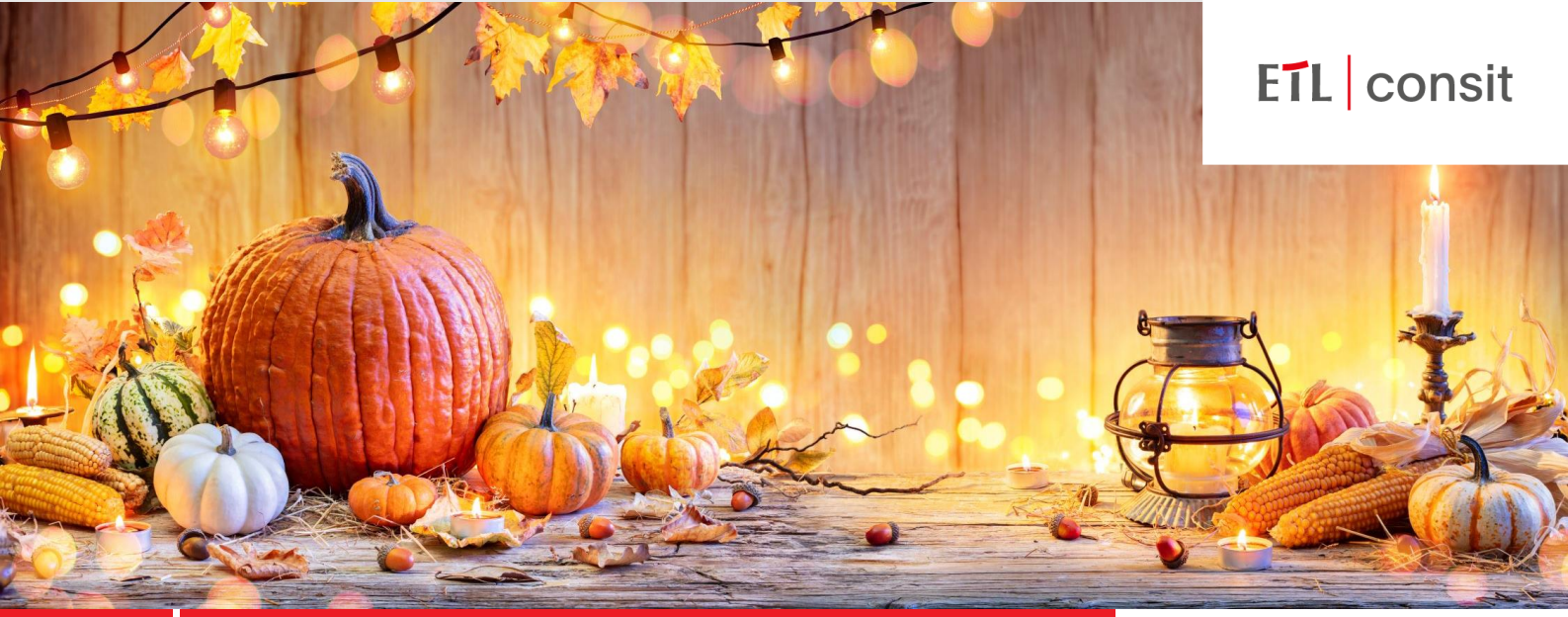


Newsletter

Liebe Kunden und Geschäftspartner,

für uns alle hat mit dem vierten Quartal wieder einmal die Jahresendrallye der Restarbeiten des Jahres begonnen.

Wir waren in den letzten Wochen außerdem auf verschiedenen Veranstaltungen und Treffen aktiv und bereiten uns, vermutlich genau wie Sie, auch auf die Aktivitäten und Herausforderungen des kommenden Jahres vor.

Gern würden wir Sie dabei wieder umfangreich unterstützen und die erfolgreiche Zusammenarbeit mit Ihnen auf den vielen gemeinsamen Ebenen fortsetzen.

