

Das neue Bundesamt für Cybersicherheit

Ein NISG 2026 Update

Wien, 08.09.2026

DI Philipp Blauensteiner, MA
BMI IV/S/2 - Netz- und Informationssystemsicherheit
post@nis.gv.at

Disclaimer

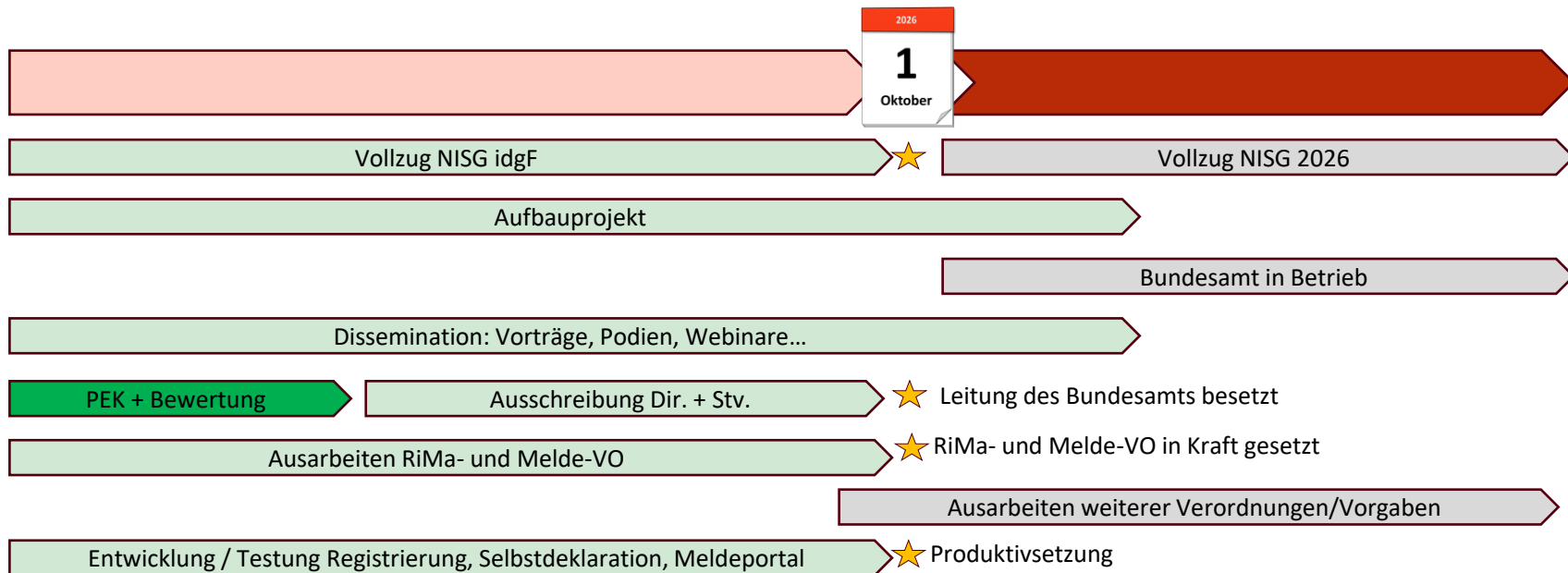
- Diese Präsentation dient dazu, **Regelungsinhalte des NISG 2026** in einer für das jeweilige Auditorium verständlichen Form aufzubereiten und zu vermitteln.
- Allfällig wahrgenommene Verkürzungen oder Generalisierungen in sprachlicher Form oder in bildlichen Darstellungen sollen **zum praktischen Verständnis beitragen** und in keiner Weise dem primär heranzuziehenden Normtext des NISG 2026 samt Erläuterungen entgegenstehen.
- Zitate von Paragraphen betreffen das **NISG 2026**, außer es wird gesondert angeführt.
- Auf die entsprechenden **urheberrechtliche Bestimmungen** im Zusammenhang mit der Weiterverwendung von Präsentationsinhalten (insbesondere Schaubilder) darf an dieser Stelle verwiesen werden.

Die Tage vergehen wie im Flug...



