Newsletter

Magische Brücken…

Liebe Kunden und Geschäftspartner,

heute möchten wir Ihnen herbstliche Grüße mit dem Bild einer der faszinierendsten und magischsten Brücken in Deutschland senden: Der Rakotzbrücke in Kromlau (Sachsen), auch Teufelsbrücke genannt, weil sie scheinbar allen Gesetzen der Natur und Technik trotzt.

Magische Brücken möchten wir auch immer wieder in bewährter Weise mit guten und pragmatischen Lösungen zu Ihnen schlagen.

DORA ist dabei aktuell ein zentrales Thema. Nach den Umsetzungsprojekten in den Häusern in 2023 und 2024 wird es spätestens 2025 auch einen wichtigen neuen Faktor im Prüfungsplan der Internen Revision darstellen.

Weitere Themen in diesem Newsletter für Sie:

- Sachkunde für Vorstände bezüglich DORA herstellen…
- DIIR: Top-Risiken 2025 im Fokus!
- Pragmatischer Check-up der Revisionsprozesse
- Erweiterte Anforderungen an das Informationssicherheitsmanagement
- Unsere KI-Empfehlungen im aktuellen Fokus: Die ETL-Akademie empfiehlt…
- Quishing: Eine neue Bedrohung im digitalen Zeitalter

Wir wünschen Ihnen einen faszinierenden Herbst!

Herzlichst

Bernd Schmid Oliver Gose

Sachkunde für Vorstände bezüglich DORA herstellen…

Ab 17. Januar 2025 gilt DORA!

Die EU-Verordnung Digital Operational Resilience Act (DORA) regelt das Risikomanagement für Informations- und Kommunikationstechnologie (IKT) in Finanzdienstleistungsunternehmen auf EU-Ebene. Bisher war dies in Deutschland nur durch die BaFin (BAIT, MaRisk) geregelt.

Größere Verantwortung für das Leitungsorgan

Die Verantwortung des Leitungsorgans wird durch DORA stärker betont als bisher. Es muss eine führende Rolle bei der Umsetzung übernehmen und sich persönlich das notwendige Wissen aneignen, um alle relevanten Aspekte beurteilen zu können. Das bedeutet, dass die gesamte Geschäftsleitung und in Grundzügen auch der Verwaltungsrat sich die grundlegenden Kenntnisse über DORA und IKT aneignen und dieses Wissen ständig aktualisieren müssen.

Unterstützung durch unsere Seminar-Reihe

Unsere Seminar-Reihe **„DORA für Vorstände und Verwaltungsräte“** hilft Ihnen dabei, Sachkunde einfach und komfortabel vorzuhalten und nachzuweisen. In unseren Seminaren vermitteln wir Ihnen alle notwendigen Grundlagen, speziell auf das Top-Management zugeschnitten. Wir verfolgen für Sie kontinuierlich alle Entwicklungen und informieren Sie über Neuerungen per E-Mail und, wenn gewünscht, in zusätzlichen Update-Seminaren. So bleibt Ihr Wissen immer auf dem neuesten Stand.

Termine:

Monatlich, jeweils von 14:00-16:30 Uhr.

Die nächsten Termine finden Sie hier:www.etl-consit.de/events

(einfach unter Themen auf Filter DORA klicken) oder alternativ: E-Mail an akademie@etl-consit.de senden.

DIIR: Top-Risiken 2025 im Fokus!

Das DIIR ist maßgeblich an der seit 2017 publizierten Studie „Risk im Focus“ beteiligt, die jährlich die wichtigsten Risiken für Unternehmen in Europa aus Sicht von Vorstands- und Aufsichtsratsmitgliedern sowie Revisionsleitungen ermittelt. Die Ergebnisse können u.a. auch wichtige Impulse für die Planung der Internen Revision liefern. Die Berichterstattung zu den aktuellen Ergebnissen erfolgt in diesen Tagen.

Wir werden in unserer nächsten Ausgabe detailliert dazu berichten!

