Newsletter

Liebe Kunden und Geschäftspartner,

die ersten warmen Tage liegen bereits hinter uns, hoffentlich viel guter Fußball für alle Sportbegeisterten unter Ihnen noch vor uns, und wir wünschen Ihnen daher von Herzen einen wunderschönen Start in den Sommer!

Die Schwerpunkte in dieser Ausgabe sind Künstliche Intelligenz, die Interne Revision, Cybersecurity und Datenschutz in Stiftungen. Außerdem unterstützen wir Sie bei der kurzfristigen Methodikänderung zu kritischen und wichtigen Funktionen gemäß DORA – hier lohnt sich schnelles Handeln!

Unsere aktuellen Themen:

- Wichtig!!! Methodikveränderung bei kritischen und wichtigen Funktionen gemäß DORA
- Künstliche Intelligenz – technologische Revolution oder doch nur eine IT-Anwendung?
- Datenschutz in Stiftungen: Ein oft unterschätztes Risiko
- Kontinuierliche Weiterentwicklung in der Revision, denn… die Praxis von heute ist die Theorie der Großväter!
- Moderne Cloud-Prüfung: Ein Blick auf die entscheidenden Bausteine
- Cybersecurity 2026: Die größte Stärke der Sparkassen liegt im Team – nicht in der Technik
- Risikoorientierter Prüfungsansatz in der Internen Revision
- Unsere Prozesse sind IKS-zertifiziert
- Ausblick

Herzliche Grüße

Bernd Schmid Oliver Gose

Wichtig!!! Methodikveränderung bei kritischen und wichtigen Funktionen gemäß DORA

Schnell sein lohnt sich!

Jede Sparkasse muss nach neuer Regelung neben **Business Impact Analyse (BIA)** auch **Schutzbedarfsfeststellung** sowie **regulatorische Vorgaben** in Betracht ziehen, um ihre kritischen oder wichtigen Funktionen neu zu bestimmen. Die mehrstufige und komplexe Methodik lässt sich am besten in Form eines kleinen Projektes umsetzen, da mehrere Organisationseinheiten und Funktionen beteiligt sind. Bisher wurde das Ergebnis quasi nebenbei im Zuge der BIA ermittelt und wurde somit vom Notfallbeauftragten gesteuert. Bei der neuen Methodik, ist zu berücksichtigen, dass die Ergebnisse der BIA lediglich einen Teilaspekt der Gesamtdurchführung liefert. Die Gesamtverantwortung für die vollständige Ermittlung und Neubestimmung der kritischen oder wichtigen Funktionen sollte daher klar geregelt werden. Es empfiehlt sich, die Prozessverantwortlichen, Asset-Verantwortlichen, den Informationssicherheitsbeauftragten sowie den Notfallbeauftragten gemeinsam in die Durchführung einzubinden, damit die relevanten Informationen aus der BIA, der Schutzbedarfsfeststellung und den regulatorischen Vorgaben zusammengeführt und die kritischen oder wichtigen Funktionen fundiert neu bestimmt werden können.

Wichtige Maßnahmen bis 30. Juni 2026

- Bis zum 30. Juni 2026 muss die **IKT-Assetmanagement-Richtlinie** individualisiert und freigegeben werden. Die Richtlinie enthält im Vergleich zur Vorgängerversion keine wesentlichen Änderungen, außer die Aufnahme der Beschreibung zur Durchführung der neuen Methodik zur Bestimmung der kritischen und wichtigen Funktionen sowie aktualisierte Beschreibungen und Klassifizierungen des Schutzbedarfs. Hier sollte ein besonderes Augenmerk angelegt werden.
- Die **BCM-Leitlinie** muss bis zum 30. Juni 2026 individualisiert und freigegeben werden. Die neue BCM-Leitlinie ist im **Umfang um das Doppelte gewachsen** und enthält viele Passagen, die bei einer ungeprüften und unabgestimmten Übernahme zu Folgeaufwand bzw. Umsetzungsproblemen in verschiedenen Organisationseinheiten (z. B. IT-Management, ZAM, IKT-Risikomanagement) führen kann. Deshalb empfiehlt es sich vor Übernahme und Freigabe genau zu prüfen und intern mit den ebenfalls betroffenen Kolleginnen eng abzustimmen, ob und wo evtl. Anpassungen erforderlich sind.

Methodisches Vorgehen zur Bestimmung kritischer oder wichtiger Funktionen

Für die Bestimmung kritischer oder wichtiger Funktionen werden zukünftig mehrere Quellen herangezogen und zusammengeführt. Zunächst werden alle Prozesse identifiziert, die im Rahmen der BIA als kritisch oder essentiell eingestuft wurden. Ergänzend werden diejenigen Prozesse berücksichtigt, die in der Schutzbedarfsfeststellung hinsichtlich Integrität oder Vertraulichkeit einen sehr hohen Schutzbedarf aufweisen. Als dritte Quelle sind die Prozesse zu berücksichtigen, die aus regulatorischer Sicht erforderlich sind und deren Ausfall die ordnungsgemäße Geschäftstätigkeit bzw. die Zulassung der Sparkasse gefährden könnten. Auf Basis dieser Informationsquellen erfolgt anschließend eine konsolidierte Bewertung und Neubestimmung der kritischen oder wichtigen Funktionen der Sparkasse. Die **erstmalige Bewertung und Neubestimmung** ist **bis spätestens zum 30. September 2026** abzuschließen.

