Newsletter

Liebe Kunden und Geschäftspartner,

vermutlich sind wir alle diesmal recht winterlich ins neue Jahr gestartet. Da hilft es oft, vorausschauend zu handeln, gut vorbereitet zu sein und möglichst immer die richtige Ausrüstung dabei zu haben. Fast genauso ist es auch bei den zahlreichen Neuerungen, Veränderungen, Anpassungen und Learnings in den Bereichen Regulatorik, Prüfungen, Audits usw.

Wir möchten einen Beitrag leisten, Sie dabei stets gut zu informieren und zu unterstützen. Wenn wir daneben auch davon berichten, was uns intern so bewegt und umtreibt, wie diesmal z. B. unsere Herzensprojekte und die Bowling-Highlights beim Jahresauftakt, menschelt es etwas, was bei teilweise sehr langjährigen und persönlichen Beziehungen zu vielen von Ihnen mit Sicherheit auch dazugehört.

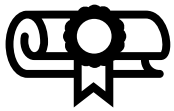
Im aktuellen und ersten Newsletter im Jahr 2026 informieren wir Sie gern zu folgenden Themen:

- ETL consit Akademie empfiehlt: Unsere Seminare, um Sachkunde herzustellen bzw. auffrischen
- Unsere Unterstützungsleistungen im Bereich ISM / DORA: Beratung, Notfallvorsorge, räumliche Sicherheit stärken!
- Neuerungen beim DIIR-Revisionsstandard Nr. 3 – dem Rahmen für externe Qualitätsbeurteilungen von Internen Revisionen
- DORA: Was beim Identitäts- und Rechtemanagement jetzt wichtig ist
- BaFin verschärft Fokus auf Finanzsanktionen – Prüfungen angekündigt!
- Interne Revision: Reagieren Sie zeitnah auf ein hochdynamisches Umfeld!
- NIS-2 im Gesundheitssektor – Sind Sie bereits betroffen?
- ♥ ♥ ♥ Herzensprojekte unserer Mitarbeitenden ♥ ♥ ♥
- Jahresauftakt in Bad Oldesloe

Herzliche Grüße

Bernd Schmid Oliver Gose

Die ETL consit Akademie empfiehlt: Unsere Seminare, um Sachkunde herzustellen bzw. auffrischen:



Aktuelles 2026 zu DORA - für Vorstände, Geschäftsführer, Aufsichts- und Verwaltungsräte

Neue Trends bei digitalen Bedrohungen: Es ist von entscheidender Bedeutung, sich stets über die neuesten Entwicklungen im Bereich digitaler Bedrohungen zu informieren. Dies ermöglicht es, die Dynamik dieser Themen zu verstehen und die potenziellen Auswirkungen auf das eigene Institut präzise zu beurteilen.

Entwicklung der Gesetzgebung: In erheblichem Umfang wurden sowohl Technische Regulierungsstandards (Regulatory Technical Standards - RTS) verabschiedet, welche die gesetzlichen Bestimmungen konkretisieren, als auch Technische Durchführungsstandards (Implementing Technical Standards - ITS). Diese ITS ergänzen die RTS, indem sie detaillierte Vorgaben zur praktischen Umsetzung der RTS enthalten, die zwingend eingehalten werden müssen, um die Anforderungen der RTS zu erfüllen.

Best Practice: Mittlerweile gibt es erste Erfahrungen aus der Praxis, die zeigen, was bislang gut gelaufen ist und was nicht so gut, und wo bzw. wie in Teilen evtl. noch nachgesteuert werden sollte. Diese bergen naturgemäß wertvolle Informationen, die sehr hilfreich für die DORA-Umsetzung im eigenen Hause sein können.

In diesem Seminar erhalten Sie als Vorstand, Geschäftsführer, Aufsichts- oder Verwaltungsrat die aktuellsten Informationen, und dies erneut in einem Format, welches speziell auf Entscheider ausgerichtet ist. Kompakt, übersichtlich, strikt auf das Wesentliche fokussiert. Nur nebenbei gilt es zu erwähnen, dass Sie mit einer Teilnahme an diesem Seminar natürlich Ihre Pflicht nach Artikel 5 Absatz 4 DORA erfüllen: „Die Mitglieder des Leitungsorgans … halten ausreichende Kenntnisse und Fähigkeiten aktiv auf dem neuesten Stand - unter anderem indem sie regelmäßig spezielle Schulungen absolvieren - entsprechend den zu managenden IKT-Risiken, um die IKT-Risiken und deren Auswirkungen auf die Geschäftstätigkeit des Finanzunternehmens verstehen und bewerten können.“

Zielgruppe:

Vorstände, Geschäftsführung, Aufsichts- und Verwaltungsräte von Finanzdienstleistungsunternehmen und von (IKT-) Dienstleistungsunternehmen, die Finanzdienstleistungsunternehmen zu ihren Kunden zählen

Preis und Termine

- **325,- EUR** zzgl. gesetzl. USt.
- 30.04.2026 Jetzt anmelden
- 21.07.2026 Jetzt anmelden
- 20.10.2026 Jetzt anmelden

NIS-2: Schulung für Vorstände und Geschäftsführer nach § 38 BSIG

Viele Unternehmen betroffen – Pflichten – Risiken – Empfehlungen

Mit der Umsetzung der NIS-2-Richtlinie in deutsches Recht Ende 2025 müssen deutlich mehr Unternehmen als zuvor umfangreiche **Anforderungen an die IT- und Cybersicherheit** erfüllen. Das neue Gesetz

- **erweitert den Kreis** der betroffenen Unternehmen **erheblich** und
- verschärft die **Pflichten, Haftungsrisiken und Sanktionsmöglichkeiten**.

In unserem Seminar erhalten Sie einen **kompakten und praxisorientierten Überblick** über die wesentlichen Inhalte des Gesetzes und erfahren, wie Sie die neuen Anforderungen rechtssicher und effizient umsetzen können.

- Überblick über die (EU-)NIS-2-Richtlinie und ihre gesetzgeberische Umsetzung
- Welche Unternehmen und Einrichtungen sind betroffen?
- Sicherheits-, Melde- und Nachweispflichten
- Rolle und Verantwortung des Vorstandes bzw. der Geschäftsführung
- Bußgelder, Haftungsrisiken und Durchsetzungsmechanismen
- Praktische Umsetzung - rechtssicher und effizient

- Sie verstehen, **ob und in welchem Umfang Ihr Unternehmen betroffen ist**
- Sie erhalten **konkrete Handlungsempfehlungen für die Umsetzung**
- Sie gewinnen Sicherheit im Umgang mit **Aufsichtsbehörden und Melde-pflichten**
- Sie können **Risiken frühzeitig erkennen und vermeiden**
- Sie erhalten ein **Zertifikat**, das Ihnen die Teilnahme nach § 38 BSIG bestätigt

Zielgruppe

Vorstände sowie Geschäftsführer, darüber hinaus begrüßen wir natürlich auch Verantwortliche aus den Bereichen IT- und Informationssicherheit, Compliance, Datenschutz und Risikomanagement sowie aus Rechtsabteilungen und Internen Revisionen.

Preis und Termine

- **325,- EUR** zzgl. gesetzl. USt.
- 25.03.2026 Jetzt anmelden
- 24.06.2026 Jetzt anmelden
- 24.09.2026 Jetzt anmelden
- 15.12.2026 Jetzt anmelden

KRITIS-Dachgesetz - Der All-Gefahren-Ansatz - Pflichten - Haftung der Vorstände und Geschäftsführer nach § 20 KRITIS-DachG

Vorstände und Geschäftsführer: Pflichten verstehen - Haftungsrisiken vermeiden

Das KRITIS-Dachgesetz (KRITIS-DachG) wird vorgeben, dass **Betreiber kritischer Anlagen** geeignete Maßnahmen zum Schutz dieser Anlagen zu treffen haben (sog. Resilienzmaßnahmen), die auf systematischen Risikoanalysen basieren - dies *zusätzlich* zu den Vorgaben der branchenspezifischen Spezialgesetze, die Vorständen und Geschäftsführerinnen/Geschäftsführer der entsprechenden Unternehmen natürlich bestens vertraut sind.

Dies bedeutet **umfangreiche Anpassungen von Prozessen, Organisation und Compliance-Strukturen**.

Unser Seminar vermittelt Ihnen **praxisnahes Wissen und konkrete Handlungs-empfehlungen**, um die gesetzlichen Anforderungen zuverlässig umzusetzen und Risiken zu minimieren.

- Sie kennen durch unser Seminar
  - die **konkreten Pflichten** aus dem KRITIS-DachG sowie
  - **Ihre Haftungsrisiken** als Vorstand bzw. Geschäftsführerin/ Geschäftsführer
- Sie erhalten **praxisnahe Handlungsempfehlungen** zur Umsetzung
- Sie können **Risiken frühzeitig identifizieren und vermeiden**
- Sie sind auf **Kontrollen und Prüfungen durch Behörden vorbereitet**
- Sie erhalten ein **Zertifikat**, das Ihnen die Teilnahme an diesem Seminar bestätigt

Zielgruppe

Vorstände sowie Geschäftsführer, darüber hinaus begrüßen wir natürlich auch Compliance-Verantwortliche, IT- und Informationssicherheitsbeauftragte, Risikomanager und Prüfer aus Internen Revisionen sowie Verantwortliche aus Rechtsabteilungen.

