Case Study

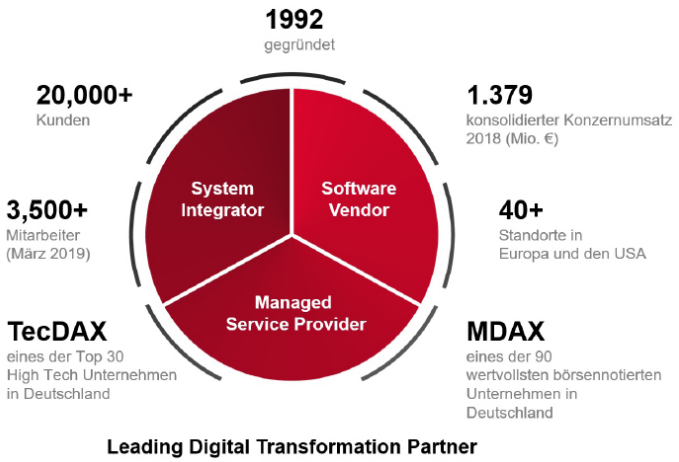
QSEC

Weltweite Einführung eines ISMS gem. ISO/IEC 27001 bei CANCOM

CANCOM vertraut in den Bereichen Informationssicherheits-, Risiko-, und Datenschutzmanagement auf das integrierte Managementsystem QSEC von Nexis GRC.

Marcel Reifenberger, Chief Information Security Officer & CSO CANCOM SE, berichtet über Herausforderungen und Erfahrungen mit QSEC sowie mögliche zukünftige Entwicklungen.

Als Hybrid IT Integrator, Service Provider und Digital Transformation Partner begleitet CANCOM Unternehmen in die digitale Zukunft. Das IT-Lösungsangebot der CANCOM Gruppe umfasst Beratung, Umsetzung, Services sowie den Betrieb von IT-Systemen. Die weltweit rund 4.000 Mitarbeiter und ein leistungsfähiges Partnernetzwerk gewährleisten Marktpräsenz und Kundennähe unter anderem in Deutschland, Österreich, Schweiz, Belgien, Slowakei, Großbritannien, Irland und den USA.



Die Ausgangssituation

Im international agierenden CANCOM Konzern wird nach aktuell 15 Normenzertifikaten und Standards gearbeitet. Diese weltweite Flut an Controls nach Reifegraden zu bewerten und die zugehörigen Dokumente und Nachweise zuzuordnen ist mit Bordmitteln (wie z.B. Excel) nicht mehr darstellbar.

So wurde die Anforderung nach einer Unified Audit Plattform für CANCOM schnell deutlich. Unter den Gesichtspunkten des Single Source Ansatz, wurde ein System gesucht, dass für die gesamten Informationen eine normübergreifende, einheitliche Darstellung von Auditinformationen, Kontrollen und Nachweisen ermöglicht.

Eine weitere Anforderung war, eine Software zu beschaffen, mit der man Aufwände deutlich reduzieren kann. Der Fokus sollte u.a. auf dem Thema Automation und Standardisierung von Prozessen liegen. Ferner sollte die zu beschaffende Software die Einsparung von Ressourcen, durch automatische Aggregation und Auswertung von Informationen sowie erleichterte Erhebung und Aufnahme der erforderlichen Daten, ermöglichen.

Die gewünschte Standardisierung ist für CANCOM im internationalen Umfeld wesentlich. Nur durch einheitliche Vorgehensmodelle kann dem massiven anorganischen Wachstum Sorge getragen werden.

Der Evaluierungsprozess

CANCOM hat insgesamt 10 Tool-Anbieter betrachtet. Das Spektrum der Anbieter umfasste kleine wie sehr große Unternehmen. Nach einem Vorevaluierungsprozess schaffte es eine Auswahl von fünf Anbietern auf die Shortlist. Diese Produkte wurden gegeneinander gebenchmarkt, deren USPs wurden verglichen.

Es kristallisierte sich schnell heraus, dass einige Punkte, wie die Auflistung von Assets, das Mapping der Assets mit Geschäftsprozessen und andere grundsätzliche Normenerfordernisse nahezu alle Anbieter umgesetzt haben.

Wesentlicher Unterschied von QSEC zu allen anderen von uns betrachteten Produkten war, die Workflowunterstützung über die integrierten Wizards. Diese Wizard Funktionen bieten eine einheitliche Vorgehen- und Umsetzungsweise bei der Erhebung von Daten und ermöglicht es den Spezialisten z.B. Interviews mit den Fachabteilungen auf elektronischer Basis zu führen. So werden Rüst-, Reise- und Anlernzeiten eingespart. Die Nutzung der Wizards ist auch für den nicht geschulten Mitarbeiter in einer

Case Study

Fachabteilung selbsterklärend. Im Umkehrschluss steigert dieser Komfort der Wizards auch die Akzeptanz der Software durch die Fachanwender aufgrund ihrer Übersichtlichkeit und der selbsterklärenden Vorgehens- und Anwendungsweise.

Der Entscheidungsprozess

Warum QSEC?