Die ETL consit kann die Sparkasse bei der Umsetzung dieser Maßnahmen unterstützen und die erforderlichen Aufgaben übernehmen. Dazu gehören **insbesondere die Individualisierung und fachliche Prüfung der IKT-Assetmanagement-Richtlinie sowie der BCM-Leitlinie** auf Basis der vorhandenen Unterlagen und internen Gegebenheiten der Sparkasse. Darüber hinaus können wir die Abstimmung mit den betroffenen Organisationseinheiten begleiten und erforderliche Anpassungen vorbereiten, sodass **eine fristgerechte Freigabe bis zum 30. Juni 2026 ermöglicht** wird.

Des Weiteren bieten wir an, die **Umsetzung der Methodik verantwortlich zu übernehmen** und auf Grundlage der im GRC-Tool der Sparkasse vorhandenen Daten die **Ergebnisse nach der neuen Methodik bis zum 30. September 2026 zu ermitteln, zu erfassen und qualitätszusichern.**

Künstliche Intelligenz – technologische Revolution oder doch nur eine IT-Anwendung?

- Unsere Expertin Christa Köhler blickt als Revisorin ganz genau darauf -

73% der Finanzunternehmen in Deutschland setzen bereits KI ein, Tendenz deutlich steigend[1]. Das Spektrum reicht von Operations über IT, Marketing und Risikomanagement bis hin zu Personal. Höchste Zeit also, diese Technologie in das Prüfungsuniversum zu integrieren.

Dabei sind unterschiedliche Ansätze denkbar - entlang des Lebenszyklus, aus der Perspektive der Governance und Organisation, durch die Compliance-Brille, projektbegleitend bei der Einführung oder als Werkzeug zur Unterstützung der Prozesse, um nur einige zu nennen. Diese Varianten schließen sich nicht gegenseitig aus, sondern ergänzen sich sinnvoll. Die Auswahl hängt in erster Linie vom Einsatzgebiet der KI in den Finanzunternehmen ab und lässt sich differenzieren nach

- der Art der KI (Fremd-KI, eigenentwickelte KI, Kombination)
- den unterstützten Prozessen (Vertrieb, Risikocontrolling, Personal usw.)
- der Phase des Einsatzes (Pilot, ausgewählte Bereiche, flächendeckende Anwendung)

Als Prüfungsgrundlage sind – neben den sektorspezifischen Regularien – insbesondere die Anforderungen aus DORA, der DSGVO, NIS2 und spätestens ab dem 2. August 2026 auch des AI Act zu beachten.

Natürlich kann man nun strikt die Erfüllung der regulatorischen Anforderungen prüfen und die fehlende oder unzureichende Umsetzung den geprüften Bereichen als Feststellung auf die ToDo-Liste setzen. Um dem Unternehmen jedoch einen Mehrwert zu bieten, empfiehlt es sich zunächst im Sinne des risikoorientierten Vorgehens, sich nicht nur auf dem Papier, sondern sich tatsächlich mit den Risiken auseinander zu setzen, die eine KI mitbringt. Wir stellen Ihnen hier einige Risiken vor, die sich aus den beiden Haupt-Angriffsflächen von KI ergeben.

[1] Quelle: Studie „Einblicke zur Künstlichen Intelligenz im deutschen Finanzsektor“ der PwC (Stand: Januar 2025)

Angriffsfläche „KI-Modell“

- Die verwendeten Modelle kommen oft verpackt in eine Grey oder Black Box. Die enthaltenen Regeln / Algorithmen sind daher nicht (vollständig) transparent, erklärbar und nachvollziehbar.
- Die KI setzt einzelne Informationen zu Ergebnissen zusammen, die schlüssig und fundiert wirken, aber de facto falsch, unbegründet und erfunden sind. Sie halluziniert also.
- Die KI verfällt in Panik und startet einen Angriff von innen.
- Während der Abfragen werden minimale, nicht wahrnehmbare Störungen eingebaut mit dem Ziel, eine Fehlentscheidung herbeizuführen (Model Evasion).
- Das Modell wird rekonstruiert oder gestohlen (Model Extraction).

