

5 vor DORA:

Warum Lieferketten die größte Herausforderung sind und was wir für NIS2 daraus lernen

Mag. Alexander Mitter, Geschäftsführer KSV1870 Nimbusec GmbH

schafft **Wissen**
sichert **Werte**

Was erwartet Sie?

- KSÖ / KSV1870
- Status Quo: Cybersicherheit in Österreich
- DORA Start am 17. Jänner 2025 als Leuchtturmprojekt für NIS2
- Was kann ich heute tun?

Seit 1870 ein verlässlicher Partner

>33.000

Mitglieder

>45.000

Kunden

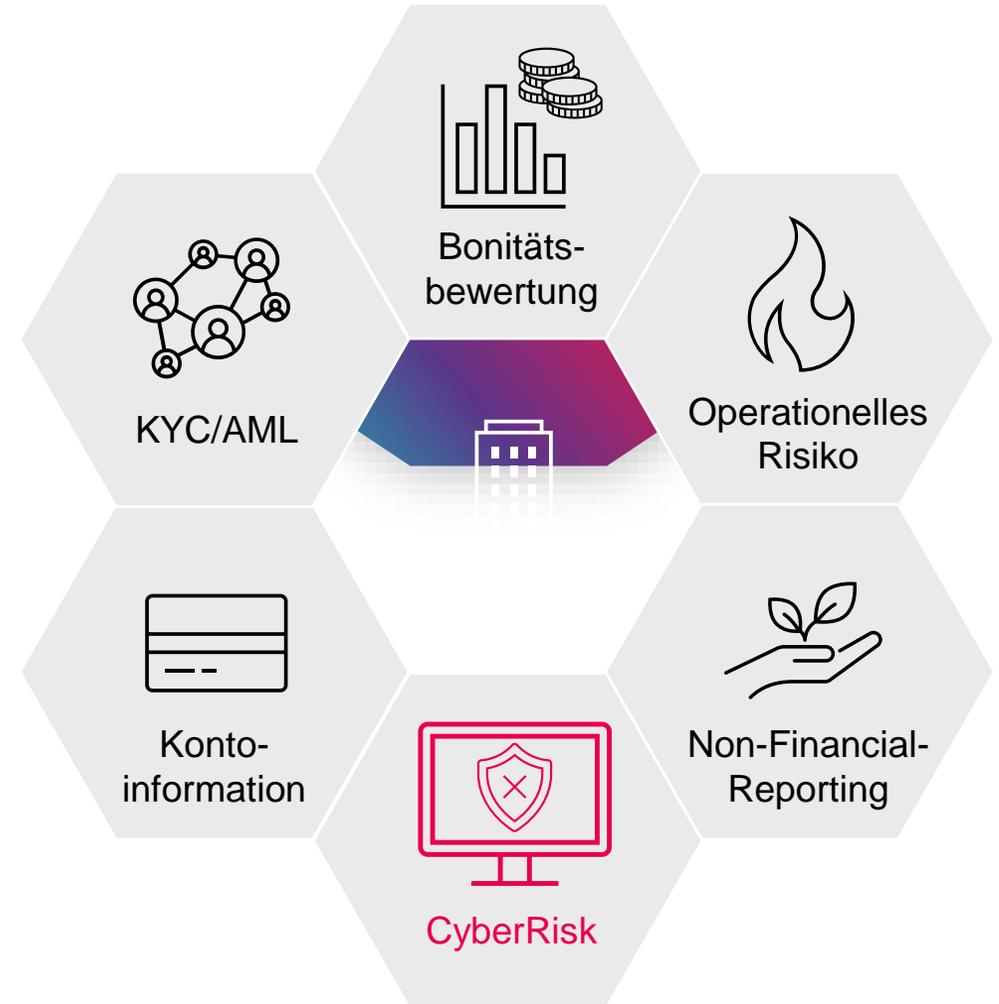
6

Gesellschaften

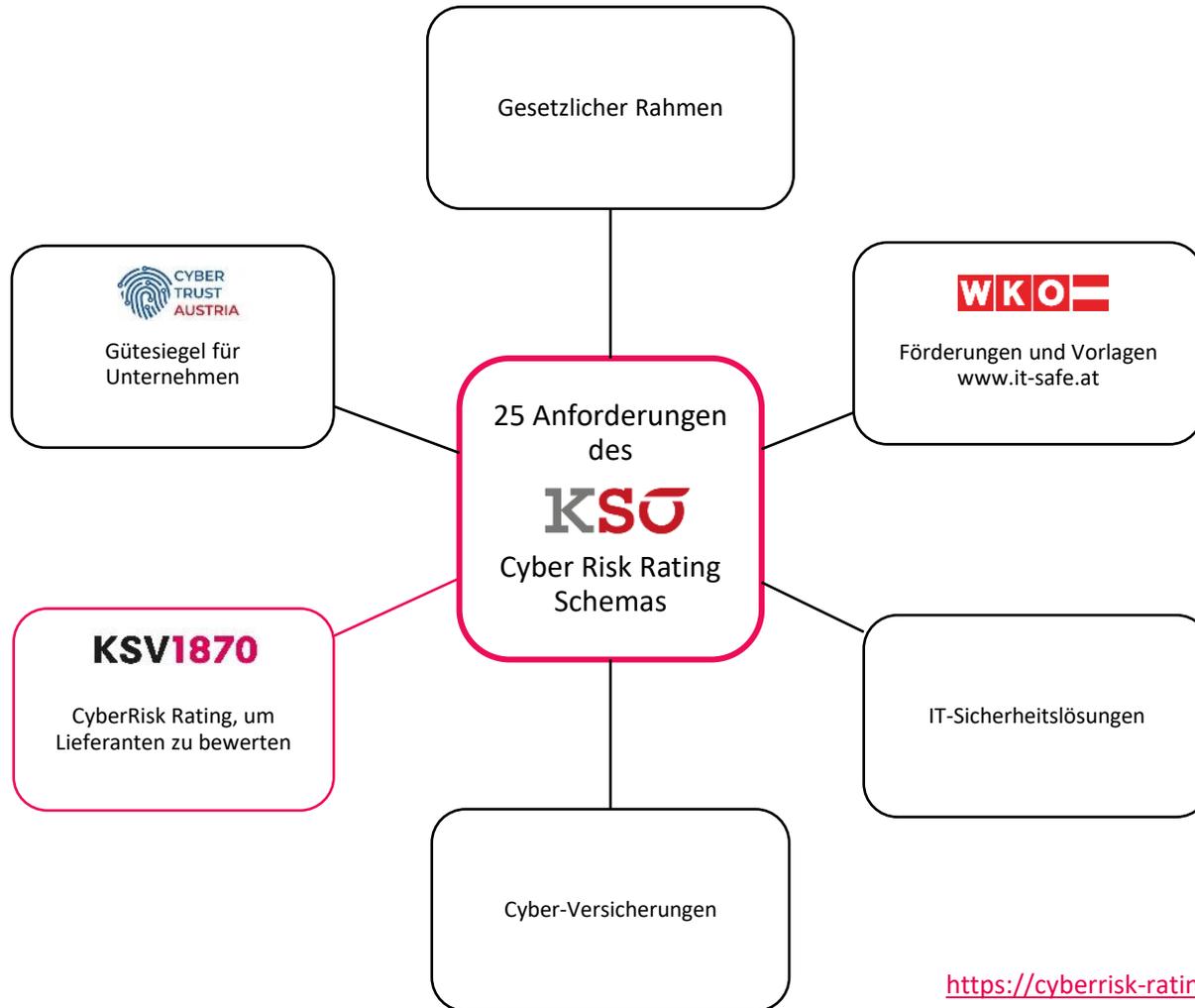
1

Ziel

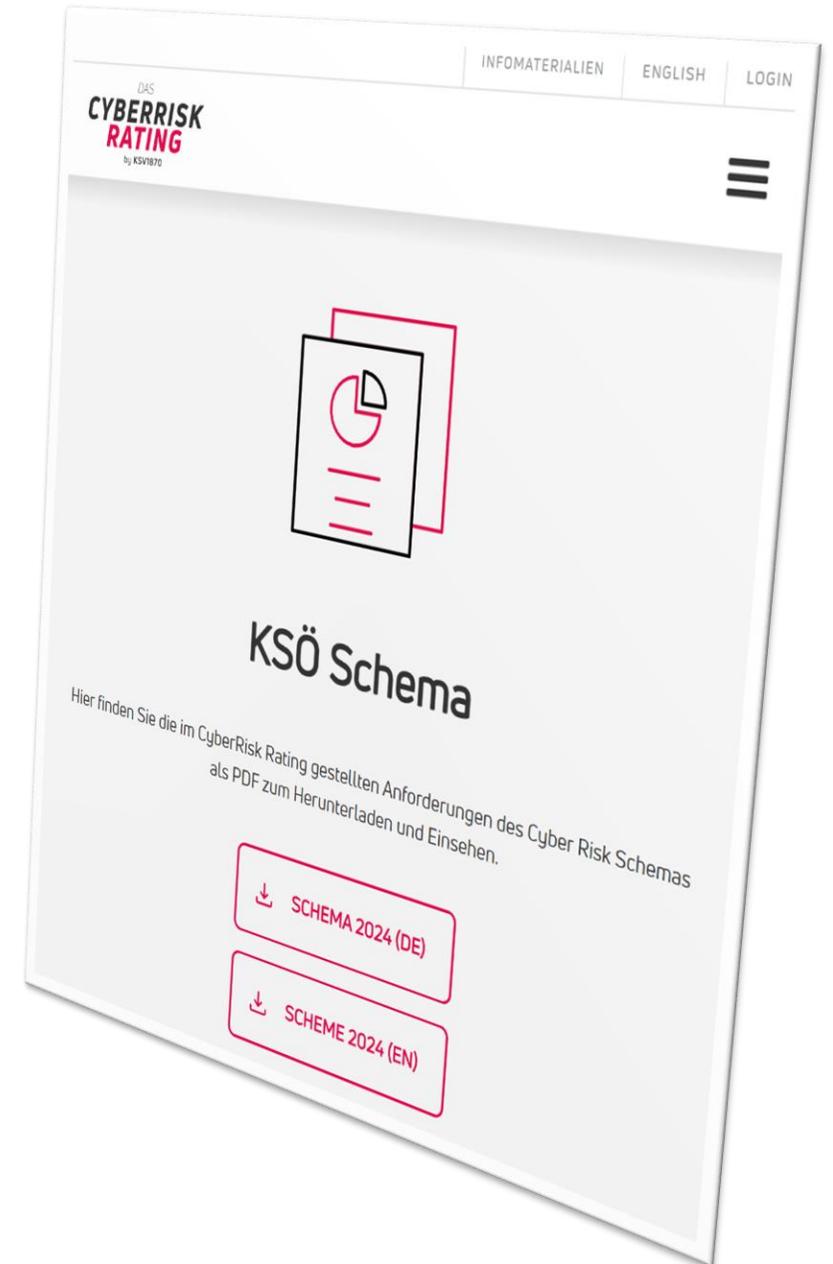
schafft **Wissen** – sichert **Werte**



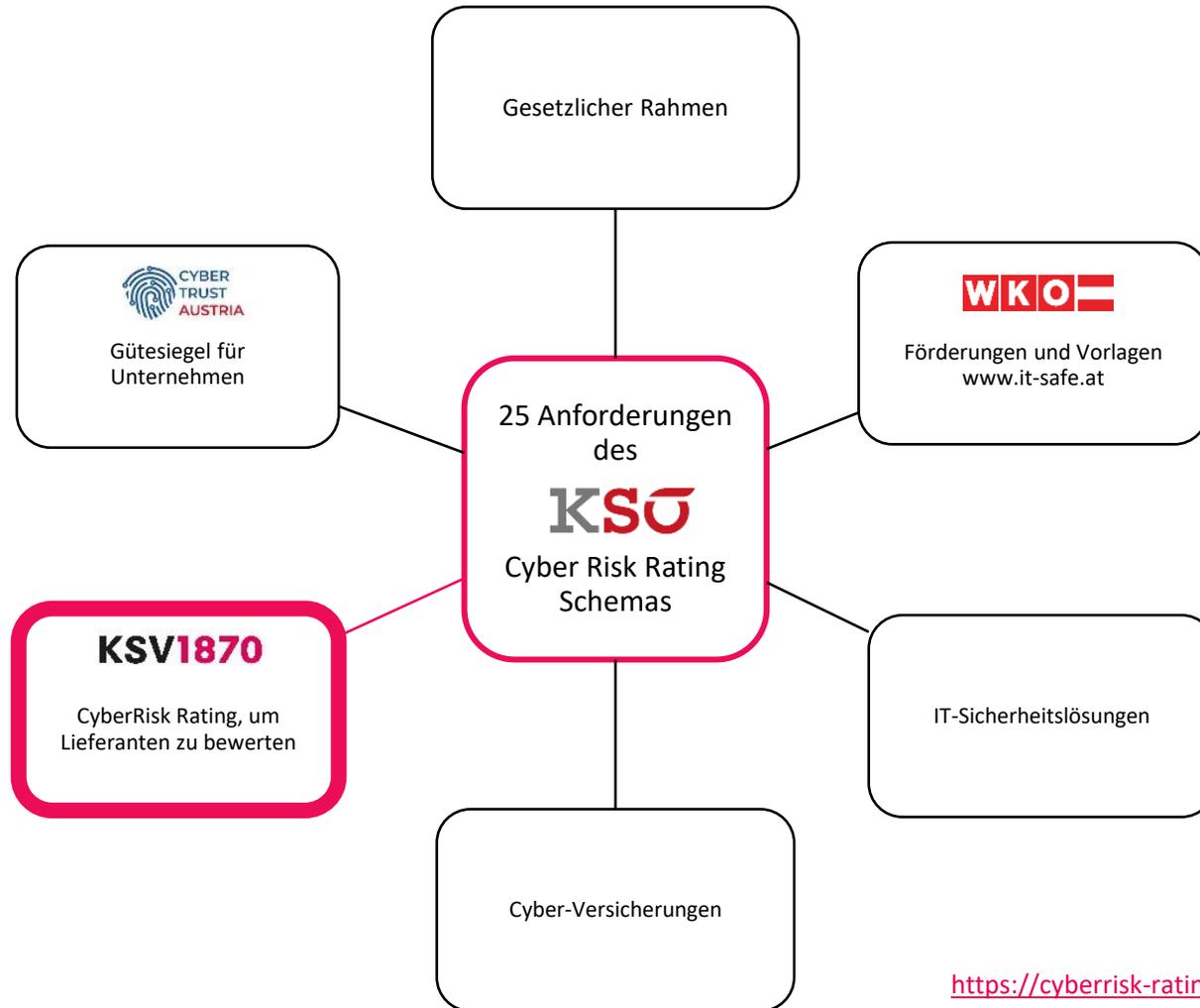