Am Ende überzeugte QSEC in der Kosten-Nutzen-Analyse sowie im Punkto Scalability als Single-Source-Tool.

QSEC unterstützt bei der Verbreitung eines einheitlichen Prozessverständnisses. Das System fungiert als zentrale Plattform, in welcher alle Geschäftsprozesse erfasst sind. Darüber hinaus werden die für die CANCOM Gruppe relevanten Normen erfasst und gemappt. QSEC hebt sich durch sog. „all-in-one Abfragen" von anderen Anbietern ab. So kann z.B. in einem Prozess abgefragt werden, zu welcher Norm das Control gehört und gleichzeitig ob es IKS- und/oder datenschutzrelevant ist. Das spart deutlich Zeit und Aufwand.

Ferner hat Nexis GRC als mittelständischer Partner von CANCOM auch im gesamten Evaluierungsprozess und bisherigen Umsetzungsprozess überzeugt. In jeder Phase der Zusammenarbeit hatten wir das Gefühl als wichtiger Geschäftspartner wahrgenommen zu werden. Die fachliche Kompetenz der Nexis GRC Mitarbeiter, vermittelte jederzeit den Anspruch auf Augenhöhe zu kommunizieren.

Die Umsetzungsphase

Die Herausforderung war, bei einer Unternehmensgröße von ca. 4000 Mitarbeitern, >50 Standorten und > 20.000 Kunden weltweit, die immer zunehmenden Daten- und Informationsmengen aus unterschiedlichen Quellen in ein Single Source Systeme zu überführen und dabei die Informationen zu kombinieren, hochgradig zu verdichten, und gleichzeitig zu standardisieren. Hierfür waren ca. 10 Monate geplant.

Wie war unser Vorgehen?

1. In Q3/18 entschieden wir uns für QSEC. Wichtig erschien uns dabei die Lösung in der Organisation so zu positionieren, dass man die Anwender „mitnimmt" um maximale Akzeptanz zu erzielen. Die Herausforderung besteht darin, Qualitätsmanager, Personalmanager, Arbeitssicherheitsmanager, Datenschutzbeauftragter usw. dazu zu motivieren in einem System zu arbeiten. Die Aussage „Wir implementieren ein Tool" ist definitiv nicht ausreichend. QSEC ist nicht nur ein Stück Software, QSEC unterstützt einen einheitlichen Weg in den Bereichen Risiko-, Sicherheits- und Datenschutzmanagement.
2. Das Projekt wurden in 3 Phase aufgeteilt – 1. Customizing 2. Input & GoLive 3. Run & Maintain. Nach einigen zügigen initialen Scoping Sessions mit Nexis GRC konnte mit Phase 1 begonnen werden. In ersten Workshops, wurde das System entsprechend unserer Anforderungen durch Nexis GRC konfiguriert und ein Testsystem bereitgestellt. Nach erfolgreicher Testdurchführung und letzten Anpassungen, wurde das System Live System in unserem Rechenzentrum aufgesetzt.
3. Aktuell befinden wir uns in Phase 3 Run & Maintain, welche einen flüssigen Übergang vom Projekt in den Betrieb darstellt. Run & Maintain bedeutet für uns weitere Quellen anzubinden, Informationen zu verdichten, aussagefähige Reports zu generieren um daraus Mehrwerte für die gesamte Organisation zu schaffen. Durch gezielte Awareness Maßnahmen konnten die Vorteile von QSEC im Projektverlauf auch anderen Abteilungen aufgezeigt werden. Dies führe dazu, dass die geschaffenen Synergien QSEC immer tiefer in der CANCOM DNA verankern. Im Rahmen der jährlichen Zertifizierungen ist QSEC schon heute ein zentraler Bestandteil.

FAZIT

Natürlich behebt kein Tool das Problem fehlender Prozesse oder verändert Organisationen im Alleingang. Dafür ist ein Tool (zu Deutsch „Werkzeug") auch nicht gedacht. Selbst mit QSEC entstehen weiterhin Input- und Pflegeaufwände, welche sich jedoch durch das Outcome massiv relativieren. Einen weiteren großen Vorteil sehen wir in der Transparenz, nicht nur bezogen auf Risiken und deren Auswirkungen. QSEC schafft ebenfalls eine Transparenz über die Strukturen und Abhängigkeiten in Unternehmen. Vor allem bei Organisationen welche schnell auf Veränderungen am Markt reagieren müssen oder stark anorganisch wachsen, ist dies ein Vorteil den man nicht unterschätzen sollte.

Stand heute haben wir bereits mehr als 200 Geschäftsprozesse aufgenommen, knapp 600 Risiken in QSEC übertragen, mehr als 10 Geschäftseinheiten, >50 Standorte erfasst. Es wurden mehr als 400 Assets und Assetsgruppen überführt und bereits mehrere Untersuchungsbereiche eingerichtet.

Wir haben mit QSEC einen erfolgreichen Weg eingeschlagen und empfinden Nexis GRC als kooperativen Partner an unserer Seite!

Kontakt

Nexis GRC GmbH
Zimmerstraße 1
DE-22085 Hamburg
T: +49 40 650336-0
info@nexis-qsec.com