Angriffsfläche „Daten“

- Die Trainingsdaten werden manipuliert mit dem Ziel einer Fehlfunktion oder Leistungsminderung der Modelle (Data Poisening).
- In die Trainingsdaten werden manipulierte Muster eingebaut mit dem Ziel, dass das Modell mit kompromittierten Trainingsdaten lernt (Backdoors).
- Die Trainingsdaten stellen, wie auch das Modell, eine Grey oder Black Box dar, so dass die Qualität der Ergebnisse potenziell nicht belastbar ist.
- Die Trainingsdaten sind zwar transparent, weisen aber eine geringe Qualität auf, wodurch die Ergebnisse nicht automatisch besser werden. Zwei Minus ergeben nicht immer ein Plus.
- Die Angriffspunkte der verwendeten Daten sind unterschiedlich. So können minimale Veränderungen bei Bildern oder Audiodateien durch das menschliche Auge oder Ohr nicht mehr oder nur noch schwer erkannt werden.

Die Ursachen dieser Risiken sind nicht immer eindeutig auf ein fehlerhaftes Modell oder fehlerhafte Daten zurückzuführen, da die Modelle durch die Daten trainiert werden und die beiden Komponenten daher eng miteinander verzahnt sind.

Was bedeutet das nun für Ihre Prüfungen?

Wenn Ihr Institut plant, demnächst KI einzusetzen oder sich noch in der Einführungsphase befindet, bietet sich eine projektbegleitende Prüfung an. Diese sollte ihren Fokus nicht nur auf die ordnungsgemäße Projektsteuerung und -durchführung legen, sondern auch die geplanten Einsatzgebiete und die Art der KI auf den Radarschirm nehmen. Nur so können Sie dazu beitragen, dass die Risiken von Beginn an angemessen adressiert werden und Ihr Institut nicht spät, oder gar zu spät ein böses Erwachen erlebt.

Wenn Sie KI bereits im Einsatz haben, kommt sowohl eine Prüfung der KI selbst als auch eine Prüfung der KI als Werkzeug in den Prozessen in Betracht, so als würden Sie eine Anwendung prüfen. Der Unterschied liegt in den neuen bzw. vergrößerten Angriffsflächen der KI:

- Bei der Angriffsfläche „KI-Modell“ ist auf die angemessene Definition, fundierte Tests und die laufende Überprüfung der Modelle sowie der Genauigkeit der Ergebnisse ebenso Acht zu geben wie auf ausreichende Schutzmechanismen vor Angriffen von innen oder außen.

- Zur Reduzierung oder Vermeidung von Risiken im Kontext der Angriffsfläche „Daten“ können offene Augen und Ohren, Fachkompetenz und auch der gesunde Menschenverstand in Kombination mit Maßnahmen, die auf die Verlässlichkeit der Datenherkunft, die Qualität der Daten und Ergebnisse und den Schutz vor Manipulationen abzielen, einen wertvollen Beitrag leisten.

Mit steigender Komplexität nimmt die Undurchsichtigkeit zu. Die Sensibilisierung und die Fachkompetenz der handelnden Personen müssen einen hohen Stellenwert einnehmen, da es sich bei KI eben nicht nur um eine IT-Anwendung handelt, sondern die technologische Entwicklung ein neues Niveau erreicht hat.

Oder um es mit den Worten von Garry Kasparow zu sagen: „Die gefährlichste Zukunft ist nicht die, in der Maschinen denken wie Menschen, sondern die, in der Menschen aufhören zu denken.“

Gern unterstützen unsere Expertinnen und Experten Sie bei der Prüfung Ihres KI-Ansatzes.

(Dieser Artikel wurde **nicht** mit KI erstellt 😉)

Datenschutz in Stiftungen: Ein oft unterschätztes Risiko

Viele Sparkassen engagieren sich über ihre Stiftungen intensiv für lokale Projekte und gesellschaftliche Verantwortung. Aus unserer Beratungspraxis wissen wir jedoch: Beim **Datenschutz** bestehen in Stiftungen häufig **deutlich größere Lücken** als in den Instituten selbst.

Das ist **verständlich – aber nicht ungefährlich**!

Wo Stiftungen besonders verwundbar sind:

- **Sensible personenbezogene Daten**
  Stiftungen, die Zustiftungen privater Personen verwalten oder Einzelförderungen vergeben, verarbeiten oft Gesundheitsdaten oder andere besonders schützens-werte Informationen. Ohne klare Prozesse entsteht schnell ein „Blindflug“ in Bezug auf die DSGVO.
- **Betroffenenrechte**
  Gerade bei abgelehnten Förderanträgen können Anfragen von Betroffenen den Datenschutz plötzlich ins Rampenlicht rücken.
- **Fehlende Grundstrukturen**
  In vielen Stiftungen fehlen zentrale Bausteine eines Datenschutzmanagements, darunter:
  - Datenschutzerklärungen
  - Hinweise in Spendenformularen
  - Verträge mit der Sparkasse (z. B. zu IT-Nutzung, Dienstleistungen, Personal)
  - Verzeichnisse von Verarbeitungstätigkeiten
  - DSFA-Prüfungen – Auftragsverarbeitungsverträge
  - Schulungen und Verpflichtungen der Stiftungsorgane

Hinzu kommen **bundeslandspezifische Regelungen** aus den Stiftungsgesetzen, die beachtet werden müssen:

- **Öffentlichkeitsarbeit als Risikofaktor**
  Eigene Webseiten, Social-Media-Aktivitäten, Event-Fotos, Veröffentlichungen von Spendern oder Förderempfängern – all das birgt datenschutzrechtliche Fallstricke.
- **Fusionen von Sparkassen**
  Was passiert mit Altstiftungen? Wie werden Daten, Zuständigkeiten und organisatorische Strukturen sauber überführt? Auch hier entstehen häufig ungeklärte Risiken.