Preis und Termine

- **325,- EUR** zzgl. gesetzl. USt.
- 23.04.2026 Jetzt anmelden
- 28.07.2026 Jetzt anmelden
- 01.10.2026 Jetzt anmelden
- 08.12.2026 Jetzt anmelden

Unsere Unterstützungsleistungen im Bereich ISM / DORA: Beratung, Notfallvorsorge, räumliche Sicherheit stärken!

In jüngster Zeit haben mehrere spektakuläre Einbrüche in Schließfachanlagen deutscher Kreditinstitute für großes Aufsehen gesorgt. Besonders der Vorfall in einer großen Sparkasse in NRW im Dezember 2025 machte Schlagzeilen, als Täter mehr als **3.000 Schließfächer** penetrierten und Bargeld sowie Wertgegenstände im Wert von geschätzten **mehreren Millionen Euro** entwendeten. Die Täter verschafften sich über ein **nebenstehendes Parkhaus Zugang zum Tresorraum**, nutzten große/ professionelle Bohrmaschinen und operierten über mehrere Tage, vermutlich während der Weihnachtszeit, ohne rechtzeitig entdeckt zu werden.

Seitdem sind auch weitere Fälle in anderen Orten bekannt geworden. All dies zeigt, dass **Schließfachaufbrüche kein Einzelfall sind** – das unterstreicht die systemische Relevanz des Themas.

Auch wenn beim spektakulären Einbruchsfall in NRW eher „analog-physikalische“ Tatmethoden an den Tag gelegt wurden, gibt es im Zuge **zunehmender Digitalisierung** auch Fälle, in denen elektronische Zutritts- und Zugangssysteme von Self-Service-Schließfachanlagen durch „bewährte“ Methoden betrügerischer Täter wie **Skimming und Phishing** zur Erlangung entsprechender Schließfach-Informationen und Zugangsdaten genutzt werden. Darüber hinaus gehen **„trittbrettfahrende“ Zweittäter** inzwischen sogar so dreist vor, die öffentlichkeitswirksamen Anlässe zu nutzen, um sich als Bankmitarbeiter auszugeben und unter Bezugnahme auf die Vorgänge zu versuchen, gezielt an persönliche Information und Kontodaten zu gelangen.

Diese Vorfälle stellen Kreditinstitute vor erhebliche **Versicherungs- und Haftungsfragen, Reputationsrisiken sowie regulatorische Herausforderungen** (z. B. im Kontext des **Digital Operational Resilience Acts – DORA**) und erfordern **präventive Konzepte im Informationssicherheits- und Notfallmanagement.**

Wie kann die ETL consit helfen?

Wir bieten Ihnen Prüfungs- und Unterstützungsleistungen zur Stärkung der organisatorischen und technischen Sicherheit von Schließfachanlagen, insbesondere:

- Reduktion physischer und digitaler Risiken
- Erhöhung der Resilienz gegenüber komplexen Angriffen
- Erfüllung regulatorischer Anforderungen (z. B. ISM / DORA)
- Sicherstellung einer effektiven Notfall- und Krisenkommunikation

Entsprechende Audits im Bereich der Schließfächer können beleuchten, inwieweit sich Ihre getroffenen Maßnahmen (noch) auf dem Stand der Technik befinden und wo ggf. Handlungsbedarf besteht.

Schwerpunkte unserer ersten beauftragten Kundenaudits sind dabei Themenstellungen wie:

- Berücksichtigung der Lage/der räumlichen lokalen Gegebenheiten
- Berücksichtigung der Geschäftsstellensituation
- Betrachtung der Verträge mit Versicherung(en)
- Betrachtung der Verträge mit Wachunternehmen
- Betrachtung der elektronischen Detektions- und Meldesysteme
- Betrachtung der Zutritts- und Zugangskontrollmaßnahmen sowie des Internen Kontrollsystems
- Verfügbarkeit des Raumes/der Schließfachanlage für Kunden (nur zu Geschäftszeiten oder 24 Std.)
- Berücksichtigung der Maßnahmen zur Videoüberwachung

Warum jetzt handeln?

Die aktuellen Vorfälle haben gezeigt, dass klassische Schließfach-Sicherheitskonzepte physisch wie organisatorisch schnell an ihre Grenzen geraten können – auch bei zeitgemäßer technischer Ausstattung.

Ein integrativer Ansatz, der **Regulatorik, physische Sicherheit und Notfallvorsorge** verbindet, ist entscheidend für **bankenaufsichtsrechtliche Absicherung und zur Wahrung des Kundenvertrauens**.

