Allgemeine Informationen | General information

- Über uns | About us
- Häufig gestellte Fragen | Frequently asked questions
- Überprüfung der PDF-Integrität | Verification of PDF Integrity

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.

Häufig gestellte Fragen | Frequently asked questions

> ***English version down below***

> **Kontaktdaten für Fragen: KSV1870 Nimbusec GmbH | office@nimbusec.com | +43 (732) / 860 626 | Kaisergasse 16b, 4020 Linz**

Inhaltsverzeichnis

- **Welche Vorteile haben Kunden?**
- **Was kostet das CyberRisk Rating von KSV1870?**
- **Wo kann das CRR verwendet werden?**
- **Warum erhalte ich eine Anfrage für ein CyberRisk Rating?**
- **Wie funktioniert der CyberRisk Rating-Prozess?**
- **Gibt es eine Frist, bis zu der eine Bewertung eingereicht werden muss?**
- **Ist es möglich, dass mehr als eine Person an der Bewertung arbeitet?**
- **Muss die Bewertung auf einmal abgeschlossen werden?**
- **Erhalte ich meine Antworten, einschließlich einer Bewertung später?**
- **Wer bekommt sonst noch die Antworten?**
- **Müssen die Antworten für jeden Kunden bereitgestellt werden?**
- **Werden die Antworten vorübergehend gespeichert?**
- **Wie wird die Vertraulichkeit meiner eigenen Informationen gewährleistet?**

Welche Vorteile haben Kunden?

Nutzer des CyberRisk Ratings von KSV1870 erhalten einen standardisierten Prozess zur Bewertung aller Dienstleister, Lieferanten und anderer Dritter in Bezug auf ihre Cyber-Sicherheit. Bewertete Unternehmen erhalten einen effizienten, objektiven Prozess, der nur einmal im Jahr durchgeführt werden muss, um ihr Cyber-Risiko allen interessierten Kunden offenzulegen. Durch den veröffentlichten Standard des "Kompetenzzentrums Sicheres Österreich" können bewertete Unternehmen ihr Cyber-Risikomanagement positiv beeinflussen. Alle Unternehmen erhalten kostenlos eine Richtlinie, um ihr eigenes Cyber-Risiko gezielt und strukturiert zu reduzieren. Diese Richtlinie wird kontinuierlich von Österreichs anerkanntesten Experten gepflegt und an neue technische Anforderungen angepasst. Die österreichische Wirtschaft wird widerstandsfähiger,

indem das Cyber-Risiko ihrer Lieferketten reduziert wird. Dies bildet die Grundlage für die notwendige Digitalisierung, um unsere internationale Wettbewerbsfähigkeit zu erhalten.

Was kostet das CyberRisk Rating von KSV1870?

Unternehmen, die bewertet werden, müssen keine Kosten tragen. Derzeit wird das CyberRisk Rating nur für große Unternehmen und kritische Infrastrukturen angeboten. Wenn Sie an weiteren Informationen interessiert sind, beantworten wir gerne Ihre Fragen.

Wo kann das CRR verwendet werden?

Das CyberRisk Rating von KSV1870 basiert auf den Anforderungen des Cyber-Risiko-Schemas des "Kompetenzzentrums Sicheres Österreich". Diese Anforderungen wurden von führenden Cyber-Risiko-Managern österreichischer Unternehmen aus allen Bereichen der kritischen Infrastruktur sowie Vertretern des Bundesministeriums für Inneres definiert. Das CyberRisk Rating kann daher in jeder Branche und jedem Wirtschaftssektor verwendet werden, in denen eine Bewertung des Cyber-Risikos von Unternehmen - insbesondere von Lieferanten - erforderlich ist.

