Sascha Kreutziger

Datenschutz und Informationssicherheit – eng verzahnt mit einem GRC Tool

Software ist aus unserem Alltag nicht mehr wegzudenken: Wir nutzen sie mehrfach täglich, privat oder beruflich. Und häufig unterbewusst, oder denken Sie noch über die Benutzung Ihrer elektrischen Zahnbürste mit Bluetooth-Schnittstelle zu Ihrer Smartphone-App nach? Letzteres könnte jedoch zu einem großen Problem werden in Punkto Datenschutz – vor allem bei der Wahrung der Privatsphäre oder der Informationssicherheit in Zeiten mobilen Arbeitens oder dem Smartphone auf dem Schreibtisch mit eben dieser aktivierten Bluetooth-Schnittstelle.

1 Anforderungen an ein Unternehmen

Wir leben in einer Zeit, in der Strukturen immer komplexer und die Menschen, die diese durchschauen, immer seltener werden. Teilweise vertrauen wir blind der Technik und Ergebnisse, die diese Technik uns präsentiert, werden immer seltener hinterfragt. Damit ist es ein Leichtes für Angreifer, diese komplexen Strukturen auszunutzen.

Als logische Schlussfolge sollte es eigentlich im Interesse von Unternehmen liegen, diese komplexen Strukturen zu hinterfragen und kontinuierlich auf den Prüfstand zu stellen.

Nachfolgend ein paar konkrete Denkanstöße zum Hinterfragen:

- Welche Daten verarbeite ich in meinem Unternehmen?
- Welche Prozesse laufen durch mein Unternehmen?
- Wie verändern sich die Datensätze im Laufe eines Prozessschrittes?
- Wie verändert sich hier die Einstufung der sicherheitsrelevanten Kriterien Vertraulichkeit, Integrität, Sensitivitätsstufe?
- Wie sehen hier die Schnittstellen und Zugriffe technischer und personeller Art aus?
- Ist die Geschäftsführung ausreichend eingebunden und sensibilisiert?
- Haben die Mitarbeiter noch die Möglichkeit, ihren Prozessschritt im großen Ganzen zu sehen?

Zusätzlich gelten regulatorische Anforderungen, die nicht mehr wegzudenken sind. Und in einer Vielzahl und Größenordnung, dass so manche Branche zu Fusionen gezwungen ist, weil diese Anforderungen allein nicht mehr gestemmt werden können. Themen wie Fachkräftemangel und steigender Vertriebsdruck durch die Globalisierung der Märkte befeuern diese rasante Entwicklung noch mehr. An dieser Stelle nur zwei Schlagwörter: EU-DSGVO und DORA.

2 Mitarbeiter motivieren ihre spezifische Rolle zu vertreten

Seit vielen Jahren etablieren sich erfolgreich sogenannte GRC (Governance, Risk, Compliance) Tools. Dabei handelt es sich um Software die versucht, diese Komplexität in eine greifbare Form zu gießen und Unternehmen ein Handwerkszeug zu sein, um

- Mitarbeitern eine Übersicht über komplexe Prozesse zu bieten
- die Widerstandsfähigkeit des Unternehmens selbst zu erhöhen
- den regulatorischen Anforderungen begegnen zu können
- die Rolle des Beauftragten zu etablieren

Die Mitarbeiter wurden hier ganz bewusst an erster Stelle genannt. Leider hat sich in den letzten Jahren das Denken verbreitet, dass Datenschutz und Informationssicherheit nur noch aufgrund der vorhandenen Regulatorik umgesetzt werden müssen. Mit dieser Perspektive wurden die beiden Themen bei den Mitarbeitern wie der Geschäftsführung verbrannt. Dabei sollte vielmehr aus dem Muss eine Chance gemacht werden: Sicher ist die Regulatorik als Motivator für die oberste Ebene nicht mehr wegzudenken, aber sie sollte nicht alleiniger Treiber sein.

Die Mitarbeiter sind der wichtigste Dreh- und Angelpunkt in einem Unternehmen. Ohne sie „läuft der Laden nicht“. Daher sollte ein Unternehmen alle Möglichkeiten ergreifen, um allen

Sascha Kreutziger

Leiter Business Development, HiScout GmbH

E-Mail: skreutziger@hiscout.com

Mitarbeitern aufzuzeigen, welchen Mehrwert sie für das Unternehmen bieten. Dies fördert die Motivation – und wir alle kennen noch die „Maslow-Pyramide“. Insbesondere für intrinsisch motivierte Mitarbeiter liegt hier ein immenser Hebel.

