IT-Risk Management beginnt mit IT-Governance

written by Christian Hafner | 22 April, 2024

Riskmanagement & IKS News

IT-Risk Management beginnt mit IT-Governance

Wenn CIO (Chief Information Officer) Fehler machen, können die Folgen verheerend sein.

Chief Information Officers (CIOs) sind für die strategische Ausrichtung und den reibungslosen Betrieb der IT-Infrastruktur verantwortlich. Doch mit dieser Verantwortung geht auch ein hohes Mass an Risiko einher.

Fehler in der IT-Governance oder im Risk Management können verheerende Auswirkungen auf das Unternehmen haben. Daher ist es entscheidend, dass CIOs diese Aspekte sorgfältig betrachten und in ihre Strategien integrieren.

Notwendigkeit einer klaren IT-Governance

Die IT-Governance muss klar definiert und an die Mission, Vision und Strategie des Unternehmens angepasst sein.

Wenn sich Geschäftspraktiken oder Unternehmensstrukturen verändern, muss die IT-Governance nahtlos überprüft und evtl. angepasst werden.

Wenn das vernachlässigt wird, resultieren Ineffizienzen und Sicherheitslücken.

Um dies zu vermeiden, gehört eine regelmässige Überprüfung und Anpassung der IT-Governance als Steuerungsaufgabe ins interne Kontrollsystem (IKS) jeder Organisation.

Risikomanagement als zentraler Bestandteil

CIOs sind idealerweise Machertypen und Problemlöser. Sie sind Wegbereiter für die Umsetzung von strategischen Initiativen und treiben sie voran.

Dabei dürfen sie nicht vergessen, alle damit verbundenen Risiken vollständig zu berücksichtigen. Sonst kann es zu Fehlentscheidungen führen und den Erfolg der Initiativen gefährden.

> Ein strukturierter Risikominderungsprozess als Teil eines umfassenden Governance-Programms ist daher unerlässlich. Dieser Prozess hilft dabei, potenzielle Risiken frühzeitig zu identifizieren und angemessen zu adressieren.

Herausforderungen der dezentralen IT-Arbeitsumgebung

Die zunehmende Dezentralisierung der IT-Arbeitsumgebung und die hohe Mitarbeiterfluktuation erhöhen das Risiko von Schäden durch Insider-Bedrohungen. Hinterlistige Mitarbeiter, die mit externen Angreifern zusammenarbeiten, können besonders gefährlich sein.

Daher ist es wichtig, neben externen Bedrohungen auch interne Risiken im Blick zu behalten und entsprechende Sicherheitsmassnahmen zu implementieren.

Praxis-Tipps für eine effektive IT-Governance:

1. Datensicherheit priorisieren:

   Sicherheit von Daten muss oberste Priorität haben. Implementierung von Best Practices für die Netzwerksicherheit und regelmässige Überprüfung der Datensicherheitsmassnahmen sind unerlässlich.

2. Cyber-Schulungen für Anwender:

   Sensibilisierung der Mitarbeiter für Cyber-Bedrohungen durch regelmässige Schulungen und Trainingsprogramme.

3. Effektives Content-Governance-Programm:

   Ein umfassendes Content-Governance-Programm ermöglicht eine zentrale Verwaltung und Kontrolle von Daten. Dadurch können böswillige Aktivitäten frühzeitig erkannt und abgewehrt werden.

Fazit: Insgesamt ist eine effektive IT-Governance und ein umfassendes Risk Management entscheidend für den Erfolg eines Unternehmens.

CIOs sollten diese Aspekte nicht nur als Pflicht betrachten, sondern als Chance, die Sicherheit, Effizienz und den Erfolg des Unternehmens langfristig zu gewährleisten.