Vorwiegend sind Betreiber wesentlicher Dienste gemäß § 11 Abs. 1 (2) in Verbindung mit Anhang 1 NISV gesetzlich verpflichtet, angemessene Sicherheitsvorkehrungen im Umgang mit Dienstleistern, Lieferanten und anderen Dritten zu treffen. Das vorliegende CyberRisk Rating von KSV1870 zielt darauf ab, diese Anforderung zu erfüllen (Überwachung von Lieferanten einer Energiegruppe oder eines Flughafens), ersetzt jedoch nicht den notwendigen Nachweis eines Betreibers wesentlicher Dienste gemäß § 17 Abs. 3 NISG (= umfassende Prüfung eines Betreibers wesentlicher Dienste, wie z. B. einer Energiegruppe oder eines Flughafens selbst).

Warum erhalte ich eine Anfrage für ein CyberRisk Rating?

Cyber-Risiken wie IT-Sicherheit, Datenschutz und Geschäftskontinuität gewinnen aufgrund der Digitalisierung zunehmend an Bedeutung. Mit dem CyberRisk Rating bietet KSV1870 einen transparenten, zeitsparenden Prozess zur Bewertung von Unternehmen in diesen Dimensionen an. Diese Bewertung ist oft aufgrund der DSGVO oder des NIS-Gesetzes erforderlich.

Als bewertetes Unternehmen tragen Sie keine Kosten und erhalten ein objektives Bild Ihres eigenen Cyber-Risikos.

Wie funktioniert der CyberRisk Rating-Prozess?

Die Bewertung besteht aus einer Beurteilung basierend auf 25 Anforderungen des öffentlich zugänglichen KSÖ Cyber Risk Schema. Informationen zum KSÖ Cyber Risk Schema finden Sie unter

https://www.kuratorium-sicheres-oesterreich.at. Nach Abschluss der Bewertung werden die positiv beantworteten Anforderungen von einem unabhängigen Experten überprüft. Dieser Experte weiß nicht, welches Unternehmen bewertet wird.

Gibt es eine Frist, bis zu der eine Bewertung eingereicht werden muss?

Ja, nach der Einladung müssen Sie die Bewertung innerhalb von 14 Tagen abschließen. Wenn Sie mehr Zeit benötigen, um die Fragen zu beantworten, kontaktieren Sie bitte das CyberRisk-Service-Team unter cr@nimbusec.com

---

Ist es möglich, dass mehr als eine Person an der Bewertung arbeitet?

Jeder, der über ein Benutzerkonto mit Berechtigungen für das CyberRisk-Portal unter dem Firmenkonto verfügt, kann die Bewertung durchführen. Allerdings gilt nur die erste Person, die mit dem Ausfüllen der Bewertung beginnt, als Ansprechpartner für die Bewertung.

Müssen Sie die Bewertung auf einmal abschließen?

Nein. Es ist wichtig, gut auf die Antworten auf die Anforderungen vorbereitet zu sein oder sie gut zu überdenken.

Dies erleichtert und beschleunigt auch den Überprüfungsprozess. Je genauer eine erfüllte Anforderung beschrieben ist, desto weniger Fragen wird der Prüfer stellen müssen.

Die Anforderungen und Fragen für die Bewertung werden vom Kuratorium Sicheres Österreich (KSÖ) veröffentlicht und können dort heruntergeladen / eingesehen werden: CRR-Schema-Policy-2020

Erhalte ich meine Antworten, einschließlich einer Bewertung später?

Ja. Nach Abschluss der Bewertung müssen Sie einen Report herunterladen und aufbewahren, das aus den Details der Bewertung besteht. Der Report wird folgende Informationen enthalten:

- CyberRisk Rating-Zertifikat + Signatur
- Vollständige Details zur CyberRisk Rating-Bewertung, einschließlich der Antworten des Prüfers + Signatur.

- Details zur CyberRisk Rating-Bewertung ohne Antworten des Prüfers + Signatur

---

Wer bekommt sonst noch die Antworten?