Das CyberRisk Rating Ökosystem



<https://cyberrisk-rating.at/schema.html>



Das CyberRisk Rating Ökosystem



DAS CYBERRISK RATING by KSV1870

CYBERRISK MANAGER
Alle Ratings auf einen Blick.

Dashboard navigation: Dashboard, LIEFERANTENMANAGEMENT, CyberRisk Manager, Datenschutz Manager, Risikominimierung, IHR ACCOUNT, Assessments, Ihre Ratings, Account Verwalten.

Key actions: RATINGS ANFORDERN, IHR CYBERRISK RATING.

CyberRisk Ratings Ihrer Lieferanten

Risiko	Unternehmen	WebRisk	B-Rating	A-Rating	verfügbar bis	DORA	Aktionen
▲	AI Telekom Austria	199	128 B	141 A	20. Januar 2025	DORA	⋮
▲	SAP Österreich GmbH	150	100 B	100 A	25. März 2025	DORA	⋮
▲	FACC Operations GmbH	145	128 B	116 A+	08. Juni 2024	DORA	⋮
▲	Siemens Aktiengesellschaft	200	100 B	125 A	09. März 2025	DORA	⋮
▲	Die Presse Verlags...	125	128 B	183 A+	14. September 2024	DORA	⋮
	KSV1870 Nimbusec GmbH						

Footer: IN FREUNDLICHER KOOPERATION MIT nimbusec & KSV

<https://cyberrisk-rating.at/schema.html>

Status Quo: Cybersicherheit in Österreich

Umfang

21.707

(internationale) Lieferanten sind in der KSV1870 CyberRisk Rating Datenbank enthalten.

Es ist bereits heute Österreichs größte Datenbank für IT-Sicherheitsnachweise.



Wir wiegen uns in falscher Sicherheit.

87,1%

der bewerteten Lieferanten überschätzen die eigene Cybersicherheit.



Kunden erwarten von Lieferanten mehr, als aktuell möglich.