Wie wir Stiftungen unterstützen

Wir kennen die Besonderheiten von Stiftungen aus zahlreichen Projekten und können:

- die **Funktion des Datenschutzbeauftragten** übernehmen – eigenständig oder parallel zum Institut
- ein Basis-**Datenschutzmanagement aufbauen**
- bestehende Datenschutzorganisationen **auditieren**
- Stiftungsorgane **schulen und sensibilisieren**

Unser Ansatz ist stets pragmatisch und lösungsorientiert: Wir bringen das Datenschutzniveau schnell auf ein angemessenes, belastbares Level. Das stärkt das Vertrauen von Spendern und Stiftern – und reduziert Reputationsrisiken für Stiftung und Sparkassen gleichermaßen. Wenn Sie in Ihrer Stiftung Handlungsbedarf sehen oder eine unabhängige Überprüfung wünschen, stehen wir Ihnen jederzeit – auf Wunsch auch vertraulich – zur Verfügung.

Kontinuierliche Weiterentwicklung in der Revision, denn… die Praxis von heute ist die Theorie der Großväter!

- Oliver Hansen (CIA, CRMA), Bereichsleiter und Prokurist -

Ein prägnanter Gedanke vom österreichisch-amerikanischen Ökonomen Joseph Schumpeter. Er beschreibt sehr treffend die **Dynamik von Innovation und Fortschritt**: Was heute selbstverständlich praktiziert wird, galt früher als neue, ungewohnte oder sogar gewagte Theorie. Das Zitat betont damit, wie sich Wissen und gesellschaftliche Vorstellungen weiterentwickeln… man könnte es auch so zusammenfassen: **Der Fortschritt von heute baut auf dem Alltag von gestern auf.**

Damit wird klar: Wer in der Internen Revision stehen bleibt, fällt zurück — denn **Methoden, Risiken, Technologien und regulatorische Anforderungen entwickeln sich ständig weiter**. Kontinuierliche Weiterentwicklung ist daher kein „nice-to-have“ für Interne Revisorinnen und Revisoren, sondern ein zentraler Bestandteil professioneller Revisionsarbeit.

Die **Global Internal Audit Standards** (GIAS) regeln die weltweite berufliche Praxis der Internen Revision und dienen als Grundlage für die Bewertung und Verbesserung der

Qualität der Internen Revision. Demnach ist eine Interne Revision am wirksamsten, wenn sie von **kompetenten Internen Revisorinnen und Revisoren** unter Einhaltung der Global Internal Audit Standards durchgeführt wird. Für die Mitarbeitenden der Internen Revision bedeutet Kompetenz, dass sie in der Lage sind, **risikobasierte, objektive Prüfungs- und Beratungsleistungen** zu erbringen. Die Kompetenz umfasst auch das Wissen und die Fähigkeiten, die erforderlich sind, um mit dem **Überwachungsorgan und der Geschäftsleitung** zusammenzuarbeiten, um eine **wirksame, effiziente Interne Revision** einzurichten und zu beaufsichtigen. Kompetente Revisorinnen und Revisoren ermöglichen es der Internen Revision **Werte zu schaffen, zu schützen und zu erhalten** und damit die Zielsetzung der Internen Revision zu erfüllen.

Die Standards zu Prinzip 3 „Zeige Kompetenz“ betonen, dass jeder Mitarbeitende der Internen Revision dafür verantwortlich ist, die zur **Erfüllung der beruflichen Verantwortung** erforderlichen **Kompetenzen kontinuierlich weiterzuentwickeln** und anzuwenden, während die Revisionsleitung sicherstellen muss, dass die Interne Revision insgesamt über die Kompetenzen verfügt, um die in der Geschäftsordnung der Internen Revision beschriebenen Dienstleistungen zu erbringen, oder dass sie die erforderlichen Kompetenzen erlangt.

