FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

DIE HOCHSCHULE,
DIE MEHR KANN.

RKE - Die große Unbekannte in der physischen Sicherheit

RICHTLINIE (EU) 2022/2557 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 14. Dezember 2022

über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates

(Text von Bedeutung für den EWR)

RKE / CER

RICHTLINIEN

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 14. Dezember 2022

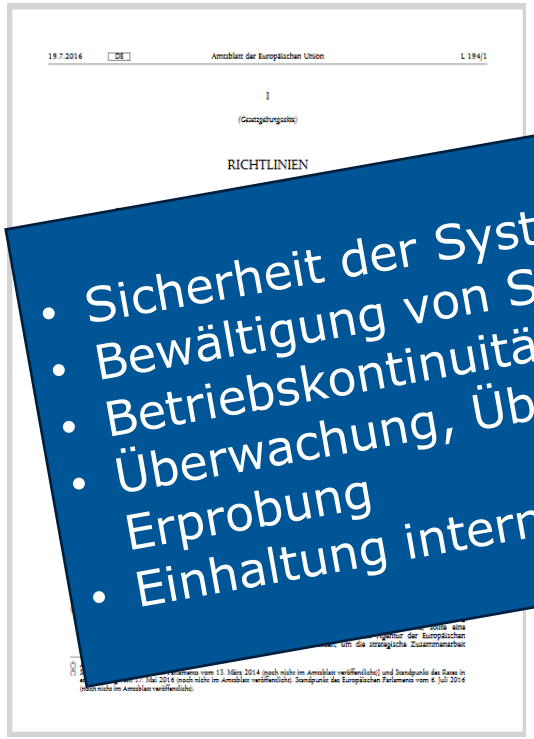
über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)

(Text von Bedeutung für den EWR)

NIS2

Hintergrundwissen NIS und Physische Sicherheit

NIS (RL-1148)



19.7.2016 DE Amtsblatt der Europäischen Union L 194/1

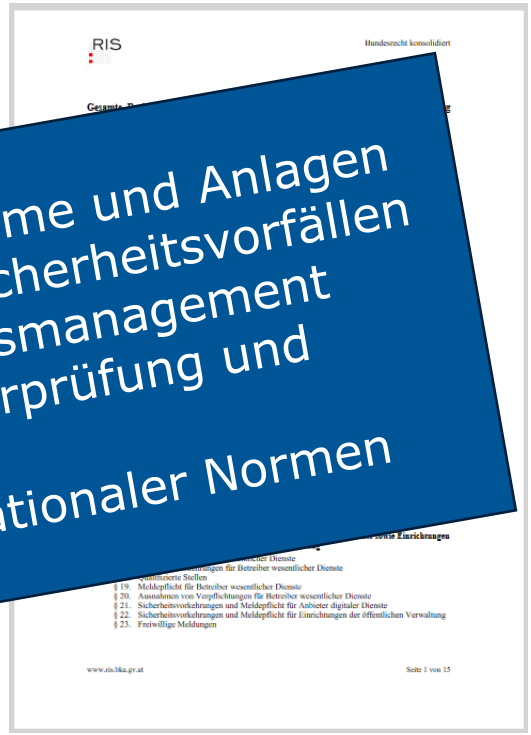
I

(Gesetzgebungsakte)

RICHTLINIEN

- Sicherheit der Systeme und Anlagen
- Bewältigung von Sicherheitsvorfällen
- Betriebskontinuitätsmanagement
- Überwachung, Überprüfung und Erprobung
- Einhaltung internationaler Normen