1 von 3

bewerteten Lieferanten kann das vom Kunden geforderte erhöhte Sicherheitsniveau nicht erreichen.



Cybersicherheitsmaßnahmen werden oft mangelhaft kommuniziert.

70%

der Angaben mussten rückgefragt werden, da die initiale Antwort nicht schlüssig oder detailliert genug war.



Gehackte Systeme werden nicht erkannt.

90%

der gehackten Webseiten von Unternehmen waren nach einem Monat noch nicht bereinigt und stellen ein aktives Sicherheitsrisiko dar.



IT-Sicherheit ist zu langsam.

14,7
Tage

benötigten Unternehmen durchschnittlich, um auf Rückfragen zur IT-Sicherheit zu antworten.



CYBERRISK **RATING**

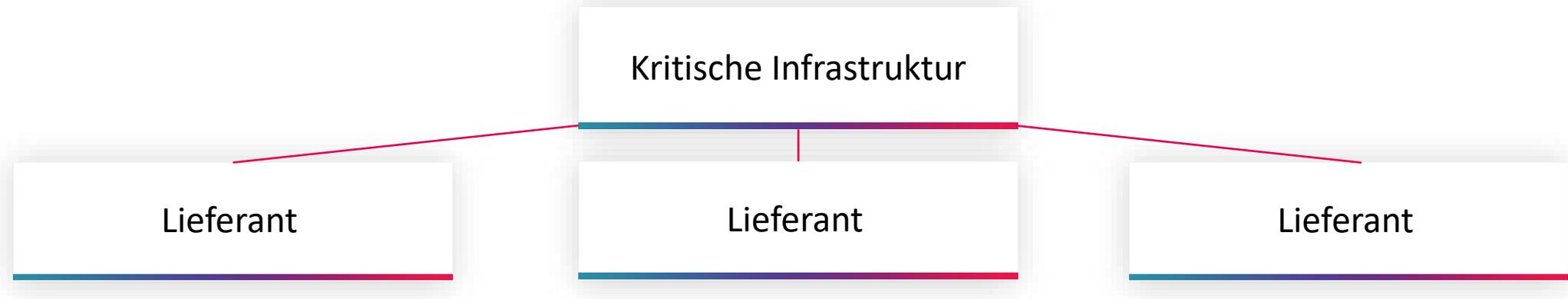
by KSV1870

DORA Start am
17. Jänner 2025 als
Leuchtturmprojekt für
NIS2



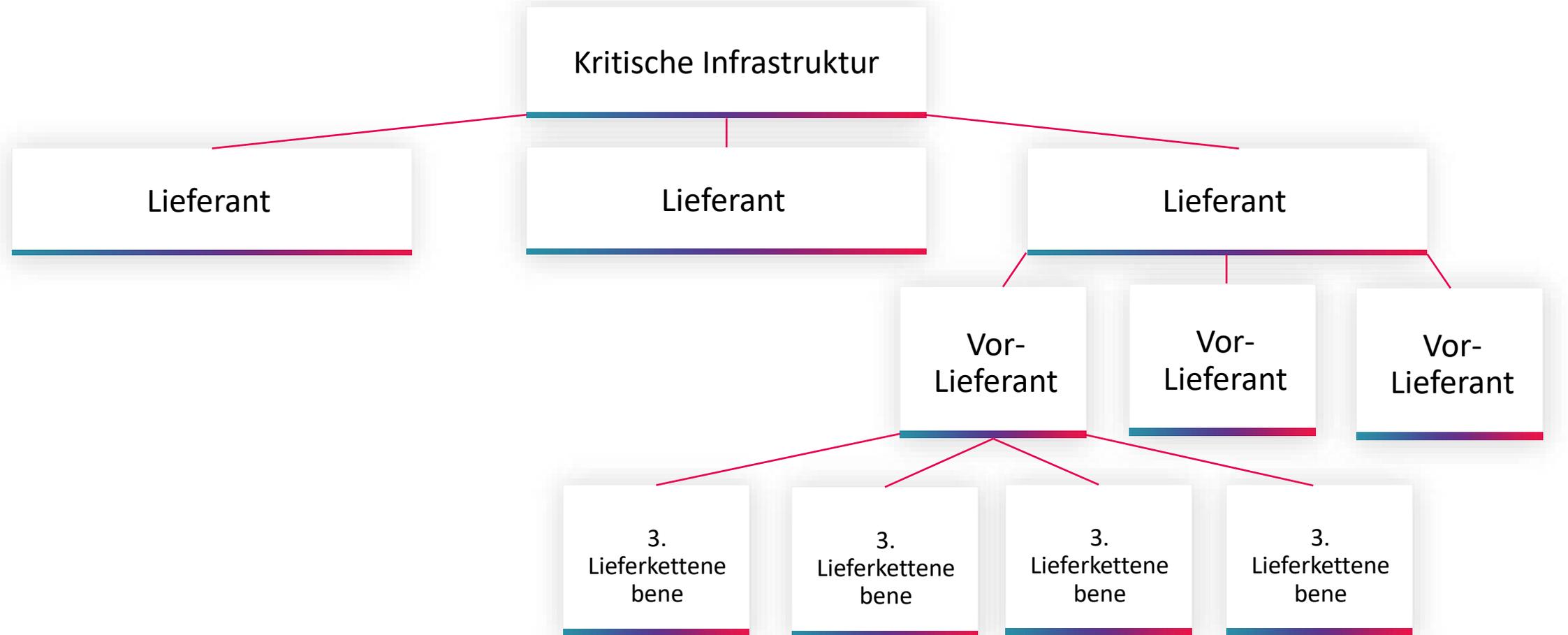
Lieferketten-Baum – NIS2

Auslagerung von IT-Risiken an Lieferanten enthebt nicht von NIS2.