Moderne Revisionsarbeit erfordert dabei ein breites Kompetenzspektrum:

- **Fachwissen:** Kenntnisse zu Governance-, Risikomanagement- und Kontrollprozessen, zu operativen Geschäftsfunktionen (z. B. Compliance, Finanzmanagement und IT) sowie zu neuen Gesetzen und Regulierungen
- **Prüfungsmethodik und IT:** Revisionsgrundsätze (z. B. GIAS), aber auch Data Analytics, KI-Prüfungstools und agile Revision
- **Soft Skills:** Kommunikation, Konfliktmanagement und Präsentationstechniken, um u. a. Prüfungsergebnisse wirksam vermitteln zu können

Um die Qualität der internen Revisionsleistungen zu verbessern, sollen die internen Revisorinnen und Revisoren nach Möglichkeiten suchen, sich über **neue Themen, künftige Risiken, Trends und Veränderungen** zu informieren, die künftig für die eigene Organisation und den Berufsstand der Internen Revision relevant sein können. Eine wichtige Informationsquelle hierfür ist die **Studie „Risk in Focus“**, 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). Diese Untersuchung identifiziert die **zentralen Herausforderungen und Risikoschwerpunkte**, denen sich Organisationen und ihre Revisionen in Europa gegenübersehen.

Interne Revisorinnen und Revisoren können ihre eigenen Fähigkeiten und Entwicklungsmöglichkeiten selbst am besten einschätzen. Dabei soll die Revisionsleitung die berufliche Entwicklung der Internen Revisorinnen und Revisoren unterstützen. Die Revisionsleitung kann **Mindesterwartungen für die berufliche Entwicklung festlegen** und soll das **Streben nach beruflichen Qualifikationen fördern**.

Ein hilfreiches **Instrument zur Strukturierung und Evaluierung** der für die Interne Revision erforderlichen Kompetenzen bietet das **Internal Auditing Competency Framework™**, herausgegeben vom Institute of Internal Auditors (IIA). Die Verwendung der ergänzenden Vorlagen zur Beurteilung und Dokumentation des Managements und der Entwicklung von Kompetenzen unterstützt die Revisionsleitung beim Nachweis der

Übereinstimmung mit vielen Anforderungen aus den GIAS. Dabei ist das Internal Auditing Competency Framework™ flexibel gestaltet, um die Prioritäten jeder Organisation im gebotenen Mix aus Kompetenzen und Kompetenzniveaus zu berücksichtigen.

Um zielgerichtet Kompetenzen zu entwickeln und nachzuweisen, können Interne Revisorinnen und Revisoren **geeignete Berufsqualifikationen** erwerben, z. B. den Certified Internal Auditor® (CIA), den Certified Information Systems Auditor® (CISA) oder andere Zertifizierungen und Bescheinigungen. Für viele dieser beruflichen Qualifikationen ist eine Mindestanzahl von Stunden kontinuierlicher beruflicher Weiterbildung (**Continuing Professional Education**, CPE) innerhalb eines bestimmten, z. B. jährlichen, Zeitraums erforderlich. So sind exemplarisch durch einen praktizierenden CIA jährlich 40 CPE-Stunden nachzuweisen, um die Qualifikation als CIA aufrecht zu erhalten. Dies schließt zwei CPE-Stunden zu Ethikschulungen mit ein. Diese Anforderung ist zwar speziell an die CIA-Zertifizierung geknüpft, aber grundsätzlich sollten sich alle Internen Revisorinnen und Revisoren regelmäßig in **ethischen Fragen weiterbilden** oder schulen.

Zusätzlich zu den gängigen **Berufsqualifikationen** und formalen Fortbildungsprogrammen kann kontinuierliche berufliche Weiterentwicklung durch eine Vielzahl anderer Aktivitäten erfolgen, u. a.:

- Selbststudium
- Training am Arbeitsplatz bzw. Gelegenheiten zum Erlernen neuer Fertigkeiten im Rahmen spezieller Aufgaben (z. B. Rotationsprogramme)
- Mentoring und Feedback von Führungskräften
- Verfassen bzw. übersetzen von oder Mitwirken an Veröffentlichungen
- Halten von Vorträgen
- Ehrenamtliche Teilnahme als Fachexperte, z. B. in Gremien bzw. Arbeitskreisen des DIIR
- Durchführung von externen Quality Assessments

Kontinuierliche Weiterentwicklung ist für die Interne Revision essenziell, um relevant, wirksam und zukunftsfähig zu bleiben. Sie ermöglicht es, Risiken frühzeitig zu erkennen, moderne Prüfungsansätze einzusetzen, regulatorische Anforderungen zu erfüllen und **als strategischer Partner echten Mehrwert zu liefern**.

Sie wollen sich praxisnah weiterentwickeln? Nutzen Sie das **vielseitige Leistungsangebot der ETL consit- Akademie** für Ihre Weiterbildung in den Bereichen Informationssicherheit, Datenschutz, Interne Revision und Compliance. Oder reduzieren Sie ihr operationelles Risiko einmalig, z. B. bei personellen oder fachlichen Engpässen, oder dauerhaft durch den **Zukauf von qualitativ hochwertigen Revisionsdienstleistungen**.