Überprüfen Sie, ob und inwieweit sie angreifbar sein könnten, und **vermeiden Sie Reputationsschäden wie auch finanzielle Schäden** für Ihr Haus.

Wir unterstützen Sie gerne dabei!

Neuerungen beim DIIR-Revisionsstandard Nr. 3 – dem Rahmen für externe Qualitätsbeurteilungen von Internen Revisionen

Zum 15. Dezember 2025 wurde der DIIR-Revisionsstandard Nr. 3 grundlegend überarbeitet, um den Global Internal Audit Standards (GIAS) gerecht zu werden.

Was bedeutet das für Ihr Institut?

Die Neufassung des Standards betrifft insbesondere die Anforderungen an die Qualität und Wirksamkeit der Internen Revision. Gemeinsam mit dem IDW wurde der DIIR-Revisionsstandard Nr. 3 weiterhin eng an den IDW Prüfungsstandard PS 983 angelehnt, sodass beide Standards weitgehend deckungsgleich bleiben.

Die wichtigsten Änderungen im Überblick:

- **Stärkere Ausrichtung auf Wirksamkeit:** Die Interne Revision muss künftig nicht nur formal korrekt, sondern auch nachweislich wirksam sein. Das Quality Assessment wird zum zentralen Prüfstein.
- **Erweiterte Anforderungen an Kontroll- und Risikomanagementsysteme:** Die Vorgaben aus dem Gesetz zur Stärkung der Finanzmarktintegrität (FISG) wurden integriert. Damit steigen die Anforderungen an die Einrichtung und Prüfung interner Kontrollsysteme deutlich.
- **Neue Maßstäbe für die Qualitätsbeurteilung:** Sowohl interne als auch externe Assessments müssen sich künftig an den GIAS orientieren. Das betrifft Prozesse, Methoden und Dokumentation gleichermaßen.
- **Erhöhte Haftungsrelevanz für Organe:** Die Geschäftsleitung und der Aufsichtsrat stehen stärker in der Verantwortung, die Wirksamkeit der Internen Revision sicherzustellen – auch im Hinblick auf persönliche Haftungsrisiken.

Was sollten Sie jetzt tun?

- **Überprüfen Sie Ihr Internes Revisionssystem und passen Sie es ggf. an:** Entspricht es den neuen Anforderungen? Ist die Wirksamkeit dokumentiert und nachvollziehbar? Die neuen Standards verlangen deutlich mehr – sowohl inhaltlich als auch methodisch.
- **Sichern Sie sich externe Expertise:** Die Umsetzung der neuen Anforderungen ist komplex. Ein unabhängiger Blick kann helfen, Schwachstellen frühzeitig zu erkennen und regulatorische Risiken zu vermeiden.

Wenn Sie wissen möchten, wie Ihr Internes Revisionssystem im Lichte der neuen Standards abschneidet oder wenn Sie ein professionelles Quality Assessment wünschen, sprechen Sie uns gerne an. Gemeinsam sorgen wir dafür, dass Ihre Revision nicht nur regelkonform, sondern auch zukunftssicher aufgestellt ist.

DORA: Was beim Identitäts- und Rechtemanagement jetzt wichtig ist

Mit dem 17. Januar 2025 wurde die DORA endgültig verpflichtend – und damit wurden aus bisherigen aufsichtsrechtlichen Erwartungen (MaRisk, BAIT) verbindliche gesetzliche Regelungen. Besonders deutlich zeigt sich das im Identitäts- und Rechtemanagement. Die relevanten Anforderungen finden sich in mehreren Artikeln der DORA sowie konkretisiert im Technischen Regulierungsstandard zur Festlegung der Tools, Methoden, Prozesse und Richtlinien für das IKT-Risikomanagement und des vereinfachten IKT-Risikomanagementrahmens (delegierte Verordnung (EU) 2024/1774) in deren Artikeln 20 Identitätsmanagement und Artikel 21 Zugangskontrolle.

Parallel dazu hat die BaFin Anfang 2025 die entsprechenden Passagen in den MaRisk gestrichen und die BAIT quasi vollständig aufgehoben. Die Spielregeln kommen damit ausschließlich aus der DORA.

Worauf ist zu achten?

„Need-to-Use-Prinzip“

Berechtigungen dürfen nur vergeben werden, wenn sie *tatsächlich* für die jeweilige Aufgabe benötigt werden. Das klingt selbstverständlich – wird aber in der Praxis oft nicht konsequent umgesetzt.

Strengere Rezertifizierungsintervalle

Zugangs- und Zugriffsrechte müssen regelmäßig überprüft werden:

- **halbjährlich** für Systeme, die kritische oder wichtige Funktionen unterstützen
- **jährlich** für alle übrigen Systeme

Das bedeutet: Rollen und Berechtigungen dürfen nicht mehr „einmal eingerichtet – nie wieder angefasst“ bleiben.