Pragmatischer Check-up der Revisionsprozesse

Regelmäßig berät die ETL consit Revisionsbereiche zur Qualität deren Methoden und Prozesse und gibt dabei wichtige und praxisbezogene Optimierungshinweise. Unser erfahrenster Spezialist hinsichtlich der Prüfung von Revisionssystemen, Herr Oliver Hansen (Dipl.-Kfm., CIA, CRMA), gibt im Interview Antworten auf die häufigsten diesbezüglichen Fragen:

Herr Hansen, welchen Mehrwert bietet ein Check-up der Revisionssysteme, insbesondere hinsichtlich einer gewissen Prüfungssicherheit bei späteren externen Prüfungen der Revision?

Unsere Check-ups, oder Quality Assessments basieren auf dem DIIR-Revisionsstandard Nr. 3 bzw. IDW PS 983. Dabei wird die Einhaltung der Global Internal Audit Standards, d.h. die Einhaltung der weltweit betriebswirtschaftlichen Normen zur Internen Revision beurteilt und zertifiziert. Strenge Nebenbedingung sind dabei stets die MaRisk. Als anerkannte berufsständische Norm wird ein Quality Assessment sehr positiv bei externen Prüfungen anerkannt, insbesondere bei Prüfungen nach §44 KWG. Mir ist bei der Durchführung der praxisorientierte Austausch mit der Revisionsleitung und dem zuständigen Vorstand immens wichtig.

Inwieweit werden konkrete Handlungsvorschläge zur Verbesserung bzw. Schließung etwaiger Lücken geliefert?

Praxisorientierte Handlungsvorschläge im Sinne von Best-Practice-Ansätzen sind stets Bestandteil unserer Dienstleistungen. Hier bringen wir über 20 Jahre Erfahrungen im Sparkassenumfeld mit. Da ich auch als 44er-Prüfer im Auftrag der BaFin tätig bin, kann ich die aufsichtliche Sichtweise konkret berücksichtigen.

Inwieweit wird die neue Logik nach BdZ-Revision bereits berücksichtigt?

Selbstverständlich wird die BdZ-Logik ggf. beim Check-up berücksichtigt (die Stärken, aber eben auch die Schwächen!), ich schule übrigens auch Revisoren hinsichtlich dieser Methodik.

Wie viel Aufwand ist seitens der Internen Revision für die Beratung einzuplanen?

Für ein Quality Assessment nach DIIR-Revisionsstandard Nr. 3 bzw. IDW PS 983 ist in der Regel mit 10 bis 12 Tagen zu kalkulieren. Mitbewerber bieten hier teilweise QA mit über 20 Tagen an, das halte ich für nicht zielführend.

Vielen Dank, Herr Hansen, für diesen hilfreichen Einblick in unsere Check-ups. Für weiterführende Infos stehen wir allen Interessenten jederzeit gerne zur Verfügung.

Als Revision gut auf DORA für 2025 eingestellt?

So langsam wird es auch für die Interne Revision konkreter mit DORA.

Haben Sie bereits alle Weichen gestellt? Können Sie sich schon entspannt zurücklehnen?

Waren die vergangenen beiden Jahre seit Inkrafttreten des Digital Operational Resilience Act (DORA) noch stark geprägt von überwiegend ablauforganisatorisch geprägter Betriebsamkeit und entsprechenden Projekttätigkeiten in den Unternehmen, so wird spätestens mit Gültigkeit der Regelungen ab 17. Januar 2025 auch die Interne Revision angemessene Prüfungstätigkeiten in den Prüfungsplan ab 2025 aufnehmen müssen.

Hierbei dürften zunächst die Projektumsetzungen im Fokus stehen. Im weiteren Verlauf wären dann z.B. folgende Schwerpunkte in den regelmäßigen Prüfungsplan zu überführen:

- IKT Risikomanagement
- Behandlung, Klassifizierung und Berichtserstattung IKT-Fälle
- IKT Drittparteienrisiko
- Überwachung von kritischen Dienstleistern
- Vereinbarung über den Austausch von Informationen sowie Cyberrisken und Notfallübungen

In unserem Online-Seminar „DORA für Revisoren“ erläutern wir Ihnen gern, worauf es dabei zukünftig ankommt.

