

COMPLIANCE MIT SYSTEM

Nach der Prävention ist die wichtigste Aufgabe eines Unternehmens und einer Verwaltung die frühzeitige Aufdeckung von internen Missständen, um Risiken für Bilanz und Image zu minimieren.

Wichtiger Bestandteil eines umfassenden Risikomanagements ist die Nutzung des intern vorhandenen Wissens (Whistleblowing).

39% der Betrugsfälle werden durch Hinweisgeber enthüllt, wobei nicht nur eigene Mitarbeiter, sondern auch Kunden und Lieferanten zur Aufdeckung beitragen. Aktuelle Studien sehen Hinweisgebersysteme als effektivste Aufklärungsmethode vor internen Kontrollen, der internen und externen Revision – vor allem bei hochdotierten Fällen. Unternehmen, die kein Hinweisgebersystem einsetzen, erleiden im Durchschnitt mehr als doppelt so hohe Verluste durch Betrugsdelikte als Unternehmen, die einen sicheren Kommunikationskanal etabliert haben.

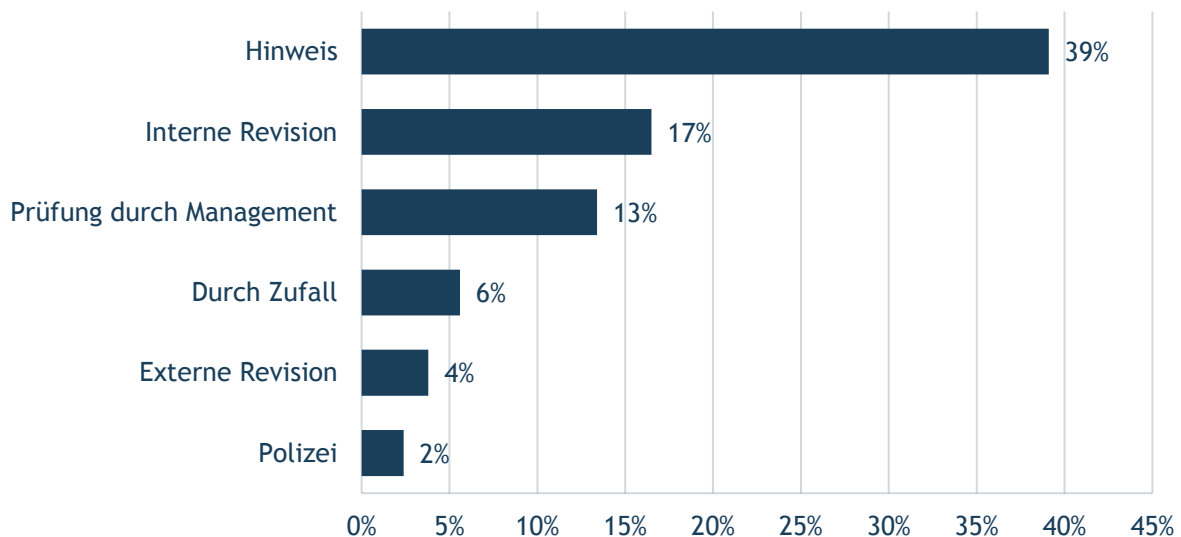


Abb. 1: Aufdeckungsmethoden Wirtschaftskriminalität (Quelle: Association of Certified Fraud Examiners 2016, Auszug)

Da Hinweisgeber in vielen Ländern rechtlich noch nicht ausreichend geschützt sind, ist die Zusicherung der absoluten Anonymität unumgänglich, um sie bei Bedarf vor negativen persönlichen Folgen zu schützen.

Bisher eingesetzte Hinweisgebersysteme können jedoch entweder die Anonymität des Hinweisgebers nicht ausreichend sichern oder haben den Nachteil, keinen weiterführenden Dialog mit dem Hinweisgeber zu ermöglichen, der insbesondere zur Überprüfung und schnellen Konkretisierung des Falls notwendig ist.

Das BKMS® System schafft erstmals die Verbindung dieser scheinbaren Gegensätze: Anonymität und Dialog. Gleichzeitig bietet es die höchstmögliche Sicherheit für brisante Daten.