Die Bewertung selbst kann von allen Kunden erworben werden. Es wird nur die Bewertungsnote angezeigt. Der Kunde kann jedoch die Details der Bewertung anfordern. Hier können Sie individuell entscheiden, ob die angeforderten Daten freigegeben werden oder nicht.

Müssen die Antworten für jeden Kunden bereitgestellt werden?

Nein. Sie müssen die Bewertung nur für die erste Anfrage eines Kunden und maximal einmal im Jahr abschließen.

Werden die Antworten vorübergehend gespeichert?

Sie können sich die Zeit nehmen, die Sie benötigen, um die Bewertung zu beantworten. Klicken Sie auf "Speichern und fortfahren", um die Antwort vorübergehend zu speichern. Sie können dann das Browserfenster schließen oder sich ausloggen und zu einem späteren Zeitpunkt fortfahren.

Wie wird die Vertraulichkeit meiner eigenen Informationen gewährleistet?

Die Vertraulichkeit wird dadurch sichergestellt, dass Nimbusec Ihre Daten niemals an Dritte weitergibt. Im Rahmen des Bewertungsprozesses sind alle beauftragten Datenverarbeiter zur Wahrung der Vertraulichkeit verpflichtet. Im Gegensatz zu üblichen Fragebögen erhalten Nimbusec-Kunden nur das CyberRisk Rating ohne weitere Details. Im Falle einer externen Prüfung oder einer Anfrage von unserem Kunden entscheiden Sie, ob Sie Ihre Daten an den Prüfer oder unseren Kunden weitergeben möchten. Wenn ja, liefert das CyberRisk Rating ein standardisiertes, maschinenlesbares Datenset, das effizient verarbeitet werden kann. Wenn nicht, können Sie auf das validierte CyberRisk Rating verweisen.

> **English version:**

> **Contact information for questions: KSV1870 Nimbusec GmbH | office@nimbusec.com | +43 (732) / 860 626 | Kaisergasse 16b, 4020 Linz**

Table of contents

- **What are the benefits for customers?**
- **What does the CyberRisk Rating by KSV1870 cost?**
- **Where can the CRR be used?**
- **Why am I receiving a request for a CyberRisk Rating?**
- **How does the CyberRisk Rating process work?**
- **Is there a deadline for submitting an assessment?**
- **Is it possible for more than one person to work on the assessment?**
- **Does the assessment need to be completed in one session?**
- **Will I receive my answers, including a rating, later?**
- **Who else gets the answers?**
- **Do the answers need to be provided for each customer?**
- **Are the answers temporarily stored?**
- **How is the confidentiality of my information ensured?**

What are the benefits for customers?

Users of the CyberRisk Rating by KSV1870 get a standardized process to assess all service providers, suppliers, and other third parties in terms of their cyber security. Rated companies receive an efficient, objective process that only needs to be conducted once a year to disclose their cyber risk to all interested customers. Through the published standard of the "Secure Austria Competence Center," rated companies can positively influence their cyber risk management. All companies receive a free guideline to reduce their own cyber risk in a targeted and structured way. This guideline is continuously maintained by Austria's most recognized experts and adapted to new technical requirements. The Austrian economy becomes more resilient by reducing the cyber risk of its supply chains, which forms the basis for the necessary digitization to maintain our international competitiveness.

What does the CyberRisk Rating by KSV1870 cost?

Companies being assessed do not incur any costs. Currently, the CyberRisk Rating is only offered for large companies and critical infrastructures. If you are interested in more information, we are happy to answer your questions.

Where can the CRR be used?

The CyberRisk Rating by KSV1870 is based on the requirements of the cyber risk scheme of the "Secure Austria Competence Center." These requirements were defined by leading cyber risk managers of Austrian companies from all areas of critical infrastructure, as well as representatives of the Federal Ministry of the Interior. The CyberRisk Rating can therefore be used in any industry and economic sector where an assessment of the cyber risk of companies - especially suppliers - is

required.

