Aufbruch in die digitale Resilienz

Interne Kontrollsysteme für EVUs | Die Digitalisierung treibt die Energiebranche voran, doch sie birgt auch neue Risiken. Wie können Energieversorgungsunternehmen inmitten von Cybergefahren, Personalengpässen und Klimarisiken resilient bleiben? Der Schlüssel liegt in einem reifen internen Kontrollsystem, das nicht nur kontrolliert, sondern kontinuierlich mitwächst.

ERIC MONTAGNE, MARIO KÖPFLI

Die Schweizer Energiebranche steht an einem entscheidenden Wendepunkt. Die beschleunigte Dekarbonisierung treibt den Ausbau der erneuerbaren Energien unaufhaltsam voran, während die Digitalisierung nahezu alle Prozesse transformiert. Intelligente Stromnetze, sogenannte Smart Grids, haben das Potenzial, die Energieflüsse dynamisch zu steuern und zu optimieren. Damit können Schwankungen in der Stromproduktion, beispielsweise durch Wind- oder Solaranlagen, effizient ausgeglichen werden. Doch diese technologischen Fortschritte bringen auch neue Herausforderungen mit sich, die von der Branche nicht unterschätzt werden dürfen.

Seit 2021 führt i-Risk in Zusammenarbeit mit dem Verband Schweizerischer Elektrizitätsunternehmen (VSE) eine jährliche Studie durch, um die Risikolandschaft der Energieversorgungsunternehmen (EVUs) zu analysieren. Die Ergebnisse dieser Erhebungen zeigen, wie stark sich die Rahmenbedingungen in den letzten Jahren verändert haben. Die Covid-19-Pandemie stellte die EVUs vor unerwartete logistische und operative Herausforderungen, gefolgt vom Ukraine-Krieg, der die Energiepreise in die Höhe schnellen liess und die Stabilität der Versorgung gefährdete. Auch geopolitische Spannungen, die globale Lieferketten betreffen, und die Zunahme extremer Wetterereignisse haben die Branche nachhaltig geprägt.

Im Jahr 2022 lag der Fokus auf der Bewältigung einer drohenden Energiemangellage und auf der Handhabung drastisch gestiegener Preise. Doch

Bild: Adobe Stock/Suriyo

bereits ein Jahr später, 2023, trat ein weiteres zentrales Thema in den Vordergrund: die Notwendigkeit, die Resilienz der Unternehmen in einer zunehmend vernetzten und digitalisierten Welt zu stärken. 2024 wurde diese Entwicklung weiter beschleunigt.

Studienergebnisse

Die Ergebnisse der i-Risk-Studie 2024 [1] verdeutlichen, welche Risiken für die Branche von grösster Bedeutung sind **(Bild 1)**:

- **IT-Risiken.** Die zunehmende Digitalisierung macht die IT-Sicherheit zu einem der zentralen Themen für EVUs. Ein Ausfall der IT-Systeme kann schwerwiegende Folgen haben: Netzsteuerungen werden unterbrochen, Kontrollzentralen verlieren den Überblick und wichtige operative Entscheidungen können nicht getroffen werden. Cyberangriffe sind dabei die grösste Bedrohung. Immer häufiger kommt es zu gezielten Attacken auf kritische Infrastrukturen, bei denen Angreifer versuchen, Betriebsprozesse zu stören oder Daten zu manipulieren. Ebenso problematisch sind Datenverluste oder Sicherheitslücken in sensiblen Systemen, die erhebliche finanzielle und regulatorische Konsequenzen nach sich ziehen können.
- **Personalrisiken.** Der Fachkräftemangel ist eines der drängendsten Probleme in der Energiebranche. Besonders betroffen sind IT-Sicherheits- und Netzbetriebsteams, die aufgrund des zunehmenden Bedarfs an qualifiziertem Personal oft unterbesetzt sind. Der Verlust von Know-how durch Pensionierungen oder Abwanderungen in andere Branchen verschärft die Situation. Fehlbesetzungen oder unzureichend geschultes Personal können dazu führen, dass wichtige Kontrollmechanismen nicht korrekt umgesetzt werden. Schulungsprogramme und Wissensmanagement sind daher von zentraler Bedeutung, um diese Risiken zu minimieren.
- **Beschaffungsrisiken.** Schwankende Energiepreise, geopolitische Entwicklungen und regulatorische Vorgaben erschweren die Beschaffung. Erneuerbare Energien stehen nicht immer bedarfsgerecht zur Verfügung, und Importabhängigkeiten bergen zusätzliche Risiken. Fehlprognosen können teure Nachkäufe oder Überschüsse verursachen. Viele EVUs setzen auf diversifizierte Beschaffungsstrategien und datenbasierte Analysen, um Marktentwicklungen besser vorherzusehen. Engpässe bei kritischen Komponenten wie Transformatoren können zudem Bauprojekte verzögern.
- **Energieversorgungsrisiken.** Die Kernaufgabe der EVUs bleibt die sichere Energieversorgung. Doch durch extreme Wetterereignisse, geopolitische Unsicherheiten und schwankende Nachfrage wird diese Aufgabe zunehmend komplexer. Im Winter 2022 stand die Schweiz kurz vor einer Energiemangellage, die durch knappe Gaslieferungen und stark gestiegene Preise verschärft wurde. Blackout-Szenarien sind nicht mehr rein theoretisch, sondern realistische Bedrohungen, die eine effektive Notfallplanung und resiliente Infrastruktur erfordern.
- **Compliance-Risiken.** Die zunehmende Regulierungsdichte führt dazu, dass EVUs neue Vorschriften oft nicht rechtzeitig erkennen und unbewusst dagegen verstossen. Besonders Umweltauflagen, Netzregulierung und Datenschutz unterliegen ständigen Anpassungen, deren Missachtung finanzielle oder reputative Folgen haben kann. Auch mutwillige Verstösse wie Korruption oder Interessenkonflikte bleiben ein Risiko. Sie können rechtliche Konsequenzen nach sich ziehen und das Vertrauen von Kunden und Behörden schädigen. Klare Compliance-Regeln und Schulungen helfen, sowohl unbeabsichtigte als auch vorsätzliche Verstösse zu vermeiden.