In unserem herbstlichen Newsletter haben wir wieder einen bunten Strauß aktueller und wichtiger Themen für Sie mitgebracht:

- ETL consit auf dem Sparkassenprüfertag 2025 in Dresden
- Prüfungsplanung 2026 – Die Interne Revision vor den sich jährlich wiederholenden bzw. immer auch neuen Herausforderungen
- Cyberangriffe: Milliardenkosten und wachsende Risiken für Unternehmen
- Topical Requirement zum Drittparteienrisiko: Ein umfassender Leitfaden für die Interne Revision
- Gleich mal reinschauen: Das Seminar-Programm 2026 der ETL consit!
- Hamburger Karrieretag 2025
- Berater- und Revisorentreffen der ETL consit – Zwei Städte, ein Spirit!
- Neues Modul Datenschutzmanagement bei bit-Compliance!

Herzlichst

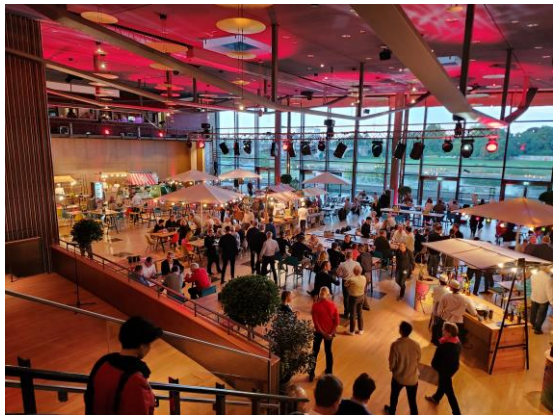
Bernd Schmid Oliver Gose

ETL consit auf dem Sparkassenprüfertag 2025 in Dresden

Am 23. und 24. September 2025 fand der Sparkassenprüfertag in Dresden statt. Zahlreiche Revisorinnen und Revisoren aus der Sparkasse-Finanzgruppe fanden sich zum kollegialen Austausch zu Fachthemen und Entwicklungen in der Internen Revision sowie zum Netzwerken ein.

Als Aussteller und Dienstleister für Revisionsunterstützung konnten wir viele bekannte und auch neue Gesichter begrüßen und vor Ort Präsenz zeigen. Angelockt von gefüllten Überraschungstassen (oder vielleicht auch der Schoki ;-)) kamen viele Besucherinnen und Besucher zu unserem Stand. Alexander Heffel und Oliver Gose führten viele interessante Gespräche und konnten auch konkrete Wünsche nach künftiger Prüfungsunterstützung mitnehmen.

Am Abend lud der DSGV dann zu einem bunten Markttreiben mit sächsischen Spezialitäten ein.



Prüfungsplanung 2026 – Die Interne Revision vor den sich jährlich wiederholenden bzw. immer auch neuen Herausforderungen

Im vierten Quartal beginnt für die Interne Revision in den Instituten traditionell die Zeit, in der die letzten Aufgaben der aktuellen Prüfungsplanung bewältigt werden müssen, und gleichzeitig die Prüfungsplanung des kommenden Jahres in den Fokus rückt. Es ist so etwas wie der ewige Kreislauf für die zuständige Leitung.

Was muss im neuen Prüfungsplan bedacht werden? Als Stichworte seien exemplarisch Internes Kontrollsystem, Schwachstellenanalyse des Hauses, Reaktionsketten und Risikoindikatoren genannt, um die Planung gut zu optimieren und an alle internen und externen Veränderungen anzupassen.

Erfahrungsgemäß sind die verfügbaren Ressourcen dabei ein knappes Gut und stoßen schnell an Grenzen!

Unsere erfahrenen Spezialisten unterstützen Sie weiterhin gern, sowohl bei komplexen Themenstellungen als auch, wenn dauerhaft oder temporär Ausfälle kompensiert werden müssen, oder im Co-Sourcing für neue Kollegen Unterstützung benötigt wird.

Planen Sie mit uns gern frühzeitig Ihre individuelle Bedarfssituation für 2026 und profitieren Sie dadurch von noch attraktiveren Gestaltungsmöglichkeiten und Angeboten.

Cyberangriffe: Milliardenkosten und wachsende Risiken für Unternehmen

289 Milliarden Euro Schaden in nur zwölf Monaten

Laut einer Umfrage des Digitalverbands bitkom unter 1.000 Unternehmen aus verschiedensten Branchen entstanden der deutschen Wirtschaft allein im letzten Jahr Schäden in Höhe von **289,2 Milliarden Euro** durch Datendiebstahl, Industriespionage und Sabotage.