Profitieren Sie von der **umfassenden Expertise** und den **langjährigen Erfahrungen** der ETL consit GmbH. Unsere Spezialisten unterstützen Sie gern bei der Bewältigung Ihrer Herausforderungen.

Moderne Cloud-Prüfung: Ein Blick auf die entscheidenden Bausteine

Die Nutzung von Cloud-Lösungen hat sich in Finanzunternehmen längst von einer technischen Option zu einem strategischen Fundament entwickelt. Gleichzeitig steigen die regulatorischen Anforderungen. Für Interne Revisionen bedeutet das: Die **Prüfung von Cloud-Services** ist kein Randthema mehr, sondern ein zentraler Bestandteil einer wirksamen Governance.

Eine zeitgemäße Cloud-Prüfung umfasst heute weit mehr als technische Sicherheitschecks. Sie betrachtet das gesamte System. Auslagerungsmanagement, Mobile Device Management (MDM), Cloud-Kollaborationsplattformen, Data Loss Prevention (DLP) und Security Monitoring (SIEM/SOAR) sind fünf zentrale Prüfbausteine, wenn Finanzunternehmen Cloud-Lösungen einsetzen. Sie beeinflussen sowohl die technische Sicherheit als auch die regulatorische Bewertung durch die Interne Revision.

Auslagerungsmanagement und Dienstleistersteuerung
Cloud-Nutzung ist im Kern Auslagerung: Risikoanalyse, Wesentlichkeitseinstufung und Informationsregister. Exit-Strategien und Konzentrationsrisiken.

Mobile Device Management (MDM)

MDM ist ein Kernbestandteil der **Cloud-Sicherheitsarchitektur**, weil mobile Endgeräte heute ein primärer Zugriffspunkt auf Cloud-Dienste sind.

- **Gerätesicherheit** — Verschlüsselung, Passwortvorgaben, Jailbreak/Root-Erkennung.
- **Zugriffskontrolle** — Durchsetzung von MFA, Conditional Access, Compliance-Status.
- **Trennung geschäftlicher und privater Daten** — Besonders relevant bei BYOD-Modellen.
- **Remote-Löschung** — Kritisch für DSGVO-Konformität bei Geräteverlust.

Für die Revision bedeutet das: Ohne wirksames MDM ist die Cloud-Nutzung **nicht prüfbar sicher**, da Endgeräte ein zentrales Einfallstor für Datenabfluss und unbefugten Zugriff darstellen.

Cloud-Kollaborationsplattformen

Hier entstehen die meisten Risiken: Zu breite Berechtigungen, externe Freigaben, fehlende Aufbewahrungsrichtlinien. Eine saubere Konfiguration entscheidet darüber, ob Zusammenarbeit sicher oder riskant ist.

Data Loss Prevention (DLP)

DLP-Mechanismen erkennen und blockieren sensible Finanz- und Kundendaten automatisch. Sie sind unverzichtbar, um Datenschutzvorgaben nachweisbar einzuhalten und Datenabfluss zu verhindern. Die Wirksamkeit hängt von Regelqualität und Kanalabdeckung ab.

Security Monitoring (SIEM/SOAR)
IKT-Vorfälle werden erkenn- und nachweisbar. In der Cloud zählt die Anbindung der Provider-Telemetrie an das eigene Monitoring – auch mit Blick auf die DORA-Meldefristen für schwerwiegende IKT-Vorfälle.

Das Zusammenspiel ist entscheidend:

MDM schützt **den Zugang**, Kollaborationsplattformen **die Verarbeitung**, DLP **die Daten selbst**, SIEM/SOAR **die Nachweisbarkeit** – eingebettet in ein sauberes **Auslagerungs- und IKT-Drittparteienmanagement**. Erst gemeinsam entsteht ein wirksamer Kontrollrahmen – und genau hier setzt eine moderne Cloud-Prüfung an.

Wir unterstützen Sie mit:

- **Cloud-Audits**
- **Risikobewertungen** für Cloud-Plattformen und Endgeräte
- **Revisionsnahe Beratung** zur Optimierung Ihres Kontrollrahmens
- **Schulungen** für Revisions- und IT-Teams

Unser Ziel: Risiken reduzieren, Transparenz schaffen und Ihre Cloud-Nutzung nachhaltig absichern.

Cybersecurity 2026: Die größte Stärke der Sparkassen liegt im Team – nicht in der Technik

Cyberangriffe auf Finanzinstitute steigen seit Jahren – 2026 jedoch rückt ein neuer Trend in den Mittelpunkt: **Die Angriffe werden menschlicher.**

Statt hochkomplexe Systemlücken auszunutzen, setzen Cyberkriminelle zunehmend auf **Social Engineering, KI-gestützte Phishing-Mails** und **personalisierte Betrugsversuche**. Besonders Sparkassen geraten dadurch verstärkt ins Visier – aufgrund ihrer regionalen Nähe, hohen Kundendichte und vertrauensvollen Markenposition.