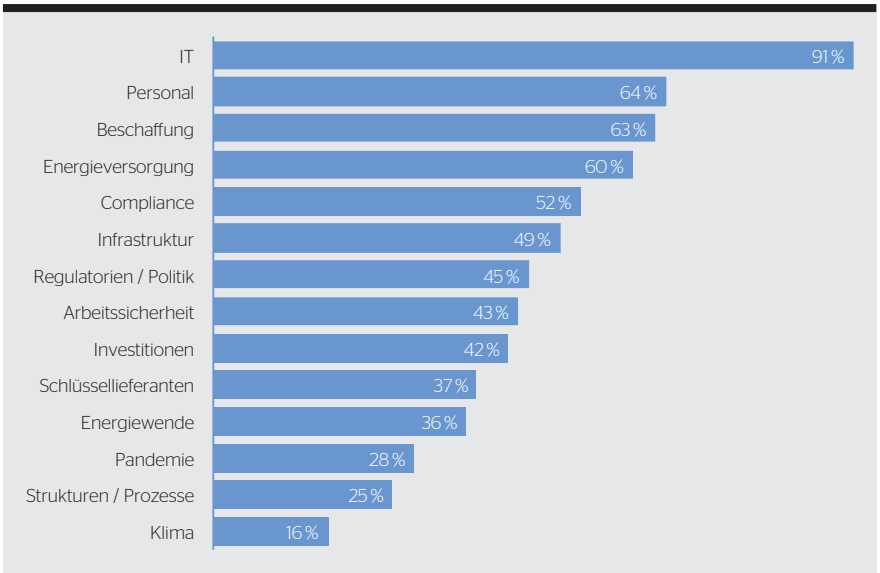

Bild 1 Die zentralen Risiken und Trends bei Energieversorgungsunternehmen.

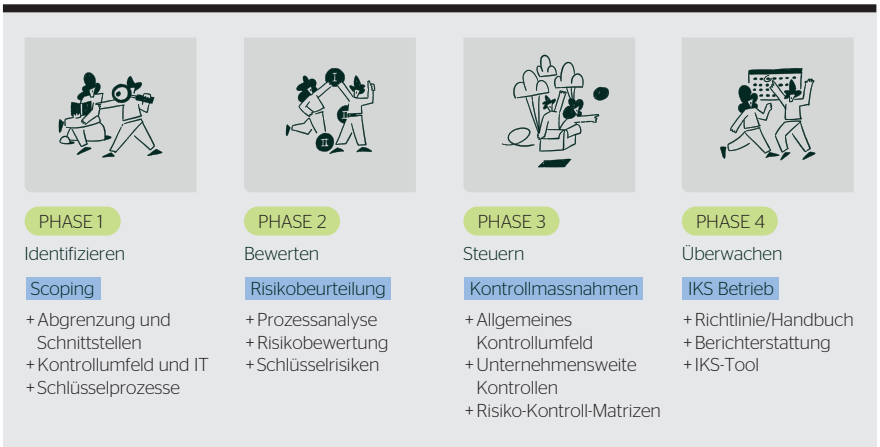

Bild 2 Die Einführungsphasen beim internen Kontrollsystem.