Davon gehen **rund 200 Milliarden Euro direkt auf Cyberangriffe** zurück. Zum Vergleich: Der Bundeshaushalt 2025 beläuft sich auf 500 Milliarden Euro.

Die Kosten entstehen nicht nur durch direkte Ausfälle oder Ersatzmaßnahmen, sondern auch durch Erpressungen, Rechtsstreitigkeiten und Umsatzeinbußen durch verlorene Wettbewerbsvorteile oder Plagiate.

Wer steckt hinter den Angriffen?

Laut bitkom berichten neun von zehn Unternehmen (87 %) von Diebstahl, Spionage oder Sabotage.

- **68 %** der Attacken lassen sich auf organisierte Kriminalität zurückführen.
- **28 %** wurden ausländischen Nachrichtendiensten zugeordnet.
- Besonders häufig werden **China und Russland** als Ursprungsländer genannt – **46 %** der betroffenen Unternehmen waren Angriffen aus diesen Staaten ausgesetzt.

Lösegeldforderungen für jedes Dritte Unternehmen

34 % der Unternehmen waren laut bitkom bereits mit Erpressung durch verschlüsselte Daten konfrontiert.

- Jedes siebte Unternehmen (**15 %**) zahlte bereits Lösegeld.
- Weitere **15 %** wollten oder konnten dazu keine Angaben machen – ein Hinweis darauf, dass die Dunkelziffer höher liegen könnte.

Frühzeitige Investitionen in IT-Sicherheitsmaßnahmen verringern die Wahrscheinlichkeit, in diese Zwangslage zu geraten.

Investitionen in IT-Sicherheit: Licht und Schatten

Deutsche Unternehmen investieren laut bitkom im Durchschnitt 18 % ihres IT-Budgets in Sicherheit – knapp unter der Empfehlung von 20 %.

- **41 %** der Unternehmen liegen über 20 %.
- **40 %** investieren zwischen 10 und 20 %.
- **8 %** zwischen 5 und 10 %.
- **2 %** unter 5 %.

Die Unterschiede zeigen: Während einige Unternehmen gut aufgestellt sind, haben andere erheblichen Nachholbedarf.

Angriffe auf die Lieferkette: Eine unterschätzte Gefahr

Cyberangriffe betreffen nicht nur die großen Konzerne. Immer häufiger geraten Zulieferer und Dienstleister ins Visier.

Ein aktuelles Beispiel: Der Ransomware-Angriff auf **Collins Aerospace** im September führte zu massiven Störungen an europäischen Flughäfen wie Berlin, Brüssel, Dublin und London Heathrow. Check-in und Gepäckaufgabe waren zeitweise unmöglich, Bordkarten mussten handschriftlich ausgestellt werden, Starts und Landungen fielen aus.

Umgekehrt können Angriffe auf große Unternehmen auch Zulieferer treffen: **Jaguar Land Rover** musste nach einer Cyberattacke Ende August die Produktion bis 1. Oktober 2025 stoppen. Der Verlust für das Unternehmen: **rund 138 Millionen Euro** – von dem Unternehmen sind nicht nur 30.000 Beschäftigte, aber auch Zehntausende Beschäftigte bei den Zuliefererunternehmen abhängig.

Was Unternehmen jetzt tun sollten

Diese Beispiele zeigen: IT-Sicherheit ist nicht nur ein Schutzschild für das eigene Geschäft, sondern auch ein **entscheidender Faktor für die Zuverlässigkeit in der Lieferkette.**

Unternehmen sollten sich fragen:

- Welche Vorsichtsmaßnahmen ergreifen unsere Dienstleister?
- Wie stark wären wir betroffen, wenn ein Partner ausfällt?

Hier greift der **Digital Operational Resilience Act (DORA)** der EU. Er verpflichtet Banken und Versicherungen, das IKT-Sicherheitsmanagement und die Steuerung ihrer Dienstleister streng zu regeln.