3 Softwaregestützte Hilfe durch ein GRC Tool – nur gemeinsam sind wir stark

Die Geschwindigkeit des Wandels und die Masse an Informationen lässt nur noch Unternehmen am Markt überleben, die

- sich über die internen Abläufe und Verarbeitungen im Klaren sind
- offen für Veränderungen sind
- flexibel genug sind, um agieren zu können

All diese Punkte haben eines gemeinsam: Sie fungieren als eine „Landkarte“ vom eigenen Unternehmen. Die unterschiedlichen Disziplinen haben viele Gemeinsamkeiten, die ausgespielt werden müssen. Nehmen wir als Bespiel die Datenkategorie „Bildaufzeichnungen“. In erster Linie bedarf dies der Einwilligung der betreffenden Person(en). Jetzt muss nur noch jeder Prozessschritt im Haus davon auch Kenntnis erlangen.

- Nehmen wir hier den Prozess „Kontoeröffnung“ mit dem Prozessschritt „Ausweislegitimation“ eines Kunden.
- Als zweiten Prozess können wir „Mitarbeitergewinnung“ mit dem Prozessschritt „Neuen Kollegen auf Facebook veröffentlichen“.

Wir sehen hier die Abteilungen Vertrieb und Personal, die beide die Einwilligung von einer Person einholen müssen. Zum einen von einem Kunden und zum anderen von einem Mitarbeiter. Der Verantwortliche für Datenschutz möchte nun diese Einwilligung an die geeigneten Stellen im Prozessschritt einbauen, und zwar so, dass die Einwilligung durchgeführt wird bevor das Bild zur Verwendung kommt. Der Verantwortliche für Informationssicherheit hat hier ebenfalls ein großes Interesse. Genau an dieser Stelle kommen Fragen auf: Mit welcher Anwendung werden diese Prozessschritte ausgeführt und wer hat hier die Zugriffsberechtigung, wo werden die Daten gespeichert, werden die Aktionen protokolliert, etc..

An diesem einfachen Beispiel wird bereits die Komplexität klar – vor allem, wenn sich nun auch noch Änderungen der Einwilligung ergeben.

- Wo wird der Vordruck überall verwendet?
- Wie wird sichergestellt, dass auch immer der aktuelle Vordruck verwendet wird?
- Wird überprüft, dass der Vordruck tatsächlich verwendet wird?
- Wo wird der unterzeichnete Vordruck gespeichert?
- In welchen Prozessschritten wird die im Vordruck angesprochene Datenkategorie verwendet?
- Ändert sich somit nicht nur der eine, sondern mehrere Vordrucke?

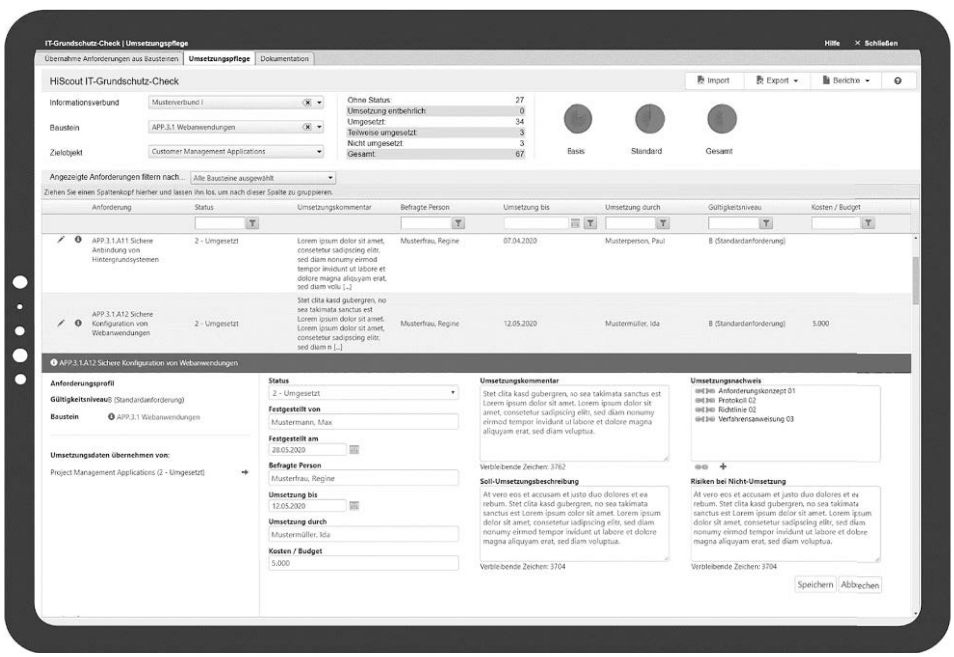
Die Zusammenarbeit der Verantwortlichen kann durch eine Softwareunterstützung gefördert und beflügelt werden. Gerade im Datenschutz und in der Informationssicherheit gehen die Themen Hand in Hand, und das ist wörtlich zu verstehen. Nur durch die Informationssicherheit kann der Datenschutz ermitteln, in welcher Anwendung die Datenkategorien verarbeitet werden und durch welchen handelnden Mitarbeiter der Vordruck ausgehändigt werden muss.

