

# Gefährdungsanalysen

## » Wozu brauche ich diese Lösung?

- Sie möchten wissen, in welchen Bereichen Ihre Organisation durch Wirtschaftskriminalität bedroht ist.
- Sie möchten die Schwächen in Ihrem Internen Überwachungssystem heilen, um zukünftig keinen wesentlichen Risiken mehr ausgesetzt zu sein.
- Sie möchten eine Prüfung der IT-Kontrollen durchführen, um auch von dieser Seite wirksam geschützt zu sein.
- Sie möchten Ihre internen Überwachungsorgane in Bezug auf best practice benchmarken.
- Sie möchten sich als Vorstand oder Geschäftsführer hinsichtlich eines möglichen Organisationsverschuldens absichern.

## » Problembeschreibung

Unter Gefährdungsanalyse (auch: Risikoevaluierung, IKS-Untersuchung) verstehen wir eine Untersuchung der Aufbau- und Ablauforganisation in einer Organisation, um

- Einfallstore für dolose Handlungen zu identifizieren,
- Bestehende (IT-)Kontrollen zu evaluieren,
- Vorhandene Kontrollschwächen zu beheben,
- Die Ausrichtung und die Prozesse der Internen Revision, wenn nötig, anzupassen

und auf diese Weise das bestehende Gefährdungsrisiko zu verringern und möglichst auszuschalten.

Als fachliche Grundlagen fließen in die Evaluierung moderne Risikomodelle wie COSO I und COSO II mit ein. Neben Best Practices der Korruptionsprävention, die wir teilweise unter anderem für Transparency German Chapter mit entwickelt haben, kommen individuelle Kodizes des Mandanten sowie die gesetzlichen Grundlagen in Betracht.

Hierbei nimmt die Evaluierung der Internen Revision mit dem Schwerpunkt Fraubekämpfung eine wichtige Rolle ein. Auf Grund der Erwartungshaltung der Stakeholder der Internen Revision ist es notwendig, sie als Bestandteil des Internen Überwachungssystems hinsichtlich ihrer Präventiv-, Aufdeckungs- und Aufarbeitungsfunktion besonders zu berücksichtigen.

Wesentlicher Bestandteil einer umfassenden Gefährdungsanalyse sind die in den ERP-Systemen abgebildeten Geschäftsprozesse der Unternehmen. Die Sicherheit der Verarbeitung sowie der zugrunde liegenden IT-Infrastruktur untersuchen Spezialisten aus unserem Netzwerk beispielsweise in einem SAP-Basischeck, bei dem u. a. die Parametrisierung, die Protokollierung, die System-sicherheit und die Berechtigungskonzeption untersucht werden. Auch die Kontrollen und Abstimmungen in den rechnungslegungsrelevanten Prozessen werden auf mögliche Einfallstore für dolose Handlungen analysiert. Bei der Beurteilung der IT-Umgebung werden die aktuellen Standards der IT (z. B. COBIT, ITIL und ISO 27001) berücksichtigt.

Der modulare und skalierbare Aufbau unseres Produkts ermöglicht eine hohe Absicherung gegen Risiken doloser Handlungen durch interne und externe Täter.

Hierbei können wir unsere umfassende Kenntnis Interner Kontrollsysteme in großen und mittelständischen Organisationen effizient und effektiv einbringen.

## » Lösung

- Einschätzung der Qualität der Soft Controls in Ihrer Organisation zur Prävention gegen Wirtschaftskriminalität
- Untersuchung des Aufbau- und Ablauforganisation hinsichtlich der konkreten Bedrohungen durch Wirtschaftskriminalität
- Aufzeigen von Kontrollschwächen und Entwicklung von wirksamen Maßnahmen zur Etablierung eines wirksamen Internen Überwachungssystems
- Auf Wunsch: Einschätzung der Internen Revision in Bezug auf deren Potential zur Bekämpfung von Wirtschaftskriminalität, Coaching und gegebenenfalls Neuausrichtung des Prüfungsansatzes

## » Kurz Gefasst

- **Produkttyp:** Modulare Prüfung (IT, Prozesse, Interne Revision)
- **Umfang:** Abhängig von der Größe und Komplexität des zu untersuchenden Organisation, skalierbar auf Wunsch nur für zentrale Prozesse oder die gesamte Organisation