Bilder: i-Risk

Diese fünf Risikofelder, die jeweils von über 50 % der befragten Unternehmen als zentral eingestuft wurden, machen deutlich, dass die Energiebranche mehr denn je auf flexible und dynamische Kontrollsysteme angewiesen ist. Nur so lassen sich sowohl bestehende als auch neu entstehende Risiken effektiv bewältigen.

Viele EVUs verfügen über ein internes Kontrollsystem (IKS), das oft nicht mit der Weiterentwicklung des Unternehmens Schritt hält. Prozesse, Verantwortlichkeiten und Strukturen verändern sich, während das IKS unverändert bleibt. Dadurch entstehen Schwachstellen, die erst bei Problemen offensichtlich werden.

Die vier Phasen eines dynamischen IKS

Ein dynamisches internes Kontrollsystem (IKS) basiert auf einem kontinuierlichen Prozess, der in vier zentrale Phasen unterteilt ist **(Bild 2)**. Diese Phasen helfen EVUs dabei, Risiken systematisch zu erfassen, zu bewerten, zu steuern und kontinuierlich zu überwachen. Anders als statische Kontrollsysteme wird ein dynamisches IKS regelmässig an neue Bedingungen angepasst und durchläuft diesen Prozess zyklisch.

Identifizieren: Den Umfang bestimmen und Risiken aufspüren. Die erste Phase beginnt mit dem sogenannten Scoping, also der Festlegung des Anwendungsbereichs des IKS. Dabei wird entschieden, welche Geschäftsprozesse und Kontrollbereiche in das System einbezogen werden. Die Granularität der Analyse hängt von der Komplexität und der Wesentlichkeit der Prozesse ab. Mittels Wesentlichkeitsanalysen werden die kritischen Prozesse priorisiert.

Beispiel: In der Identifikationsphase wird bei einem EVU der Prozess Energiebeschaffung aufgrund seiner finanziellen Relevanz meist als Schlüsselprozess identifiziert und genauer untersucht. Dabei werden die internen Abläufe, Schnittstellen zu anderen Prozessen wie Netzsteuerung oder IT sowie externe Abhängigkeiten von Lieferanten und schwankenden Marktpreisen erfasst. Da die IT und ihre Systeme mittlerweile bei fast jedem Arbeitsschritt eine Rolle spielen, wird die IT-Umgebung per se heutzutage als IKS-Schlüsselthema verstanden.

Bewerten: Risiken analysieren und Schwerpunkte setzen. In der Bewertungsphase erfolgt eine detaillierte Analyse der identifizierten Prozesse. Dabei werden potenzielle Schwachstellen identifiziert, und es wird abgeschätzt, wie wahrscheinlich das Eintreten eines bestimmten Risikos ist und welche Auswirkungen es auf das Unternehmen haben könnte. Die wichtigsten Risiken werden als sogenannte Schlüsselrisiken klassifiziert.

Beispiel: Im Bereich der IT-Sicherheit eines EVUs wird im Rahmen der Bewertungsphase festgestellt, dass veraltete Zugangsrichtlinien und unzureichend geschulte Mitarbeitende ein hohes Risiko für Cyberangriffe darstellen. Die Eintrittswahrscheinlichkeit eines solchen Angriffs wird als hoch eingestuft, und die potenziellen Auswirkungen reichen von finanziellen Verlusten bis zur Beeinträchtigung der Stromversorgung.

Steuern: Massnahmen zur Risikominderung entwickeln. Basierend auf den identifizierten und bewerteten Risiken werden gezielte Kontrollmassnahmen entwickelt und implementiert. Für jedes Schlüsselrisiko wird mindestens eine spezifische Kontrolle definiert, die darauf abzielt, das Risiko zu minimieren oder zu eliminieren. Dabei können sowohl technische als auch organisatorische Massnahmen zum Einsatz kommen.

Beispiel: Um das Risiko eines IT-Ausfalls durch Cyberangriffe zu verringern, implementiert das EVU mehrere Massnahmen: eine Zwei-Faktor-Authentifizierung, regelmässige Penetrationstests und Schulungen der Mitarbeitenden zur Erhöhung des Sicherheitsbewusstseins. Im Bereich der Energiebeschaffung wird ein automatisiertes Monitoring-System eingeführt, das Preisänderungen und Lieferengpässe frühzeitig erkennt.