Je klarer und präziser die Datenkategorien beschrieben werden, um so einfacher ist auch dem Mitarbeiter zu vermitteln, aus welchem Grund er diese Anforderungen aus dem Datenschutz umsetzen muss. In dem genannten Beispiel ist es besonders plakativ, da der Mitarbeiter auch selbst als Person betroffen ist. Für den Mitarbeiter ist im Fazit Transparenz für ein komplexes Thema geschaffen worden, was seine Motivation steigert und sich zugleich positiv auf den Kunden auswirkt. „Wir müssen diesen Vordruck ausfüllen“ hört sich nicht so gut an wie „Durch diesen Vordruck schützen wir Ihre Privatsphäre und Rechte am Bild“. Auf den Kunden wirkt diese Motivation positiv und vertrauensbildend.

4 Vorgegebene Strukturen eines GRC-Tools sorgen für Standardisierung

Die Software unterstützt durch einen vorgegebenen Weg, durch ein intuitives Bedienkonzept und vor allem durch eine kontinuierliche Aktualisierung und Weiterentwicklung. Durch diese Unterstützung wird die Schulung und Akzeptanz im Unternehmen gefördert, wenn die Software ausgerollt wird. Hierbei ist zu beachten, ob ein zentraler oder dezentraler Ansatz gewählt wird. Um ein tragfähiges Datenschutz- oder Informationssicherheits-

Abbildung 1 | Festgelegte Vorgehensweise beispielsweise in HiScout Grundschutz



konzept zu etablieren, ist ein breites Einbinden der Mitarbeiter immer von Vorteil. Schließlich sind die Mitarbeiter eng mit den Prozessschritten verwoben und bekommen am schnellsten Fehler oder Unstimmigkeiten mit. Wenn dann sofort ein Bezug zu einem Managementsystem hergestellt wird, können Probleme erkannt werden, bevor sie zu einem Risiko werden.

An zentraler Stelle für ein Managementsystem wie Datenschutz oder Informationssicherheit steht die schriftlich fixierte Ordnung. Diese bildet das Rahmenwerk und gibt konkret die Sollanforderungen vor. So gut geschrieben die meisten Richtlinien auch sind, steht dabei immer die Frage im Raum, ob diese auch gelebt werden. Spätestens wenn der erste Mitarbeiter sensible Kundendaten an den falschen Adressaten per Mail versandt hat, ist klar: hier wurde die Richtlinie nicht beachtet. Interne Konsequenzen für den Mitarbeiter sind hier kein Mittel, um den Schaden für die Person und natürlich auch für das Unternehmen abzuwenden. Also stellen sich folgende Fragen:

- Wie können Richtlinien zum Leben erweckt werden?
- Welche Richtlinien werden überhaupt benötigt?
- Wann sind Richtlinien veraltet und wer ist für die Aktualisierung verantwortlich?

An dieser Stelle kommt es maßgeblich auf die Motivation der Mitarbeiter an. Natürlich kann mit Strafe gedroht werden, aber dieser Schritt sollte immer das letzte Mittel bleiben. Die Erfahrung hat gezeigt, dass Mitarbeiter, die sich mit dem Thema identifizieren und für sich einen Mehrwert erkennen, auch auf diese Vorgaben einlassen. So kann die Software zum einen durch ein Management der Richtlinien unterstützen und zum anderen zu einer Transparenz für den Mitarbeiter beitragen. Am Ende muss immer ein klarer Mehrwert und Vorteil für den Mitarbeiter in seinem Prozessschritt stehen.

