Über uns | About us

> ***English version down below***

Inhaltsverzeichnis

- **Allgemeines**
- **Für kritische Infrastrukturen & Unternehmen**
- **Für bewertete Unternehmen**

Allgemeines

Das CyberRisk Rating von KSV1870 wurde im Jahr 2020 entwickelt. Das Konzept wurde vom Kompetenzzentrum Sicheres Österreich in Zusammenarbeit mit CISOs, DPOs und Managern aus kritischen Infrastrukturen, Regierung und Industrie entwickelt, um einen Standard für die Bewertung zu entwickeln. Die Anforderungen des Cyber-Risikoschemas wurden von führenden Cyber-Risikomanagern aus allen Bereichen der kritischen Infrastruktur sowie Vertretern bekannter österreichischer Unternehmen definiert - das Rating ist daher für jede Branche und jeden Wirtschaftsbereich geeignet. Ziel ist es, ein höheres Maß an IT-Sicherheit in der gesamten EU zu gewährleisten und digitale Risiken in Lieferketten zu identifizieren. Das öffentlich und frei zugängliche Schema wird vom Cyber Risk Advisory Board jährlich aktualisiert und überarbeitet, um schnell auf neue Anforderungen aus der Praxis oder der ausführenden NIS-Behörde (BMI) reagieren zu können. Diese Standards bilden die Grundlage des CyberRisk Ratings von KSV1870.

Link zum KSÖ-Schema 2024

Die DSGVO und die EU-NIS-Richtlinie verlangen von allen Organisationen, insbesondere von Betreibern wesentlicher Dienste, ein Cyber-Risikomanagement für Lieferanten und Dritte. Das CyberRisk Rating von KSV1870 stellt einen standardisierten Prozess dar, um diese Anforderungen zu erfüllen. Cyber-Risiken in globalen Lieferketten werden transparent und können gezielt reduziert werden.

Link zur EU-NIS-Richtlinie

Das CyberRisk Rating von KSV1870 ist in zwei Bereiche unterteilt:

Einerseits eine Plattform für das Cyber-Risikomanagement für alle Lieferanten weltweit für kritische Infrastrukturen und Unternehmen und andererseits ein effizienter Bewertungsprozess für bewertete Unternehmen.

Für kritische Infrastrukturen & Unternehmen

Das CyberRisk Rating von KSV1870 bietet Ihnen ein einheitliches System, um die Anforderungen des EU-NIS-Gesetzes und der DSGVO für Lieferanten zu erfüllen.

Das CyberRisk Rating von KSV1870 verwendet drei grundlegende Prozesse zur Bewertung globaler Lieferantenbasen:

1. Die Bewertung öffentlicher IT-Sicherheitsdaten für alle Lieferanten Ihrer Organisation,
2. Die validierte CyberRisk Rating-Bewertung gemäß dem KSÖ Cyber Risk Schema auf der Grundlage direkter Informationen von Lieferanten und falls erforderlich:
3. Audits der CyberRisk-Bewertungen durch Drittauditoren.

Für bewertete Unternehmen

Unsere Lösung bietet zwei Bewertungstiefen: Zunächst erstellt der automatisierte Web Risk Indikator eine Basislinie für alle Ihre Lieferanten. Anschließend entscheiden Sie, welche Lieferanten für den Bewertungsprozess ausgewählt werden, der zu einer vollständigen A+- oder B-Bewertung führt.

Sobald eine CyberRisk-Bewertung für Ihr Unternehmen angefordert wird, erhalten Sie eine E-Mail mit dem Einladungslink zur Bewertung. Ihre Cyber-Risikobewertung besteht aus 25 Ja/Nein-Fragen. Wenn Sie mit "Ja" antworten, beschreiben Sie bitte die Umsetzung der Anforderung in Ihrer Organisation. Nach der Bewertung werden Ihre Antworten von einem IT-Sicherheitsexperten validiert.

