Governance, Risk and Compliance

Ganzheitliches Compliance-Management mit DocSetMinder

Die Einhaltung von europäischem und nationalem Recht und Vorschriften (Compliance) durch die Einführung und Aufrechterhaltung einer effektiven Corporate Governance stellt die Führungskräfte und Mitarbeiter in Organisationen jeder Art und Größe vor erhebliche Herausforderungen. Aus der Einbeziehung von beispielsweise EU-Datenschutz-Grundverordnung, NIS-Richtlinie oder BSI-Kritisverordnung in die Geschäftstätigkeit erwachsen komplexe Aufgaben, die auf dem Weg zu einer gesetzeskonformen Organisation bewältigt werden müssen. Durchdachte Planung und geeignete Compliance-Management-Software können den Aufwand zur Erfüllung regulatorischer und normativer Anforderungen signifikant senken.

Von Krzysztof Paschke und Anselm Rohrer, Allgeier CORE GmbH

Bei der immer weiter steigenden Zahl von gesetzlichen Auflagen und Normanforderungen ist es sinnvoll, einen organisationsweiten, ganzheitlichen Planungs- und Dokumentationsansatz in Form eines Compliance-Management-Systems (CMS) zu etablieren. Eine mögliche Ausgestaltung des CMS kann aus den zwei anerkannten Standards IDW PS 980 und ISO 19600 entnommen werden. Sie bauen beide auf dem Grundgedanken der Schaffung einer ganzheitlichen Perspektive auf die Geschäftstätigkeit der Organisation auf. Anstatt die Umsetzung diverser regulatorischer und normativer Auflagen einzeln zu planen und mit unterschiedlichen Tools zu realisieren, ist eine gemeinsame Betrachtung von enormem Vorteil. Die Compliance-Management-Software DocSetMinder stellt eine Reihe von aufeinander abgestimmten Modulen zur Abbildung einschlägiger Anforderungen bereit. Primär handelt es sich hier um Managementsysteme für Informationssicherheit, Datenschutz und Business Continuity. Ergänzt werden diese durch Module aus dem Bereich der TAX-Compliance, wie zum Beispiel internes Kontrollsystem oder Verfahrensdokumentation GoBD. In Abhängigkeit von der individuellen Situation der Organisation und den zu erfüllenden Anforderungen können die Module (ISO 27001, BSI 200-x, TISAX, ISIS12, IDW PS 261, PS 951, ISAE 3402, GoBD etc.) beliebig miteinander kombiniert werden.

Organisation und IT

Eine genaue Kenntnis der Organisation und ihrer Prozesse ist eine elementare Voraussetzung für die Planung und Umsetzung von Compliance-Anforderungen. Aus dem Grund bietet das Basismodul „Organisation“ die notwendigen Strukturen und Vorlagen für die Dokumentation der Aufbau- und Ablauforganisation im erforderlichen Detaillierungsgrad und unterstützt damit Unternehmen und Behörden bei der Erfassung und Pflege ihrer Organisationseinheiten (Bereiche, Abteilungen, Teams etc.), Geschäftsprozesse und Verantwortlichkeiten (Rollen). Für die Dokumentation der IT-Prozesse steht die aktuelle ITIL-Struktur zur Verfügung. Sämtliche Leit- und Richtlinien der Organisation können als richtungsweisender Bestandteil eines jeden Compliance-Management-Systems effizient vorbereitet, genehmigt und den Mitarbeitern zur Verfügung gestellt werden. Eine nicht weniger wichtige Rolle für das CMS spielen geltende Verträge mit Geschäftspartnern und die sich daraus ergebenden Verpflichtungen. Ein in DocSetMinder vollständig integriertes Vertragsmanagement liefert hierzu alle notwendigen Informationen. Die dokumentierte Aufbau- und Ablauforganisation bildet zusammen mit der IT-Dokumentation die logischen Zusammenhängte zwischen Geschäftsprozessen, Anwendungen, Serversystemen und Speicherorten für die entstehenden Informationen (Daten) ab. Diese sogenannte Strukturanalyse stellt die zur Planung, Umsetzung und Aufrechterhaltung von ISO 27001, BSI 200-x, TISAX, ISIS12, IDW PS 261, IDW PS 951, ISAE 3402, GoBD und weiteren Standards als Bestandteile eines CMS erforderlichen Sachverhalte bereit. Die gemeinsame Nutzung von strukturellen Informationen verhindert Redundanzen und vereinfacht Aktualisierungen.

Risikoanalyse

Eine Risikoanalyse liefert wichtige Erkenntnisse für die Planung und Umsetzung eines CMS.