Lieferketten-Baum – DORA (Finanzbranche)

DORA fordert Transparenz bis zum letzten Sub-Lieferanten um Cluster-Risiken transparent zu machen.



DORA – Register of Information – Dry Run

eba European Banking Authority

Extranet | Log in

ABOUT US | ACTIVITIES | RISK AND DATA ANALYSIS | PUBLICATIONS AND MEDIA

Search...

Preparation for DORA application

The Digital Operational Resilience Act (DORA) will become applicable on 17 January 2025. From that date all financial entities in its scope will need to have a comprehensive register of their contractual arrangements with ICT third-party service providers available at entity, sub-consolidated and consolidated levels.

The registers will serve for:

- financial entities to monitor their ICT third-party risk,
- the EU competent authorities to supervise ICT and third-party risk management at the financial entities and
- the ESAs to designate the critical ICT third-party service providers (CTPP) which will be subject to an EU-level oversight.

To help financial entities be ready with the preparation and submission of their registers of information from January 2025, the ESAs and competent authorities will carry out a dry run exercise on a best-efforts basis in 2024.

Timeline and milestones

Introductory workshop for the industry
April 24

Registers of information collected
August 24
from participating FEs through their competent authorities (which may set specific deadlines within this window)

ESAs' 'lessons learnt' workshop on data quality open to the entire industry
November 24

ESAs' workshops with participating FEs and competent authorities
June 24
including FAQs and support

End of the data cleaning and quality checks
October 24
feedback and cleaned files provided to the participating FEs via their competent authorities

Public aggregated data quality report
December 2024

623

eba European Banking Authority | eopa European Supervisory Authority | ESMA European Supervisory Authority

1

2 **TEMPLATE RT.05.02: ICT service supply chains**

3

4 b_05.02.0010	b_05.02.0020	b_05.02.0030	b_05.02.0040	b_05.02.0050	b_05.02.0060	b_05.02.0070
Contractual arrangement reference number	Type of ICT services	Identification code of the ICT third-party service provider	Type of code to identify the ICT third-party service provider	Rank	Identification code of the recipient of sub-contracted ICT services	Type of code to identify the recipient of sub-contracted ICT services
5	6	6	6	6	6	6
7 Alphanumerical	Closed set of options	Alphanumerical	Pattern	Natural number	Alphanumerical	Pattern
7 XXX1	eba_IA:504	MMNZEH82I26030ED3198	LEI		1 254900M35PF1CW97E173	LEI
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						

Wie erheben wir die DORA Daten bis 17. Jänner 2025?

Aktueller Status: Mehr als 20.000 (IT-)Lieferanten hinterlegt.

1. Teilnehmende Finanzunternehmen konnten bis zum **13. September 2024** angeben, welche Lieferanten aus Ihrer Sicht relevant sind.
2. KSV1870 kontaktiert koordiniert seit **16. September 2024** ALLE genannten Lieferanten und teilt Ihnen mit, welche Kunden DORA Daten benötigen.
3. **Follow-Ups bis 17. Jänner 2025:** DORA-Datensatz ist erst dann komplett, wenn Lieferant bestätigt, dass **ALLE Sub-Lieferanten auch gemeldet haben**.

The screenshot displays the 'DORA EXPLORER' web application interface. On the left is a dark sidebar with the logo 'DAS CYBERRISK RATING by KSV1870' and a navigation menu including 'Dashboard', 'LIEFERANTENMANAGEMENT' (with sub-items: 'CyberRisk Manager', 'Datenschutz Manager', 'Risikominimierung', and 'DORA Explorer'), and 'IHR ACCOUNT' (with sub-items: 'Assessments', 'Meine Ratings', 'Account verwalten'). At the bottom of the sidebar, it says 'IN KOOPERATION MIT nimbusec und KSV'. The main content area shows the breadcrumb 'Dashboard > DORA Explorer > WebApp' and user options for 'Sprache', 'Support', 'Mittellungen', and 'Benutzer'. Below this is the title 'DORA EXPLORER' and an introductory paragraph about the DORA regulation. A 'WebApp' status indicator shows 'STATUS: Lieferkette in Bearbeitung'. A red button labeled '← ZURÜCK ZUR SERVICE-ANSICHT' is visible. The central part of the screen features a supply chain diagram with three levels: 'Level 1 Lieferanten' (three 'KSV1870 Nimbusec GmbH' nodes), 'Level 2 Lieferanten' ('XYZ Unternehmen GmbH' and 'Infrastruktur Provider GmbH'), and 'Level 3 Lieferanten' ('ABC Unternehmen' and 'Rechenzentrum Betreiber GmbH'). Each node includes a 'Sicherheitsüberprüfung' status indicator and a 'Lieferanten ID' field. At the bottom, there are links for 'Datenschutzerklärung', 'Impressum', and 'Nutzungsbedingungen'.

Wie erheben wir die DORA Daten bis 17. Jänner 2025?

Was erheben wir genau?

1. Allgemeine Firmendaten
2. Information zu übergeordneter Konzernmutter

DORA MODULE

With DORA, Regulation (EU) 2022/2554 on digital operational resilience in the financial sector (Digital Operational Resilience Act), the European Union has created a financial sector-wide regulation for cybersecurity, ICT risks and digital operational resilience. One requirement of DORA is to fully document IT supply chains down to the last link. The DORA Module takes care of this data collection for you.

[Company Data](#) [Inquiries](#)

05.01.0030
Your company name

KSV1870 Nimbusec GmbH

05.01.0050
In which country is your head office located?

AUSTRIA

E-mail address of your contact person for DORA inquiries

office@nimbusec.com

05.01.0040
What type of provider are you?

Legal person, excluding individual acting in a business capacity Individual acting in a business capacity

05.01.0010 / 05.01.0020
Please provide your company identification.