Klare, vollständige Berechtigungskonzepte

Ein häufiges Problem aus Prüfungen der Deutschen Bundesbank: Institute verwechseln technische Sollrollenkonzepte mit einem vollständigen Berechtigungskonzept.

Ein technisches Rollenmodell *allein* erfüllt die regulatorischen Anforderungen nicht. Es bildet lediglich ab, was zuvor konzeptionell festgelegt wurde – ersetzt aber nicht das Konzept für die seitens des Instituts eingesetzten Anwendungen selbst.

Wie sieht ein vollständiges Berechtigungskonzept aus?

Ein wirksames und DORA-konformes Berechtigungskonzept besteht aus drei Ebenen:

1. Informationssicherheitsrichtlinie

Sie bildet das Fundament. Hier werden die Grundsätze des Identitäts- und Rechtemanagements festgelegt – unabhängig von konkreten Anwendungen oder Systemen.

2. Übergreifendes / übergeordnetes Berechtigungskonzept

Es übersetzt die Grundsätze in operative Regeln. Dazu gehören u. a.:

- Grundsätze der Rechtevergabe
- Prozesse für Beantragung, Genehmigung und Umsetzung
- Umgang mit verschiedenen Benutzerarten (interne/externe User, technische User, Administratoren)

- Anforderungen an die Funktionstrennung
- Verantwortlichkeiten im gesamten Berechtigungsprozess
- Logik zur Bildung von Rollen und Profilen
- Verfahren zur regelmäßigen Überprüfung und Rezertifizierung

Dieses Konzept gilt institutseinheitlich und bildet den Rahmen für alle Anwendungen und Standorte.

3. Anwendungs- bzw. standortbezogene Berechtigungskonzepte

Hier wird es konkret. Für jede Anwendung, jedes System und jeden Standort muss beschrieben werden:

Zugriffsrechte (IT-Anwendungen / IT-Systeme)

- Welche Benutzerarten existieren
- Wie Rechte vergeben werden (Einzelrechte, Profile)
- Welche Profile welchen Benutzerarten zugeordnet werden
- Welche toxischen Kombinationen es gibt und welche Funktionstrennungen einzuhalten sind
- Wer genehmigt, einrichtet und kontrolliert
- Wie die technische Administration erfolgt

Zutrittsrechte (Gebäude / Räume)

- Welche Zutrittsmedien genutzt werden
- Wie Ausgabe, Verwaltung und Rücknahme erfolgen
- Wer genehmigt einrichtet und kontrolliert
- Wie regelmäßig überprüft wird
- Welche Bereiche standortabhängig besonders geschützt werden müssen

Und wenn jetzt noch Fragezeichen bleiben?

Das Thema ist komplex – wenn Sie Unterstützung benötigen, sei es bei der Erstellung eines vollständigen Berechtigungskonzepts oder bei der Überprüfung Ihres bestehenden Konzepts im Rahmen eines Audits, sprechen Sie uns gerne jederzeit an. Gemeinsam sorgen wir dafür, dass Ihr Institut die gesetzlichen und regulatorischen Anforderungen sicher erfüllt.

BaFin verschärft Fokus auf Finanzsanktionen – Prüfungen angekündigt

Die BaFin legt derzeit einen deutlich verschärften Fokus auf die wirksame Umsetzung von Finanzsanktionen. Vor dem Hintergrund geopolitischer Entwicklungen und massiv ausgeweiteter Sanktionsregime hat die Aufsicht angekündigt, in einem Verbandsgebiet des DSGV **sämtliche Sparkassen einer Sonderprüfung zu unterziehen**.

Im Mittelpunkt stehen dabei insbesondere:

- Qualität und Reichweite des Sanktions-Screenings
- Aktualität der Datenquellen
- Klare Rollen, Verantwortlichkeiten und Eskalationswege
- Nachvollziehbare Bearbeitung von Treffern und False Positives

Die Aufsicht macht unmissverständlich klar: **Finanzsanktionen sind kein Unterthema der Geldwäscheprävention mehr**, sondern ein eigenständiges, hochrelevantes Compliance-Risikofeld. Fehler können zu erheblichen Reputationsschäden, aufsichtsrechtlichen Maßnahmen und empfindlichen Bußgeldern führen.