Konkret unterstützt eine Software im ersten Schritt beim Aufbau des Informationsverbundes und der Einstufung des Schutzbedarfs. Hierbei ist zu Beginn weniger mehr – und je nach Reifegrad des Unternehmens kann der Informationsverbund komplexer gestaltet werden, um noch feiner steuern zu können. Im ersten Aufbau kann ganz einfach gestartet werden:

- Datenkategorie (CI)
- Prozess Ebene 3 (A)
- Vertragstyp
- Anwendungstyp
- Gerätetyp
- Netztyp
- Raumtyp
- Standorttyp

[Vertraulichkeit (C), Integrität (I), Verfügbarkeit (A)]

Diese Darstellung spiegelt eine hohe Gruppierung wieder. Besonders für Unternehmen im Anfangsstadium ist dies eine valide Vorgehensweise. In der weiteren Ausbaustufe können die Objekte detaillierter angelegt und den Typen zugeordnet werden. Die Typen geben dann die Einstufung des Schutzbedarfs weiter.

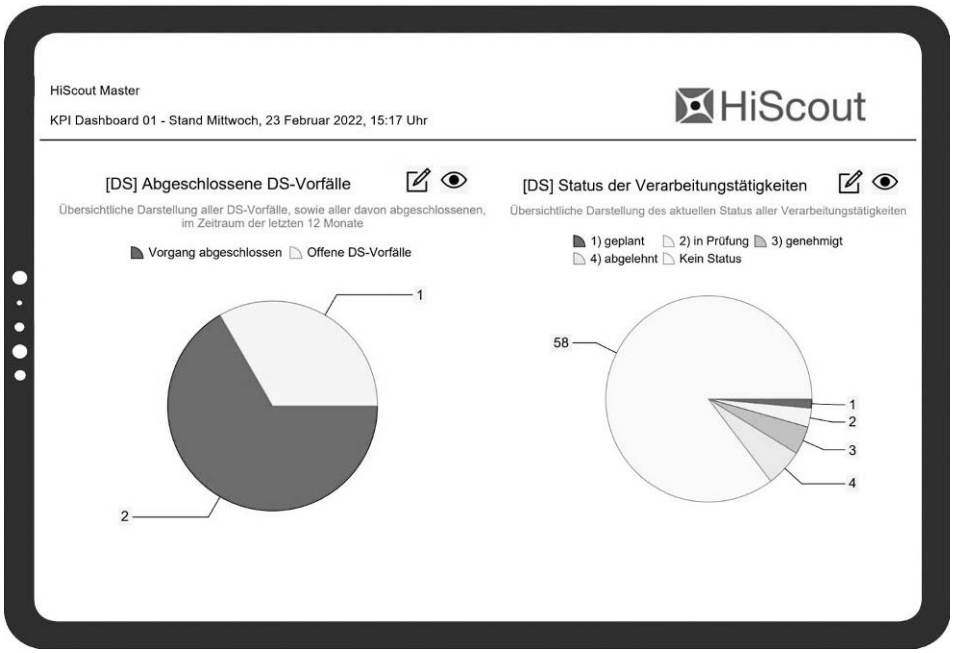
In der Vererbung sind die Datenkategorien die vorgebende Instanz für die Vertraulichkeit und die Integrität. Maßgeblich abgeleitet aus den Sensitivitätsstufen (S1 bis S4). Die Verfügbarkeit wird wiederum aus den Prozessen ermittelt und bildet an dieser Stelle auch das Tandem zum Notfallmanagement (Business Continuity Management).

Nun können die konkreten Anforderungen aus internen Vorgaben oder der Regulatorik (Grundschutz, ISO 27001, EU-DSGVO, …) entsprechend der Einstufung des Schutzbedarfs zugeordnet werden. An diesem Punkt ist es gängige Praxis, dass mit dem Schutzbedarf „sehr hoch“ und „hoch“ begonnen wird. Das BSI spricht in diesem Kontext von „Kronjuwelen“, die es an erster Stelle zu schützen und abzusichern gilt. Eine Softwareunterstützung hält hierfür die Kataloge des Grundschutzes, der ISO 27001 und weitere bereit.

