



## **Risikobasiert die Resilienz Ihrer IT-Systeme erkennen und verbessern**

- > Schafft Transparenz zu aktuellen Risiken der IT-Umgebung und -Organisation.
- > Sensibilisiert Entscheidungsträger:innen und zeigt zentrale Handlungsfelder auf.
- > Kann Stärkung der IKT-Sicherheit in messbaren Zahlen aufzeigen (durch Folge-Assessment).



### Vorteile des Assessments

- > Das Assessment bietet eine unabhängige Aussensicht von Expert:innen auf alle sicherheitsrelevanten Aspekte Ihrer IT-Umgebung und der Organisation.
- > Der strukturierte Austausch zwischen unterschiedlichen Akteur:innen innerhalb der Organisation und die Analysen von IKT-Security-Auditoren sensibilisieren für Sicherheitsfragen und -lücken.
- > Entscheidungsträger:innen erhalten faktenbasiert spezifische IKT-Sicherheitsbedürfnisse übersichtlich dokumentiert.
- > Basiert auf bewährtem Framework für Schweizer Behörden.
- > Periodisches Durchführen des Assessments kann den Erfolg der Sicherheitsmassnahmen ausweisen.

### Optionen

- > Periodische Durchführung des Assessments
- > Unterstützung bei der Umsetzung der konkreten Handlungsempfehlungen

Für weiterführende Informationen kontaktieren Sie uns bitte.

### Die wichtigsten Erfolgskriterien

#### Transparenz schaffen

Die Erfahrung zeigt: In jeder Organisation finden sich blinde Flecken, und diese können durch ein behördenfokussiertes Assessment entdeckt und bewertet werden. Parallel wird die verwaltete Infrastruktur ausgeleuchtet und es werden mögliche Lücken in der IKT-Resilienz sichtbar.

#### Entscheidungsgrundlage bilden

Das Assessment bildet die fundierte Grundlage, um eine aktive Sicherheitsstrategie (z.B. ISDS-Konzept, Sicherheits-Architektur, Supply-Chain-Aspekte, das Element Mensch...) zu entwickeln. Sie können dedizierte Massnahmen ableiten, um den Business-Impact zu bewerten, risikobasiert Schwachstellen zu beheben und künftige Bedrohungen besser abzuwehren.

#### Konkrete Empfehlungen für die Praxis erhalten

Als Basis wird das vom Bundesamt für wirtschaftliche Landesversorgung BWL entwickelte Framework mit Know-how von Security-Experten kombiniert. Die resultierenden, übersichtlichen Spinnendiagramme werden mit Empfehlungen komplettiert, die spezielle Bedürfnisse der öffentlichen Hand und für kritische Infrastrukturen berücksichtigen.

#### Ressourcenbasiert Handlungsbedarf benennen

Als Resultat kann die Organisation konkrete Handlungsanweisungen benennen und priorisieren, welche auch die vorhandenen Ressourcen berücksichtigen. Die Umsetzung der definierten Verbesserungen führen zu einer höheren Bewertung der IKT-Sicherheit, die in einem Folge-Assessment aufgezeigt werden können, um getätigte Investitionen zu rechtfertigen.

#### Kundenservice

Unser Kundensupport gewährleistet schnelle und kompetente Unterstützung. Dabei profitieren Sie von unserer jahrelangen Erfahrung im Bereich der öffentlichen Hand und von der Fach- und Branchenkompetenz unserer Mitarbeitenden.



#### Weitere Informationen

[verkauf@abraxas.ch](mailto:verkauf@abraxas.ch)  
Telefon 058 660 00 00