Aktueller Anlass: Durchsuchung bei der Deutschen Bank

Wie aktuell bekannt wurde, hat die Staatsanwaltschaft Frankfurt a. M. die Zentrale der Deutschen Bank sowie den Standort Berlin durchsuchen lassen. Hintergrund ist der **Verdacht der Geldwäsche**, u. a. im Zusammenhang mit mutmaßlich verspätet abgegebenen Verdachtsmeldungen zu Firmen eines unter EU-Sanktionen stehenden russischen Oligarchen. Der Fall unterstreicht, wie schnell Defizite bei Sanktionen, Monitoring und Meldewesen zu **straf- und aufsichtsrechtlicher Relevanz** führen können.

Was Institute jetzt tun sollten

Die angekündigten Prüfungen und aktuellen Ermittlungen senden ein klares Signal: Die Aufsicht erwartet **robuste, technisch und organisatorisch belastbare Lösungen** – keine „Best-Effort"-Ansätze**. Jetzt ist der richtige Zeitpunkt**, Prozesse, Systeme und Zuständigkeiten kritisch zu überprüfen:

- unabhängiger Review von Sanktions- und Screening-Prozessen
- gezielte Schwachstellenanalysen vor Sonderprüfungen
- Unterstützung bei Optimierung, Dokumentation und Schulung

Gerne unterstützen wir Sie kurzfristig und praxisnah – von der strukturierten Bestandsaufnahme bis zur prüfungssicheren Umsetzung. Sprechen Sie uns an, bevor die Prüfer vor der Tür stehen.

Unsere Newsletter-Reihe: Basis für eine moderne, erfolgreiche und akzeptierte Interne Revision

Interne Revision: Reagieren Sie zeitnah auf ein hochdynamisches Umfeld!

Die **Global Internal Audit Standards (**GIAS) setzen die Rahmenbedingungen für Interne Revisoren und sind als global anerkannte betriebswirtschaftliche Norm für alle Internen Revisionen verbindlich.

Gemäß Standard 9.2 muss die Revisionsleitung einen **Revisionsplan** erstellen, der das Erreichen der Organisationsziele unterstützt. Hierfür muss sie den Revisionsplan auf eine dokumentierte Beurteilung der Strategien, Ziele und **Risiken der Organisation** stützen. Diese Beurteilung muss mindestens jährlich durchgeführt werden.

Um auf Veränderungen in den Risiken der Organisation zu reagieren, sollte die Revisionsleitung ein Verfahren zur Ermittlung und Beurteilung wesentlicher, neuer und aufkommender Risiken entwickeln, die im Revisionsplan zu berücksichtigen sind.

Als eine Informationsquelle kann hierfür die **Studie „Risk in Focus 2026“** herangezogen werden, die seit 2017 jährlich vom Europäischen Dachverband der Revisionsinstitute (ECIIA) gemeinsam mit einer Reihe nationaler Revisionsinstitute in Europa herausgegeben wird, darunter auch das Deutsche Institut für Interne Revision (DIIR).

Die alljährliche Aufnahme der Risikolandschaft aus Sicht der Internen Revision in Europa erfolgt mit dem **Ziel**,

- die Sicht der befragten Revisoren, Vorstands- und Aufsichtsratsmitglieder auf aktuelle Risiken festzuhalten,
- Erkenntnisse über aktuelle Herausforderungen in namhaften europäischen Unternehmen und Organisationen abzubilden sowie
- Anregungen für die Prüfungsplanung zu geben.

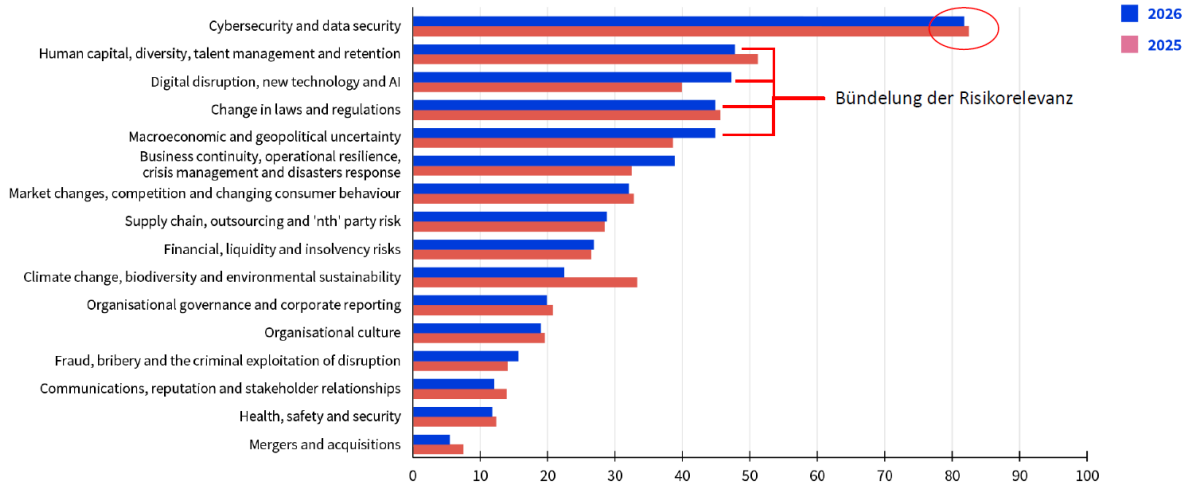
Hierzu wurden im vergangenen Jahr branchenübergreifend 879 europäische Revisionsleitungen in 15 Ländern sowie Mitglieder von Aufsichts- und Leitungsgremien, Wissenschaftlerinnen und Wissenschaftler sowie Branchenexpertinnen und -experten befragt.