NISG 2018



RIS

Bundesrecht konsolidiert

§ 19. Meldepflicht für Betreiber wesentlicher Dienste
§ 20. Ausnahmen von Verpflichtungen für Betreiber wesentlicher Dienste
§ 21. Sicherheitsvorkehrungen und Meldepflicht für Anbieter digitaler Dienste
§ 22. Sicherheitsvorkehrungen und Meldepflicht für Einrichtungen der öffentlichen Verwaltung
§ 23. Freiwillige Meldungen

www.ris.bka.gv.at Seite 1 von 15

NIS-VO

6.	**Systemwartung und Betrieb**
6.1	Systemwartung und Betrieb: Abläufe und Vorgänge zur Gewährleistung eines sicheren Systembetriebs von Netz- und Informationssystemen sind einzuführen und periodisch zu überprüfen.
6.2	Fernzugriff: Fernzugriff ist eingeschränkt nach dem Minimalrechtsprinzip und zeitlich beschränkt zu vergeben. Die Fernzugriffsrechte sind periodisch zu überprüfen und gegebenenfalls anzupassen. Die Sicherheit des Fernzugriffs ist zu gewährleisten.
7.	**Physische Sicherheit**
7.1	Physische Sicherheit: Der physische Schutz der Netz- und Informationssysteme, insbesondere der physische Schutz vor unbefugtem Zutritt und Zugang, ist zu gewährleisten.
8.	**Erkennung von Vorfällen**
8.1	Erkennung: Mechanismen zur Erkennung und Bewertung von Vorfällen sind umzusetzen.
8.2	Protokollierung und Monitoring: Mechanismen zu Protokollierung und Monitoring, insbesondere von für die Erbringung des wesentlichen Dienstes essentiellen Tätigkeiten und Vorgängen, sind umzusetzen.
8.3	Korrelation und Analyse: Mechanismen zur Erkennung und adäquaten Bewertung von Vorfällen durch die Korrelation und Analyse der ermittelten Protokolldaten sind umzusetzen

Hintergrundwissen NIS2 und Physische Sicherheit

NIS (RL-2555)

Art. 21 (2) […] genannten Maßnahmen müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen […]

NISG 2024

Analog Art. 21 (2) ist §32 (2) Z. 2. formuliert

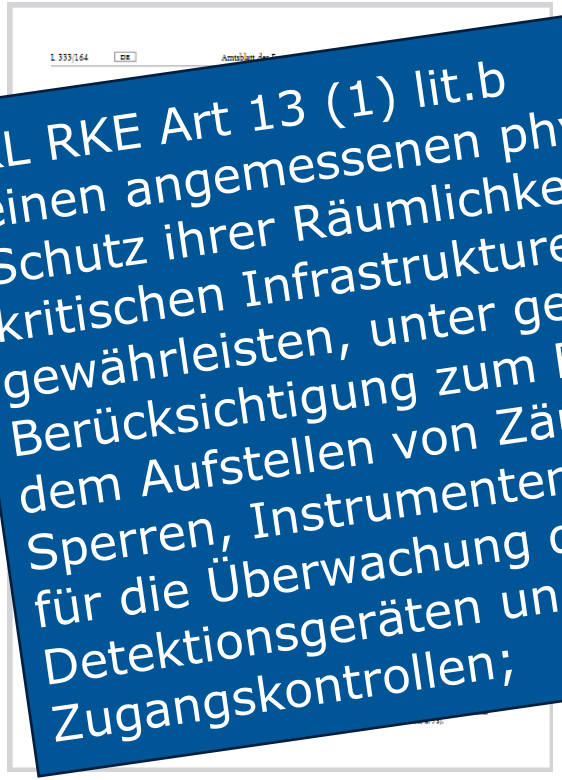
Zusätzlich Anlage 3 – 13a,b und c

Hintergrundwissen RKE – Physische Sicherheit im Fokus

RKE (RL 2557)

RKEG (vorauss. Okt)