LEI **Company register number** **VAT**

m23142323 ATU67830957

[+ ADD PARENT COMPANY](#)

! Information regarding the parent company must be stated in accordance with DORA regulations.

Wie erheben wir die DORA Daten bis 17. Jänner 2025?

Was erheben wir genau?

1. Allgemeine Firmendaten
2. Information zu übergeordneter Konzernmutter
3. Informationen zu allen Services und Produkten, die von unseren Projektpartnern angefragt wurden.
4. Informationen zu allen daran beteiligten Sub-Lieferanten.

DORA inquiry from **Nimbusec Test GmbH**

2 / 2 – ICT Services

Please provide information on the following services

ICT services in use

#	ICT Service	Direct ICT TPPs	Status
1	Infrastructure	1	STATUS: created

05.02.0020
Name
Infrastructure
My company does not provide this service.

Type of Service
S14. ICT operation management(including m

02.02.0130
Country of provision of the ICT service
Austria

02.02.0140
Does this service store data?
 Yes No

02.02.0150
Storage location of the data
Austria

02.02.0160
Location of data management
Austria

05.02
Indirect ICT Third-Party Providers for this Service

! For the purposes of the DORA, you are required to identify all ICT TPPs that support your organization in the provision of this service, including their contact email address.

Add a new provider

+ ADD ICT THIRD-PARTY PROVIDER

#	Company Name	Contact e-mail address	Reference	Action
1	NextLayer GmbH	office@nextlayer.at	KSV1870 Nimbusec Infrastructure	

✓ CLOSE

Wie erheben wir die DORA Daten bis 17. Jänner 2025?

Was erheben wir genau?

1. Allgemeine Firmendaten
2. Information zu übergeordneter Konzernmutter
3. Informationen zu allen Services und Produkten, die von unseren Projektpartnern angefragt wurden.
4. Informationen zu allen daran beteiligten Sub-Lieferanten.
5. Wenn Sub-Lieferanten beteiligt sind, springt das DORA-Modul weiter und wiederholt die Datenerhebung eine Ebene tiefer.

DORA inquiry from **Nimbusec Test GmbH**

2 / 2 – ICT Services

Please provide information on the following services

ICT services in use

#	ICT Service	Direct ICT TPPs	Status
1	Infrastructure	1	STATUS: created

05.02.0020
Name
Infrastructure
My company does not provide this service.

Type of Service
S14. ICT operation management(including m

02.02.0130
Country of provision of the ICT service
Austria

02.02.0140
Does this service store data?
 Yes No

02.02.0150
Storage location of the data
Austria

02.02.0160
Location of data management
Austria

05.02
Indirect ICT Third-Party Providers for this Service

! For the purposes of the DORA, you are required to identify all ICT TPPs that support your organization in the provision of this service, including their contact email address.