- 1.10.1994: Tim Berners-Lee gründet das **World Wide Web Consortium (W3C)**
- 1.10.2001: Der Österreichische Kaffeesiederverband ruft den **internationalen Tag des Kaffees** aus.
- 1.10.2026: In Österreich nimmt das  Bundesamt für Cybersicherheit den Betrieb auf

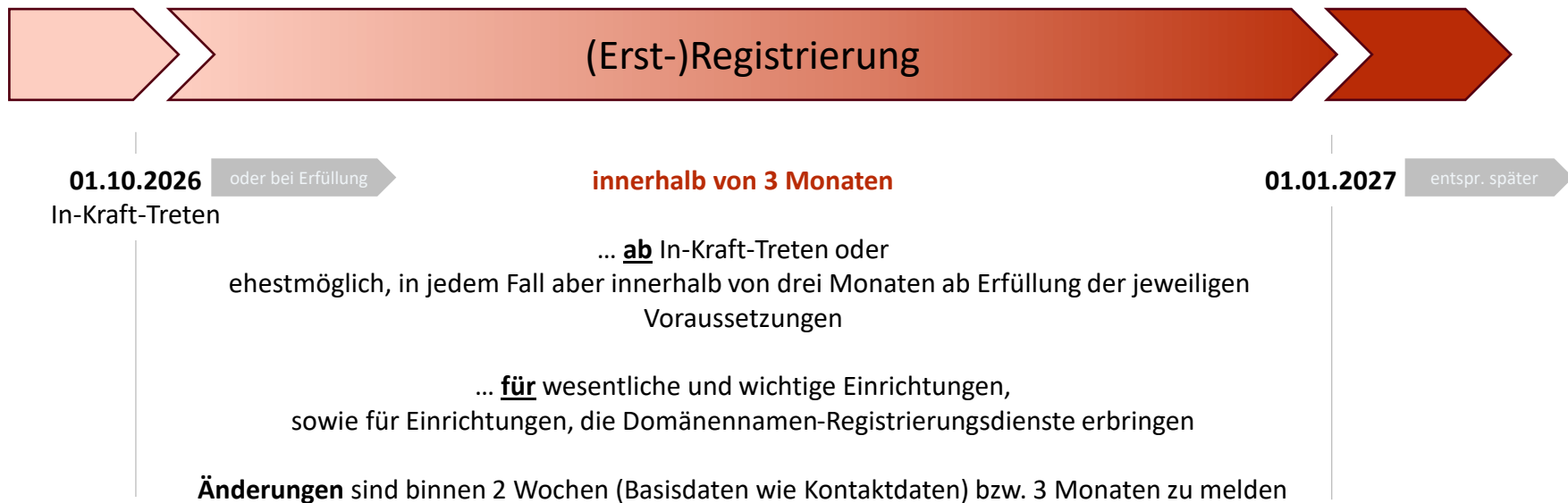
NISG2026 Timeline



Überblick: Aufgaben der Cybersicherheitsbehörde (§ 4 Abs 1)

Kooperation & Strategie		Aufsicht & Durchsetzung		Beratung & Unterstützung	Vorfälle & CSIRTs	Organisation & Recht
Koordination der Österreichischen Strategie für Cybersicherheit und Policies (CVD,...)	Berichtswesen (BMI, NR, ...)	Aufsichts- und Durchsetzungsmaßnahmen	Nationale und sektorale Risikoanalysen	Erst- und Weiterg. von Lagebildern & Erst-, Analyse und Weitergabe von Informationen zur Vorbeugung von Vorfällen	Betrieb des GovCERT	Personalmgmt. und Ausbildung und berufsbegleitende Fortbildung der Mitarbeiter
Leitung der Koordinierungsstrukturen (CSS, IKDOK und OpKoord)	Vertretung in EU-weiten und internationalen Gremien	Zulassung und Aufsicht unabhängiger Prüfer	Entgegennahme, Analyse und Weiterleitung von Meldungen	Betrieb von IKT-Lösungen	Nationale Behörde für Management großer Cybersicherheitsvorfälle	Controlling, Ressourcen und Budget sowie diesbzgl. Schnittstellen BMI
Nationales Koordinierungszentrum für Cybersicherheit (NCC) und PPP	Konsultation und Zusammenarbeit mit anderen EU Mitgliedstaaten	Behördliche Zusammenarbeit (BVBs, RKE, DSB, LSG, KommAustria, RTR, DORA, NCCS, CSZG, ...)	Betrieb der zentralen Anlaufstelle	Awarenessaktivitäten (Schulungen, Broschüren,...)	Ermächtigung und Aufsicht von nationalem CSIRT sowie sektorspezifischer CSIRTs	Erarbeitung und Erlassen von Verordnungen und Vorgaben (UPrÜ, RMM, Cybersicherheitsvorfall, Selbstdeklaration, Prüfungen, ...)