Ein kontinuierlicher Auditzyklus ist elementar, um eine Überprüfung der umgesetzten Maßnahmen auf ihre Wirksamkeit hin zu kontrollieren, sowie die Lücken zu ermitteln. Dabei kann es hilfreich sein, wenn auch externe Dienstleister ein Audit in der eingesetzten Software durchführen können. Letztendlich spart es immensen Aufwand, wenn nicht mehrere Listen im Unternehmen kursieren und eine weitere Liste notwendig wird, um einen aktuellen Stand zu haben. Generell sollte die Datenaktualität einen sehr hohen Stellenwert haben, sonst droht die Gefahr, Entscheidungen auf unsicherer Datenlage zu treffen. Um hier sauber arbeiten zu können, sind wiederum aktuelle Kataloge notwendig und wenn möglich, eine Durchführung von kombinierten Audits. Für den Fachbereich ist nichts leidiger, als in zwei Audits ähnliche Fragen beantworten zu müssen. Insbesondere Anforderungen mit dem Hintergrund der Vertraulichkeit sind in den Disziplinen Datenschutz und Informationssicherheit ähnlich. Somit können mehrere Anforderungen in einer Frage gebündelt werden und die Software verteilt die Antwort dann wieder auf die Anforderungen. Für den Fachbereich bedeutet dies eine immense Zeitersparnis und für den Auditor eine Chance, für mehr Akzeptanz in dem Themenfeld zu werben.

Nicht alles kann zu einhundert Prozent umgesetzt werden. In vielen Fällen ist auch einfach nicht das Budget gegeben, um Themen umzusetzen. In solchen Fällen muss ein Risikokatalog integriert werden. Es ist durchaus legitim, Risiken zu akzeptieren. Am wichtigsten ist jedoch, dass einem Unternehmen alle Risiken bekannt sind. Eine Vorgehensweise für die Ermittlung der Risiken sollte inzwischen in jeder Softwareunterstützung vorhanden sein. Der Trick ist, dass diese auch zum Unternehmen passen muss. Die Philosophie jedes Unternehmens ist völlig unterschiedlich und individuell. Letztlich muss am Ende eine Lösung existieren, die die Geschäftsführung akzeptiert. Sobald sie hierbei Bauchschmerzen hat, ist die Software schon zum Scheitern verurteilt. Im Grunde geht es an dieser Stelle als Erstes um die Ermittlung der Risiken. Einfach wie komplex ist der Grundsatz: sobald eine Anforderung nicht umgesetzt wurde, muss ein Risiko aufgemacht werden. Oder die Anforderung wird durch eine interne Richtlinie konkretisiert, sodass sie nicht an Wirkung verliert und einer externen Prüfung standhalten würde. Dieses Risiko wird beispielweise mit Eintrittswahrscheinlichkeit und Schadenshöhe bewertet und in der Folge einer Behandlung unterzogen. Die Behandlung stellt eine Übernahme, Reduzierung, den Transfer oder die Eliminierung dar. Die Übernahme ist gerade bei niedrigen Eintrittswahrscheinlichkeiten mit hohen Ausgaben für die Maßnahmenumsetzung ein gängiges Mittel. Es sollte nur darauf geachtet werden, dass nicht zu viele Risiken in die Übernahme einfließen. Übersteigt die Schadenshöhe aller Risikoübernahmen irgendwann ein bestimmtes Maß, sind diese Übernahmen nicht mehr akzeptabel. Auch an dieser Stelle überschneiden sich wieder die Themen Datenschutz und Informationssicherheit. Die Philosophie des Risikovorgehens ist für beide Disziplinen durch die Geschäftsführung vorgeben und sollte in einem einheitlichen Risi-

Abbildung 2 | übersichtliche Darstellung beispielsweise in HiScout Datenschutz



kokatalog Einzug finden. Eine übersichtliche Darstellung unterstützt dabei, nicht den Überblick zu verlieren (Abbildung 2).

