„Fantasie ist wichtiger als Wissen, denn Wissen ist begrenzt.“

Albert Einstein

Liebe Kunden und Geschäftspartner,

an dieser Stelle hätten wir gleich wieder das Logo der vorherigen Ausgabe platzieren können, denn die Digitalisierung bietet uns natürlich tagtäglich neue Chancen und stellt uns in allen Bereichen immer wieder vor neue Herausforderungen. Eng damit verknüpft ist u.a. auch das Thema „Künstliche Intelligenz“, auf welches wir in diesem Newsletter ebenfalls eingehen möchten.

Unser erfahrener Fachbereichsleiter im Bereich IT-Revision, Alexander Heffel, lässt uns an seinen Überlegungen zu den digitalen Entwicklungen und Möglichkeiten in der IT-Revision teilhaben. Herzlichen Dank dafür, Alex!

Bei DORA möchten wir heute auf konkrete Anforderungen und Herausforderungen bezüglich „Schwachstellen-Scans“ aufmerksam machen.

Die EU hat kürzlich mit dem AI Act als erste staatliche Institution Leitplanken und Regelungen im Umgang mit künstlicher Intelligenz geschaffen.

Und, last but not least, die DSGVO feiert ihren sechsten Geburtstag! Vielleicht die Gelegenheit, einmal ein kurzes Resümee zu ziehen.

Weitere Themen in diesem Newsletter für Sie:

- Seminare im Fokus: Unsere aktuell am häufigsten nachgefragten Seminare
- Meldestelle gemäß Hinweisgeberschutzgesetz: Unser Service für Sie
- Unsere Aktion: „Kickertische für den guten Zweck“

Wir wünschen Ihnen einen schönen Start in den Frühling und weiterhin maximalen Erfolg bei allen anstehenden Herausforderungen und Projekten!

Herzlichst

Bernd Schmid Oliver Gose

Schwachstellen-Scans gemäß DORA

Hinsichtlich Schwachstellen-Scans gibt es, zusammengefasst, u.a. folgende Anforderungen des Digital Operational Resilience Act (DORA):

Automatische Schwachstellen-Scans in der IT-Sphäre der Institute, abhängig von „Klassifizierung“ und „Gesamtrisikoprofil“ der jeweiligen Assets.

Bei kritischen und wichtigen Funktionen sind diese **mindestens wöchentlich** durchzuführen.

Im dazu am 16.04.2024 veröffentlichten Kurzleitfaden des DSGV zum DORA-Projekt heißt es diesbezüglich: „***Schwachstellenauswertungen erfordern Spezialwissen und sind in der Regel noch schwieriger auszuwerten als z.B. die üblichen Sicherheitsüberwachungsprotokolle in IT-Audit-Dienstleistungen. Das Spezialwissen ist in Sparkassen oft nicht verfügbar und müsste entweder durch geeignete Schulungen aufgebaut werden, geschultes Personal beschafft oder die Auswertung ausgelagert werden. Diese Herausforderung besteht unabhängig davon, ob institutsindividuelle Scan-Tools beschafft werden oder zentrale Schwachstellenscans der Finanz Informatik bezogen / ausgeweitet werden.“***

Benötigen Sie hierbei praxisnahe Unterstützung, Beratung oder Schulung? Können wir Ihnen Aufgaben zu Ihrer Entlastung abnehmen? Dann sprechen Sie uns gerne an!

Digitale Entwicklungen in der IT-Revision

Die zunehmende Digitalisierung hat einen erheblichen Einfluss auf die Durchführung von IT-Revisionsprüfungen in Unternehmen. Traditionelle Prüfmethoden werden durch innovative Technologien und Ansätze ersetzt, um den Anforderungen einer digitalisierten Geschäftsumgebung gerecht zu werden.

In der Ära der Digitalisierung sind Unternehmen mit komplexen IT-Systemen konfrontiert, die ständigen Veränderungen unterliegen. Dies erfordert eine Anpassung der IT-Revisionsprüfungen, um den neuen Herausforderungen gerecht zu werden. Eine zentrale Veränderung liegt in der verstärkten Nutzung von Datenanalytik und künstlicher Intelligenz (KI) zur Identifizierung von Risiken und Schwachstellen in den digitalen Systemen.

Durch den Einsatz von fortschrittlichen Analysetools können IT-Revisionsprüfer riesige Datenmengen analysieren und potenzielle Risiken schneller und präziser identifizieren. Dies ermöglicht eine proaktivere Herangehensweise an Sicherheitsaspekte und trägt dazu bei, potenzielle Schwachstellen zu beheben, bevor sie zu ernsthaften Problemen führen.