Registrierung (§ 29 Abs 3)



Registrierungsformular

NIS Registrierung

 Bundesministerium
Inneres

Info Eingabe Kontaktdaten IP-Adressen Kontrolle Abschluss

Art der Einrichtung (§ 29 Abs. 2 Z 3)

Verrichtet die Einrichtung eine oder mehrere der in den Anlagen 1 und 2 NISG 2024 beschriebenen Tätigkeiten? *

☒ ja ☐ nein

Wählen Sie den zutreffenden Sektor, ggf. Teilsektor und die Art der Einrichtung aus, unter die die Einrichtung aufgrund der von ihr verrichteten Tätigkeit fällt.

Sektor * Anlage 1 - 1. Energie

Teilsektor * 1.1. Elektrizität

Art der Einrichtung * 1.1.2. Verteilernetzbetreiber

Handelt es sich bei der Tätigkeit, die zur Einstufung unter diese Art der Einrichtung führt, um eine Haupttätigkeit oder Nebentätigkeit? *

☒ Haupttätigkeit ☐ Nebentätigkeit

Falls die Tätigkeit, aufgrund deren Verrichtung die Einrichtung von Ihnen unter diese Art der Einrichtung eingestuft wird, von der Einrichtung in weiteren 1 wählen Sie diese aus:

☐ Belgien	☐ Frankreich	☐ Litauen	☐ Rumänien
☐ Bulgarien	☐ Griechenland	☐ Luxemburg	☐ Schweden
☐ Dänemark	☐ Irland	☐ Malta	☐ Slowakei
☐ Deutschland	☐ Italien	☐ Niederlande	☐ Slowenien
☐ Estland	☐ Kroatien	☐ Polen	☐ Spanien
☐ Finnland	☒ Lettland	☐ Portugal	☐ Tschechische Rep.

➕ weitere Arten der Einrichtung

 Unternehmensservice
Portal

NIS Registrierung

 Bundesministerium
Inneres

Info Eingabe Kontaktdaten IP-Adressen Kontrolle Abschluss

Angaben zu Ermittlung der Unternehmensgröße gemäß § 25 NISG 2024 (§ 29 Abs. 2 Z 7)