Es kann vorkommen, dass die Validierung eine oder mehrere Ihrer Antworten als unklar einstuft. In diesem Fall werden wir Ihnen Feedback geben und um weitere Details bitten. Sie erhalten dann eine Benachrichtigung von uns. Sie haben die Möglichkeit, Ihre Antworten einmal zu korrigieren. Anschließend wird Ihre Bewertung erneut validiert, was zur endgültigen Bewertung führt.

Als letzten Schritt können Sie auswählen, welche CyberRisk-Bewertung für Ihr Unternehmen veröffentlicht werden soll - A (erweiterte Anforderungen) oder B (Grundanforderungen)? Um Ihnen die Auswahl zu erleichtern, wird eine Empfehlung angezeigt. Nachdem Sie die gewünschte Bewertung ausgewählt haben, ist der Prozess abgeschlossen. Ihre CyberRisk-Bewertung ist ein Jahr lang gültig.

> **English version:**

Table of contents

- **General Information**
- **For Critical Infrastructures & Companies**
- **For Rated Companies**

General Information

The CyberRisk Rating by KSV1870 was developed in 2020. The concept was created by the Secure Austria Competence Center in collaboration with CISOs, DPOs, and managers from critical infrastructures, government, and industry to develop a standard for assessment. The requirements of the cyber risk scheme were defined by leading cyber risk managers from all areas of critical infrastructure as well as representatives of well-known Austrian companies - the rating is therefore suitable for every industry and economic sector. The goal is to ensure a higher level of IT security throughout the EU and to identify digital risks in supply chains. The publicly and freely accessible scheme is updated and revised annually by the Cyber Risk Advisory Board to respond quickly to new requirements from practice or the executing NIS authority (BMI). These standards form the basis of the CyberRisk Rating by KSV1870.

Link to the KSÖ-Scheme 2024

The GDPR and the EU NIS Directive require all organizations, especially operators of essential services, to implement cyber risk management for suppliers and third parties. The CyberRisk Rating by KSV1870 provides a standardized process to meet these requirements. Cyber risks in global supply chains become transparent and can be specifically reduced.

Link to the EU NIS Directive

The CyberRisk Rating by KSV1870 is divided into two areas:

On one hand, a platform for cyber risk management for all suppliers worldwide for critical infrastructures and companies, and on the other hand, an efficient assessment process for rated companies.

For Critical Infrastructures & Companies

The CyberRisk Rating by KSV1870 offers you a unified system to meet the requirements of the EU NIS Act and GDPR for suppliers.

The CyberRisk Rating by KSV1870 uses three fundamental processes to assess global supplier bases:

1. The assessment of public IT security data for all suppliers of your organization,

2. The validated CyberRisk Rating assessment according to the KSÖ Cyber Risk Scheme based on direct information from suppliers, and if necessary:
3. Audits of CyberRisk assessments by third-party auditors.

For Rated Companies

Our solution offers two levels of assessment: Initially, the automated Web Risk Indicator creates a baseline for all your suppliers. Then, you decide which suppliers will be selected for the assessment process, leading to a full A+ or B rating.

Once a CyberRisk assessment for your company is requested, you will receive an E-Mail with the invitation link to the assessment. Your cyber risk assessment consists of 25 yes/no questions. If you answer "yes," please describe the implementation of the requirement in your organization. After the assessment, your answers will be validated by an IT security expert.

It may happen that the validation considers one or more of your answers as unclear. In this case, we will provide feedback and ask for further details. You will then receive a notification from us. You have the opportunity to correct your answers once. Your assessment will then be re-validated, leading to the final rating.

As the last step, you can choose which CyberRisk rating for your company should be published - A (advanced requirements) or B (basic requirements). To help you make the selection, a recommendation will be displayed. After you select the desired rating, the process is completed. Your CyberRisk rating is valid for one year.

Revision #33
Created 2024-05-02 12:23:04 UTC by Edis Hadzic
Updated 2025-08-12 10:31:22 UTC by Viktor Mühlberger