Case Study

QSEC

HanseMerkur

HanseMerkur Krankenversicherung AG

– Datenschutz, Informationssicherheit und internes Kontrollsystem (IKS) „all in one“ auf der Basis des integrierten Managementsystems QSEC

Aufbau eines ganzheitlichen Managementsystems unter Berücksichtigung der versicherungsrechtlichen Aspekte nach VAIT.

Thomas Prigge, Datenschutzbeauftragter und Informationssicherheitsbeauftragter, berichtet über Herausforderungen und Erfahrungen mit QSEC.

Die HanseMerkur ist eine konzernunabhängige mittelständische Versicherungsgruppe mit Sitz in Hamburg. Sie bietet Versicherungsschutz für die Versicherungsrisiken Gesundheit, Pflege, Leben, Risiko- und Altersvorsorge, Reise und Freizeit, Schaden und Unfall sowie betrieblicher Zusatzversicherung.

Innovative Produkte, finanzielle Stärke und Traditionsbewusstsein – diese Eigenschaften schätzen Kunden und Vertriebspartner an der HanseMerkur. Das Unternehmen ist ein finanziell solider mittelständischer Personenversicherer und die einzige selbständige und konzernunabhängige Versicherungsgruppe am Finanzplatz Hamburg, die bundesweit tätig ist. Als „Versicherungsverein auf Gegenseitigkeit“ ist die Organisation nur Kunden und Mitarbeitern verpflichtet – nicht Aktionären oder Investoren. Dieses Prinzip prägt das Handeln, ist Teil der Unternehmenskultur und äußert sich in einer klaren Haltung. Das alte hanseatische Prinzip des Ehrbaren Kaufmannes ist für eine traditionsreiche hanseatische Versicherung wie die HanseMerkur grundlegend. Einschlägige gesetzliche Vorschriften und interne Regelungen einzuhalten ist für uns deshalb Bestandteil unserer Unternehmensphilosophie.

Das Motto „Hand in Hand ist... HanseMerkur“ spiegelt dieses Selbstverständnis wider. Es geht dabei sowohl um die partnerschaftliche Zusammenarbeit im Haus, zwischen Mitarbeitern und Führungskräften sowie den Mitgliedern des Vorstandes, als auch um das ehrliche Bemühen den Kunden gegenüber. Die Leitidee „Hand in Hand ist HanseMerkur“ übersetzt den Gemeinschaftsgedanken in ein zutiefst menschliches Prinzip. Denn mit gegenseitiger Unterstützung – also Hand in Hand – funktioniert einfach alles besser.

Die Ausgangssituation

Als Versicherungsunternehmen unterliegt die HanseMerkur neben den grundsätzlich geltenden Anforderungen an Informationssicherheit und Datenschutz ergänzend den regulatorischen Bestimmungen der BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht). Im Kontext der Informationssicherheit hat die BaFin die versicherungsaufsichtlichen Anforderungen an die IT, abgekürzt VAIT, im März 2019 veröffentlicht. Erläutert werden hier im Wesentlichen die aufsichtsrechtlichen Anforderungen an IT-Strategie, IT-Governance, Informationsrisiko-Management, Informationssicherheitsrisikomanagement, Benutzerberechtigungs-Management, IT-Projekte, IT-Betrieb und Ausgliederungen von IT-Dienstleistungen.

Bereits vor dem Inkrafttreten der VAIT-Anforderungen hat sich die HanseMerkur seit 2017 auf künftig steigende Herausforderungen zu Datenschutz, Informationssicherheit und Risikomanagement vorbereitet. Während der intensiv betriebenen IST-Analyse in diesen Themenbereichen wurde deutlich, dass nachhaltige Verfahren und Prozesse für zukünftige Anforderungen mit den bis zu diesem Zeitpunkt etablierten Bordmitteln wie Word, Excel oder PowerPoint nicht sinnvoll und ressourcensparend abgebildet werden können.

Es wurde klar, dass die komplexen Anforderungen toolgestützt deutlich besser zu managen sein würden. Für die Auswahl eines geeigneten Lösungsanbieters war die erklärte Anforderung, einen Partner zu finden, der nicht nur eine im Markt gut etablierte Managementlösung für Datenschutz und Informationssicherheit nach allen Anforderungen der Versicherungsbranche anbietet, sondern auch den gewünschten Zusatznutzen zum Aufbau eines ganzheitlichen internen Kontrollsystems (IKS) innerhalb der Software darstellen kann. Außerdem war es für die HanseMerkur wesentlich, dass der zukünftige Partner über langjährige Beratungserfahrung und Referenzen in großen Sicherheits- und Datenschutzprojekten verfügt, weil für die Umsetzung ein partnerschaftliches und professionelles Hand in Hand arbeiten zwischen Auftraggeber und Auftragnehmer vorausgesetzt wurde.