RKE-VO



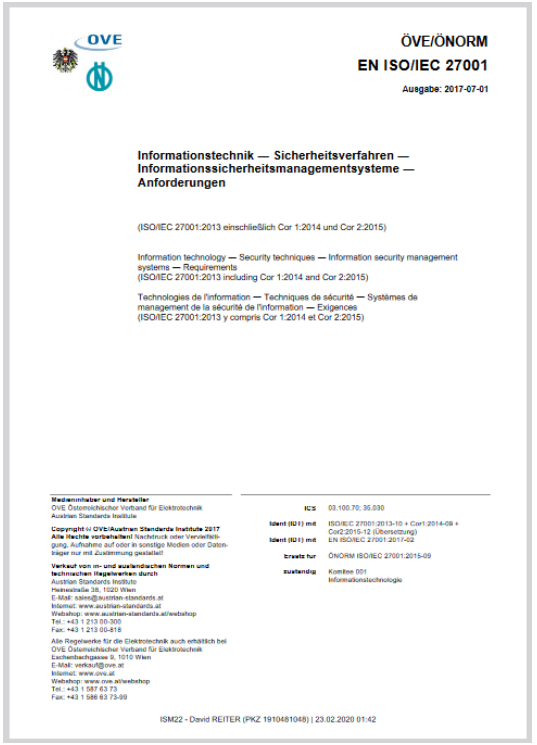
RL RKE Art 13 (1) lit.b
einen angemessenen physischen Schutz ihrer Räumlichkeiten und kritischen Infrastrukturen zu gewährleisten, unter gebührender Berücksichtigung zum Beispiel von dem Aufstellen von Zäunen und Sperren, Instrumenten und Verfahren für die Überwachung der Umgebung, Detektionsgeräten und Zugangskontrollen;

herheit
eführt

...

Physische Sicherheit – Abdeckungsanforderung durch Normenserie

ISO 27001 – Anhang A



ÖVE/ÖNORM
EN ISO/IEC 27001
Ausgabe: 2017-07-01

Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen

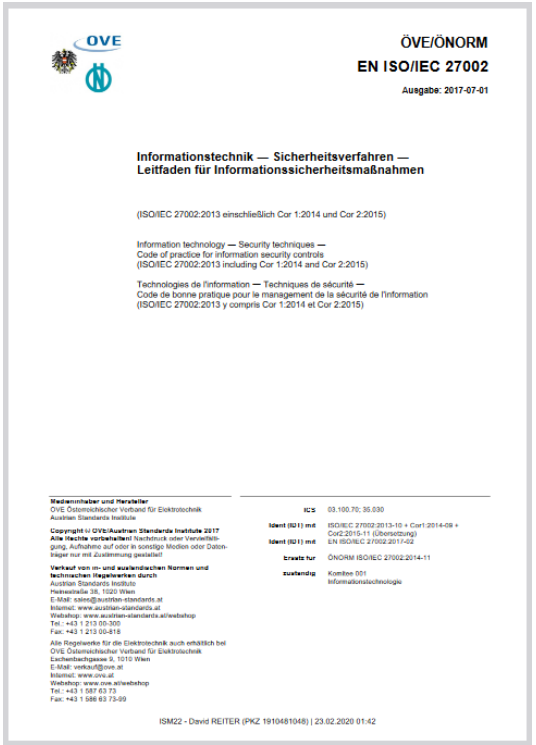
(ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015)

Information technology — Security techniques — Information security management systems — Requirements
(ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015)

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences
(ISO/IEC 27001:2013 y compris Cor 1:2014 et Cor 2:2015)

ICS 03.100.70; 35.030
Ident (ID1) mit ISO/IEC 27001:2013-10 + Cor1:2014-08 + Cor2:2015-12 (Übersetzung)
Ident (ID1) mit EN ISO/IEC 27001:2017-02
Ersetzt für ÖNORM ISO/IEC 27001:2015-09
Zuständig Komitee 001 Informationstechnologie

ISO 27002



ÖVE/ÖNORM
EN ISO/IEC 27002
Ausgabe: 2017-07-01

Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen

(ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015)

Information technology — Security techniques — Code of practice for information security controls
(ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015)

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information
(ISO/IEC 27002:2013 y compris Cor 1:2014 et Cor 2:2015)

ICS 03.100.70; 35.030
Ident (ID1) mit ISO/IEC 27002:2013-10 + Cor1:2014-08 + Cor2:2015-11 (Übersetzung)
Ident (ID1) mit EN ISO/IEC 27002:2017-02
Ersetzt für ÖNORM ISO/IEC 27002:2014-11
Zuständig Komitee 001 Informationstechnologie

Physische Sicherheit – einschlägige Standards und Erweiterung Scope

Gemäß Art. 16 wird bei der RKE auf die einschlägigen europäischen Normen zum Thema Physische Sicherheit zurückgegriffen.