Termin:

03.12.2024 14.00-16.30 Uhr **Jetzt anmelden**

Noch einfacher: Die ETL consit übernimmt auch gern die DORA-Prüfungen in/ab 2025 für Ihr Institut. Gerne Anfragen: +++ Wir prüfen für Sie +++

Erweiterte Anforderungen an das Informationssicherheitsmanagement

Die Anforderungen an ein effektives Risikomanagement für Unternehmen bezüglich Cyberbedrohungen und Risiken für Informations- und Kommunikationstechnologien (IKT) gewinnen u.a. durch DORA zunehmend an Komplexität.

Unter dem Arbeitstitel „ISB+“ werden z.B. im Rahmen des DSGV-Projektes der Sparkassen-Finanzgruppe die künftigen erweiterten Anforderungen an Informationssicherheitsbeauftragte zusammengefasst, um das IKT-Risikomanagement auf das geforderte, noch höhere Niveau zu heben.

Experten zufolge bedeuten die erweiterten Anforderungen einen ca. 30% höheren Ressourceneinsatz als bei der herkömmlichen Tätigkeit als Informationssicherheitsbeauftragter. Bereits heute erreichen uns viele diesbezügliche Kundenanfragen.

Sollten auch Sie Interesse an Unterstützung bei den erweiterten Anforderungen haben, stehen wir Ihnen jederzeit gern für ein unverbindliches individuelles Angebot zur Verfügung.

Unsere KI-Seminare im aktuellen Fokus: Die ETL-Akademie empfiehlt…

Künstliche Intelligenz ist für viele Experten der nächste Quantensprung, der nicht zuletzt unsere Arbeitsprozesse ein weiteres Mal revolutionieren könnte. Verschaffen Sie sich schon jetzt in unseren spannenden Seminaren dazu einen lehrreichen und unterhaltsamen Überblick:

S-KiPilot, ChatGPT & Dall-E: Grundl. inkl. Datenschutz und Risiken	Nächster Termin:	14.01.2025
ChatGPT Neuerungen – Was kann es (noch) besser als der S-KiPilot?	Nächster Termin:	28.01.2025
ChatGPT in der Anlageberatung	Nächster Termin:	12.02.2025
ChatGPT in der Informationssicherheit und für alle anderen Beauftragten	Nächster Termin:	26.02.2025
Einsatz des Microsoft Copiloten in der Sparkasse	Nächster Termin:	11.03.2025

Unser Gesamtprogramm 2025

Quishing: Eine neue Bedrohung im digitalen Zeitalter

In der heutigen digitalen Welt entwickeln sich Cyberbedrohungen ständig weiter. Eine der neuesten Bedrohungen ist das sogenannte “Quishing”. Der Begriff “Quishing” setzt sich aus “QR-Code” und “Phishing” zusammen und beschreibt eine Methode, bei der Cyberkriminelle QR-Codes nutzen, um ahnungslose Nutzer zu täuschen und ihre persönlichen Daten zu stehlen.

Wie funktioniert Quishing?

- **Erstellung eines gefälschten QR-Codes**: Angreifer erstellen einen QR-Code, der auf eine gefälschte Website verweist.
- **Verteilung des QR-Codes**: Der QR-Code wird an öffentlichen Orten, in E-Mails oder auf Social-Media-Plattformen verbreitet.
- **Täuschung des Benutzers**: Der Benutzer scannt den QR-Code und wird auf die gefälschte Website geleitet.
- **Datendiebstahl**: Auf der gefälschten Website gibt der Benutzer seine vertraulichen Informationen ein, die dann von den Angreifern gestohlen werden.

Schutzmaßnahmen gegen Quishing

Um sich vor Quishing zu schützen, sollten Benutzer folgende Vorsichtsmaßnahmen treffen:

- **QR-Codes überprüfen**: Scannen Sie nur QR-Codes von vertrauenswürdigen Quellen.
- **URL prüfen**: Achten Sie darauf, dass die URL der Website, auf die Sie geleitet werden, korrekt und vertrauenswürdig ist.
- **Sicherheitssoftware verwenden**: Nutzen Sie Sicherheitssoftware, die vor Phishing-Angriffen schützt.
- **Aufmerksam bleiben**: Seien Sie skeptisch gegenüber QR-Codes, die an ungewöhnlichen Orten oder in unerwarteten Kontexten auftauchen.

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