

**Stellungnahme zur Einführung und Zertifizierung eines Informationssicherheits-Managementsystems gemäß DIN EN/ISO 27001 bei der Deutschen Börse Commodities GmbH**

Die Einführung eines ISMS und vor allem dessen Zertifizierung gemäß DIN EN/ISO 27001 (oder von entsprechenden Derivaten) ist prinzipiell immer eine rein freiwillige Entscheidung der Leitung. Diese Freiwilligkeit verfällt erst dann, sobald das Unternehmen durch externe Vorgaben (etwa wir in der Automobilindustrie durch TISAX®) oder im Finanzbereich durch die BaFin (MaRisk/BAIT/VAIT etc.) zur Zertifizierung angehalten ist, da ansonsten Sanktionen drohen. Aufgabe war es daher, zu eruieren, ob die Einführung eines ISMS gemäß DIN EN/ISO 27001 nicht nur sinnvoll, sondern aus rechtlicher oder regulatorischer Sicht als zwingend notwendig einzuordnen ist.

Dazu wurde die aktuelle prozessuale und infrastrukturelle Situation der Deutschen Börse Commodities GmbH auf der Basis der von der Geschäftsführung bereitgestellten Informationen geprüft und bewertet. Hierbei wurde insbesondere das Augenmerk auf die Integration der wesentlichen IT-gestützten Unternehmensprozesse in die ausgelagerten Prozesse (z.B. Deutsche Börse AG) geachtet und auch darauf, ob die drei regelmäßigen wesentlichen Stakeholder (Revision, Wirtschaftsprüfung und Informationssicherheitsbeauftragter) zum einen in diesem Punkt relevant sind und zum anderen, ob sie ggf. entsprechende relevante Anforderungen formulieren könnten.

*Beurteilung*

Wenngleich der Unterzeichner anmerkt, dass im Zuge des Fortschreitens der Anforderungen an die Informationssicherheit – vor allem für Unternehmen im Finanzsektor – eine ständige Anpassung und Überwachung grundsätzlicher Informationssicherheitsprozesse und deren Dokumentation anzuraten ist, ergab die Prüfung, dass eine ISMS-Zertifizierung gemäß DIN EN/ISO 27001 bei der Deutschen Börse Commodities GmbH nach Ermessen des Unterzeichners weder aus rechtlicher noch aus regulatorischer Sicht zwingend erforderlich ist.

Egelsbach, 24.05.2022



Alf Leue

ALF LEUE | CONSULTING · IM KAMMERECK 1 · 63329 EGELSBACH · DEUTSCHLAND / GERMANY

INFORMATION SECURITY AWARENESS KOORDINATOR (TÜV RHEINLAND – ZERT.NR. 3466375)

INFORMATION SECURITY OFFICER ACCORDING TO ISO/IEC 27001 (TÜV SÜD – CERT.NO. 2035#313520307)

ZERTIFIZIERTER DATENSCHUTZBEAUFTRAGTER (TÜV NORD – CERT.NO. 44-02-DSB-02.08.2018-DE02-1 009243)

SPARKASSE LANGEN-SELIGENSTADT · BLZ 50652124 · KONTO 26130377 · BIC: HELADEF1SLS · IBAN: DE 05 5065 2124 0026 1303 77

MOBIL: +49 176 57584041 · FON: +49 6103 4875918 · CONSULTING@ALFLEUE.COM · WWW.ALFLEUE.COM · STEUER-NR.: 028 841 31567 · USTID.: DE235201497