Unsere Unterstützung

Wir beraten Sie umfassend zur Umsetzung von DORA in Ihrem Unternehmen. Darüber hinaus stehen wir Ihnen mit **unserem Notfallmanagement und erfahrenen Notfallbeauftragten** bei akuten Vorfällen jederzeit zur Seite.

Weiterführende Informationen

Cyberangriff auf Flughafensysteme: Nur Spitze des Eisbergs – Deutschlandfunk

Russland und China im Visier – bitkom

Festnahme nach Cyberangriffen auf Flughäfen – tagesschau.de

Jaguar Land Rover verlängert Produktionsstopp – Spiegel

Aus unserer Reihe: Basis für eine moderne, erfolgreiche und akzeptierte Interne Revision

Topical Requirement zum Drittparteienrisiko: Ein umfassender Leitfaden für die Interne Revision

International Professional Practices Framework® (IPPF)

Topical Requirements formulieren als Bestandteil der Internationalen Grundlagen für die berufliche Praxis (IPPF - International Professional Practices Framework) klare Erwartungen an die Internen Revision, indem sie einen Mindestrahmen für die Prüfung bestimmter Risikothemen vorgeben. Die Einhaltung ist für Prüfungsleistungen verbindlich.

(Quelle IIA)

Das Topical Requirement zum Drittparteienrisiko ist seit dem 15. September 2025 offiziell gültig und bietet einen einheitlichen Ansatz zur Bewertung der Governance, des Risikomanagements und der Kontrollprozesse im Umgang mit externen Dienstleistern. Eine Anwendbarkeit ist gegeben, wenn ein Drittparteienrisiko im Prüfungsplan der internen Revision enthalten ist, bei einer Prüfung identifiziert wird oder bei einer Sonderprüfung, die nicht im ursprünglichen Prüfungsplan enthalten war.

Als Drittpartei wird eine externe Einzelperson, Gruppe oder Einrichtung definiert, mit der eine Organisation eine Geschäftsbeziehung aufbaut, um Produkte oder Dienstleistungen zu erhalten. Die Beziehung kann durch einen Vertrag, eine Vereinbarung oder auf andere Weise formalisiert werden, um der Organisation Produkte, Dienstleistungen, Arbeitskräfte, Fertigung oder IT-Lösungen, wie z. B. Datenspeicherung, -verarbeitung und -pflege, zur Verfügung zu stellen.

Kernpunkte des neuen Topical Requirements

Mit dem neuen Topical Requirement werden für den Berufsstand der Internen Revision klare Anforderungen für eine effektive und strukturierte Prüfung von Drittparteien definiert. Wichtige Bestandteile sind hierbei:

- **Governance zum Einsatz von Drittparteien:** Prüfung der Governance-Strukturen zur Auswahl, Überwachung und Kommunikation mit Drittparteien (Richtlinien, Aufgaben und Zuständigkeiten). Zentral ist Frage der Steuerung der Drittanbieterbeziehung während des gesamten Lebenszyklus der Beauftragung. Eine regelmäßige Berichterstattung über Risiken und Schwachstellen ist essenziell, damit das Management fundierte Entscheidungen treffen kann.

- **Effektives Risikomanagement:** Prüfung standardisierter Prozesse zur fortlaufenden Identifizierung, Bewertung und Steuerung von Risiken im Zusammenhang mit Drittparteien über den gesamten Lebenszyklus. Die Risikobewertung umfasst dabei strategische, finanzielle, operationelle, ethische, rechtliche und andere relevante Risiken (u. a. IT, Cybersicherheit, Compliance, Nachhaltigkeit). Maßnahmen zur Risikoreaktion und Eskalationsprozesse sind zentrale Elemente.
- **Kontrollen und Überwachung von Drittparteien:** Existenz eines soliden Due-Diligence-Prozesses zur Auswahl von Drittparteien, eines effektiven Vertragsmanagements und fortlaufender Überwachungsprozesse zur Sicherstellung der Vertragserfüllung (kontinuierliche Leistungsbewertung). Die schließt einen formalisierten „Offboarding“-Plan mit ein.

