

Gut gerüstet: Die Top-Risiken 2026

written by Christian Hafner | 9 Januar, 2026



Riskmanagement & IKS News

Gut gerüstet: Die Top-Risiken 2026

Risiko-Prognosen für KMU und Gemeinden – mit integrierter IKS-Ableitung

2026 ist kein Jahr neuer Risiken, sondern ein Jahr, in dem bekannte Risiken schneller, gleichzeitiger und finanziell wirksamer eintreten.

Cyberanfälligkeit, Betriebsunterbrüche, Extremwetter und regulatorischer Druck wirken nicht mehr isoliert, sondern verstärken sich gegenseitig.

Für Schweizer KMU und Gemeinden entscheidet deshalb weniger die Risikoidentifikation als die Fähigkeit, Risiken aktiv zu steuern und im Ereignisfall handlungsfähig zu bleiben.

Risiko-Radar 2026 (Schweiz)

Risiko-Radar 2026 (Schweiz)

KMU & Gemeinden - Prognosen aus Beratung, Versicherungen & Forschung

Strategische Risiken

- Geopolitische Fragmentierung & EU-Beziehungen
- KI als Wettbewerbs- und Governance-Risiko
- Reputationsschäden durch Desinformation / Deepfakes

Operative Risiken

- Cyber: Ransomware, Lieferantenangriffe, Cloud-Abhängigkeiten
- Betriebsunterbruch (IT/OT, kritische Dienstleister)
- Fachkräftemangel & Wissensverlust (Demografie)

Finanzielle Risiken

- Naturkatastrophen / Extremwetter → Sach- & Ertragsausfälle
- Zins-/Inflationsvolatilität, Budgetdruck in Gemeinden
- Versicherungslücken / steigende Prämien (Cyber, NatCat)

Regulatorik & Aussenwirtschaft

- DORA/NIS2/CRA/AI-Regeln: indirekter Druck via EU
- ESG- & Lieferketten-Transparenzanforderungen
- Wechselkursrisiken (starker CHF) & Handelshemmnisse

swissaxis AG • Januar 2026

Zentrale Risikofelder

1. Strategische Risiken

Geopolitische Fragmentierung und EU-Nähe

Die internationale Lage bleibt volatil. Für exportorientierte KMU gewinnen Markt- und Lieferkettenzugang eine strategische Dimension. Für Schweizer Organisationen wirkt Regulierung häufig indirekt – über Kunden, Banken und Partner im EU-Raum.

KI als Wettbewerbs- und Governance-Risiko

Künstliche Intelligenz beschleunigt Entscheidungen – und potenziert Fehlentscheide. Die zentralen Risiken liegen weniger in der Technologie selbst, sondern in fehlender Governance: unklare Verantwortlichkeiten, mangelhafte Datenqualität und Automatisierung ohne Kontrollpunkte.

Reputation und Vertrauen (Desinformation / Deepfakes)

Manipulierte Inhalte und täuschend echte Deepfakes entwickeln sich zu einem ernsthaften Reputationsrisiko. Gemeinden und KMU stehen vor der Herausforderung, Kommunikationskanäle und Identitäten aktiv zu schützen.

2. Operative Risiken

Cyber- und Datensicherheit (inkl. Lieferanten und Cloud)

Cyber bleibt das dominierende Einzelrisiko. KI-gestützte Angriffe senken die

Eintrittsbarrieren, gleichzeitig steigt die Abhängigkeit von wenigen IT- und Cloud-Dienstleistern. Besonders kritisch sind Angriffe über Drittparteien.

Betriebsunterbruch durch IT-, OT- oder Dienstleisterausfälle

Neben gezielten Angriffen gewinnen technische Störungen und Abhängigkeiten von kritischen Dienstleistern an Bedeutung. Für Gemeinden betrifft dies zunehmend E-Government-, Zahlungs- und Versorgungsprozesse.

Fachkräftemangel und Wissensverlust

Der demografische Druck verschärft Engpässe in IT, Bau, Pflege und Verwaltung. Schlüsselpersonenrisiken und Projektverzögerungen nehmen spürbar zu.

3. Finanzielle Risiken

Naturkatastrophen und Extremwetter – direkte Bilanzwirkung

Naturgefahren führen häufiger zu Sachschäden und längeren Unterbrüchen. Für Gemeinden und KMU werden Objektschutz, Versicherungslösungen und Notfallfähigkeit zu zentralen Steuerungsgrössen.

Zins-, Inflations- und Budgetvolatilität

Unsichere Kosten- und Zinsentwicklungen erschweren Investitions- und Budgetentscheide. Bei Gemeinden treffen steigende Sozial- und Infrastrukturkosten zunehmend auf begrenzte Ertragsspielräume.

Versicherungslücken und steigende Prämien

Cyber- und Naturgefahrenversicherungen werden restriktiver und teurer. Organisationen unterschätzen häufig Auflagen und Selbstbehalte – mit trügerischer Scheinsicherheit.

4. Regulatorik und Aussenwirtschaft

Regulatorischer Druck über EU-Vorgaben (DORA, NIS2, CRA, AI-Regeln)

Auch ohne direkte Unterstellung steigt der Handlungsdruck. Kunden und Partner erwarten belastbare Nachweise zu Cyber-Resilienz, Vorfallmanagement und Lieferantensteuerung.