Mitarbeiteranzahl

Wie viele Mitarbeiter beschäftigt die Einrichtung? *

☐ weniger als 50

☐ 50-249

☒ 250 oder mehr

Jahresumsatz und Jahresbilanzsumme

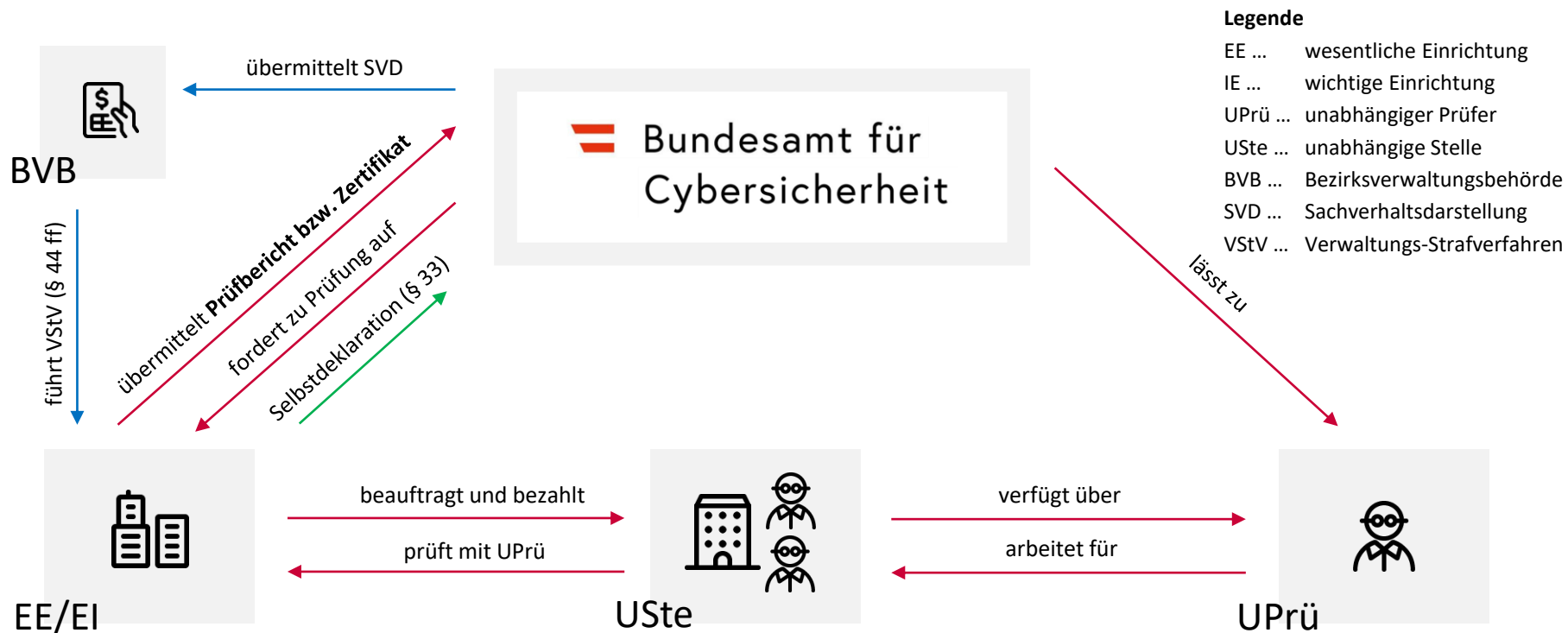
Wie hoch sind der Jahresumsatz und die Jahresbilanzsumme der Einrichtung? *

☐ Die Einrichtung erwirtschaftet einen Jahresumsatz von weniger als 10 Millionen Euro und die Jahresbilanzsumme beläuft sich auf unter 10 Millionen Euro

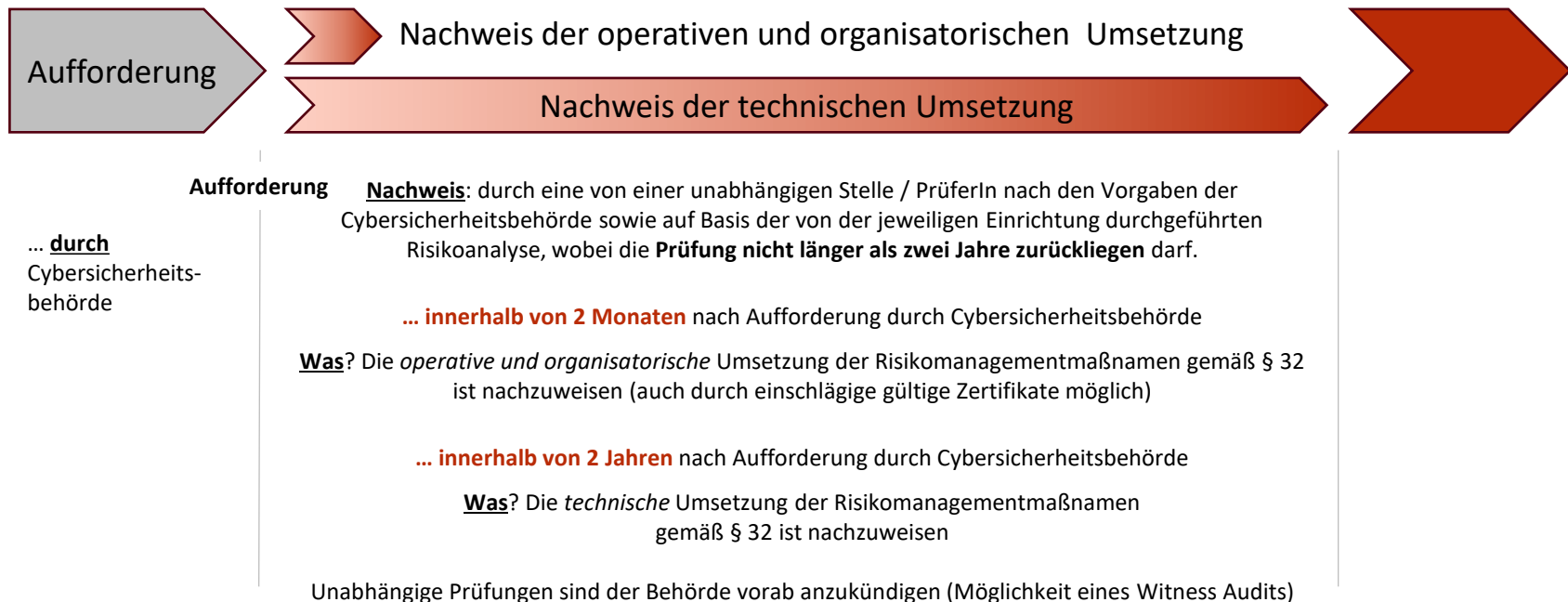
☐ Die Einrichtung erwirtschaftet einen Jahresumsatz von über 10 Millionen Euro und die Jahresbilanzsumme beläuft sich auf über 10 Millionen Euro

