ISACA Germany Chapter Berufsverband der
IT-Revisoren und IT-Sicherheitsmanager e. V.

Stellungnahme zum

Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes und zur Regelung des Datenschutzaudits– Stand 22.10.2008

Artikel 2

Zu §4 Zulassung der Kontrollstellen und Entziehung der Zulassung

Hier: (1), 2.
Die hier als ausschließliches Kriterium genannte DIN EN 45011, Allgemeine Anforderungen an Stellen, die Produktzertifizierungssysteme betreiben, ist u. E. nicht sachgerecht.

Begründung:
Datenschutz ist unserer Auffassung nach nicht als Produkt, sondern als laufender Prozess in den Unternehmen anzusehen. Ein direkter Bezug der DIN-Vorschrift zum gesetzlichen Gegenstand oder zum Umfeld (Informationstechnologie) ist nicht gegeben.

Der Standard DIN ISO/IEC 17021, „Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren“, trifft eher den Charakter des Datenschutzes, der im wohlverstandenen Sinne Teil eines integrierten Managementsystems der Unternehmen und des IKS sein sollte.

Hier stellt sich auch die Frage der Akkreditierungsstelle, da der Deutsche Akkreditierungsrat im Wesentlichen aus Vertretern nicht-öffentlicher Institutionen gebildet ist. Unseres Wissens plant das BMWi hierzu eine Neuregelung, die ggf. flexibel mit einbezogen werden sollte.

Es stellt sich hier auch im Weiteren die Frage, ob eine Akkreditierung nicht unmittelbar mit der Zulassung, also generisch, verbunden sein sollte. Dies würde zum einen den Vorteil einer größeren Unabhängigkeit der zulassenden Stelle erbringen und zum anderen zur Effizienzsteigerung des Zulassungsprozesses führen. Darüber hinaus wäre eine – in Verbindung mit den Kriterien des §9 (s .u.) – größere Flexibilität bei der Auswahl und Bewertung der Kontrollstellen möglich.

Zu §9 Anforderungen an Kontrollstellen

Hier: (3)
Der einleitende Satz zur grundsätzlichen Eignung der Kontrollstelle in Bezug auf ihr zur Verfügung stehendes Personal (Ausbildung, berufl. Bildung, Berufserfahrung) findet unsere ausdrückliche Zustimmung. Die dazu erforderlichen Nachweise, die sich in die Bereiche „Recht“ und „Informationstechnik“ gliedern, sind u. E. wesentlich zu eng gefasst und aus unserer Erfahrung nicht praxisgerecht.

Begründung:
Es sollte u. E. zunächst klar definiert werden, dass die Einsatzmöglichkeit eines Juristen, oder eines Technikers Mindestvoraussetzung für die Zulassung ist. Dieser Eindruck wird durch die Aufteilung in Bereiche erweckt, ist aber nicht so gefordert.

Zu den Nachweisen im Bereich Informationstechnik ist aus unserer Sicht zu sagen, dass die geforderten Alternativen nicht der Erfahrung der Praxis entsprechen:

- ein Naturwissenschaftler mit Schwerpunkt Informatik ist z.B. ein Chemiker mit Schwerpunkt Anlageninformatik; es ist u. E. evident, dass diese Qualifikation zwar den formalen gesetzlichen Bedingungen entspricht, aber nicht unbedingt dem eigentlichen Auftrag gerecht wird;
- nicht enthalten ist der Zweig der Betriebswirte mit Schwerpunkt Informatik; hier ist der Diplom-Kaufmann, -Betriebswirt oder Bachelor mit solidem informationstechnischen Wissen aufgrund seiner Kenntnisse der betrieblichen Zusammenhänge sicher im Sinne des Auftrags geeignet, wäre aber nach den o. a. Kriterien abzuweisen;
- um auch im Sinne der Arbeit unseres Verbandes hier ein Zeichen zu setzen: eine Person mit Ausbildung als Datenverarbeitungskaufmann und mit der Qualifikation als CISA[1] stellt sich wie folgt dar:
  - ° CISA bedeutet das erfolgreiche Ablegen eines qualifizierenden Berufsexamens im Bereich IT-Audit;
  - ° CISA bedeutet mehrjährige Berufserfahrung als Voraussetzung zur Zertifizierung;
  - ° CISA bedeutet die Verpflichtung zur berufsbezogenen Weiterbildung zur Erhaltung der Zertifizierung, insbesondere durch den Zwang zur Vorlage einer jährlichen Mindestanzahl von CPE Stunden;
  - ° CISA bedeutet die bindende Verpflichtung auf einen strikten Ethik-Kodex
  - ° CISA bedeutet auch den automatischen Verlust der Zertifizierung bei Nichteinhaltung der o.a. Kriterien