OVE Richtlinie R2:2017, OVE Richtlinie R9:2012, OVE Richtlinie R10:2016,

EN 1627:2021, EN 1630:2021, EN 356:2000,

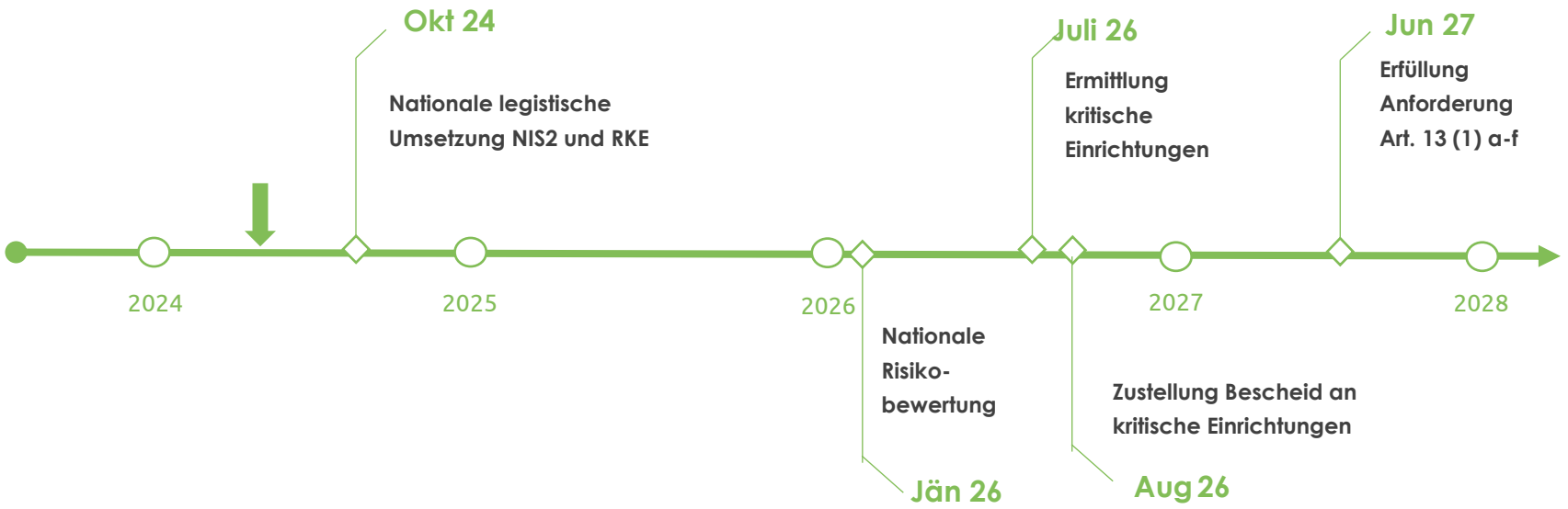
EN 60839-11-1:2014, EN 60839-11-2:2016, EN 50130-4:2015, EN 50131-4:2019, EN 50131-2-6:2013, , EN 50136-2:2014, VDS 2367:2004, VDS 2311:2021, VDS 2366:2017, VDS 3802:2019,

S2420:2013, S2412:2017, S2413:2017, S2414-2:2018, S2415-1:2014, S2415-2:2014, B 1301:2016; Wirtschaftsgrundschutz Baustein IS1:2017,

S2450:2014, EN 12433-1:2000, EN 12433-2:2000, EN 1143-1:2019, EN 14450:2018, EN 1047-1:2017, EN1047-2:2019, EN 15659:2019, EN 15713:2009,

EN 1522:1999, EN 1063:2019, EN 13123-1:2001, EN 13123-2:2004, EN 13541:2012 etc.

