Control 7.1.1: Inwieweit wird die Einhaltung regulatorischer und vertraglicher Bestimmungen sichergestellt?

Eine der MUSS-Anforderungen dieses Controls lautet:

„Gesetzliche, regulatorische und vertragliche Anforderungen und Vorgaben mit Relevanz zur Informationssicherheit (siehe Beispiele) werden regelmäßig ermittelt."

Doch welche gesetzlichen und regulatorischen Anforderungen haben Relevanz für die Informationssicherheit?

Als Hilfestellung werden im VDA ISA die nachfolgenden Anforderungen beispielhaft genannt: Urheberrecht, Kryptografie, Copyright (Lizenzen, Bilder), Intellectual Property (Patente, Know-How), Archivierung, Informationssicherheitsgesetze, Datenschutz, Geschäftsgeheimnisgesetz.

Compliance-Verstöße, also Verstöße gegen Anforderungen wie Gesetze und Regularien, können zu Risiken in der Informationssicherheit von Kunden und der eigenen Organisation führen. Daher ist wichtig, dass diese Vorgaben bekannt und umgesetzt sind.

Zunächst gilt es, sich einen Überblick zu verschaffen, welche Quellen von Vorgaben es für das Unternehmen gibt und über welche Prozesse das Unternehmen an diese Informationen kommt.

Systematisch müssen diese Informationsquellen in die Firmenprozesse eingebunden werden, um eine regelmäßige und vollständige Erfassung der Anforderungen zu gewährleisten.

Es empfiehlt sich, die ermittelten Gesetze, Regularien und vertraglichen Anforderungen in einem Compliance-Register zu dokumentieren. Folgende Unterverzeichnisse wären denkbar:

- Eigene Richtlinien, ggf. auch übergeordnete (Konzern)-Richtlinien
- Kundenrichtlinien bzw. -regularien
- Gesetzliche Bestimmungen

Die Verzeichnisse sollten in jedem Fall Freigabevermerke, eine kurze Erläuterung, Angaben zur Veröffentlichung der Anforderungen (z.B. ein Link) und Angaben zum Prüfzyklus enthalten. Wichtig dabei ist auch eine Klassifizierung der Dokumente in Bezug auf das Schutzziel Vertraulichkeit, da nicht alle Richtlinien oder Verträge für jeden Mitarbeiter einsehbar sein dürfen (z.B. Betriebshandbücher).

Im Compliance-Register der eigenen Richtlinien sollten alle freigegebenen Richtlinien des ISMS der Organisation genannt sein. Bei größeren Unternehmen kann es sinnvoll sein, auch eine Übersicht aller übergeordneten Konzern-Richtlinien, die für das Unternehmen mitgelten, zu dokumentieren und zu pflegen. Gegebenenfalls empfiehlt sich auch der Einsatz einer Richtliniendatenbank für das Unternehmen.

Kundenrichtlinien wie beispielsweise IT-Sicherheitshandlungsleitlinien, zu deren Einhaltung man aufgrund vertraglicher Bestimmungen verpflichtet ist, müssen daher ebenfalls Teil des Compliance-Registers sein. Diese existieren oftmals bei der Zusammenarbeit mit größeren Unternehmen (z.B. OEMs).

Für interne Vorgaben / Regelungen gilt: Neben den allgemeinen Richtlinien zur Informationssicherheit können das auch IT-Richtlinien, ein „Code of Conduct" oder eine „Reisekostenrichtlinie" sein.

Gesetzliche Vorgaben können über einschlägige Auskünfte bzw. über das Legal Department ermittelt werden. Die nachfolgend genannten Gesetze haben einen Bezug zur Informationssicherheit und somit ggf. eine Relevanz zur Betrachtung innerhalb des Compliance-Registers.

BAIT	Bankaufsichtliche Anforderungen an die IT
BDSG neu	Bundesdatenschutzgesetz
EU-DSGVO	Europäische Datenschutzgrundverordnung
BSI-KritisV	BSI-Kritisverordnung
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
GeschGehG	Gesetz zum Schutz von Geschäftsgeheimnissen
GoBD	Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)
GoDV	Grundsätze für eine ordnungsmäßige Datenverarbeitung

IT-SiG	IT-Sicherheitsgesetz - „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)
MaRisk	Mindestanforderungen an das Risikomanagement in deutschen Kreditinstituten
NIS-RiLi	EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-Richtlinie)
StGB	Strafgesetzbuch §§ 202a, 202b, 263a, 303a, 303b
SÜG	Sicherheitsüberprüfungsgesetz
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
UrhG	Urheberrechtsgesetz
VAIT	Versicherungsaufsichtliche Anforderungen an die IT

Darüber hinaus sind sicherlich das „Baseler Rahmenwerk“ zu nennen mit allen gültigen Standards des Baseler Ausschusses für Bankenaufsicht und der „Sarbanes Oxley Act“ für alle in- und ausländischen Unternehmen, deren Wertpapiere in den USA angeboten bzw. börslich oder außerbörslich gehandelt werden.

Diese Übersicht dient lediglich als Hilfestellung und erhebt keinen Anspruch auf Vollständigkeit. Wer hier mehr Aufwand investieren will, kann zu jedem Gesetz kurz die relevante Passage / den Paragrafen zitieren und den in der Firma zuständigen / verantwortlichen Prozess-Owner dokumentieren, durch den diese Regelung umzusetzen ist.

Achtung: Die Vorgaben sind immer aktuell zu halten. Daher empfiehlt sich ein regelmäßiger Review-Prozess. Bei internen und Kunden-Vorgaben ist die feste Integration in interne Prozesse oder Review sinnvoll. Bei gesetzlichen Vorgaben kann z.B. ein Abgleich mit der Web-Seite dejure.org erfolgen.

Ein Compliance-Register bietet die Grundlage dafür, Prozesse und Vorgehen im täglichen Betriebs-Alltag „compliant“ zu halten, d.h. gesetzes- und regelkonform zu handeln.