ESG- und Lieferketten-Transparenz

Nachhaltigkeit wird operativ. Datenqualität, Nachvollziehbarkeit und dokumentierte Kontrollen entscheiden über Aufträge, Finanzierung und Reputation.

Wechselkursrisiken durch starken Franken

Für Exporteure bleibt der CHF ein struktureller Risikotreiber. Ohne aktive Absicherungs- und Preismodelle kippen Margen innerhalb weniger Monate.

Risiko-Matrix 2026: Priorisierung nach Impact und Eintritt

Risiko-Matrix 2026 (Schweiz)

Auswirkung (Impact)	5		Extremwetter / Naturgefahren	Cyber / Ransomware		
	4	Fachkräftemangel	Regulatorischer Druck (EU)	Betriebsunterbruch IT / Cloud		
	3	Wechselkursrisiko CHF	KI-Fehlentscheidungen			
	2					
	1					
		1	2	3	4	5
		Eintretenswahrscheinlichkeit				

swissaxis AG • Januar 2026

Cyber / Ransomware

Angriffe auf IT- und OT-Systeme mit Datenverschlüsselung, Erpressung und längeren Betriebsunterbrüchen.

Betriebsunterbruch IT / Cloud

Ausfälle von internen IT-Systemen oder kritischen Cloud- und Managed-Service-Dienstleistern mit direkter Wirkung auf Kernprozesse.

Extremwetter / Naturgefahren

Schäden durch Hochwasser, Hitze, Sturm oder andere Naturereignisse mit Auswirkungen auf Infrastruktur, Gebäude und Lieferketten.

Regulatorischer Druck (EU)

Indirekte Auswirkungen von EU-Regulierungen (z. B. DORA, NIS2, CRA) über Kunden, Banken und Geschäftspartner.

KI-Fehlentscheidungen

Fehlentscheide oder falsche Priorisierungen durch unzureichend gesteuerte oder unkontrollierte KI-Anwendungen.

Fachkräftemangel

Engpässe bei qualifiziertem Personal mit Auswirkungen auf Projektumsetzung, Betriebssicherheit und Servicequalität.

Wechselkursrisiko CHF

Margen- und Budgetbelastungen durch einen starken oder stark schwankenden Schweizer Franken.

IKS-Ableitung: Von Risiken zu wirksamen Kontrollen

Ein wirksames IKS fokussiert sich 2026 auf wenige, gut verankerte Kontrollen mit messbarer Steuerungswirkung.

Risiko	Schlüsselkontrolle	KPI KRI	Owner
Cyber / Ransomware	MFA, Offline-Backups, Patch-Standards, Incident-Runbooks	MTTD/ MTTR, Restore-Tests	IT / CISO
Betriebsunterbruch	BCM, Notfallorganisation, Szenario-Übungen	RTO/RPO, Übungsquote	GL
KI-Einsatz	KI-Governance, Freigabeprozesse, Human-in-the-loop	Genehmigte Use-Cases, Findings	Business / IT
Naturgefahren	Objektschutz, Versicherung, Notfallpläne	Schadenshöhe, Ausfalltage	Facility Finanzen
Regulatorik / ESG	Dokumentierte Kontrollen, Vier-Augen-Prinzip	Audit-Findings, Fristen	Compliance

swissaxis AG • Januar 2026

BCM: Business Continuity Management (Management der Geschäftskontinuität)

MFA: Multi-Faktor-Authentifizierung

MTTD (Mean Time to Detect): Durchschnittliche Zeit bis zur Erkennung eines Sicherheits- oder Störungsereignisses

MTTR (Mean Time to Respond / Recover): Durchschnittliche Zeit bis zur Reaktion bzw. Wiederherstellung nach einem Ereignis

RTO (Recovery Time Objective): Maximal tolerierte Wiederanlaufzeit eines Prozesses oder Systems

RPO (Recovery Point Objective): Maximal tolerierter Datenverlust gemessen in Zeit

KPI (Key Performance Indicator): Kennzahl zur Messung der Leistung eines Prozesses oder einer Kontrolle

KRI (Key Risk Indicator): Kennzahl zur Überwachung der Risikoentwicklung

ESG: Environmental, Social, Governance (Nachhaltigkeitskriterien)

CISO (Chief Information Security Officer): Verantwortliche Rolle für Informationssicherheit

6. Fazit

2026 wird zum Stresstest für Risikomanagement und IKS. Organisationen, die Risiken konsequent priorisieren, Kontrollen wirksam ausgestalten und Reaktionsfähigkeit üben, gewinnen Resilienz – und damit strategische Handlungsfreiheit.

Quellen:

- Allianz Risk Barometer (Top-Risiken: Cyber, Betriebsunterbruch, Naturkatastrophen)
- PwC Switzerland – Global Digital Trust Insights 2026
- Swiss Re – Outlook 2026/2027 (Regime shifts: Geopolitik, Klima, Wirtschaft)
- ETH Zürich (CSS) – Risk & Resilience Reports
- Cyber Resilience Act (EU) – Umsetzungsphase ab 2026 (relevant via Lieferketten/Kundenanforderungen)
- Everbridge – Global Risk & Resilience Outlook 2026