Der Entscheidungsprozess

Einige wesentliche Anforderungen für den Entscheidungsprozess waren, einen Hersteller zu evaluieren, der in seiner Lösung

- neben den Standardmodulen einer ISMS-Anwendung auch den Datenschutz nach EU-DSGVO komplett in seine Lösung integriert anbietet, um die bereits bei der HanseMerkur etablierte Zusammenarbeit zwischen Datenschutz und Informationssicherheitsverantwortlichen bestmöglich zu unterstützen
- im Standard die Möglichkeit bietet, ein komplettes internes Kontrollsystem (IKS) zu etablieren
- übergreifende Sichten über sämtliche Abteilungen und Prozesse ermöglicht
- die Konsolidierung der Daten für das Informationssicherheitsrisikomanagement und deren sichere und umfassende Auswertung benutzerfreundlich und ressourcensparend ermöglicht

Bei der persönlichen Vorstellung der Anbieter wurde schnell deutlich, dass Nexis GRC mit QSEC diese Anforderungen professionell abdecken kann. Besonders haben hier die integrierten Datenschutz-, Informationssicherheits-Funktionalitäten und die Ausbaufähigkeit von QSEC zum ganzheitlichen internen Kontrollsystem (IKS) im Vergleich zu anderen Wettbewerbern überzeugt.

Ferner konnte Nexis GRC in allen Gesprächen im Evaluierungsprozess die langjährige Kompetenz bei der Umsetzung ähnlich gelagerter Projekte überzeugend unter Beweis stellen. Die räumliche Nähe des Hamburger Unternehmens war zwar nicht ausschlaggebend, eröffnete aber zusätzlich die Möglichkeit eines „kurzen Drahts“ mit den Vorteilen des schnellen Agierens.

Warum QSEC?

QSEC überzeugte u.a. dadurch, dass die HanseMerkur ihre aus der Geschäftsstrategie abgeleiteten Vorgehensweisen zur IT-Strategie in QSEC komfortabel über die Standardfunktionalitäten implementieren konnte. QSEC ermöglicht HanseMerkur die IT Governance, das effiziente Steuern, Überwachen und Weiterentwickeln, aller erforderlicher Maßnahmen. Die etablierten Prozesse orientieren sich dabei exakt an den Vorgaben der gängigen internationalen Standards. Dabei unterstützt QSEC bei der Etablierung eines einheitlichen Prozessverständnisses.

Die Schutzziele „Vertraulichkeit, Integrität, Verfügbarkeit und Datenschutzrelevanz“ werden in QSEC von HanseMerkur im Rahmen des Informationsrisikomanagements bei der Ermittlung des Schutzbedarfs und etwaiger Abweichungen in QSEC betrachtet. Die ermittelten Risiken können sehr effizient im Risikomanagement von QSEC angemessen bewertet, überwacht, gesteuert und ausgewertet werden.

Die in QSEC umgesetzte lückenlose Historisierung und nachvollziehbare, durchgehende Dokumentation ermöglichen für die HanseMerkur die Darstellung im Rahmen von Audits und BaFin Prüfungen das Aufzeigen verantwortungsvollen Handelns.

Die Möglichkeit in QSEC die Anforderungen unterschiedlichster weiterer Normen, sowie interner Standards über mitgelieferte Tools zu implementieren unterstützten das Ziel, die Lösung über die Informationssicherheits- und Datenschutzziele hinaus auch als internes Kontrollsystem zu etablieren.

Die Einführungsphase

Die Einführung wurde in mehrere Projektphasen gegliedert, um eine reibungslose Ablösung der bisher genutzten Verfahren und die Akzeptanz aller Verantwortlichen zu erreichen.

1. Phase: in dieser Phase wurden alle vorhandenen Unterlagen gesichtet und auf dieser Basis die Konzeptions- und Einrichtungsphase gestartet. Wesentlich dabei war u.a., dass das QSEC DIMS Framework an die Dokumentenvorgaben der Hanse Merkur angepasst wurde. In dieser Phase wurden auch mit Unterstützung durch Nexis GRC die erforderlichen Richtlinien der Hanse Merkur angepasst, aktualisiert und ergänzt.

2. Phase: diese Phase wurde in drei Teilphasen gegliedert:
   a) in einen Workshop mit Festlegung aller Customizing Anforderungen,
   b) die Testphase und
   c) die Produktivsetzungsphase nach Abnahme aller gewünschter Einstellungen

Alle in unterschiedlichen Formaten vorhandenen Prozessdarstellungen wurden in QSEC importiert und stehen den Fachabteilungen zur Bewertung zur Verfügung. Die Fachabteilungen können in einem Bewertungsvorgang alle Anforderungen der Informationssicherheit, des Datenschutzes und des IKS bewerten.

3. Phase: in Phase 3 wurden die QSEC Schulungen durchgeführt und das Roll Out in der Hanse Merkur-Organisation umgesetzt.

FAZIT

Mit QSEC hat die HanseMerkur heute deutlich mehr Transparenz über potenzielle Risiken und deren Auswirkungen und kann effizient angemessene Maßnahmen zur Verbesserung und Weiterentwicklung des Reifegrads für alle Anforderungen aus Datenschutz, Informationssicherheit, IKS-Kontrollen und VAIT-Vorgaben entwickeln.

„Mit Nexis GRC haben wir einen Partner gewonnen, der unsere „Sprache“ spricht und offen auf unsere Anforderungen und Ideen reagiert. Die Partnerschaft mit Nexis GRC hat mich durch die gesamte Laufzeit der Zusammenarbeit überzeugt“ so Thomas Prigge, Informationssicherheitsbeauftragter der HanseMerkur.

Kontakt
Nexis GRC GmbH • Zimmerstraße 1, 22085 Hamburg • +49 40 650336-0 • info@nexis-qsec.com