Add a new provider

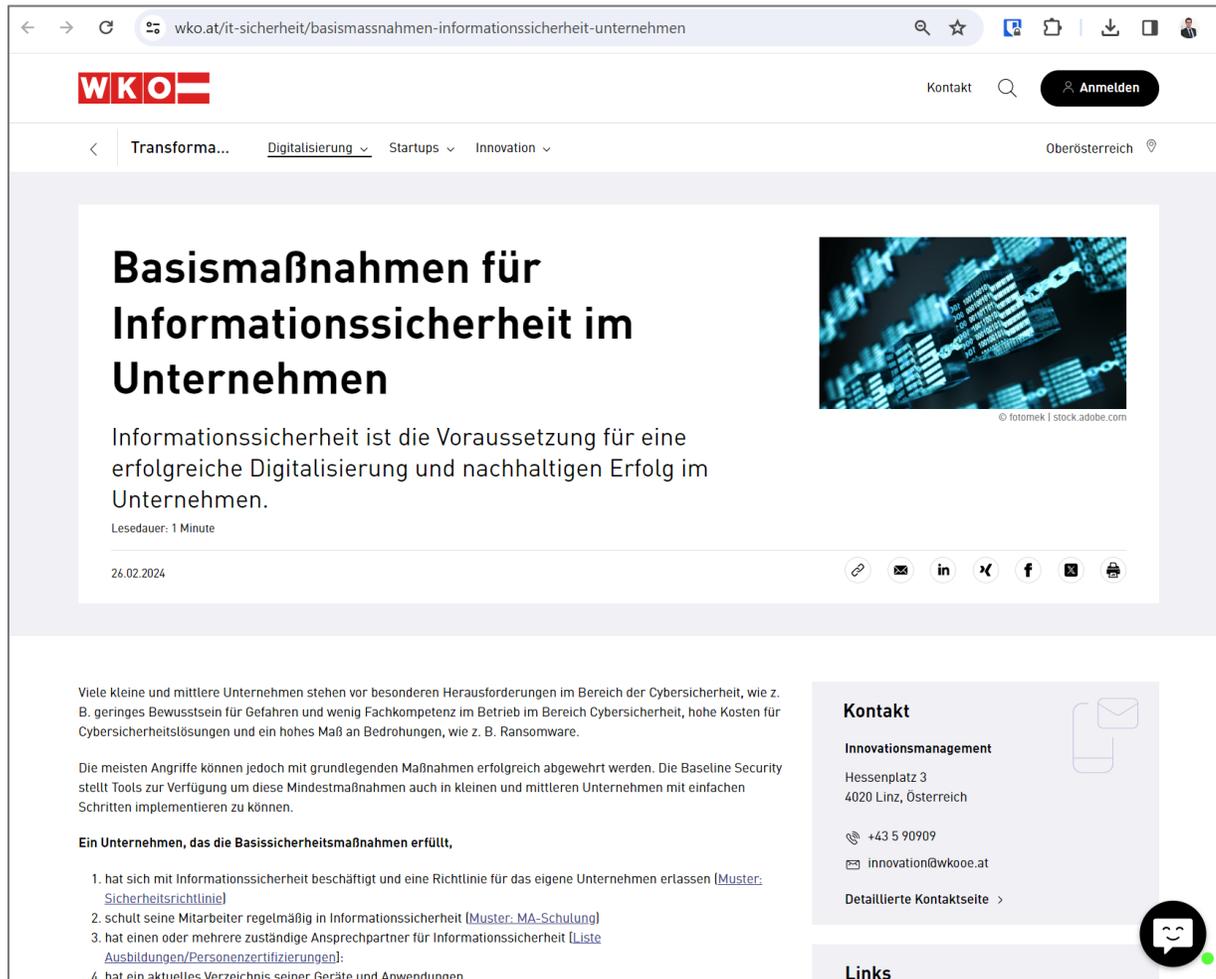
+ ADD ICT THIRD-PARTY PROVIDER

#	Company Name	Contact e-mail address	Reference	Action
1	NextLayer GmbH	office@nextlayer.at	KSV1870 Nimbusec Infrastructure	

✓ CLOSE

Was kann ich heute tun?

WKO unterstützt mit kostenlosen Vorlagen



The screenshot shows a webpage from wko.at with the following content:

- Header:** WKO logo, navigation menu (Transforma..., Digitalisierung, Startups, Innovation), and a location indicator for Oberösterreich.
- Main Content:**
 - ## Basismaßnahmen für Informationssicherheit im Unternehmen
 - Informationssicherheit ist die Voraussetzung für eine erfolgreiche Digitalisierung und nachhaltigen Erfolg im Unternehmen.
 - Lesedauer: 1 Minute
 - 26.02.2024
 - © fotomek | stock.adobe.com
 - Social sharing icons: link, email, LinkedIn, Facebook, Twitter, YouTube, Print.
- Text Content:**

Viele kleine und mittlere Unternehmen stehen vor besonderen Herausforderungen im Bereich der Cybersicherheit, wie z. B. geringes Bewusstsein für Gefahren und wenig Fachkompetenz im Betrieb im Bereich Cybersicherheit, hohe Kosten für Cybersicherheitslösungen und ein hohes Maß an Bedrohungen, wie z. B. Ransomware.

Die meisten Angriffe können jedoch mit grundlegenden Maßnahmen erfolgreich abgewehrt werden. Die Baseline Security stellt Tools zur Verfügung um diese Mindestmaßnahmen auch in kleinen und mittleren Unternehmen mit einfachen Schritten implementieren zu können.
- Ein Unternehmen, das die Basissicherheitsmaßnahmen erfüllt,**
 1. hat sich mit Informationssicherheit beschäftigt und eine Richtlinie für das eigene Unternehmen erlassen ([Muster-Sicherheitsrichtlinie](#))
 2. schult seine Mitarbeiter regelmäßig in Informationssicherheit ([Muster-MA-Schulung](#))
 3. hat einen oder mehrere zuständige Ansprechpartner für Informationssicherheit ([Liste Ausbildungen/Personenzertifizierungen](#)):
 4. hat ein aktuelles Verzeichnis seiner Geräte und Anwendungen
- Contact Sidebar:**
 - Kontakt**
 - Innovationsmanagement**
 - Hessenplatz 3
4020 Linz, Österreich
 - +43 5 90909
 - innovation@wko.at
 - [Detaillierte Kontaktseite >](#)
- Links**
- Footer:** WhatsApp chat icon.

Vorlagen für

- Sicherheitsrichtlinie
- Mitarbeiterschulung
- Ausbildungsliste
- Datenzugriffskonzept
- Schutz der Unternehmenswebseite
- Notfallplan

WKO und Bundesministerium Arbeit und Wirtschaft unterstützt mit Förderung

KMU.DIGITAL

Startseite KMU.DIGITAL KMU.DIGITAL & GREEN Services Infos für Berater:innen Über KMU.DIGITAL

Mit dem Förderungsprogramm KMU.DIGITAL soll das große Potenzial an Chancen, das die Digitalisierung den österreichischen kleinen und mittleren Unternehmen (KMU) eröffnet, von diesen genutzt werden können. Im Zusammenhang mit der zunehmenden Automatisierung und Digitalisierung sämtlicher Dienstleistungs- und Produktionsbereiche steigen auch die Herausforderungen für österreichische KMU. Daher wird mit dem Förderungsprogramm „KMU.DIGITAL“ ein Anreiz für KMU geschaffen, Digitalisierungsprojekte zu konzipieren, umzusetzen und in den Markt überzuführen. Die Förderung soll zusätzlich dazu beitragen, die österreichische Wirtschaft in den nächsten Jahren bei der Transformation zu einer nachhaltigen, auf erneuerbaren Energien basierenden und digitalisierten Wirtschaft zu unterstützen.

KMU.DIGITAL fördert im Modul Beratung die individuelle Beratung österreichischer KMU durch zertifizierte Berater:innen zu den 4 Themen Geschäftsmodelle und Prozesse (inkl. Ressourcenoptimierung), E-Commerce und Online-Marketing, IT- und Cybersecurity sowie Digitale Verwaltung. Dafür stehen jeweils geförderte Status- und Potenzialanalysen bzw. Strategieberatungen zur Verfügung. Die Gesamtförderung für eine Kombination mehrerer Beratungs-Tools beträgt maximal 3.000 Euro pro Unternehmen.