Während technische Schutzmechanismen in vielen Häusern gut etabliert sind, zeigt die Praxis: **Der entscheidende Faktor für Informationssicherheit bleibt der Mensch.** Selbst modernste Systeme können keine falschen Klicks, unklaren Prozesse oder überlasteten Teams kompensieren.

KI verändert die Angriffsmethoden

Cyberangriffe werden heute automatisiert vorbereitet. KI erzeugt täuschend echte E-Mails, imitiert Schreibstile oder erstellt gefälschte Audioaufnahmen.

Für Institute bedeutet das:

- klassische Awareness-Kampagnen reichen nicht mehr
- Sensibilisierung muss realitätsnah, kontinuierlich und rollenbasiert erfolgen
- Führungskräfte tragen stärkere Verantwortung für Informationssicherheitskultur

Prozesssicherheit wird zur Verteidigungslinie

Nicht nur die IT, sondern auch Fachbereiche sind gefordert.

In internen Untersuchungen zeigen sich immer wieder ähnliche Schwachstellen:

- fehlende Vier-Augen-Prinzipien
- unklare Verantwortlichkeiten in Ausnahmefällen
- unterschätzte Risiken in Schnittstellenprozessen
- mangelnde Dokumentation bei Eilentscheidungen

Stabile und geübte Prozesse sind daher ein zentrales Element der digitalen Resilienz.

Informationssicherheit ist Kulturarbeit

Eine nachhaltige Sicherheitskultur lebt nicht von Regeln, sondern vom Verhalten.

Sparkassen, die Mitarbeitende aktiv einbinden, profitieren klar:

- weniger Sicherheitsvorfälle
- höhere Meldebereitschaft
- stärkere Akzeptanz neuer Maßnahmen

Hier zeigt sich: **Informationssicherheit ist keine IT-Aufgabe, sondern Teamarbeit.**

Wie wir als ISB unterstützen können

Wir begleiten Sparkassen bei

- Awareness-Strategien und Trainingsprogrammen
- rollenbasierten Schulungen
- Prozessanalysen & Risikobewertungen
- Durchführung der Notfallübungen
- Aufbau einer nachhaltigen Sicherheitskultur

So entsteht Sicherheit, die nicht nur Technik, sondern den gesamten Geschäftsbetrieb schützt.

Risikoorientierter Prüfungsansatz in der Internen Revision

Der risikoorientierte Prüfungsansatz ist das zentrale Fundament einer modernen Internen Revision. Sie steht dabei unter einem hohen Erwartungsdruck: Das Aufsichtsrecht erfordert eine **klare Priorisierung der Prüfungstätigkeiten** nach Risiko, die Geschäftsleitungen erwarten **Mehrwert und Orientierung**, und gleichzeitig verändern **Digitalisierung, Cyberbedrohungen und neue regulatorische Anforderungen** das Risikoprofil der Institute in immer kürzeren Zyklen. Eine Interne Revision, die ihre Prüfungsaktivitäten nicht konsequent an diesen Entwicklungen ausrichtet, verliert schnell an Wirksamkeit.

Im Kern bedeutet Risikoorientierung, dass die Interne Revision ihre Planung und Durchführung nicht mehr an festen Zyklen oder starren Themenkatalogen ausrichtet, sondern an der tatsächlichen Risikolage des Hauses**. Risiken werden systematisch erhoben, bewertet und in ihrer Bedeutung für das Institut eingeordnet**. Auf dieser Grundlage entsteht ein Prüfungsplan, der dynamisch bleibt und sich an neue Erkenntnisse anpasst.

Auch die Prüfungsdurchführung selbst folgt diesem Prinzip: **Tiefe, Umfang und Methodik richten sich nach dem Risikoprofil des jeweiligen Prüfungsobjekts**. Bereiche mit hohem Schadenspotenzial oder auffälligem Kontrollumfeld werden intensiver beleuchtet als solche mit stabilen Prozessen und geringem Risiko.

Ein besonders anschauliches Beispiel für gelebte Risikoorientierung bietet der Ansatz der Sparkassenorganisation mit ihrer Unterscheidung zwischen Basis- und Vertiefungsprüfungen. Dieses zweistufige Modell zeigt, wie Breite und Tiefe in einem risikoorientierten Prüfungsansatz sinnvoll miteinander verbunden werden können. Die **Basisprüfungen** dienen dabei als flächendeckende Grundabdeckung. Sie stellen sicher, dass alle wesentlichen Geschäftsprozesse regelmäßig betrachtet werden und ein vollständiges Bild über das Kontrollumfeld entsteht. Die Prüfungstiefe ist bewusst moderat gehalten, denn Ziel ist nicht die Detailanalyse, sondern die Identifikation von Auffälligkeiten, strukturellen Schwächen oder Risikohinweisen.