Ein weiterer wichtiger Aspekt der Digitalisierung in der IT-Revisionsprüfung ist die Automatisierung von Prozessen. Routineaufgaben, wie die Überprüfung von Zugriffsrechten oder Compliance-Checks, können durch automatisierte Systeme effizienter durchgeführt werden. Dies ermöglicht den Prüfern, sich verstärkt auf komplexe Analysen und strategische Aspekte zu konzentrieren.

Die Digitalisierung hat jedoch auch Herausforderungen mit sich gebracht, insbesondere im Bereich der Datensicherheit und -integrität. Der Schutz sensibler Informationen vor Cyberbedrohungen ist zu einer zentralen Aufgabe der IT-Revisionsprüfung geworden. Die Implementierung von verschlüsselten Kommunikationsprotokollen und modernen Sicherheitslösungen ist entscheidend, um den Datenschutz zu gewährleisten.

Zusammenfassend lässt sich feststellen, dass die Digitalisierung die IT-Revisionsprüfungen grundlegend verändert hat. Die Integration von Datenanalytik, künstlicher Intelligenz und Automatisierung ermöglicht eine effizientere und präzisere Überprüfung der digitalen Systeme. Dennoch müssen Unternehmen auch auf die Sicherheitsaspekte achten, um die Integrität ihrer Daten zu gewährleisten. Die kontinuierliche Anpassung der Prüfmethoden an die sich wandelnde Technologielandschaft bleibt ein Schlüsselfaktor für den Erfolg von IT-Revisionsprüfungen in der digitalen Ära.

Bleiben Sie mit der ETL consit GmbH als Partner bei ihren IT-Prüfungen stets auf der Höhe der Zeit!

AI Act beschlossen: EU-Parlament verabschiedet risikoorientierte Regeln für den Umgang mit künstlicher Intelligenz

Die EU geht voran und stellt sich als erste staatliche Institution der Herausforderung, Leitplanken und Regelungen im Umgang mit künstlicher Intelligenz zu schaffen. Der dabei gewählte risikoorientierte Ansatz soll zugleich vor Gefahren schützen, als auch der Entwicklung von Innovationen förderlich sein. Der AI Act ergänzt insofern die EU-DSGVO.

Durch die Risikoorientierung soll ein belastbares Gleichgewicht zwischen wirtschaftlichen Chancen und Neuerungen, sowie technischem Fortschritt auf der einen Seite und dem Schutz der Rechte der Bürgerinnen und Bürger auf der anderen Seite geschaffen werden.

Dazu unterscheidet der AI Act, neben Einsatzgebieten mit geringem oder nur als marginal eingeschätztem Risiko (z.B. erkennbare Chatbots), im Kern zwischen **verbotenen Anwendungsbereichen**, z.B. biometrischen Kategorisierungen anhand sensibler Merkmale oder ungezieltes Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungskameras, weiterhin algorithmische Bewertungssysteme, Emotionserkennungssysteme am Arbeitsplatz oder in Schulen sowie den Einsatz von KI um menschliche Verhaltensweisen und Schwächen auszunutzen, um nur einige Beispiele zu nennen, **sowie Hochrisikosystemen**, bei denen besondere Verpflichtungen, insbesondere bezüglich Dokumentation, Datenschutz und Transparenz notwendige vorherige Voraussetzung sind, um die Sicherheit, Gesundheit oder die Grundrechte in der EU zu schützen.

Für Verstöße sind hohe Sanktionen vorgesehen.

Unternehmen müssen bei Einsatz und Speicherung von Daten sicherstellen, dass diese ordnungsgemäß kategorisiert und nur im erlaubten Rahmen verwendet werden. Auch auf den ersten Blick nur kleinere Automatisierungsvorgänge können hierbei unter den AI Act fallen.

Unsere Spezialisten helfen und beraten bei allen Fragen zu diesem Thema, von der KI-Strategie, dem Datenmanagementprozess bis zu Einzelfragen bei Dokumentation, Transparenz und Kontrollverfahren.

6 Jahre EU-DSGVO – Wie gut sind Sie im Datenschutz aufgestellt?

Die EU-Datenschutz-Grundverordnung (DSGVO) feiert in Kürze sechsten Geburtstag! Ein guter Zeitpunkt für Unternehmen, um zu schauen, ob auch sie alle ihre „Schulaufgaben“ gemacht haben und die Prozesse bezüglich des Datenschutzes noch auf der Höhe der Zeit sind. Die Anforderungen und die Komplexität sind weiterhin hoch, und auch kleineren Unternehmen drohen im Falle von Pannen und Verstößen massive Konsequenzen und Sanktionen. Auch das Reputationsrisiko kann immens sein. Zusätzlich sorgt die voranschreitende Digitalisierung unserer Gesellschaft regelmäßig für neue Chancen, aber eben auch für Herausforderungen, gerade beim Datenschutz!