Die **Top-4 Risiken** im Jahr 2026 sind:

- **Cybersicherheit und Datensicherheit** – bereits seit 2019 das größte Risiko, verschärft durch KI-basierte Angriffe und aktuelle Herausforderungen, u. a. geopolitische Situation, Fachkräftemangel.
- **Humankapital und Talentmanagement** – Fachkräftemangel, kurze Betriebszugehörigkeit, erwartete Arbeitsplatzflexibilität und KI-bedingte Kompetenzanforderungen sind die dominierenden Themen.
- **Digitale Disruption und Künstliche Intelligenz** – Unternehmen müssen die Chancen neuer Technologien nutzen und zugleich Risiken durch schnelle technologische Entwicklungen und mögliche Abhängigkeiten von einzelnen Anbietern managen.
- **Makroökonomische und geopolitische Unsicherheit** – Handelskonflikte, Zölle, Kriege und politische Instabilität prägen die Rahmenbedingungen und wirken sich auf zahlreiche andere Risikobereiche aus.

Trotz zunehmender Extremwetterereignisse ist das Thema **Klimawandel und Nachhaltigkeit** im Ranking auf den 10. Platz zurückgefallen. Lange Wirkungshorizonte und regulatorische Unsicherheit, z. B. das sog. Omnibus-Paket I, führen dazu, dass Klimarisiken aus dem Fokus geraten sind.

Insgesamt zeigen die Ergebnisse: Risiken sind stärker miteinander vernetzt als je zuvor. Damit wird es für Organisationen immer schwieriger, Strategien langfristig zu planen. Interne Revisionen sind daher gefordert, nicht nur Risiken aufzuzeigen, sondern auch als Sparringspartner der Unternehmensführung zu agieren. Der Trend geht klar zu einem stärkeren **Beratungsansatz**.



Die detaillierten Ergebnisse der Studie „Risk in Focus 2026“ können direkt beim DIIR abgerufen werden: [Risk in Focus (diir.de)]

Nutzen Sie die Ergebnisse der Studie als unverbindliche Hinweise und vergleichen Sie die genannten Risiken mit Ihrer eigenen Risikobeurteilung. Passen Sie auch die Revisionskapazitäten und die fachlichen Kompetenzen in den relevanten Themenfeldern an die Bedeutung der Risiken an. Wir unterstützen Sie gern bei der Bewältigung Ihrer Herausforderungen.

NIS-2 im Gesundheitssektor – Sind Sie bereits betroffen?

Wussten Sie, dass z. B. eine Arztpraxis bereits unter NIS-2 fallen könnte?

NIS-2 verändert die IT-Sicherheit auch im Gesundheitssektor grundlegend und viele Unternehmen haben das noch gar nicht bemerkt.

Die überraschende Wahrheit über NIS-2

Seit Dezember 2024 gilt die NIS-2-Richtlinie auch in Deutschland. Was viele nicht wissen: Es geht im Gesundheitssektor längst nicht nur um die großen Kranken-häuser. Die Regulierung erfasst mittlerweile auch:

- Arztpraxen mit mindestens 50 Mitarbeitenden oder Jahresumsätzen über 10 Millionen Euro
- MVZ-Verbünde und Ärztenetze ab dieser Größe
- Zahnarztkliniken und Dentallabore mit entsprechender Betriebsgröße
- Apotheken und Apothekenketten ab 10 Millionen Euro Umsatz
- Medizinische Labore und Diagnostikzentren
- Physiotherapie- und Reha-Einrichtungen mit 50+ Mitarbeitenden
- Medizinproduktehersteller und Arzneimitteldistributoren

Dazu kommen automatisch alle klassischen KRITIS-Betreiber wie Krankenhäuser mit 30.000+ vollstationären Fällen pro Jahr.

Warum ist das ein Problem?

Unternehmen, die unter NIS-2 fallen, müssen ab sofort stringente Cybersecurity-Anforderungen erfüllen, von technischen Schutzmaßnahmen über Incident-Response-Pläne bis hin zur persönlichen Haftung der Geschäftsführung. Nicht-Compliance kann zu erheblichen Bußgeldern führen.

