Gorodenkoff – stock.adobe.com

Starke Kombi: QM und Informationssicherheit

Warum QM und Informationssicherheitsmanagement zusammengehen

Qualitätsmanagement bleibt nicht stehen, die nachhaltig beschleunigte Digitalisierung hält Einzug in alle Lebensbereiche und bereichert auch das QM. Doch wo Chancen sind, entstehen auch Risiken. Wie also umgehen mit den Herausforderungen der Digitalisierung im Qualitätsmanagement? Die Verbindung von QM und Informationssicherheitsmanagement hat sich als konstruktiv und zukunftsfähig erwiesen.

Tabea Daunus, Klaus Kilvinger, Thomas Salvador

Das internationale Qualitätsmanagement kann heute, seit Ersteinführung der Norm-Familie rund um ISO 9001, auf eine jahrzehntelange Tradition auf dem Weg zu Business-Excellence und zu nachhaltigem Geschäftserfolg zurückblicken. Auch in der Praxis und in den meisten Unternehmen sind Prozessmanagement, risikobasiertes Denken, Qualitätswerkzeuge, Tools und der nachhaltige Einsatz von Ressourcen angekommen oder langjährig etabliert.

Gleichzeitig kommen immer wieder neue Anforderungen im Rahmen von Governance, Risk und Compliance (GRC) auf Unternehmen zu, um im fortwährenden internationalen Wettbewerb bestehen zu können. Die durch Covid-19 beschleunigte Digitalisierung hält längst Einzug auch in die Managementsystemwelt. *Informations- und Datensicherheit* sowie *Informationssicherheitsmanagementsysteme (ISMS)* sind neue Schlagworte, wenn es darum geht im internationalen Wettstreit Schritt zu halten und das höchstes Gut, nämlich das Wissen und Know-How eines Unternehmens, zu schützen. Gefordert sind neben dem Qualitäts-

Themenkreis	27001:2013	9001:2015	Beispiele für Synergieeffekte
Kontext der Organisation	Kap. 4	Kap. 4	Gesamtkontextanalyse der Organisation im Hinblick auf interne und externe Themen sowie auf interessierte Parteien. Etablierung eines einheitlichen Prozessmanagements.
Führung	Kap. 5	Kap. 5	Etablierung von Führungsprozessen mit einem gemeinsamen Führungsverständnis, die alle Managementsysteme im Blick haben und die Anforderungen in der Organisation verankern.
Planung	Kap. 6	Kap. 6	Implementierung eines einheitlichen Risikomanagementprozesses welcher alle Teilbereiche transparent abdeckt.
Unterstützung	Kap. 7	Kap. 7	Gesamtressourcenbetrachtung sowie übergreifendes Kompetenzmanagement in den Personalprozessen. Etablierung von durchgängigen Kommunikationsstrukturen und Kreisen. Implementierung eines globalen Dokumentenmanagements.
Betrieb	Kap. 8	Kap. 8	Erarbeitung eines Lieferantenmanagementprozesses, der Qualitäts- u. IS-Anforderungen enthält.
Bewertung der Leistung	Kap. 9	Kap. 9	Aufbau von Controlling Prozessen über Kennzahlenmanagementsysteme, einem gemeinsamen Managementreview oder einer integrierten Auditplanung.
Verbesserung	Kap. 10	Kap. 10	Aufbau eines einheitlichen Prozesses zum Umgang mit Nichtkonformitäten und Korrekturmaßnahmen sowie KVP.

Tabelle. Zusammenhänge und Gemeinsamkeiten zwischen ISO 9001 und ISO 27001 auf Basis der High-Level-Structure gemäß Annex SL der ISO Directives.

Quelle: Opexa Advisory

managementbeauftragten (QMB) auch Rollen und Funktionen wie die des Informationssicherheitsbeauftragten (ISB) oder Chief-Information-Security-Officer (CISO).

In der Praxis stellt sich oft die Frage, wer diese Rolle übernehmen soll. Kann dies ggf. aus der bestehenden Qualitätsmanagementstruktur und/oder -Mannschaft gestemmt werden? Kann der Qualitätsmanagementbeauftragte auch Aufgaben im Bereich Informationssicherheit übernehmen?

Informationssicherheitsbeauftragter - wer kann das?