Dort, wo diese Basisprüfungen erhöhte Risiken sichtbar machen – oder wo bereits im Vorfeld ein besonders kritisches Risikoprofil besteht –, setzt die zweite Ebene an: die **Vertiefungsprüfung**. Sie geht deutlich stärker in die Tiefe, nutzt analytische und datenbasierte Methoden und konzentriert sich auf die Prozesse, in denen Risiken besonders relevant oder komplex sind. Damit entspricht sie exakt dem Grundgedanken der risikoorientierten Revision: Ressourcen werden dort eingesetzt, wo sie den größten Erkenntnisgewinn und die höchste Risikoreduktion versprechen.

Dieses Modell zeigt eindrucksvoll, wie Risikoorientierung strukturiert umgesetzt werden kann. Die **Kombination aus breiter Grundprüfung und gezielter Vertiefung** schafft Transparenz, ohne Ressourcen zu überdehnen. Gleichzeitig erfüllt sie die Erwartungen der Aufsicht, die sowohl eine angemessene Breite der Prüfungsabdeckung als auch eine risikoorientierte Tiefe verlangt.

Insgesamt wird deutlich, dass der risikoorientierte Prüfungsansatz weit mehr ist als eine methodische Vorgabe. Er ist ein **strategisches Steuerungsinstrument**, das die Interne Revision in die Lage versetzt, Risiken frühzeitig zu erkennen, das Management fundiert zu beraten und die Governance des Instituts nachhaltig zu stärken.

Wir unterstützen Sie gern beim Umgang mit Ihrer individuellen Risikosituation – mit Beratung, Prüfungen oder bei der modernen Weiterentwicklung Ihres Prüfungskonzeptes.

Unsere Prozesse sind IKS-zertifiziert

Kreditinstitute müssen ihre Auslagerungen nach strengen regulatorischen Vorgaben, insbesondere aus den MaRisk (Mindestanforderungen an das Risikomanagement) und der DORA-Verordnung (Digital Operational Resilience Act), steuern. Dies beinhaltet auch eine laufende Überwachung der erbrachten Dienstleistungsqualität anhand von regelmäßigen Berichten des beauftragten Dienstleisters.

Hierzu informiert die ETL consit als Dienstleister mit ihrem jährlichen Qualitätsbericht über die Qualität der erbrachten Leistungen. Mit diesen Informationen soll die vertrauensvolle Zusammenarbeit mit unseren Kunden unterstrichen und über die ordnungsgemäße Erfüllung der übernommenen Aufgaben und die Einhaltung der eingegangenen Verpflichtungen berichtet werden.

Zusätzlich erhalten unsere Kunden einen Quartalsbericht mit Informationen zu ggf. aufgetretenen Datenpannen und Sicherheitsvorfällen sowie Veränderungen am Gesamtrisikoprofil.

Ergänzend hat die ETL consit seit dem Jahr 2024 ihr dienstleistungsbezogenes Internes Kontrollsystem (IKS) auf Basis des **Prüfungsstandards 982 des Instituts der Wirtschaftsprüfer (IDW PS 982**) zertifizieren lassen. Als Basis hierfür wurde eine IKS-Beschreibung erstellt sowie Kontrollaktivitäten für die Dienstleistungsprozesse

- „Interne Revision“,
- „Datenschutzbeauftragter“ und
- „Informationssicherheitsbeauftragter“

definiert.

Im Ergebnis der Berichte des beauftragten Wirtschaftsprüfers

- sind die implementierten Grundsätze, Verfahren und Maßnahmen des IKS in der IKS-Beschreibung in Übereinstimmung mit den angewandten IKS-Grundsätzen in allen wesentlichen Belangen **angemessen** dargestellt,

- waren die in der IKS-Beschreibung dargestellten Regelungen in Übereinstimmung mit den angewandten IKS-Grundsätzen in allen wesentlichen Belangen
    - **geeignet**, mit hinreichender Sicherheit die IKS-Ziele in Bezug auf die Dienstleistungen „Interne Revision“, „Datenschutzbeauftragter“ und „Informationssicherheitsbeauftragter“ zu erreichen und
    - **wirksam.**

Die ETL consit stellt an ihre Dienstleistungsqualität höchste Ansprüche. Wir sehen mit den externen Zertifizierungen unsere hohen Qualitätsziele auch durch einen unabhängigen Wirtschaftsprüfer bestätigt.

Sollten Sie Interesse an den Prüfungsergebnissen zu unserem IKS haben, sprechen Sie uns gerne an.

Ausblick - Themen im nächsten Newsletter:

Auch im Juli/August erwarten Sie spannende Themen rund um unsere Kompetenzfelder:

- Ausgestaltung KI-Compliance
- MaRisk-Novelle 2026 konkret
- AMLA: Was jetzt zu tun ist
- Interim-Report zu Risk in Focus 2026/2027 des DIIR
- GIAS: Konsultation zum Topical Requirement „Korruptionsbekämpfung“ gestartet
- Nächster Teil „Unsere Herzensprojekte“

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