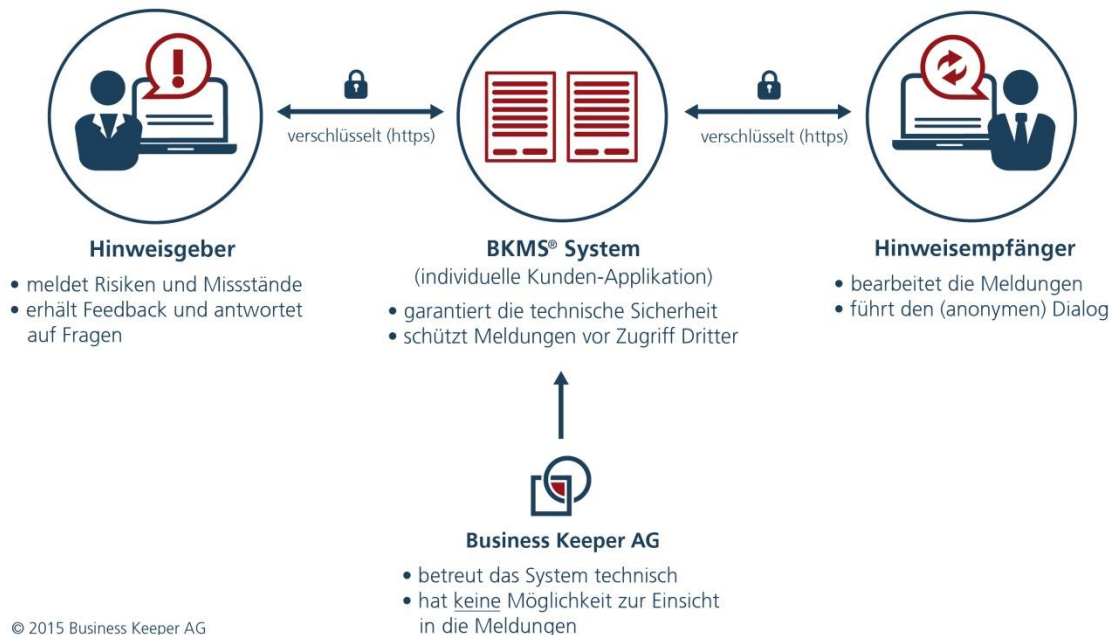


Abb. 2: Sicherheitskonzept BKMS® System

Internetbasiert nimmt das BKMS® System Hinweise der Mitarbeiter und des gesamten Umfeldes weltweit und rund um die Uhr auf. Mit technisch individuellen Verschlüsselungskonstellationen wird jeder Hinweis bezüglich Inhalt und Kanal gesichert und kann nur vom Kunden entschlüsselt werden – auch die Business Keeper können nicht auf die Meldungen zugreifen. Der externe BKMS®-Server befindet sich in einem Hochsicherheitsrechenzentrum in Deutschland.

Die Besonderheit des zertifizierten BKMS® Systems ist der anonyme Dialog zwischen Hinweisgeber und einem Hinweisbearbeiter direkt beim Kunden (Korruptionsbeauftragte, Ombudsleute, Revision im Unternehmen oder in der Verwaltung), so dass der Hinweisgeber über den Stand der Bearbeitung informiert oder zum Tatbestand weiter befragt werden kann. Um der Problematik des Einbahnstraßencharakters anonymer Meldungen zu begegnen, hinterlegt der Hinweisgeber seine Meldung in einem von ihm selbst eingerichteten, geschützten Postkasten.

Oft stoßen Ermittler an Grenzen, wo weitere Informationen fehlen. Über das BKMS® System kann das Insiderwissen des Hinweisgebers kontinuierlich genutzt werden, um die Ermittlungen zu lenken und zu beschleunigen. Das kritische Potential der Beschäftigten ist eine wichtige betriebliche Ressource, ein Frühwarnsystem, um Fehlverhalten zeitig aufzudecken – dies erspart erhebliche Folgekosten und Imageschäden.

Durch die Prävention bzw. interne Klärung von Abweichungen vermeidet eine Organisation materielle und immaterielle Schäden und schafft damit einen vertrauens- und wertbildenden Faktor für Investoren und Kunden.