Auch hier gilt, Compliance-Anforderungen nicht isoliert, sondern ganzheitlich zu betrachten. Wichtig dabei ist die Vereinheitlichung des Risikomanagementprozesses, Dimensionierung der Risikomatrix, Risikofaktoren (Eintrittswahrscheinlichkeit und Auswirkung) und Risikoakzeptanz. Somit können die Risiken aus den unterschiedlichen Themenbereichen, wie zum Beispiel ISMS, BCM, DSMS, IKS etc. vergleichbar gemacht und in einem Management Review übersichtlich zusammengefasst werden. Für die Durchführung der Risikoidentifikation, -analyse, -bewertung und -behandlung stehen in DocSetMinder eine Risikoanalyse gemäß ISO 31000 und daraus abgeleitete Risikoanalysemethoden gemäß ISO 27005 und BSI-Standard 200-3 zur Verfügung. Die Identifikation der Risiken kann unter Einbeziehung diverser Kataloge für Gefährdungen und Schwachstellen (BSI-Kompendium, ISO 27005 u. Ä. oder benutzerdefiniert) erfolgen. Die Risikobewertung definiert sich als Produkt aus Eintrittswahrscheinlichkeit und Auswirkung (Schadenshöhe) und wird mithilfe einer im Standard 4x4-dimensionierten Matrix durchgeführt. Die Dimensionierung der Matrix kann organisationsspezifisch angepasst werden. In der Risikoanalyse können Schutzziele V-I-V-A, Gewährleistungsziele aus dem Standard-Datenschutzmodell (SDM) und Ziele nach IDW betrachtet werden. Die Risiken werden mit geeigneten Maßnahmen (präventiv, reaktiv und korrektiv) behandelt. Auch hier können Maßnahmenkataloge von BSI und ISO herangezogen und individuell erweitert werden.

Awareness – Bewusstsein schaffen

Ein wichtiger Bestandteil eines Compliance-Management-Systems ist die Sensibilisierung von Mitarbeitern für potenzielle Gefahren. Bei der Betrachtung unterschiedlicher Standards und Normen, die im Rahmen der Etablierung eines organisationsweiten CMS umgesetzt werden, wird die Bedeutung dieser Aufklärungsarbeit sehr deutlich: Die ISO 27001 fordert ein angemessenes Bewusstsein der beteiligten Personen und das BSI veröffentlicht im IT-Grundschutz einen eigenen Baustein und eine Vielzahl von Maßnahmen hierzu. ISIS12 widmet der Sensibilisierung von Mitarbeitern einen von 12 Schritten zur vollständigen Umsetzung eines ISMS. Sucht man in TISAX nach Bewusstseinsbildung und Sensibilisierung, wird man allein im Basismodul „Informationssicherheit“ bereits 18 Mal fündig. Die DSGVO fordert zwar keine explizite Schulungspflicht, jedoch ist eine gesetzeskonforme Umsetzung des Datenschutzes ohne Sensibilisierung der Mitarbeiter nicht möglich. Diese Entwicklung trägt der Tatsache Rechnung, dass Irrtum und Nachlässigkeit eigener Mitarbeiter noch immer den größten Risikofaktor darstellen (Quelle: <kes>/Microsoft-Sicherheitsstudie 2018). Zur Umsetzung der notwendigen Awareness reichen einmalige Maßnahmen nicht aus. Vielmehr ist eine stetige, zielgruppengerechte Sensibilisierung erforderlich. Als Nachweis können, im Falle von Präsenzveranstaltungen, Unterschriften auf Teilnahmelisten dienen oder elektronische Listen im Falle von Webinaren oder E-Learning-Modulen. Je intensiver die technischen und organisatorischen Maßnahmen den Bewegungsrahmen von Anwendern einschränken, desto geringer ist der Sensibilisierungsbedarf. Gleichzeitig nehmen derartige Einschränkungen dem Anwender die Möglichkeit, flexibel auf Ereignisse im Tagesgeschäft zu reagieren. Hier ist deshalb ein ausgewogenes Verhältnis gemäß den Business-Anforderungen gefragt. Um bewusst mit Informationen umzugehen, muss der Einzelne die Konsequenzen des eigenen Handelns nachvollziehen können. Transparente Prozesse und für Anwender nachvollziehbare Richtlinien vereinfachen die Bewusstseinsbildung immens.

Fazit

Der Compliance-Druck auf Organisationen nimmt immer mehr zu und ergibt sich nicht ausschließlich aus dem Charakter der Anforderungen wie bei Gesetzen und Verordnungen. Auch die bloße Teilnahme am Markt kann mit verpflichtenden Aufgaben verbunden sein (z. B. TISAX). Dabei ist die Compliance kein einmalig zu absolvierendes Programm. Der P-D-C-A-Zyklus und die damit einhergehende Verpflichtung zur kontinuierlichen Planung, Umsetzung, Überprüfung und Verbesserung wurde in national und international anerkannte Standards wie ISO 27001 und geltende Gesetze wie DSGVO eingenäht. Der Erfolg der Etablierung und Aufrechterhaltung von Compliance hängt entscheidend von der gelebten Methode und Integration der partikulären Ziele von Informationssicherheit, Datenschutz, Business Continuity in die Geschäftsziele ab. Der Nachweis darüber wird über eine entsprechende Dokumentation erbracht. Eine geeignete Compliance-Management-Lösung ermöglicht deshalb einen ganzheitlichen Blick auf die Organisation und schafft Synergien in allen Etappen der Arbeit zur Realisierung der Anforderungen aus ISO 27001, DSGVO, IDW PS 261, PS 951, GoBD etc.

DocSetMinder bildet die anerkannten Standards und Gesetze vollständig und auf Basis einer übergreifenden Strukturanalyse ab. Der Funktionsumfang der Software macht den Einsatz weiterer Tools oder Office-Anwendungen für die Dokumentation und Prüfung überflüssig. Die Lösung ist einfach zu implementieren und intuitiv bedienbar. Die gemeinsame Nutzung der erfassten Informationen bietet allen beteiligten Mitarbeitern und Verantwortlichen einen enormen Mehrwert durch die Aktualität der Dokumentation und eine signifikante Zeitersparnis bei der Vorbereitung interner und externer Audits. DocSetMinder ist Best Practice – und Sie sind jederzeit „Ready for Audit“.