Bei der uintent GmbH, einem Unternehmen mit Schwerpunkt im Bereich User-Experience (UX) mit Standorten in Hamburg und München, hat das funktioniert. Dort galt es, aus Compliance-Gründen und aus Kundenanforderungen der Automobilindustrie heraus neben der eingeführten QM-Organisation auch eine ISMS-Organisation aufzubauen. Dabei sollte mit der bestehenden Mannschaft eine pragmatische Lösung gefunden werden. Das Unternehmen ist seit Jahren ISO 9001-zertifiziert und hat mit der Auswahl der Qualitätsmanagementbeauftragen für die Rolle des ISB einen Innovativen und zunächst mutigen Weg beschritten.

Hilfreich dabei war, dass die ISO 27001 als internationale Norm für die Informationssicherheit stark an der ISO 9001 angelehnt ist (Tabelle 1). Andererseits baut der vom VDA veröffentlichte Prüf- und Austauschmechanismus TISAX (Trusted Information Security Assessment Exchange) in großen Teilen auf ISO 27001 auf. Damit konnten Kenntnisse zu Normen, Prozessen, Nachweisfähigkeit sowie zum Auditmanagement genutzt werden. Innerhalb von vier Monaten wurde das ISMS aufgebaut, der QMB zum ISB geschult, eine ISMS-Softwarelösung eingeführt und die interne Organisation angepasst. Mit Hilfe einer externen Implementierungsberatung durch Opexa Advisory, München, wurden alle notwendigen Vorbereitungen getroffen. Dazu zählten z.B. Aufstellung interner Regelwerke und Anpassung von allgemeinen und TISAX-spezifischen Prozessen und Nachweisen, Synchronisation mit dem Qualitätsmanagement und dem Datenschutz, bauliche Maßnahmen (Einbruchmeldeanlage, Sichtschutz) sowie Optimierung der IT-Organisation und der Berechtigungsstruktur inkl. Datensicherung. Die TISAX-Prüfung (Assessment Level 3) wurde im Februar 2022 überdurchschnittlich erfolgreich absolviert.

Die Kombination bringt neue Kenntnisse und Synergien

Zu Beginn des Projektes kam für Tabea Daunus der Gedanke, sich sowohl als QMB auch als ISB zu betätigen und das ISMS zu betreuen, ziemlich kühn und herausfordernd vor, aber mit der Zeit fand sie die Idee spannend und so konnte sie – aufbauend auf ihren Kenntnissen als QMB – interessante neue Themen kennenlernen und ihr Wissen erweitern. Die Praxis bei Uintent hat für Tabea Daunus gezeigt, dass die Vereinigung der beiden Rollen (vor allem in kleineren Unternehmen) sinnvoll ist und Synergieeffekte genutzt werden können.

Die Idee, eine erprobte QM-Organisation mit dem ISMS-Thema zu verquicken, hat sich hier mehr als bewährt. So konnte mit einem schlanken Ansatz (unter Wiederverwendung von Prinzipien und Prozessen des Qualitätsmanagements und enger Anlehnung an zentrale TISAX®-Standard sowie von Opexa gestellter Dokumente) das Ziel einer TISAX-Zertifizierung in Rekordzeit erreicht werden. Gerade bei kleinen und mittelständischen Unternehmen bietet sich eine frühzeitige Integration an. Die Synergien zwischen diesen beiden Managementsystemen sind so weitrechend, dass auf Ebene der dokumentierten Informationen kein Weg mehr an der ISO 27001 vorbeiführt, um Unternehmen zukunftssicher zu machen und Know-How gegen digitale Angriffe bis hin zur Erpressung zu schützen.

QMB und ISB Tabea Daunus ist überzeugt: „Das gute Zusammenspiel im Unternehmen, wo die gesamte Organisation zusammen mit Geschäftsleitung, IT-Organisation und dem Datenschutzbeauftragten an einem Strang zogen, sowie flexibel auf die neuen Anforderungen reagierten, brachte uns den Erfolg". ■

INFORMATION & SERVICE

AUTOREN

Tabea Daunus ist Qualitätsmanagement- und Informationssicherheitsbeauftragte der uintent GmbH in Hamburg.

Klaus Kilvinger ist Geschäftsführender Gesellschafter der Opexa Advisory GmbH, München.

Dipl.-Ing. Thomas Salvador ist unabhängiger Gutachter und Sachverständiger für ISO-Zertifizierungsleistungen und Spezialist für Informationssicherheit.

KONTAKT

Klaus Kilvinger
klaus.kilvinger@opexa.de