  Im dargestellten Beispiel wäre die beschriebene Person trotz der o. a. Qualifikation dennoch nicht geeignet, da kein abgeschlossenes Studium in Jura oder Informatik vorliegt.

  Dies ist u. E. nicht praxisgerecht oder im Sinne des Auftrags erfolgversprechend.

Dies führt zu einem weiteren, unserer Auffassung nach nicht sachgerechten Anspruch an den Aspekt der Qualifizierung der Kontrollstelle.

Die Qualifikationsanforderungen im Bereich „Audit“ fehlen vollständig.

Begründung:
Es ist unserer Erfahrung nach nicht damit getan, dass eine Person, die Audits durchführen möchte, allein Fachkenntnisse über das zu prüfenden Objekt besitzt. Vielmehr ist die Voraussetzung für einen erfolgversprechenden Auditprozess mit der notwendigen Methodenkompetenz in Auditverfahren und –techniken verbunden. Eine derartige Qualifikation als Eignungskriterium fehlt hier aber in Gänze.

Der Hinweis auf die Akkreditierung nach DIN EN 45011 in §64 ist nicht geeignet, um dieses Manko aufzufangen. Vielmehr ist die Fähigkeit, IT-Systeme und Prozesse in der notwendigen Qualität, mit einem hinreichenden Methoden-Know-How prüfen zu können, gerade für den informationstechnischen Teil des Datenschutzaudits unabdingbar.

Darüber hinaus werden Auditoren in der Regel zu den Themen Konfliktmanagement, Moderation, Verhandlungstechniken und Präsentationstechniken eingehend geschult, damit sie in der Lage sind, die Ergebnisse der Audits der Unternehmensführung sachgerecht darzustellen. Insbesondere hängt der Erfolg eines erfolgreichen Audits davon ab, dass die

[1] CISA = Certified Information Systems Auditor

geprüften Bereichen, gerade bei negativen Befunden, die Ergebnisse anerkennen und Verbesserungsvorschläge umsetzen.

Naturgemäß können wir als Verband nur auf die Qualifikationsmöglichkeit unseres Verbands (CISA) hinweisen und bitten darum, diese sachdienliche und hochqualitative berufliche Bildung, angemessen zu berücksichtigen.

Zu §12 Mitglieder des Datenschutzauditausschusses
Hier: (1)
Die Zusammensetzung des Datenschutzauditausschusses aus verschiedenen Wirkungskreisen begrüßen wir im Sinne des gesellschaftlichen Pluralismus. Es wäre aus unserer Sicht politisch angemessen und sachlich notwendig, neben den Unternehmerverbänden, die sicher ein berechtigtes Interesse an einer gut funktionierenden Verfahrenskontrolle und –entwicklung haben, gerade auch Vertreter aus den Berufsverbänden, die sich sowohl in ihrer täglichen Arbeit als auch in konzeptionellen Fragen mit der Thematik befassen, in diesem Ausschuss zu beteiligen.

Gerne sind wir als Berufsverband der IT-Auditoren (und IT-Sicherheitsmanager) bereit, hier auch Verantwortung zu übernehmen und uns an der Arbeit des Ausschusses zu beteiligen.