Für kleinere und mittelständische Unternehmen gibt es nur wenige „Hands on-Ansätze“, um die eigene Betroffenheit einschätzen und analysieren zu können bzw. überhaupt eine erste Awareness für diese Themen zu schaffen.

Im Rahmen einer allgemeinen Erstinformation und individuellen Betroffenheitsanalyse beraten wir gern und verschaffen eine erste Positionsbestimmung und Einschätzung der individuellen Gefährdungs- und Risikosituation (inklusive potentielle Sanktions- und Imageschäden) bezüglich Datenschutz, IT-Sicherheit, Cyber-Security und Compliance. In diesem Checkup geht es z.B. um effektive Prävention, Datenschutzanfragen, Datenschutzverletzungen / -pannen, IT-Sicherheitsvorfälle, Schadsoftwarebefall, Phishing, CEO-Fraud, Erpressungsversuche, Verschlüsselungstrojaner, sonstige individuelle Situation sowie spezielle Fragestellungen.

Sichern Sie sich gern einen Termin bei unseren Spezialisten!

Seminare im aktuellen Fokus: Die ETL-Akademie empfiehlt…

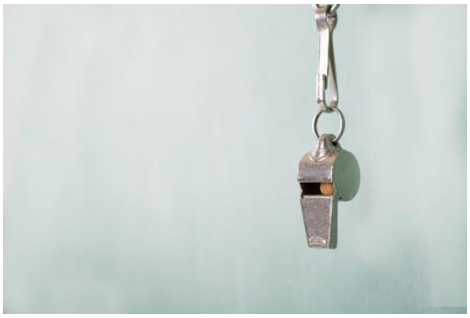
DORA für Vorstände und Verwaltungsräte	Nächster Termin:	06.05.2024	Jetzt anmelden
Die Global Internal Audit Standards 2024	Nächster Termin:	30.07.2024	Jetzt anmelden
Nachhaltigkeit in Kreditinstituten	Nächster Termin:	02.07.2024	Jetzt anmelden
Künstliche Intelligenz - ein Praxistest	Nächster Termin:	01.10.2024	Jetzt anmelden

Unser Gesamtprogramm

Kickertische für den guten Zweck!

Im Rahmen unserer Aktion „Wir bauen Kickertische für den guten Zweck“ wurden die letzten beiden Kickertische an antonius – gemeinsam Mensch übergeben. Einer der Kickertische hat seinen Platz im Hofcafe gefunden und der anderen kam dem neuen Jugendraum zugute!

Meldestelle gemäß Hinweisgeberschutzgesetz (HinSchG)



Das Hinweisgeberschutzgesetz trat im Sommer 2023 in Kraft.

Durch das Hinweisgeberschutzgesetz werden interne Hinweisgeber geschützt und einheitliche Standards zur Meldung von Missständen im Unternehmen und zum Schutz der Meldenden vorgeschrieben. Bei Nichtbeachtung drohen Bußgelder bis zu 20.000 Euro.

Viele mittelständische Unternehmen nutzen die Gelegenheit, zusammen mit anderen Unternehmen eine „gemeinsame Meldestelle“ zu betreiben.

Selbst für sehr kleinere Unternehmen kann eine Meldestelle Sinn machen.

Gern unterstützt Sie unsere Experten bei der Einrichtung einer internen Meldestelle oder der Optimierung Ihres Whistleblower-Systems bzw. übernehmen gleich deren Aufgaben für Sie.

Profitieren auch Sie von unserer langjährigen Erfahrung mit Hinweisgebersystemen.

Immer eine gute Idee…sprechen Sie uns gerne an!

Dipl.-Betriebswirt

Oliver Gose

Mitglied der Geschäftsführung

04531 6696-422

oliver.gose@etl-consit.de

Dipl. Bankbetriebswirt | CISA, CDPSE

Bernd Schmid

Geschäftsführer

04531 6696-28

bernd.schmid@etl-consit.de

Impressum

Redaktion: Oliver Gose, Bernd Schmid

Anschrift: ETL consit GmbH, Schützenstr. 25 a,
23843 Bad Oldesloe

Telefon: (04531) 66 96-422

Bildquellen: Eigene, MS Word Archiv, pixabay.com