein öffentlicher Nachweis
Kartendaten in SAP	nein · zu klären	**Vermutung: ja**	Haushaltskunden und Lade-App
Weitere Länder im SAP-Scope	DE, ES, IT, RO, AL	**Offen**	Gesellschaften laut Impressum, SAP-Scope je Land unbestätigt

Jeder Wert trägt Konfidenz und Beleg. Offene Werte werden im Gespräch geklärt, nicht geraten.

© 2026 Xiting AG. All rights reserved

Ergebnis der Normenzuordnung (KI-generiert)

Anhang · zu Folie 7 und 8

Anwendbar

Buchführung und Aufbewahrung: UGB §§ 190, 212; BAO §§ 131, 132

Datenschutz: DSGVO, DSG

Mitbestimmung: ArbVG § 96

Strafrecht: StGB §§ 146, 153

Cybersicherheit: NISG

Energie: ElWOG (Adressat noch zu bestätigen)

Begründet nicht anwendbar

SOX / SEC: nur ADR Level 1, keine SEC-Berichtspflicht

DORA: kein Finanzunternehmen

Geldwäsche: FM-GwG gilt nur für den Finanzsektor

Offen, im Gespräch zu klären

PCI-DSS: Kartendaten aus der Lade-App in SAP?

IEC 62443: SAP mit Leittechnik gekoppelt?

KRITIS / RKEG: Einstufung nicht öffentlich

Länder-Scope DE, ES, IT, RO, AL

Nicht in der Sammlung

RKEG

Gaswirtschaftsgesetz 2011

REMIT (Energiegroßhandel)

Österreichische Prüfungsstandards

Als Lücke ausgewiesen, nicht stillschweigend weggelassen

Auch was nicht gilt oder fehlt, steht im Ergebnis, jeweils mit Begründung.

© 2026 Xiting AG. All rights reserved

Von der Norm zum Risiko (KI-generiert)

Anhang · zu Folie 13

Risiko	Beschreibung	UGB § 190	BAO § 131 Radier-verbot	BAO § 132	DSGVO Art. 32	StGB § 153	StGB § 146	ElWOG	NISG
ZITCD1	Änderungsbelege löschen		**P**	**P**	S				S
ZITDU1	Update-Berechtigungen debuggen	S	**P**		S	**P**			S
ZITUA1	Benutzerverwaltung				**P**			S	**P**
ZFIN015	Kreditorenstammdaten pflegen UND Zahlung vorschlagen/freigeben	S				**P**	**P**		
ZFIN003	Zahlungseingang buchen UND Bankabstimmung durchführen	**P**				**P**			
ZFIN004	Anlagenstammdaten pflegen UND Anlagenbeleg buchen	**P**				S		**P**	

P = primär, S = sekundär. Auszug: 6 von 21 Risiken, 8 von 15 Pflichtnormen. Jede Zuordnung ist im Original einzeln begründet.

Jede Regel lässt sich bis zur Norm zurückverfolgen, und jede Norm bis zu ihren Regeln.

© 2026 Xiting AG. All rights reserved

Katalogeintrag (Auszug; KI-generiert)

Anhang · zu Folie 11

ZFIN015 · Kreditorenstammdaten pflegen UND Zahlung vorschlagen/freigeben

Beschreibung

Eine Person kann zahlungsrelevante Merkmale eines Kreditors ändern, etwa die Bankverbindung, und Zahlungen an denselben Kreditor vorschlagen und freigeben. Erst beide Berechtigungen zusammen erzeugen das Risiko.

Szenario fahrlässig

Eine fehlerhaft erfasste Bankverbindung bleibt unentdeckt; der Fehler fällt erst bei Mahnung oder Lieferstopp auf.

Szenario vorsätzlich

Die Bankverbindung wird auf ein eigenes Konto geändert, die Zahlung selbst freigegeben, die Stammdaten danach zurückgesetzt. Ein Komplize ist nicht nötig.

Kontrollziel

Stammdatenpflege und Zahlungsfreigabe liegen nie in einer Hand; jede Änderung des Zahlungsziels wird vor der Freigabe unabhängig bestätigt.

Standard-Risikostufe

55 / High

Allgemeiner Mindestwert ohne Land, Branche oder Kundenkontrollen. Die kundenspezifische Bewertung kann höher liegen.

Fachlich und systemneutral formuliert. Die technische Ausprägung folgt je System.

© 2026 Xiting AG. All rights reserved

Risikobewertung: Rechenweg (Auszug; KI-generiert)

Anhang · zu Folie 17

	Dimension	Gewicht	Wert	Begründung (gekürzt)
Schaden-potenzial (S)	Finanzieller Schaden	0,35	**0,70**	An offene Posten gebunden, aber wiederholbar
	Regulatorisches Risiko	0,30	**1,00**	Strafrechtliche Sanktion mit Freiheitsstrafe
	IT-Sicherheit	0,20	**0,50**	Integrität der Stammdaten, nicht des Berechtigungssystems
	Reputation	0,15	**0,80**	Börsennotiert, Prüfungsfeststellung wahrscheinlich
Ausnutz-barkeit (A)	Technische Ausführbarkeit	0,40	**0,90**	Standardfunktionen, Zahlungsausführung liegt außerhalb
	Entdeckungsrisiko	0,40	**0,80**	Änderungsbelege werden selten systematisch ausgewertet
	Betroffene Population	0,20	**0,80**	***Schätzung ohne Beleg, durch Rollenanalyse zu ersetzen***

Ergebnis

S = 0,765 A = 0,840

Basis = (0,6 · S + 0,4 · A) · 100

Basis Score 80

K = 0,366

Kontrollwirkung aus dem Profil geschätzt, keine Kundendokumente

Net = Basis · (1 − K)

Net Score 51

Beispiel ZFIN015, Werte illustrativ. Kundenspezifische Normbezüge sind hier ausgeblendet.

Jeder Wert ist begründet, Schätzungen sind markiert. Geprüft wird gegen Primärquellen und System.

© 2026 Xiting AG. All rights reserved