Primarily, operators of essential services according to § 11 Abs. 1 (2) in conjunction with Annex 1 NISV are legally obliged to take appropriate security measures when dealing with service providers, suppliers, and other third parties. The CyberRisk Rating by KSV1870 aims to fulfill this requirement (monitoring suppliers of an energy group or an airport), but it does not replace the necessary proof of an operator of essential services according to § 17 Abs. 3 NISG (= comprehensive audit of an operator of essential services, such as an energy group or an airport itself).

Why am I receiving a request for a CyberRisk Rating?

Cyber risks such as IT security, data protection, and business continuity are becoming increasingly important due to digitization. The CyberRisk Rating by KSV1870 offers a transparent, time-saving process to assess companies in these dimensions. This assessment is often required due to GDPR or the NIS Act.

As a rated company, you incur no costs and receive an objective view of your own cyber risk.

How does the CyberRisk Rating process work?

The assessment consists of an evaluation based on 25 requirements of the publicly accessible KSÖ Cyber Risk Scheme. Information about the KSÖ Cyber Risk Scheme can be found at https://www.kuratorium-sicheres-oesterreich.at. After the assessment, the positively answered requirements are reviewed by an independent expert. This expert does not know which company is being assessed.

Is there a deadline for submitting an assessment?

Yes, after the invitation, you must complete the assessment within 14 days. If you need more time to answer the questions, please contact the CyberRisk Service Team at cr@nimbusec.com.

Is it possible for more than one person to work on the assessment?

Anyone with a user account with permissions for the CyberRisk portal under the company account can perform the assessment. However, only the first person who starts filling out the assessment is considered the contact person for the assessment.

Does the assessment need to be completed in one session?

No. It is important to be well-prepared for the answers to the requirements or to think them through carefully.

This also facilitates and speeds up the review process. The more precisely a fulfilled requirement is described, the fewer questions the reviewer will need to ask.

The requirements and questions for the assessment are published by the Secure Austria Competence Center (KSÖ) and can be downloaded/viewed there: CRR-Schema-Policy-2020

Will I receive my answers, including a rating, later?

Yes. After completing the assessment, you must download and keep a report consisting of the details of the assessment. The report will contain the following information:

- CyberRisk Rating certificate + signature
- Full details of the CyberRisk Rating assessment, including the reviewer's answers + signature
- Details of the CyberRisk Rating assessment without the reviewer's answers + signature

---

Who else gets the answers?

The assessment itself can be purchased by all customers. Only the rating grade is displayed. However, the customer can request the details of the assessment. Here you can decide individually whether to release the requested data or not.

Do the answers need to be provided for each customer?

No. You only need to complete the assessment for the first request from a customer and at most once a year.

Are the answers temporarily stored?

You can take the time you need to answer the assessment. Click "Save and continue" to temporarily save the answer. You can then close the browser window or log out and continue at a later time.

How is the confidentiality of my information ensured?

Confidentiality is ensured by Nimbusec never sharing your data with third parties. In the course of the assessment process, all commissioned data processors are obligated to maintain confidentiality. Unlike usual questionnaires, Nimbusec customers only receive the CyberRisk Rating without further details. In the case of an external review or a request from our customer, you decide whether to share your data with the reviewer or our customer. If so, the CyberRisk Rating provides a standardized, machine-readable data set that can be processed efficiently. If not, you can refer to the validated CyberRisk Rating.

Überprüfung der PDF-Integrität | Verification of PDF Integrity

> ***English version down below***

Inhaltsverzeichnis

- **Integritätsprüfung über die Befehlszeile**
- **CyberRisk Rating Signature Public Key**

Das Cyber Risk Rating Portal stellt am Ende des Bewertungsprozesses für jeden Lieferanten mehrere Dokumente aus. Dazu gehören unter anderem das Cyber Risk Rating-Zertifikat, das die Gesamtbewertungspunkte für den Lieferanten sowie den WebRisk-Score enthält, und der Cyber Risk Rating-Report, der die Antworten des Lieferanten zusammen mit den Validierungsergebnissen auflistet.