☒ Die Einrichtung erwirtschaftet einen Jahresumsatz von über 50 Millionen Euro und die Jahresbilanzsumme beläuft sich auf über 43 Millionen Euro

Prozess Risikomanagementmaßnahmen (RMM) (§ 32, 33)



Nachweis der Wirksamkeit von Risikomanagementmaßnahmen für wesentliche Einrichtungen (§ 33 Abs 2)



Nachweis der Wirksamkeit von Risikomanagementmaßnahmen für wichtige Einrichtungen (§ 33 Abs 2)



... durch
Cybersicherheits-
behörde

Aufforderung **Nachweis:** durch eine von einer unabhängigen Stelle / PrüferIn nach den Vorgaben der Cybersicherheitsbehörde sowie auf Basis der von der jeweiligen Einrichtung durchgeführten Risikoanalyse, wobei die **Prüfung nicht länger als zwei Jahre zurückliegen darf**.

... **innerhalb von 2 Jahren** nach Aufforderung durch Cybersicherheitsbehörde

Was? Die *technische, operative und organisatorische* Umsetzung der Risikomanagementmaßnahmen gemäß § 32 ist nachzuweisen

Unabhängige Prüfungen sind der Behörde vorab anzukündigen (Möglichkeit eines Witness Audits)
(Nachweis der *operativen und organisatorischen* Umsetzung ist auch durch einschlägige gültige Zertifikate möglich)

„Einschlägige gültige Zertifikate“ - § 33 Abs 2 NISG 2026

Aus den Erläuterungen:

- Zertifikate auf **etablierten europäischen und internationalen Normen**
(im Sinne der Verordnung (EU) 1025/2012 zur europäischen Normen)
- Rahmenbedingungen müssen erfüllt sein
 - entsprechend gewählter **Scope**
 - Äquivalenz der Anforderungen
- Explizites Beispiel: OVE/ÖNORM **EN ISO/IEC 27001**
- Nur für Nachweise zur Umsetzung **organisatorischer/operativer RMM**
Nachweis **technischer Umsetzung** von RMM **nur über USte/UPrü**

Risikomanagementmaßnahmen (RMM) (§ 32)

- **RMM sind eine zentrale Verpflichtung im NISG 2026** zur Sicherstellung eines hohen Niveaus der Sicherheit von Netz- und Informationssystemen durch Verpflichtung für wesentliche und wichtige Einrichtungen zur Umsetzung von RMM.
- Orientierung bezüglich **Vorgaben zu RMM** an Durchführungsverordnung (EU) 2024/2690 betreffend Einrichtungen digitaler Infrastruktur (Verweis darauf in nationaler Verordnung geplant).

