B-Rating

> ***English version down below***

Die "B-Fragen" im Kontext des CyberRisk Ratings sind Teil eines umfassenden Fragebogens, der dazu dient, das Risikoprofil einer Organisation im Bereich der Cybersicherheit zu bewerten. Diese spezifischen B-Fragen sind für die Beurteilung von grundlegenden Aspekten des CyberRisiko-Managements und der Sicherheitspraktiken in einem Unternehmen vorgesehen. Sie decken verschiedene Kategorien ab, wie z.B.:

- **Risiko-Verstehen und Risikobewertung**: Hierbei geht es darum, wie das Unternehmen identifiziert, quantifiziert und managt seine Cyberrisiken.
- **Politik und Strategie**: Diese Fragen beziehen sich auf die Existenz und Umsetzung von Richtlinien für Cybersicherheit im Unternehmen, einschließlich der Zuteilung von Rollen und Verantwortlichkeiten.
- **Technische Maßnahmen**: Hier werden technische Sicherheitsprotokolle und -lösungen erfasst, die das Unternehmen implementiert hat, um seine Daten und Systeme zu schützen.
- **Datenschutz**: Fragen in dieser Kategorie abrunden, wie das Unternehmen den Datenschutz gewährleistet und datenschutzrechtliche Verpflichtungen erfüllt.
- **Zusammenarbeit und Kommunikation**: Dieser Bereich befasst sich mit der Zusammenarbeit innerhalb des Unternehmens sowie mit externen Partnern im Falle eines Cyberangriffs oder einer Sicherheitsverletzung.
- **Inzidenreaktion und -bewertung**: Hierbei geht es um die Vorbereitung und das Vorgehen bei dem Ausbruch einer Cyberinfrastruktur.

Die B-Fragen sind entscheidend, um einen Überblick über die Maßnahmen zu erhalten, die ein Unternehmen zur Abschreckung von Cyberangriffen ergriffen hat, und um festzustellen, wie gut das Unternehmen auf solche Ereignisse reagieren kann.

> **English version:**

The "B questions" in the context of CyberRisk Ratings are part of a comprehensive questionnaire designed to assess an organization's risk profile in the field of cybersecurity. These specific B questions are intended for evaluating fundamental aspects of cyber risk management and security practices within a company. They cover various categories such as:

- **Risk Understanding and Assessment:** This pertains to how the company identifies, quantifies, and manages its cyber risks.

- **Policy and Strategy:** These questions relate to the existence and implementation of cybersecurity policies within the company, including the allocation of roles and responsibilities.
- **Technical Measures:** This section captures technical security protocols and solutions implemented by the company to protect its data and systems.
- **Data Privacy:** Questions in this category address how the company ensures data privacy and fulfills data protection obligations.
- **Collaboration and Communication:** This area deals with collaboration within the company and with external partners in the event of a cyberattack or security breach.
- **Incident Response and Assessment:** This involves the preparation and procedures for responding to a cyber infrastructure breach.

The B questions are crucial for gaining insight into the measures taken by a company to deter cyberattacks and determining how well the company can respond to such events.

Revision #5
Created 2024-05-03 10:00:32 UTC by Viktor Mühlberger
Updated 2024-05-23 09:17:03 UTC by Edis Hadzic