5 Auswahl der geeigneten Lösung für das Unternehmen

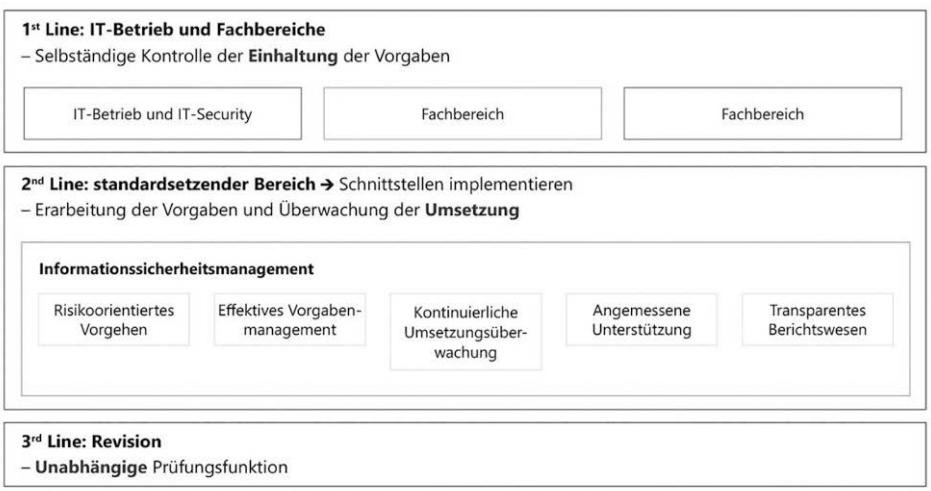
In den meisten Fällen wird eine Methodenkompetenz im Beauftragtenwesen sichergestellt. Hierbei spielt es vorerst keine Rolle, ob es sich um einen internen oder externen Kollegen handelt. Einige Unternehmen lagern diese Kompetenz an Drittanbieter aus. Wichtig ist, dass ein klares Verständnis über die Trennung der Funktionen besteht. Hier hat beispielsweise die Bundesanstalt für Finanzdienstleistungsaufsicht das „Three-Lines-of-Defence-Modell" etabliert (Abbildung 3).

Demnach steht in der ersten Verteidigungslinie der Fachbereich, in der zweiten der Datenschutz- oder Informationssicherheitsbeauftragte und in der dritten eine Revision. Finanzunternehmen oder nicht – die Aufteilung hat in jeder Branche ihre Richtigkeit. Es sollte nicht passieren, dass ein Datenschutz- oder Informationssicherheitsbeauftragter die Antworten für den Fachbereich abgibt. Hier sollte eine klare Trennung bestehen, um ein unverfälschtes Bild zu erhalten sowie die Akzeptanz des Themas im Fachbereich zu erhöhen. Aus diesem Grund ist es immens wichtig, dass die Softwareunterstützung eine Oberfläche bietet, die dem Fachbereich eine intuitive Arbeit ermöglicht. Hier bieten Softwareunterstützungen sogenannte Fragebögen an, die nach dem Ausfüllen wieder in die Datenbank importiert werden. Gängige Praxis sind hier PDF Formulare, um auch netzwerkübergreifend eine Befragung sicherzustellen. Moderne Tools nutzen auch Webformulare, welche die Bearbeitung deutlich effizienter gestalten (Abbildung 4). An dieser Stelle sei auch die Dienstleistersteuerung erwähnt.

Heute arbeitet kein Unternehmen mehr ausschließlich in Excel. Daher bildet eine Einbindung der Softwareunterstützung in die aktuelle Landschaft eine Pflichtanforderung. Es müssen „lebende" Schnittstellen sichergestellt sein, sodass beispielsweise Anwendungen nach Freigabe am nächsten Morgen um acht Uhr auch für den Datenschutz oder Informationssicherheitsbeauftragte in der Softwareunterstützung zur Verfügung stehen.

Durch diese Vorgehensweise wird eine Effizienz geschaffen, die nicht nur wertvolle Zeit der handelnden Mitarbeiter, sondern auch monetäre Mittel einspart. Konkret schafft eine Softwareunterstützung Freiräume und Sicherheit. Sicherheit, sich innerhalb der vorgegebenen und sauber dokumentierten Vorgehensweise eines Prozesses zu bewegen und Sicherheit, weil ein Hersteller hinter der Software steht, der im Zweifel auch bei Know-how-Verlust im Unternehmen neue Mitarbeiter unterstützen kann – besonders in Zeiten des demographischen Wandels kein zu unterschätzender Aspekt.

