carmasec
security. done. right.

Checkliste: IT-Risikomanagement - alles im Griff?

Ist Ihr Risikomanagement wirklich wirksam, und gehen Sie gezielt mit Ihren Risiken um? Wie stark fließt es in Ihre strategischen Entscheidungen ein? Mit unserer Checkliste können Sie Schritt für Schritt die wichtigsten Punkte abhaken und sich Klarheit verschaffen – strukturiert, pragmatisch und effektiv.

1. Risikoregister

- ☐ Gibt es ein aktuelles und vollständiges Risikoregister?
- ☐ Sind alle relevanten Risiken (interne und externe) erfasst?
- ☐ Sind alle Risiken einem Verantwortlichen (Risiko-Owner) zugeordnet?
- ☐ Sind Risiken in Kategorien eingeteilt (z. B. strategisch, operativ, finanziell, rechtlich)?
- ☐ Sind für jedes Risiko Eintrittswahrscheinlichkeit und potenzielle Auswirkungen bewertet?

2. Maßnahmen zur Risikobehandlung

- ☐ Sind Maßnahmen zur Risikobehandlung für jedes zu mindernde Risiko definiert?
- ☐ Wurden die Verantwortlichkeiten für die Umsetzung der Maßnahmen klar zugewiesen?
- ☐ Gibt es einen Umsetzungsplan mit Deadlines und Meilensteinen?
- ☐ Werden die Maßnahmen regelmäßig überwacht und dokumentiert?
- ☐ Gibt es Mechanismen, um die Wirksamkeit der Maßnahmen zu überprüfen?

3. Kommunikation und Verantwortlichkeiten

- ☐ Sind alle relevanten Stakeholder über das Risikomanagement informiert?
- ☐ Gibt es klare Verantwortlichkeiten für die Risikoüberwachung?
- ☐ Werden regelmäßige Risikomanagement-Meetings durchgeführt?
- ☐ Gibt es eine Eskalationsmatrix für kritische Risiken?
- ☐ Werden Berichte oder Dashboards für das Management erstellt, um den Status der Risiken darzustellen?

4. Risikobeurteilung und -bewertung

- ☐ Werden Risiken regelmäßig überprüft und aktualisiert?
- ☐ Ist geklärt, wann und wie eine erneute Risikobeurteilung durchgeführt wird?
- ☐ Werden Veränderungen bei internen und externen Bedrohungen (wirtschaftlich, politisch, technologisch) beachtet?
- ☐ Gibt es standardisierte Methoden oder Tools für die Risikobewertung (z. B. SWOT- oder Szenario-Analyse)?
- ☐ Sind Schwellenwerte definiert, die eine erneute Beurteilung auslösen?

5. Dokumentation

- ☐ Werden alle Änderungen, Entscheidungen und neue Rahmenbedingungen zeitnah dokumentiert und regelmäßig aktualisiert?
- ☐ Werden alle relevanten Risikodokumente zentral und zugänglich abgelegt?
- ☐ Ist die Dokumentation revisionssicher?
- ☐ Werden behandelte Risiken und deren Historie dokumentiert?
- ☐ Werden Erfahrungen ausgewertet und festgehalten?
- ☐ Wird Risikomanagement-Software zur Unterstützung der Prozesse eingesetzt?

6. Schulung und Sensibilisierung

- ☐ Werden neue Mitarbeitende in das bestehende Risikomanagementsystem eingeführt?
- ☐ Werden Mitarbeitende regelmäßig im Umgang mit Risiken geschult?
- ☐ Gibt es eine Kultur der Offenheit für die Meldung von Risiken?
- ☐ Werden Erfahrungsberichte aus Risikosituationen aktiv geteilt und diskutiert?

7. Kontinuierliche Verbesserung

- ☐ Gibt es Mechanismen zur kontinuierlichen Verbesserung des Risikomanagements?
- ☐ Werden Benchmarks oder Audits für das Risikomanagement genutzt?
- ☐ Werden Feedback und Verbesserungsvorschläge von Stakeholdern berücksichtigt?
- ☐ Wird das IT-Risikomanagement genutzt, um die Unternehmensstrategie kontinuierlich weiterzuentwickeln?

Sie haben nicht alle Checkboxen abgehakt? Kontaktieren Sie uns jetzt für eine Erstberatung!

Ihr Ansprechpartner

Till Bormann
Senior Security Consultant

Tel.: +49 (0) 201 426 385 905
E-Mail: vertrieb@carmasec.com