### *Control 1.3.3: Inwieweit wird sichergestellt, dass nur evaluierte und freigegebene organisationsfremde IT-Dienste zum Verarbeiten von Informationswerten der Organisation eingesetzt werden?*

Eine der MUSS-Anforderungen dieses Controls lautet: „Es werden keine organisationsfremden IT-Dienste ohne explizite Bewertung und Umsetzung der Informationssicherheitsanforderungen eingesetzt."

Die erste Reaktion der Unternehmen auf diese Anforderung geht oftmals in die Richtung: „Wir nutzen keine Cloud-Dienste. Das trifft auf unser Unternehmen nicht zu." Dieses Control wird folglich bei der Selbsteinschätzung ausgeschlossen.

Was viele Unternehmen in diesem Moment jedoch vergessen, ist das heutige breite Angebot von IT-Diensten im Internet, wie z.B. E-Mail, Messenger-Dienste, Übersetzungsdienste, Datenaustauschportale, etc. Diese Dienste stehen den Mitarbeitern der Organisation heute schnell, unkompliziert und zum Teil sogar kostenlos zur Verfügung. Beispielsweise ist vielen Mitarbeitern oftmals gar nicht bewusst, dass ein einfach über den Browser aufrufbare Service wie der Google-Translator, einen externen (Cloud-)Dienst darstellt.

Auditoren ist es in diesem Zusammenhang wichtig, dass neben den kostenpflichtigen Diensten, für die es in der Regel etablierte Prozesse in Hinblick auf deren Einführung und Nutzung gibt, auch die kostenlosen Dienste bei der Betrachtung berücksichtigt werden. Dies sollte mindestens eine Sensibilisierung der Mitarbeiter zu dieser Thematik umfassen.

Da sich Angebot und Anforderungen ständig ändern, ist ein reines Black- oder Whitelisting in der Praxis nicht sinnvoll. Vielmehr sollten eine Kombination und klare Regelungen zur Anwendung festgelegt werden. Identifizierte, nicht zulässige Dienste sollten – soweit technisch möglich - gesperrt sein. Für die Nutzung zulässiger und nicht erfasster Dienste sollten mit den Mitarbeitern klare Regelungen zur Anwendung vereinbart werden. Beispielsweise dürfen vertrauliche Informationen nicht online übersetzt werden oder es existiert ein Verbot zur Weiterleitung betrieblicher E-Mails an private Accounts.