„Schlüsselwörter“ bzgl. Umsetzung von RMM 1/3 (§ 32)

- **Abs. 1:** ... geeignete und verhältnismäßige Risikomanagementmaßnahmen in technischer, operativer und organisatorischer Hinsicht...
- **Abs. 2:** ... Berücksichtigung des Stands der Technik und [...] Normen sowie bewährter Verfahren und der Kosten der Umsetzung [...] das dem bestehenden Risiko angemessen ist ...

„Schlüsselwörter“ bzgl. Umsetzung von RMM 2/3 (§ 32)

- **Abs. 3:** Beurteilung der **Verhältnismäßigkeit** der Risikomanagementmaßnahmen [...] Ausmaß der **Risikoexposition** der Einrichtung sowie ihrer Dienste, die **Größe der Einrichtung** und die **Wahrscheinlichkeit des Eintretens** von Cybersicherheitsvorfällen und deren **Schwere**, einschließlich ihrer **gesellschaftlichen und wirtschaftlichen Auswirkungen** ...
- **Abs. 4:** ... Risikomanagementmaßnahmen haben auf einem **gefahrenübergreifenden Ansatz** zu beruhen, der auf den **Schutz der Netz- und Informationssysteme** samt deren **physischen Komponenten** vor Cybersicherheitsvorfällen abzielt ...

„Schlüsselwörter“ bzgl. Umsetzung von RMM 3/3 (DVO 2024/2690)

- **Erw.G. 5:** Können [...] Einrichtungen einige der [...] Anforderungen [...] **wegen ihrer Größe nicht umsetzen**, so sollten sie [...] die Möglichkeit haben, andere **Ausgleichsmaßnahmen** zu ergreifen...
- **Erw.G. 6:** ... **nicht angemessen, nicht anwendbar oder nicht durchführbar**, bestimmte [...] Anforderungen [...] sollte sie ihre diesbezügliche **Begründung in verständlicher Weise dokumentieren**. Die zuständigen nationalen Behörden können [...] eine angemessene Frist berücksichtigen, die betreffende Einrichtungen benötigen, um die [...] Anforderungen [...] umzusetzen.

Ausgleichsmaßnahmen (kompensierende Maßnahmen)

- Wenn einzelne Anforderungen **unverhältnismäßig** oder **vorübergehend nicht umsetzbar** sind, müssen **Ausgleichsmaßnahmen** ergriffen werden, welche geeignet sind, den **übergeordneten Zweck** der jeweiligen Anforderung zu **erreichen** und der **Minimierung** damit zusammenhängender **Risiken** dienen.
- Die Umsetzung von Ausgleichsmaßnahmen muss nachvollziehbar **begründet** und zu **dokumentiert** sein und in **regelmäßigen** Abständen **auf Wirksamkeit überprüft** werden.

Ausblick: Geplante NIS2 Adaptionen (Auszug)

im Zuge der CSA2 Verhandlungen

Ein kleines Midcap-Unternehmen

- ist ein Unternehmen, dass
- **kein KMU** ist
 - **weniger als 750 Personen** beschäftigt
 - **max. 150 Mio Euro Jahresumsatz** bzw. **max. 129 Mio Euro Bilanzsumme**

Empfehlung (EU) 2025/1099 der Kommission vom 21. Mai 2025 zur Definition kleiner Midcap-Unternehmen

Digitale Infrastruktur

Klein- und Kleinstanbieter von DNS
Diensten werden **aus Anwendungsbereich gestrichen**

Auswirkungen auf NISG 2026

- Nationale Umsetzung **notwendig** (2/3 Mehrheit)
- Kleine Midcap-Unternehmen in Bereichen der Anlage 1 in Hinkunft **wichtige Einrichtung**
- Achtung:
kritische Einrichtungen nach RKE bleiben **größenunabhängig wesentlich**

Danke für Ihre Aufmerksamkeit!

DI Philipp Blauensteiner, MA
Bundesministerium für Inneres
BMI IV/S/2 - Netz- und Informationssystemsicherheit
post@nis.gv.at