Um die Integrität der Dokumente zu gewährleisten und potenzielle Kompromisse durch Dritte während des Downloadvorgangs zu verhindern, wird für jedes Dokument eine Signatur hinzugefügt, die den signierten Digest pro Dokument enthält. Durch die Signatur des Digests wird die Integrität des Dokuments garantiert, da eine Änderung des Dokumenteninhalts zwangsläufig einen anderen Digest erzeugen würde, der nicht mit der bereitgestellten Signatur übereinstimmt. Darüber hinaus kann die Signatur nicht verändert werden, da sie mit unserem eigenen geheimen RSA Private Key signiert wurde. Die für den Prozess verwendeten Algorithmen sind SHA256 zur Erstellung des Digests des Dokuments und RSA PKCS#1 v1.5 für die Signatur.

Integrität über die Befehlszeile verifizieren

Es wird empfohlen, die Integrität jedes Dokuments nach dem Herunterladen als ZIP-Archiv zu überprüfen. Für jedes Dokument repräsentiert die entsprechende Signaturdatei `.sig` den signierten Digest in Byte-Form. Darüber hinaus wird der Public Key benötigt, der auf unserer Seite verwendet wurde. Er kann hier heruntergeladen werden: Cyber Risk Rating Signature Public Key

Die Überprüfung kann mit OpenSSL Version `v1.1.1f` oder höher durchgeführt werden.

```
$ openssl dgst -sha256 -verify crr-signature-key.pub -signature CyberRisk-Rating-Report-
Valid.pdf.sha256.sig CyberRisk-Rating-Report-Valid.pdf
Verified OK
```

Wenn die Dokumente kompromittiert sind, schlägt die Überprüfung fehl. In diesem Fall kontaktieren Sie sofort support@nimbusec.com für weitere Unterstützung.

```
$ openssl dgst -sha256 -verify crr-signature-key.pub -signature CyberRisk-Rating-Report-
Valid.pdf.sha256.sig CyberRisk-Rating-Report-Compromised.pdf
Verification Failure
```

CyberRisk Rating Signature Public Key

Sie können den Signaturschlüssel als Datei hier herunterladen: Cyber Risk Rating Signature Public Key

Oder Sie verwenden die untenstehende Klartextversion:

```
-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAwGd+TC2FkOrz/CqU9lUk
xNi8uhQ73D9YVlQ93Jkl4plVRYcquGOK0hLqWSTDkHAfd9fKCqgmJWF1X6eF/fz7
B6a7HeCHAPlut3aclEneJef03JWsLZWoMD724v7vDXHolUcDNHuICWQpWMpZ/xaM
E1FzNlzqSH41tF3YPOaxGiQA39+POxaWItYk7hBKBWhU6F4PBzZfM2gE/3AOqcRi
4DRFYPh3ZwIVTGqDtfiYMWUYLDI5u0KzdFne6qvBHflBwB1Nd9l3ckEFiv91s2Sg
3AaiXEqgSvLIL02tbmVnbfImVXksE9VeNWpr0LKWnTApheX++DQ0itB7zbg9JIfv
rEG9JNuP/dXlFjYRsBlsaz950vulzwwWjeHs6LikqHUz+4xy8+GU6vs0QFbvkHlD
DRcJGeCWsCiijh9dtM+yDcZfr8WjEr9AQfskMSfoWuVqAMBqJ05C51fDnZdbNLGy
0ubtIoI4cSIf7Rrow1iq8l4WsPoIZDRq2S0jJc3gLnAS6erlQoox/9A2ZWeCQPw9
iHixIVpQR/h6TKT6M4VQn+Ilw+Nj5o6yTzYEhq5nY64yH9zn0brhycANLhO/PnA1
rYaCorVRMFbr9UeysulqKBEk4TkEAWdUXdqSzM/Wdm2P0pQM7Y0vhMbqMSeYoGkX
o2lNrkxDioheGnwTsaFejtMCAwEAAQ==
-----END PUBLIC KEY-----
```

