

Trust and Technology Blog

By PwC Deutschland | 07. Februar 2024

Der Informationsverbund – die Grundlage für ein funktionierendes Informationssicherheits- und Informationsrisikomanagement

Hintergrund und Praxiserfahrung

Hintergrund: Anforderungen und Ziele

Unternehmen haben grundsätzlich bereits intrinsisch ein Interesse daran, die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit Ihrer Informationen sicherzustellen. Vor allem Finanzinstitute sind durch entsprechende Anforderungen (BAIT, VAIT, KAIT etc.) sogar regulatorisch dazu verpflichtet.

Da geschäftsrelevante und somit schützenswerte Informationen im Unternehmen an verschiedensten Stellen verarbeitet werden, ist es notwendig zu erheben, welche dieser Informationen, in welchen Prozessen, Anwendungen, IT-Systemen und schlussendlich auch Gebäuden und Räumen verarbeitet werden. Die Summe dieser informationsverarbeitenden „Assets“ definieren den Informationsverbund und müssen folglich geschützt werden. Um dies zu ermöglichen, muss der Informationsverbund vollständig erfasst und die Assets inklusive deren Abhängigkeiten und Schnittstellen zueinander holistisch in einer auswertbaren Form abgebildet werden.

Darüber hinaus ist die vollständige Erhebung und Abbildung des Informationsverbundes für eine Vielzahl von weiteren Informationssicherheits- und Informationsrisikomanagementprozessen essenziell. Beispielsweise können Sollvorgaben nur dann ganzheitlich angewandt, im Rahmen eines Soll-Ist-Abgleichs überprüft und daraufhin etwaige Risikoentscheidungen getroffen werden, wenn die zugrunde liegenden Assets des Informationsverbundes vollständig erhoben und systemisch abgebildet wurden. Ebenso erfolgt die Vererbung des Schutzbedarfs auf Basis der Abhängigkeiten zwischen den Assets des Informationsverbundes. Bei der Behandlung von Incidents und im Rahmen des Change-Managements ist es ebenso von zentraler Bedeutung, die jeweils betroffenen Assets zu verknüpfen und somit die daraus resultierenden Risiken steuerbar zu machen.

Praxiserfahrung – technische Abbildung des Informationsverbundes

Oftmals liegen Unternehmen mehrere Asset-Inventare mit unterschiedlicher Datenqualität vor. Für die ganzheitliche Abbildung des Informationsverbundes ist es notwendig zu verstehen, welche Asset-Informationen jeweils den korrekten Datenbestand darstellen. So muss nicht zwingend ein „zentrales Inventar“ existieren, sondern es kann der Informationsverbund beispielsweise über eine Prozesslandkarte, ein Anwendungs- und IDV-Inventar, eine Configuration Management Database (CMDB) und ein Auslagerungsinventar inhaltlich abgebildet werden. Dabei muss allerdings sichergestellt werden, dass die Abhängigkeiten der Assets zueinander über die verschiedenen dezentralen Asset-Inventare hinweg abgebildet werden können. Dies hat den Hintergrund, dass innerhalb des Informationsverbundes Auswirkungen von Assets auf andere Assets nachvollzogen werden müssen. So muss es beispielsweise möglich sein, im Fall eines Ausfalls einer Datenbank die zugehörigen Anwendungen und davon betroffene Prozesse zu identifizieren, um das Ausmaß und die Auswirkung des Vorfalls zu verstehen und entsprechende Maßnahmen zielgerichtet einleiten zu können. Gleich verhält es sich beim Ausfall eines Dienstleisters. Auch diese Abhängigkeit muss im Rahmen des Informationsverbundes abgebildet werden können, um negativen Auswirkungen auf den Geschäftsbetrieb entgegenwirken zu können. Daher wählen mehr und mehr Unternehmen den Ansatz, den gesamten Informationsverbund an einer zentralen Stelle softwarebasiert abzubilden. Die Software kann dann entweder für einen Teilbereich des

Informationsverbundes selbst den korrekten Datenbestand verwalten oder über Schnittstellen den Datenbestand aus den verschiedenen dezentralen Asset-Inventaren abbilden. Herausforderungen bestehen hier oft darin, die Datenqualität in den dezentralen Quellsystemen sicherzustellen und die qualitätsgesicherten Daten über eine effektive Schnittstellenanbindung unter Berücksichtigung des Datenmodells zu integrieren.

Insgesamt zeigt sich also, dass die vollständige Erhebung und Abbildung des Informationsverbundes nicht nur für viele Unternehmen regulatorisch notwendig ist, sondern vor allem im laufenden Geschäftsbetrieb ein Erfolgsfaktor für eine angemessene und zielgerichtete Risikosteuerung ist – in Summe aber in der technischen Implementierung noch viele Hürden und diverse Herausforderungen bei den Unternehmen bestehen.

Wir haben die Erfahrung gemacht, dass eine effiziente Implementierung eines Informationsverbundes nur dann gelingt, wenn alle relevanten Datenbestände identifiziert und inhaltlich qualitätsgesichert bzw. bereinigt werden. Dabei müssen bereits von Beginn an die Anforderungen aus den nutzenden Prozessdisziplinen (bspw. Schwachstellen-, Change-, Incident-, Informationsrisiko- und Problemmanagement) erhoben und berücksichtigt werden. Zusätzlich müssen klare Prozesse zur laufenden Pflege und Sicherstellung der Aktualität und Richtigkeit der Daten definiert werden.

Gerne unterstützen wir Sie mit unserer Marktkenntnis und Expertise und erörtern gemeinsam die Möglichkeiten für Ihr Unternehmen.

[Laufende Updates zum Thema erhalten Sie über das regulatorische Horizon Scanning in unserer Recherche-Applikation PwC Plus. Lesen Sie hier mehr über die Möglichkeiten und Angebote.](#)

[Zu weiteren PwC Blogs](#)

Schlagwörter

[IT-Sicherheit](#), [Informationstechnologie \(IT\)](#), [Risk Management Banking](#), [Risk Management Insurance](#), [WpHG Compliance](#)

Kontakt



Karsten Wilop

Düsseldorf

karsten.wilop@pwc.com