Sind Sie betroffen?

Fragen Sie sich:

- Beschäftige ich mindestens 50 Personen?
- Liegt mein Jahresumsatz über 10 Millionen Euro?
- Betreibe ich eine kritische Gesundheitseinrichtung?

Bei einem Ja zu einer dieser Fragen, sind Sie wahrscheinlich bereits betroffen.

Wir unterstützen Sie!

Sie wissen nicht, wo Sie stehen? Sie benötigen eine Betroffenheitsanalyse, ein Audit oder die Implementierung von NIS-2-Maßnahmen?

Wir bieten Ihnen vollständige Unterstützung:

- Status-Check und NIS2-Reifegradanalyse (Gap-Analyse, Self-Assessment)
- Individuelle Beratung zu Governance, Technik, Organisation, Lieferkette und weiteren Themen
- Entwicklung und Begleitung von Maßnahmen-/Roadmaps
- Unterstützung bei Management-Review, Audit und Dokumentation
- Schulungen, Workshops und Awareness-Kampagnen
- Fortschrittstracking & Umsetzungskontrolle (regelmäßiges Reporting)

♥ ♥ ♥ Herzensprojekte unserer Mitarbeitenden ♥ ♥ ♥

Die ETL consit spendet jedes Jahr jeweils 250,- EUR an die Herzensprojekte ihrer Mitarbeiterinnen und Mitarbeiter. Gern stellen wir regelmäßig einige davon vor:

Bernd Schmid:

„Als Spendenempfänger habe ich CircArtive Pimparello (JuKi – Zukunft für Kinder und Jugendliche e. V.) ausgewählt. Der Verein verbindet Artistik mit Kinder- und Jugendarbeit. Im Rahmen der Arbeit werden verschiedene Veranstaltungen angeboten, in deren Rahmen Kinder und Jugendliche die Möglichkeit haben verschiedene „Zirkuskünste“ zu erlernen und dabei das Selbstvertrauen zu verbessern sowie einfach eine gute Zeit zu erleben. Die neu erlernten Fähigkeiten können dann in einem Auftritt entsprechend gezeigt werden. Es ist immer wieder eine Freude zu sehen, wie stolz die Kinder und Jugendlichen sind, hier ihre neu erlernten Fähigkeiten zu präsentieren. Das Foto ist im letzten Sommer im Rahmen der „Stadtranderholung“ entstanden, bei der ich dem Abschlussauftritt beiwohnen durfte.“

Claas Müller:

„Mit der Spende der ETL consit konnte die Badmintonabteilung des TV Datteln 09 u. a. die Weihnachtsfeier der Badmintonkids gestalten. Neben einem Schleifchenturnier, an dem auch die Eltern der Kinder teilgenommen haben, sorgten weitere kleine Aktionen und Spiele für einen kurzweiligen und sportlichen Abend. Zum Abschluss gab es Getränke und die im Ruhrgebiet allseits beliebte Currywurst zur Stärkung.“

Jahresauftakt in Bad Oldesloe

Am 09. Januar 2026 war es wieder soweit – das traditionelle Jahresauftakttreffen der ETL consit fand statt. Ein perfekter Anlass, um das vergangene Jahr Revue passieren zu lassen, Erfolge zu feiern und einen Ausblick auf die kommenden Herausforderungen zu wagen.

Im Mittelpunkt stand der persönliche Austausch unter den Kolleginnen und Kollegen. Bei leckerem Essen und entspannten Gesprächen wurde viel gelacht und gefachsimpelt.

Zum krönenden Abschluss ging es, ebenfalls fast schon traditionell, zum allseits beliebten Bowling, wo der Teamgeist gestärkt und der Abend in geselliger Runde ausklang. Sven Lammers hob seine herausragenden Beraterfähigkeiten auch hierbei hervor, da auf magische Weise jeder Mitspielende sofort einen Strike warf, nachdem ihm Sven die richtige Bowlingkugel empfahl, Chapeau!!

ETL consit - Immer eine gute Idee… Sprechen Sie uns gerne an!

Ihre Ansprechpartner

Bernd Schmid
Geschäftsführer

Telefon (04531) 66 96-28
Mobil (0160) 90 17 50 68
bernd.schmid@etl-consit.de

Oliver Gose
Mitglied der Geschäftsführung

Telefon (04531) 66 96-422
Mobil (0162) 372 42 17
oliver.gose@etl-consit.de

ETL consit GmbH

Schützenstraße 25a
23843 Bad Oldesloe
Telefon (04531) 66 96-0
Fax (04531) 66 96-45
info@etl-consit.de
www.etl-consit.de