

### ***Control 1.6.1: Inwieweit werden Informationssicherheitsereignisse verarbeitet?***

Eine zusätzliche Muss-Anforderung für Informationen mit hohem Schutzbedarf bei diesem Control lautet:

„Anforderungen aus Geschäftsbeziehungen (z. B. Meldepflichten an die Auftraggeber) sind ermittelt und umgesetzt.“

Diese eigentlich unkomplizierte Anforderung wird von vielen Unternehmen oftmals vergessen bzw. falsch interpretiert. Doch was genau ist jetzt eigentlich damit gemeint?

Wie auch in Control 7.1.1 (Vertragliche Bestimmungen) gefordert, sollten zunächst alle Verträge mit Auftraggebern geprüft werden, inwieweit in diesen auch Anforderungen an die Informationssicherheit festgelegt wurden. In der Regel sind dies mitgeltende Unterlagen, zum Beispiel in Form von Sicherheitsrichtlinien oder Handlungsleitlinien für Dienstleister.

Schaut man sich diese genauer an, findet man recht schnell auch Anforderungen zum Verhalten bei Sicherheitsvorfällen, sofern Informationen des Auftraggebers betroffen sind.

In der Handlungsleitlinie eines OEM heißt es beispielsweise: „Informationssicherheitsereignisse (z. B. auftretende Störungen, Verstöße gegen das Informationssicherheits-Regelwerk), welche Daten oder Systeme des Auftraggebers betreffen, sind unverzüglich der zuständigen Stelle zu melden.“ Eine entsprechende Hotline und auch eine E-Mail-Adresse der zuständigen Stelle sind zusätzlich genannt.

Um diese Anforderung zu erfüllen, sollten daher alle vorliegenden vertraglichen Regelungen identifiziert und auf vergleichbare Passagen abgeprüft werden. Verweise auf die entsprechenden identifizierten Kontaktstellen sollten dann in den eigenen internen Richtlinien aufgelistet sein.