Abbildung 3 | Three-Lines-of-Defence-Modell



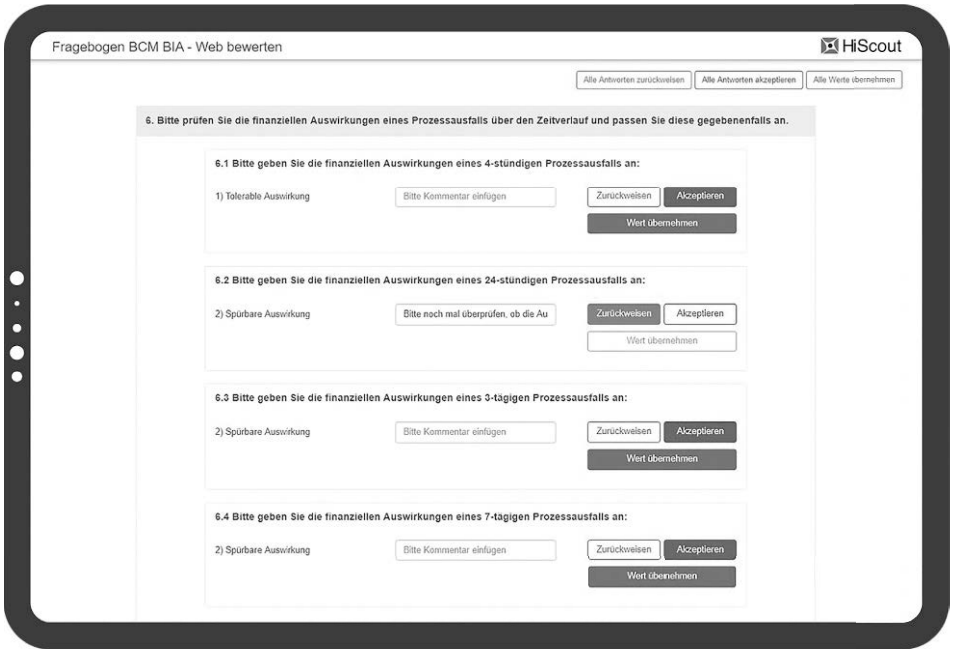
© Quelle: Eigene Darstellung – in Anlehnung an Three-Lines-of-Defence-Modell aus dem Occasional Paper Nr. 11 der BIS, 2015, Bank for International Settlements (BIS).

6 Die Entscheidung liegt beim Unternehmen

Als Fazit lassen sich die Vorteile einer Softwareunterstützung wie folgt zusammenfassen:

- Standardisierte Prozesse bereitstellen. Eine Software kann standardisierte Prozesse für die Implementierung und Verwaltung des Managementsystems bereitstellen. Damit wird sichergestellt, dass Unternehmen die notwendigen Schritte durchführen, um die Informationssicherheit sowie den Datenschutz zu gewährleisten.
- Automatisierung ermöglichen. Ein Software-Tool kann Prozesse wie zum Beispiel Risikobewertungen, Compliance-Überwachung und Berichterstellungen automatisieren, um die Effizienz zu verbessern und menschliche Fehler zu minimieren.
- Zentrale Dokumentenverwaltung. Ein Software-Tool kann eine zentrale Plattform für die Verwaltung von Dokumenten und Richtlinien bereitstellen, die für die Einhaltung des Managementsystems erforderlich sind. Dies erleichtert die Zusammenarbeit und ermöglicht eine schnelle Suche und Überprüfung von Dokumenten.
- Verfolgung und Überwachung. Eine geeignete Software ermöglicht die Verfolgung und Überwachung von Sicherheitsvorfällen oder Datenschutzverstößen und Änderungen am Managementsystem, um schnell auf potenzielle Sicherheitsbedrohungen zu reagieren.
- Berichterstellung und Analyse. Eine Software kann Berichte und Analysen zur Effektivität des Managementsystems bereitstellen, um Organisationen bei der kontinuierlichen Verbesserung zu unterstützen.
- Konfigurierbare Fragebögen. Ein Software-Tool kann Webfragebögen erstellen, die individuell gestaltet sind. Der Mitarbeiter muss sich hier in seinem „Look and Feel“ wiederfinden. Das fördert die Akzeptanz bei der Beantwortung der Fragen und steigert das Marketing der eigenen Rolle als Beauftragter.

Abbildung 4 | HiScout Questionnaire (Web Fragebogen)



Literatur

[1] GENKIN, Boris M. Bedürfnistheorie des Menschen als Grundlage der Motivation der Arbeitsproduktivität. Wissenschaftliche Beiträge 2004, 2004, 9. Jg., S. 15-19.

[2] https://www.bafin.de/SharedDocs/Bilder/DE/BaFinPerspektiven/bp_1_18_beitrag_gampe_abb1.html