Überwachen: Kontrollen evaluieren und anpassen. In der letzten Phase wird sichergestellt, dass die implementierten Kontrollmassnahmen wirksam sind und bleiben. Dies erfolgt durch eine regelmässige Überprüfung der Kontrolldurchführung sowie Beurteilung der Kontrollwirkung. Klare Verantwortlichkeiten müssen definiert sein, um sicherzustellen, dass vom Zielwert abweichende Feststellungen frühzeitig erkannt und behoben werden können.

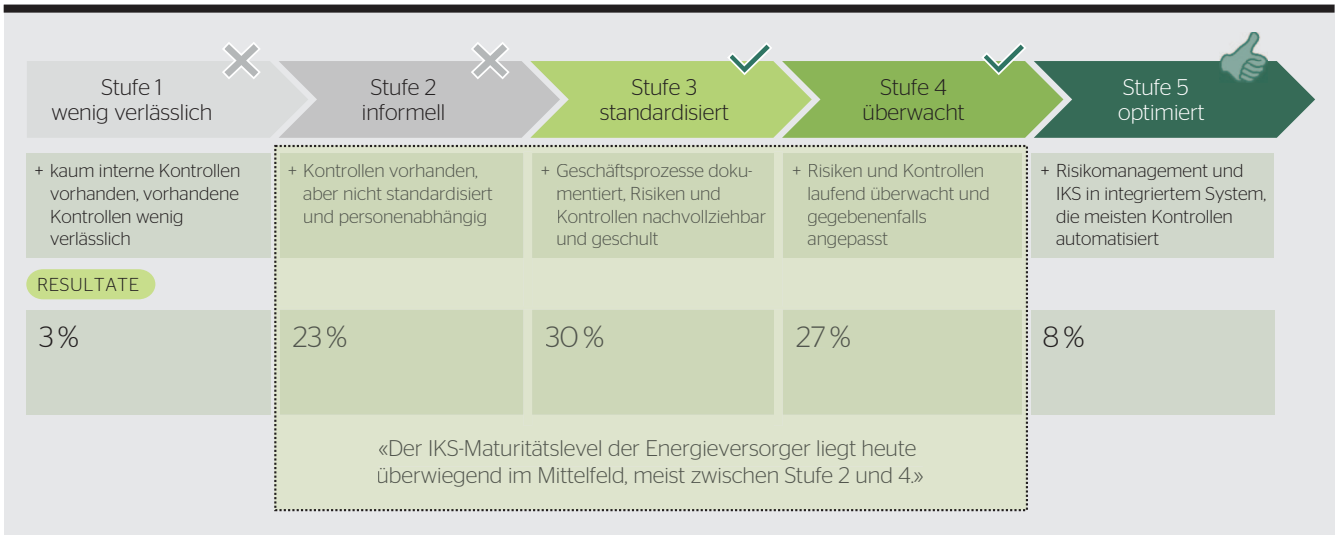

Bild 3 Maturitätslevel des internen Kontrollsystems von Unternehmen.

Beispiel: Ein Dashboard zur Echtzeitüberwachung der IT-Sicherheitsmassnahmen gibt dem Management einen umfassenden Überblick über den Status aller relevanten Kontrollen. Fällt eine Kontrolle aus oder wird eine Schwachstelle entdeckt, wird dies automatisch gemeldet, sodass sofortige Korrekturmassnahmen eingeleitet werden können.

Doch selbst ein gut strukturiertes IKS kann seine Grenzen haben. In vielen Unternehmen zeigt sich, dass Kontrollmechanismen zwar vorhanden sind, aber nicht immer effektiv greifen.

Die Maturitätsstufen: Wo stehen Schweizer EVUs?

Ein modernes IKS entwickelt sich über mehrere Reifegrade, die sogenannten Maturitätsstufen **(Bild 3)**. Diese beschreiben, wie gut die Kontrollmechanismen in den operativen und strategischen Prozessen des Unternehmens verankert sind:

- **Stufe 1:** Wenig verlässlich – Es gibt kaum dokumentierte Kontrollen. Risiken werden situativ oder ad hoc behandelt. Entscheidungen hängen stark von individuellen Einschätzungen ab. Es fehlen klare Prozesse oder Leitlinien.
- **Stufe 2:** Informell – Es existieren Kontrollen, die jedoch nicht systematisch dokumentiert oder standardisiert sind. Die Umsetzung ist stark personenabhängig. Es mangelt an Schulungen oder strukturierten Überprüfungen.
- **Stufe 3:** Standardisiert – Die wesentlichen Prozesse sind dokumentiert und Risiken werden systematisch identifiziert und bewertet. Kontrollmassnahmen sind zwar definiert, werden jedoch nicht immer umfassend überwacht.
- **Stufe 4:** Überwacht – Es gibt strukturierte Überwachungsmechanismen, um die Wirksamkeit der Kontrollen sicherzustellen. Dabei werden Risiken und Massnahmen kontinuierlich evaluiert und bei Bedarf angepasst.
- **Stufe 5:** Optimiert – Das IKS ist vollständig integriert und automatisiert. Es arbeitet eng mit dem Risikomanagement zusammen und passt sich dynamisch an veränderte Rahmenbedingungen an. Die Kontrollen sind weitgehend digitalisiert und der Fokus liegt auf kontinuierlicher Verbesserung.

Die meisten Schweizer EVUs befinden sich derzeit zwischen Stufe 2 und 4 **(Bild 3)**. Die Ergebnisse der aktuellen i-Risk-Studie zeigen, dass viele Unternehmen zwar über standardisierte und dokumentierte Prozesse verfügen, jedoch häufig Schwierigkeiten haben, diese kontinuierlich zu überwachen und anzupassen. Besonders im Bereich der IT-Sicherheit und der Beschaffung zeigt sich, dass dynamische Kontrollmechanismen fehlen, um auf plötzliche Veränderungen oder überraschende externe Schocks schnell zu reagieren.

Fazit: Ein IKS, das mit den Risiken wächst

In einer zunehmend vernetzten Welt ist es unvermeidlich, dass sich die Risiken weiterentwickeln. EVUs, die darauf vorbereitet sind und ihr IKS kontinuierlich anpassen, werden nicht nur besser geschützt sein, sondern auch langfristig wettbewerbsfähig bleiben. Die Fähigkeit, Risiken zu kontrollieren, wird zu einem entscheidenden Erfolgsfaktor – nicht nur für die Sicherheit, sondern auch für die Zukunftsfähigkeit der gesamten Energiebranche. Denn in einer vernetzten Welt gewinnt nicht derjenige, der Risiken vermeidet – sondern derjenige, der sie beherrscht.

Referenz

[1] Eric Montagne et al., «Risiken der Energiebranche – in einer vernetzten Welt», Präsentation bei den Betriebsleitertagungen des VSE 2024.

Autoren

Dr. **Eric Montagne** ist Gründer und Partner der i-Risk GmbH.
→ i-Risk GmbH, 8005 Zürich
→ eric.montagne@i-risk.ch

Mario Köpfli ist Partner der i-Risk GmbH.
→ mario.koepfli@i-risk.ch

RÉSUMÉ

Vers la résilience numérique

Systèmes de contrôle interne pour les EAE

Depuis 2021, i-Risk mène chaque année une étude, en collaboration avec l'AES, afin d'analyser les risques pour les entreprises d'approvisionnement en énergie (EAE). Les résultats de ces enquêtes montrent à quel point les conditions-cadres ont changé ces dernières années, et mettent en évidence les risques les plus importants pour le secteur. Les risques informatiques arrivent en tête : la digitalisation croissante fait de la sécurité informatique l'un des principaux enjeux pour les EAE. Viennent ensuite les risques liés au personnel : la pénurie de main-d'œuvre qualifiée est l'un des problèmes les plus urgents dans le secteur de l'énergie. Les équipes chargées de la sécurité informatique et de l'exploitation du réseau sont particulièrement touchées. En troisième position viennent les risques liés aux acquisitions : la fluctuation des prix de l'énergie, les développements géopolitiques et les exigences réglementaires les rendent difficiles. Les risques liés à l'approvisionnement en énergie arrivent en quatrième position : la mission principale des EAE reste de garantir un approvisionnement énergétique sûr, mais les événements météorologiques extrêmes, les incertitudes géopolitiques et la fluctuation de la demande rendent cette tâche de plus en plus complexe. Enfin, les risques en matière de conformité arrivent en cinquième position : la densité réglementaire croissante a pour conséquence que les EAE ne reconnaissent souvent pas à temps les nouvelles réglementations, telles que celles liées aux exigences environnementales, à la régulation du réseau et à la protection des données, et les enfreignent inconsciemment.

Ces cinq domaines à risque, considérés comme essentiels par plus de 50 % des entreprises interrogées, montrent clairement que le secteur de l'énergie a plus que jamais besoin de systèmes de contrôle dynamiques et flexibles. C'est la seule façon de maîtriser efficacement les risques existants et émergents.