Online unter
<https://kmudigital.at>

Welche Digitalisierungsförderung brauchen Sie?

Status & Potenzialanalyse



© WKO

Förderung von Digitalisierungsprojekten – 80 %
Zuschuss (max. 400 Euro pro Tool)

Strategieberatung



© WKO

Förderung von Digitalisierungsprojekten – 50 %
Zuschuss (max. 1.000 € pro Tool)

Umsetzungsförderung



© WKO

Förderung von Digitalisierungsprojekten – 30 %
Zuschuss (max. 6.000 Euro)



Nationalen Koordinierungszentrum für Cybersicherheit (NCC-AT) unterstützt mit Förderung

The screenshot shows the top navigation bar of the FFG website. On the left is the FFG logo (Forschung wirkt.) with links for 'Förderungen', 'Beratung und Service', and 'Die FFG'. In the center is a search bar containing 'eCall Projektverwaltung'. Below the navigation bar is a red search bar with the text 'Förderungen suchen.' and two dropdown menus for '- Thema -' and '- Zielgruppe -'. To the right of the search bar are two buttons: 'Aktuelle Ausschreibungen' and 'Förderungen und Services'. Below the search bar are two radio buttons: 'nationale Förderung' (selected) and 'internationale Förderung'.

Online unter

<https://www.ffg.at/ausschreibung/cybersecuritychecks2024>

Cyber Security Checks 2024

Förderung von Cyber Security Maßnahmen

Ausschreibung offen von **02.09.2024 09:00** bis **29.11.2024 12:00**

Programmeigentümer/Geldgeber



[Info](#) [Kontakt](#) [Links & Downloads](#)

Mit der Ausschreibung Cyber Security Checks 2024 werden österreichische kleine und mittlere Unternehmen bei der Umsetzung von Sicherheitsmaßnahmen im Bereich Cybersicherheit unterstützt. Ziel ist es, das Bewusstsein für

Was kann ich heute tun?

Was kann ich heute tun?

1. Lernen Sie die Anforderungen Ihrer Kunden kennen.

- <https://www.nis.gv.at/nis-2-richtlinie.html>
- <https://www.fma.gv.at/dora-management-ikt-drittparteienrisiko/>

Was kann ich heute tun?

1. Lernen Sie die Anforderungen Ihrer Kunden kennen.

- <https://www.nis.gv.at/nis-2-richtlinie.html>
- <https://www.fma.gv.at/dora-management-ikt-drittparteienrisiko/>

2. Helfen Sie Ihren Kunden diese Anforderungen zu erfüllen.

- KSV1870 DORA-Anfragen beantworten
- Externen IT-Sicherheitsnachweis erlangen:
 - ÖISHB: Zusammenarbeit mit Externen, Evaluierung von Zertifizierungen, Lieferantenbeziehungen
 - ISO/IEC 27001: Information security in supplier relationships
 - IEC 62443 2-1: Supply chain security
 - CIS CSC v8.0: Service Provider Management
 - KSÖ Cyber Risk Rating: Anforderungen für A bzw. B Rating: <https://cyberrisk-rating.at/schema.html>

Was kann ich heute tun?

1. Lernen Sie die Anforderungen Ihrer Kunden kennen.

- <https://www.nis.gv.at/nis-2-richtlinie.html>
- <https://www.fma.gv.at/dora-management-ikt-drittparteienrisiko/>

2. Helfen Sie Ihren Kunden diese Anforderungen zu erfüllen.

- KSV1870 DORA-Anfragen beantworten
- Externen IT-Sicherheitsnachweis erlangen:
 - ÖISHB: Zusammenarbeit mit Externen, Evaluierung von Zertifizierungen, Lieferantenbeziehungen
 - ISO/IEC 27001: Information security in supplier relationships
 - IEC 62443 2-1: Supply chain security
 - CIS CSC v8.0: Service Provider Management
 - KSÖ Cyber Risk Rating: Anforderungen für A bzw. B Rating: <https://cyberrisk-rating.at/schema.html>

3. Nutzen Sie die angebotenen Hilfen

- **Gratis Vorlagen:** <https://www.wko.at/it-sicherheit/basismassnahmen-informationssicherheit-unternehmen>
- **Bis zu 10.000€ abholen:** <https://www.ffg.at/ausschreibung/cybersecuritychecks2024>
- **Bis zu 9400€ abholen:** <https://www.kmudigital.at/kmudigital/start.html>

Was kann der KSV1870 für mich tun?

1. CyberRisk Manager: Plattform für Lieferkettenbewertung:

- **NUR NOCH bis 17. Oktober 2024** um einmalig 480€ zzgl. MwSt. für eine Lifetime-Lizenz

2. CyberRisk Rating oder Cyber Trust Label:

- Kann Alternative zu Zertifizierung darstellen – je nach Kundenanforderung.
- Rund um 1.000€ je nach Ausprägung, gültig ein Jahr
- akzeptierte Best Practise nach NIS Fact Sheet 9/22 <https://www.nis.gv.at/rechtliches-und-dokumente.html>

3. Upload von bestehenden IT-Sicherheitszertifikaten in die KSV1870 CRR Datenbank:

- **Kostenlos**
- Einfach IT-Sicherheitsnachweis (z.B. ISO27001,...) an support@cyberrisk-rating.at senden
- Scheint bei allen Lieferanten auf, die die KSV1870 CRR Datenbank verwenden.

Vielen Dank!

Alexander Mitter

Geschäftsführer KSV1870 Nimbusec GmbH

KSV1870 Nimbusec GmbH

Kaisergasse 16b

4020 Linz

T: +43 732 860 626

Mail: a.mitter@nimbusec.com

www.ksv.at/cyberrisk-rating