Informationssicherheits- und Qualitätsmanagement

Eine **vorteilhafte** Ehe

Der Schutz sogenannter „kritischer Infrastrukturen" steht im Fokus des verabschiedeten IT-Sicherheitsgesetzes. Schließlich können Störungen und Ausfälle weite Bevölkerungsteile unmittelbar betreffen.

Aus diesem Grund wurden KRITIS - Einrichtungen aufgefordert, ein Informationssicherheitsmanagement aufzubauen. Nach herrschender Meinung kann dies sowohl nach ISO 27001 als auch nach BSI IT-Grundschutz erfolgen. Im Regelfall fehlt es den Organisationen jedoch an Ressourcen im Sinne von Personal, KnowHow und Zeit. Ein Informationssicherheitssystem wird als notwendiges Übel verstanden, jedoch nicht gewinnstiftend eingeschätzt.

Die meisten Organisationen verfügen aber bereits über ein funktionierendes Qualitätsmanagement. Die ISO 9001: 2008 oder seit November 2015 die ISO 9001:2015 steht für die Abbildung der Ablauf- oder Aufbauorganisation inkl. Geschäftsprozessen, Wissensmanagement, Kompetenzmanagement und Risikomanagement. Viele dieser Anforderungen sind sehr ähnlich der Anforderungen wie der ISO 27001 oder dem BSI IT-Grundschutz, beispielsweise die Abbildung der Geschäftsprozesse oder Verfahren. Diese beschreiben den internen Geschäftsablauf einer Organisation. Sämtliche Ressourcen (Anwendungen, IT-Systeme, Netze, Standorte) hängen an den Geschäftsprozessen und sind notwendig, damit diese einwandfrei funktionieren können.

Integrativer Ansatz

Wenn diese Parallelen erkannt werden, können Organisationen die Überschneidungen integrativ nutzen. Sollte bspw. bereits ein Qualitätsmanagement (QM) nach ISO 9001:2015 bestehen, kann dieses im Rahmen des BSI IT-Grundschutzes genutzt werden. Als erster gemeinsamer Nenner steht hier der Geschäftsprozess oder das Verfahren. In den meisten Fällen hat das QM bereits eine sehr gute Vorarbeit geleistet, wovon der BSI IT-Grundschutz profitiert. Eine weitere Überschneidung findet sich im Risikomanagement. Die ISO 9001:2015 schreibt keinen gesonderten Ansatz vor, sodass der BSI 100-3 Standard eine Möglichkeit wäre. Wird der BSI 100-3 im QM als Risikomanagement genutzt, kommt es zu einem Ineinandergreifen der Normen, welches Ressourcen spart.

„Es ist nur ein kleiner Schritt von einem Qualitätsmanagement zu einem Informationssicherheitsmanagement, vor allem, wenn es toolgestützt erfolgt"

Sascha Kreutziger, Senior Account Manager, HiScout GmbH

Toolgestützte Zusammenarbeit

GRC-Suiten (Governance, Risk und Compliance) sind darauf ausgelegt, mehrere Managementsysteme in einer Plattform abzubilden. Für die genutzte Technologie sollte eine 3-Layer Architektur vorgesehen werden, bestehend aus einer Datenbank-Ebene, einer Applikations-Ebene und einer Oberflächen-Ebene. Die Trennung ermöglicht es auch bei individuellen Änderungen keinen Verlust der Update & Release Fähigkeit zu riskieren. Änderungen sind insbesondere bei der Abbildung von kundeneigenen Methodiken zu berücksichtigen.

Werden sämtliche Stammdaten in einer Datenbank gespeichert und durch ein stringentes Rollen- und Rechtesystem geregelt, lassen sich Inkonsistenzen und Redundanzen vermeiden. Gleichzeitig ermöglicht es verteiltes, organisationsweites Zusammenarbeiten. So kann das QM die Prozesshoheit behalten und die Geschäftsprozesse anlegen und ändern. Der IT-Bereich kann jedoch auf die Ergebnisse nur lesend zugreifen und die Ressourcen verknüpfen. Ratsam ist an dieser Stelle eine Unterstützung durch Workflows, sodass beispielsweise der IT-SiBe über Änderungen an einem Geschäftsprozess automatisch informiert wird und die zugeordneten Ressourcen entsprechend der Sicherheitskriterien überprüfen kann.

Die Normen und die GRC-Suiten sind bereit für den integrativen Ansatz, jetzt müssen nur noch die jeweiligen Disziplinen in den Organisationen zueinander finden. Vieles spricht dafür, die Managementsysteme nicht getrennt voneinander zu betrachten, sondern einen integrierten Ansatz zu verfolgen.

Sascha Kreutziger

HiScout GmbH
Bouchéstraße 12
12435 Berlin // Germany
Tel. +49 30 33 00 888-0
Fax +49 30 33 00 888-99
E-Mail: GRC-Suite@hiscout.com

WEB-TIPP:
www.hiscout.com

Weiterführende Informationen:
www.it-daily.net

Webinar