Bewertung und Zitate des Auftraggebers:

„Sehr fokussiert in der Sache, ausgesprochen verbindlich und proaktiv im persönlichen Kontakt. Die Zusammenarbeit war in jeder Hinsicht eine Bereicherung.“

canacoon Case Study

Non Compliance-Handling

Der Kunde in Stichpunkten

- deutsche Finanzgesellschaft eines Automobilherstellers
- weltweit mehrere Landesgesellschaften
- Umsatz im dreistelligen Milliardenbereich
- verwaltet die Finanz-, Leasing- und Mietgeschäfte des Automobilherstellers und seiner Marken

Das Unternehmen wird überwacht von den Bankaufsichtsbehörden BaFin sowie EZB und unterliegt damit einer Vielzahl an Regularien wie z.B. PCI-DSS, MaRisk und BAIT sowie der Datenschutzverordnung (GDPR).

Die Aufgabenstellung

Aufgrund regulatorischer Auflagen ist ein Finanzunternehmen nach MaRisk und BAIT dazu verpflichtet, IT-Risiken zu erfassen und diese in die operationellen Risiken zu überführen. Der Kunde hatte bereits ein vollständiges Informationssicherheitsmanagementsystem und entsprechende Richtlinien etabliert. Im Kundenunternehmen kann sich ein IT-Risiko in Form einer Abweichung von Sicherheitsrichtlinien äußern. Ziel war es, einen ganzheitlichen Prozess zu konzipieren, der nach Identifikation der Richtlinienabweichung das IT-Risiko an das Risk Management meldet. Zudem sollen alle notwendigen Mitarbeiter bzw. Fachabteilungen von der Abweichung in Kenntnis gesetzt werden. Die verantwortlichen Managementebenen mussten das Risiko akzeptieren oder Mitigationsmaßnahmen veranlassen. Das beschriebene Vorgehen sollte durch eine digitale Lösung unterstützt werden.

Die Lösung

Die canacoon wurde mit der Projektleitung, der Anforderungsanalyse und der Konzeption des Non Compliance-Prozesses beauftragt. Nachdem canacoon in einem Kickoff-Meeting das Ziel und die Problemstellung des Projektes erfasst hatte, wurden die Anforderungen an den Prozess der betroffenen Stakeholder analysiert. Weiterhin wurden rechtliche Rahmenbedingungen sowie Vorgaben aus konzerninternen Richtlinien evaluiert und in den zu konzipierenden Non Compliance-Prozess einbezogen. Nach erfolgreicher To-Be Analyse des Prozesses wurden die Gaps zwischen diversen Ansichten der einzelnen Stakeholder gegenüber dem SOLL-Prozess ermittelt und in einem Abstimmungsmeeting beseitigt. Der abgestimmte SOLL-Prozess wurde dokumentiert und das Vorgehen auf den internen Informationsplattformen und in Form eines Newsletters an beteiligte Abteilungen kommuniziert. Die technische und operative Umsetzung des Non Compliance-Prozesses unterteilte sich dabei in zwei Phasen. In Phase 1 wurde der Compliance Gap anhand eines digitalen Formulars erfasst. In diesem wurden u. a. die Abweichungen von Richtlinien, die betroffenen Systeme und bei Patchmanagement und Härtungsrichtlinienverstößen die nicht eingespielten Patches bzw. nicht umgesetzten Härtungsvorgaben dokumentiert. Weiterhin wurden die Schadenshöhe und die Eintrittswahrscheinlichkeit des IT-Risikos vom Asset Owner geschätzt. Nach dem vollständigen Befüllen des Formulars erfolgte die Prüfung und Akzeptanz des IT-Risikos durch die nächsthöhere Kompetenzstufe. Das Formular wird danach von weiteren Abteilungen und Kompetenzträgern, wie z. B. vom Chief Information Security Officer oder der Security-Abteilung des jeweiligen Unternehmensbereichs geprüft. Wurde das Risiko von allen Instanzen akzeptiert, erfolgte die Meldung des IT-Risikos an die Chief IT Risk Officer, welcher die IT-Risiken in die operationellen Risiken des Konzerns überführt. In Phase 2 wurde der gesamte Prozess im MicroFocus Service Manager abgebildet. Dadurch löste man den Non Compliance-Prozess von dem Formular und verlagerte die Erfassung des Compliance Gaps in den ITSM. Weiterhin wurden die angelegten Anträge für einen Compliance Gap automatisiert an die zuständigen Prüfungsinstanzen weitergeleitet. Die Akzeptanz und Meldung des IT-Risikos an das Chief IT Risk Officer erfolgte ebenfalls in dem System. Laut der Aussage des Kunden erwies sich canacoon bei der Anforderungsanalyse und Projektleitung dieses Workflows wieder mal als kompetenter und professioneller Partner bei der Konzeption sowie der Umsetzung von Security- und Compliance-Prozessen. Nach Projektabschluss und Go-Live der ITSM-Funktionalität zur Erfassung von Compliance Gaps und Meldung von IT-Risiken wurde die Anwender- und Administrations-dokumentation erstellt und an den Kunden übergeben. Anschließend erfolgte eine Folgebeauftragung, in der canacoon als Prüfungsinstanz für den Kunden im Non Compliance-Prozess agierte sowie eine Guideline & Control Management im Unternehmen etablierte.