Drittparteien als ein kritischer Prüfungsbereich

Die zunehmende Auslagerung von Geschäftsprozessen an externe Dienstleister macht es für die auslagernde Organisationen unerlässlich, die damit verbundenen Risiken wie z. B. Cybersicherheit, Compliance, Reputations- und Transparenzprobleme zu steuern. Fehlende Transparenz und Kontrolle über ausgelagerte Prozesse können Auswirkungen auf die auslagernde Organisation haben, wenn eine Drittpartei nicht die vertraglich vereinbarte Leistung erbringt, sich an unethischen Praktiken beteiligt oder eine Disruption ihres eigenen Geschäfts erfährt. Die Interne Revision spielt eine entscheidende Rolle dabei, sicherzustellen, dass auslagernde Organisationen angemessene Governance-, Risikomanagement- und Kontrollprozesse zur Überwachung ihrer Drittparteien etabliert haben.

Spezifische Anforderungen an Kreditinstitute gemäß AT 9 der MaRisk

Die Topical Requirements sind weltweit anzuwenden und bilden einen prüferischen Mindestrahmen für die Abdeckung bestimmter Risikobereiche durch die Interne Revision, unabhängig von der Größe, der Branche oder dem Reifegrad einer Organisation.

Die Organisation kann jedoch auch regulatorischen Anforderungen, externen Standards oder Rahmenwerken unterliegen, die sich mit dem Anwendungsbereich eines Topical Requirements überschneiden oder darüber hinausgehen. Dies betrifft z. B. deutsche Kreditinstitute mit den Mindestanforderungen an das Risikomanagement (MaRisk), herausgegeben von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). So enthalten die MaRisk im Abschnitt AT 9 spezielle Anforderungen an die Zusammenarbeit mit externen Dienstleistern. Diese umfassen u. a.:

- **Risikoanalyse:** Umfassende Analyse der potenziellen Risiken, die aus der Zusammenarbeit mit Drittparteien entstehen können.
- **Vertragsgestaltung:** Klar definierte Verträge, welche die Verantwortlichkeiten und Haftungs- und Überprüfungsregelungen festlegen.
- **Überwachung und Kontrolle:** Regelmäßige Leistungsbeurteilung und Überprüfung der Dienstleistungserbringung externer Partner.

Das Topical Requirement zum Drittparteienrisiko und AT 9 der MaRisk weisen zunächst viele Gemeinsamkeiten auf. So betonen beide Dokumente die Notwendigkeit einer umfassenden Risikoanalyse und fordern klare

Vertragsgestaltungen und regelmäßige Überwachungsmechanismen. Das Topical Requirement bietet jedoch detailliertere praktische Anwendungsbeispiele und Handlungsempfehlungen, während AT 9 der MaRisk spezifische Anforderungen an die Vertragsinhalte sowie einschränkende Bedingungen zur Auslagerbarkeit der Risikocontrolling- und der Compliance-Funktion sowie der Internen Revision formuliert.

Mögliche Handlungsfelder

Die auslagernde Organisation behält die Verantwortung für die Risiken, die mit einer Zusammenarbeit mit Drittparteien verbunden sind. Hierfür gibt es mehrere Ansätze, um die Qualität der Governance-, Risikomanagement- und Kontrollprozesse zum Drittparteienrisiko zu verbessern, beispielweise:

- **Schulung und Sensibilisierung:** Regelmäßige Schulungen für alle relevanten Abteilungen, um das Bewusstsein für Drittparteienrisiken zu erhöhen.
- **Vertragsmanagement:** Einführung eines strukturierten Vertragsmanagements, das alle Verträge mit externen Dienstleistern erfasst und regelmäßig überprüft.
- **Risikomanagement-Tools:** Implementierung von spezialisierten Risikomanagement-Tools zur kontinuierlichen Überwachung und Analyse der Risiken.
- **Audits und Reviews:** Regelmäßige interne Überprüfungen der Zusammenarbeit mit Drittparteien, um sicherzustellen, dass die vertraglich vereinbarten Dienstleistungen ordnungsgemäß erbracht und die regulatorischen Anforderungen erfüllt werden.