> **English version:**

Table of contents

- **Integrity check via command line**
- **CyberRisk Rating Signature Public Key**

The Cyber Risk Rating Portal issues several documents for each supplier at the end of the evaluation process. These include the Cyber Risk Rating Certificate, which contains the overall rating points for the supplier as well as the WebRisk score, and the Cyber Risk Rating Report, which lists the supplier's responses along with the validation results.

To ensure the integrity of the documents and prevent potential compromises by third parties during the download process, a signature containing the signed digest for each document is added. By signing the digest, the integrity of the document is guaranteed, as any alteration of the document's content would inevitably generate a different digest that would not match the provided signature. Furthermore, the signature cannot be altered because it is signed with our own secret RSA private key. The algorithms used for this process are SHA256 for creating the document digest and RSA PKCS#1 v1.5 for the signature.

Integrity check via command line

It is recommended to verify the integrity of each document after downloading as a ZIP archive. For each document, the corresponding signature file `.sig` represents the signed digest in byte form.

Additionally, the public key used on our side is required. It can be downloaded here: Cyber Risk Rating Signature Public Key

The verification can be performed using OpenSSL version `v1.1.1f` or higher.

```
$ openssl dgst -sha256 -verify crr-signature-key.pub -signature CyberRisk-Rating-Report-
Valid.pdf.sha256.sig CyberRisk-Rating-Report-Valid.pdf
Verified OK
```

If the documents are compromised, the verification will fail. In this case, please contact support@nimbusec.com immediately for further assistance.

```
$ openssl dgst -sha256 -verify crr-signature-key.pub -signature CyberRisk-Rating-Report-
Valid.pdf.sha256.sig CyberRisk-Rating-Report-Compromised.pdf
Verification Failure
```

CyberRisk Rating Signature Public Key

You can download the signature key file here: Cyber Risk Rating Signature Public Key

Or, you can use the plaintext version provided below:

```
-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAwGd+TC2FkOrz/CqU9lUk
xNi8uhQ73D9YVlQ93Jkl4plVRYcquGOK0hLqWSTDkHAfd9fKCqgmJWF1X6eF/fz7
B6a7HeCHAPlut3aclEneJef03JWsLZWoMD724v7vDXHolUcDNHuICWQpWMpZ/xaM
E1FzNlzqSH41tF3YPOaxGiQA39+POxaWItYk7hBKBWhU6F4PBzZfM2gE/3AOqcRi
4DRFYPh3ZwIVTGqDtfiYMWUYLDI5u0KzdFne6qvBHflBwB1Nd9l3ckEFiv91s2Sg
3AaiXEqgSvLIL02tbmVnbfImVXksE9VeNWpr0LKWnTApheX++DQ0itB7zbg9JIfv
rEG9JNuP/dXlFjYRsBlsaz950vulzwwWjeHs6LikqHUz+4xy8+GU6vs0QFbvkHlD
DRcJGeCWsCiijh9dtM+yDcZfr8WjEr9AQfskMSfoWuVqAMBqJ05C51fDnZdbNLGy
0ubtIoI4cSIf7Rrow1iq8l4WsPoIZDRq2S0jJc3gLnAS6erlQoox/9A2ZWeCQPw9
iHixIVpQR/h6TKT6M4VQn+Ilw+Nj5o6yTzYEhq5nY64yH9zn0brhycANLhO/PnA1
rYaCorVRMFbr9UeysulqKBEk4TkEAWdUXdqSzM/Wdm2P0pQM7Y0vhMbqMSeYoGkX
o2lNrkxDioheGnwTsaFejtMCAwEAAQ==
-----END PUBLIC KEY-----
```