Fazit

Das Topical Requirement zum Drittparteienrisiko bietet einen wertvollen Rahmen zur Identifikation, Bewertung und Steuerung von Risiken, die aus der Zusammenarbeit mit externen Dienstleistern entstehen. Durch die Berücksichtigung der spezifischen Anforderungen gemäß AT 9 der MaRisk können Kreditinstitute ihre Governance-, Risikomanagement- und Kontrollprozesse verbessern und zeitgleich die regulatorischen Anforderungen erfüllen.

Für weitere Informationen oder zur Unterstützung bei der Umsetzung des Topical Requirements zum Drittparteienrisiko stehen wir Ihnen gerne zur Verfügung.

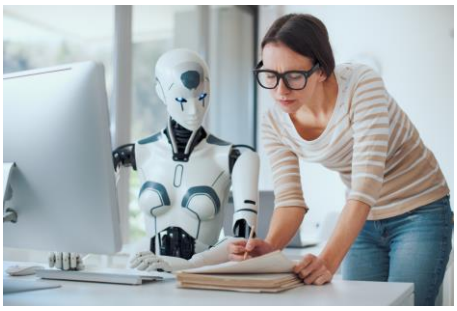
Gleich mal reinschauen: Das Seminar-Programm 2026 der ETL consit!

Das neue Seminar-Programm der ETL consit für das Jahr 2026 ist verfügbar!

Neben bewährten Programmpunkten werden auch aktuelle und neue Themen für Sie im Angebot sein, vornehmlich aus unseren zentralen Kernbereichen Informationssicherheit, Datenschutz, Revision sowie aktueller Regulatorik.

Seien Sie also gern Gast auf unserer Homepage etl-consit.de oder lassen Sie sich ganz bequem regelmäßig über alles Neue rund um unsere Akademie informieren. Kurze Info an akademie@etl-consit.de genügt!

Unsere aktuelle Empfehlung:



Künstliche Intelligenz (KI)-Kompetenz-Schulungen gemäß AI Act.

Mit dem AI Act möchte die EU den Einsatz der KI fördern, gleichzeitig aber auch rechtliche Spielregeln und Leitplanken im Umgang mit KI schaffen und insbesondere die Anwender in den Unternehmen sensibilisieren.

KI-Basisschulung branchenübergreifend

- Grundbegriffe und Funktionsweise von KI verstehen
- Chancen und Risiken realistisch einschätzen
- Grundlegende Beispiele zum Einsatz von KI
- Erste Schritte im Umgang mit KI-Tools wie ChatGPT, Copilot & Co.
- Datenschutz, AI Act, Regulierung und Ethik im Überblick

Nächste freie Termine:

17.06.2026 10.00-12.30 Uhr Jetzt anmelden

12.11.2026 10.00-12.30 Uhr Jetzt anmelden

Individuell können jederzeit kurzfristige Termine vereinbart werden!

Vertiefender Workshop KI branchenübergreifend

- KI-Werkzeuge gezielt auswählen und einsetzen
- Prompts professionell gestalten und optimieren
- Eigene Anwendungsfälle entwickeln und testen
- Chancen für Effizienz, Kreativität und Automatisierung nutzen
- Diskussion rechtlicher, ethischer und sicherheitsrelevanter Fragen in der Praxis einschl. spezieller Aspekte des AI Act

Nächste freie Termine:

25.06.2026 10.00-12.30 Uhr Jetzt anmelden

17.12.2026 10.00-12.30 Uhr Jetzt anmelden

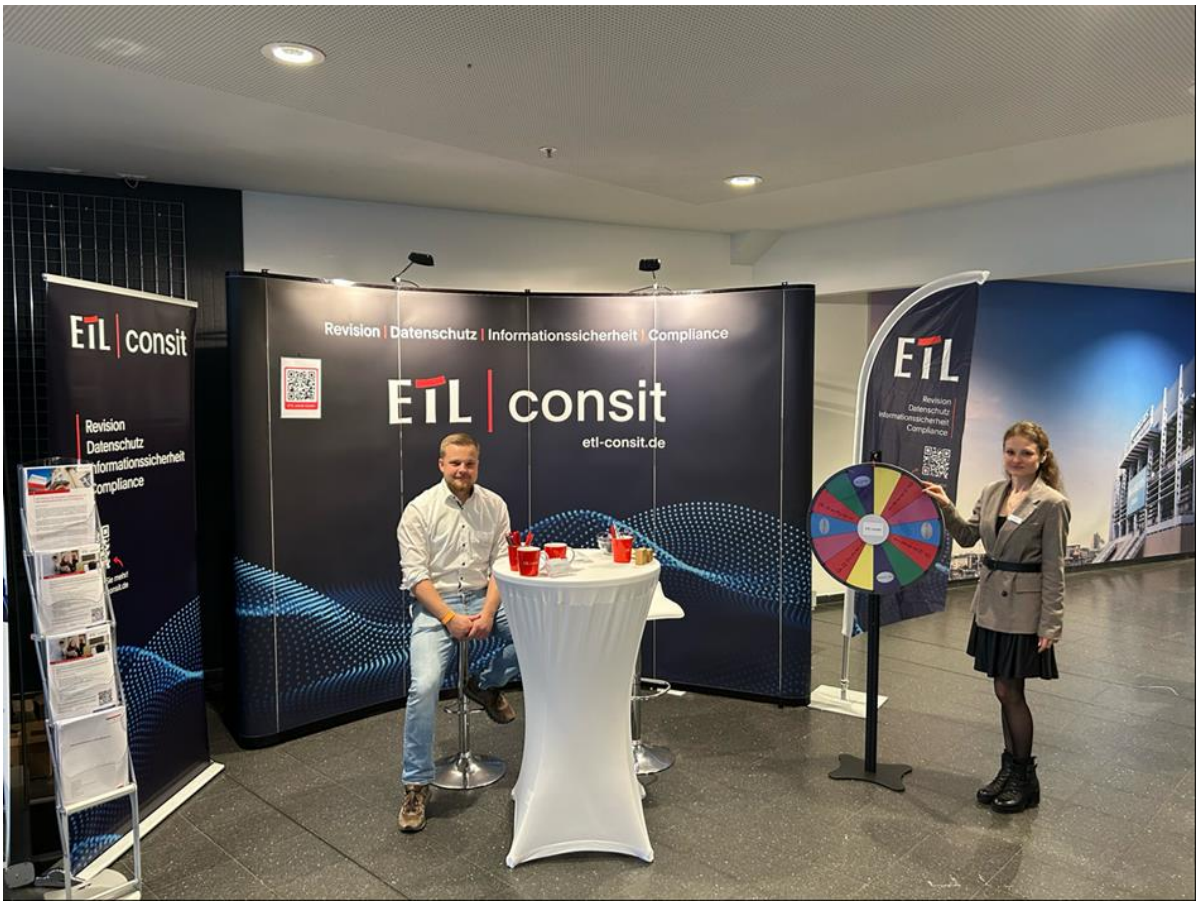
Individuell können jederzeit kurzfristige Termine vereinbart werden!

Hamburger Karrieretag 2025

Am Mittwoch, den 15. Oktober 2025, durfte sich die ETL consit auch in diesem Jahr als Arbeitgeber auf Norddeutschlands größter und interdisziplinärer Job- und Weiterbildungsmesse in der Barclays-Arena in Hamburg vorstellen.

Wir konnten den Interessenten an unserem Messestand sowohl die ETL consit als Unternehmen als auch konkrete Jobangebote präsentieren.

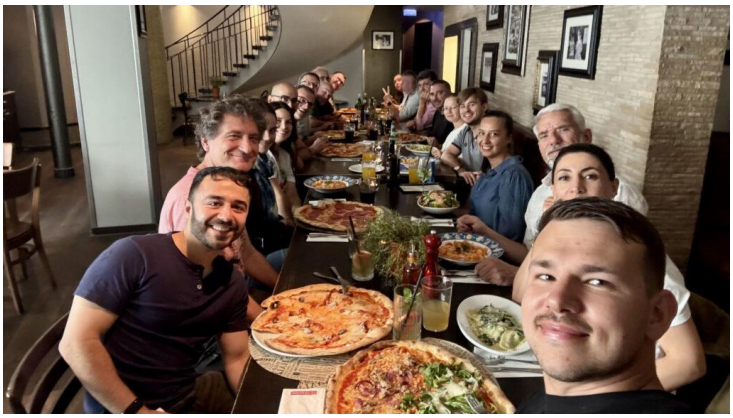
Dabei wurden viele gute Gespräche geführt und wir sind zuversichtlich, in naher Zukunft dann auch von Zuwachs im Team der ETL consit berichten zu können!



Berater- und Revisorentreffen der ETL consit – Zwei Städte, ein Spirit!

In Hannover und Trier wurde kürzlich nicht nur fachlich diskutiert, sondern auch ausgelassen gefeiert – unsere Berater und Revisoren haben sich jeweils zu ihren jährlichen Treffen versammelt und dabei gezeigt, wie lebendig Austausch und Teamgeist bei der ETL consit gelebt werden.

Beratertreffen in Hannover – Fachlich stark, im Escape Room noch stärker



Das Beratertreffen in Hannover war ein echtes Highlight: Neben spannenden Themen wie dem neuen bit-Compliance Quick-Check, Betriebskonzepten für die 1. Linie, Schwachstellen-management und dem Informationsregister ging es auch um die Frage, wie Künstliche Intelligenz unsere Arbeit noch smarter machen kann.

Und weil gute Gespräche bei Pizza und BBQ noch besser schmecken, wurde der Abend im Escape Room von Hidden Hannover zum perfekten Teambuilding-Event. Zwei Tage voller Input, Lachen und Zusammenhalt – so geht Beratung bei uns!

Revisorentreffen in Trier – Regulatorik trifft Rennstrecke

Unsere Revisorinnen und Revisoren trafen sich im wunderschönen Trier. Auf der Agenda standen Themen wie Geldwäsche, Zahlungsverkehr, Regulatorik, Prozessoptimierung und natürlich der Einsatz von KI.

Nach getaner Arbeit ging’s auf die Battle Kart-Bahn: Mario Kart in echt! Mit Ölflecken, Raketen und jeder Menge Ehrgeiz wurde um die Ideallinie gekämpft – und in den Rennpausen gab’s Pizza, Drinks und tolle Gespräche in der Boxengasse.

Auch hier wurde klar: Fachlicher Austausch und Spaß schließen sich nicht aus – im Gegenteil, sie bringen uns als Team noch näher zusammen.

Fazit: Zwei Teams, zwei Städte, ein gemeinsames Ziel – mit Know-how und Teamspirit die Zukunft gestalten. Wir freuen uns schon auf die nächsten Treffen!

Neues Modul Datenschutzmanagement bei bit-Compliance!

Im November 2025 wird bit-Compliance um das Modul **Datenschutzmanagement** erweitert. Mit diesem Modul reagiert die bit Informatik gezielt auf den Wunsch vieler Anwender nach mehr Übersicht, Automatisierung und Entlastung bei der Einhaltung datenschutzrechtlicher Anforderungen. Ziel ist es, den Umgang mit DSGVO-relevanten Themen spürbar zu erleichtern – ganz ohne zusätzlichen Verwaltungsaufwand und mit höchster Integration in die anderen Module.

Das neue Datenschutzmodul bietet unter anderem folgende Funktionen:

- zentrale Verwaltung relevanter Datenschutzdokumente
- höchste Integration in die bestehende Datenstruktur
- Nachvollziehbarkeit aller Maßnahmen zur Einhaltung der DSGVO
- Klare Zuständigkeiten und strukturierte Abläufe für mehr Sicherheit und Effizienz

Damit aktuelle oder zukünftige bit-Compliance-Nutzer den vollen Nutzen des Moduls von Anfang an ausschöpfen können, bieten wir die Möglichkeit, sich bei der Einführung aktiv unterstützen zu lassen. Unser erfahrenes Team begleitet Sie dabei.

Im Rahmen unserer Einführungsunterstützung bieten wir vollen Service – von der Vorbereitung über die Integration bis zur Qualitätssicherung der Implementierung.

Wir freuen uns darauf, Sie dabei zu unterstützen, Ihr Datenschutzmanagement in bit-Compliance abzubilden. Selbstverständlich stehen wir Ihnen bei weiteren Fragen zum Thema Datenschutz auch gerne zur Verfügung.

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