Zeitstrahl


Okt 24
Nationale legistische Umsetzung NIS2 und RKE
Juli 26
Ermittlung kritische Einrichtungen
Jun 27
Erfüllung Anforderung Art. 13 (1) a-f
2024
2025
2026
2027
2028
Nationale Risiko-bewertung
Jän 26
Zustellung Bescheid an kritische Einrichtungen
Aug 26

RICHTLINIE (EU) 2022/2557 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 14. Dezember 2022

über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates

(Text von Bedeutung für den EWR)

RKE / CER

RICHTLINIEN

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

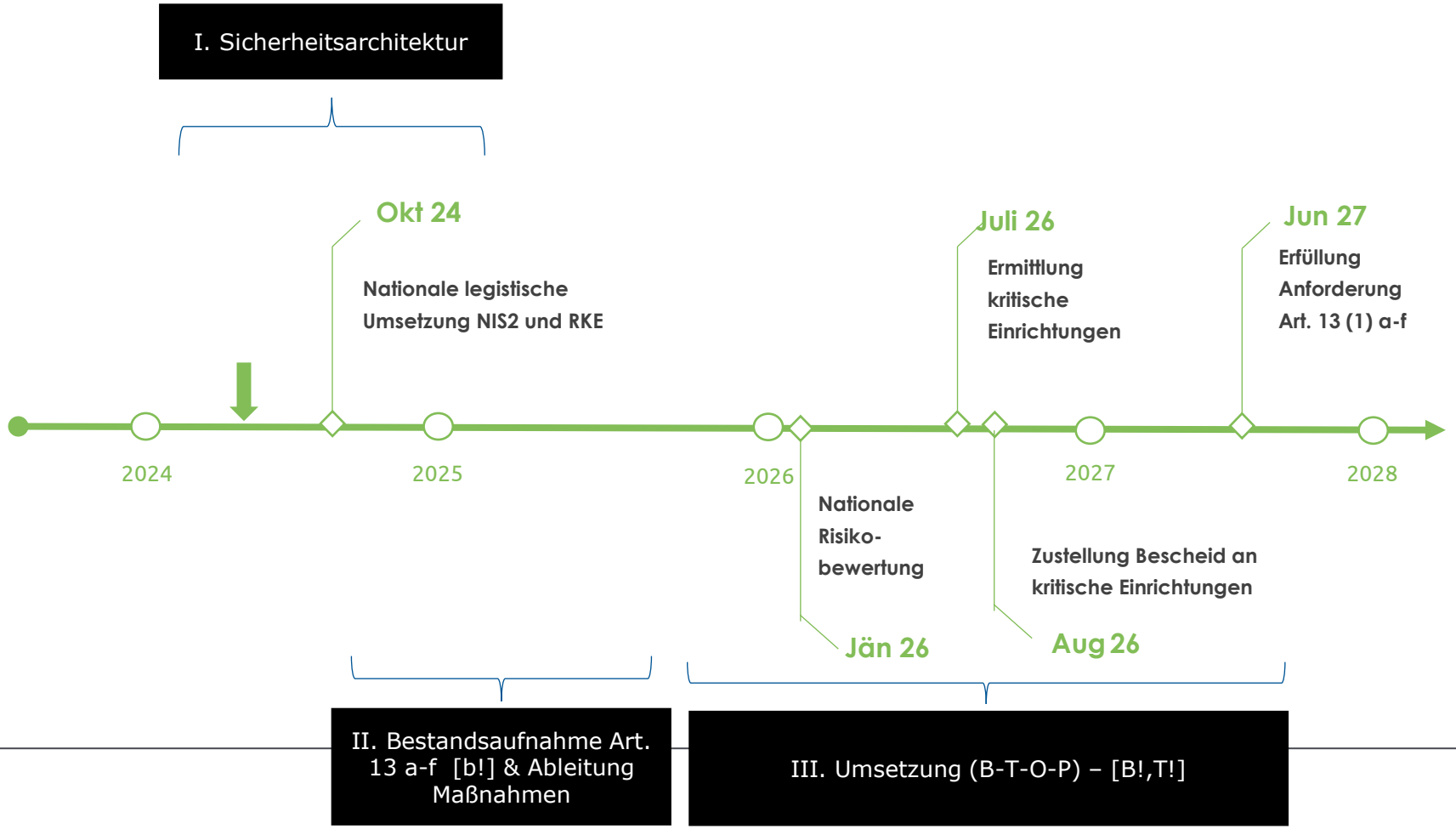
vom 14. Dezember 2022

über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)

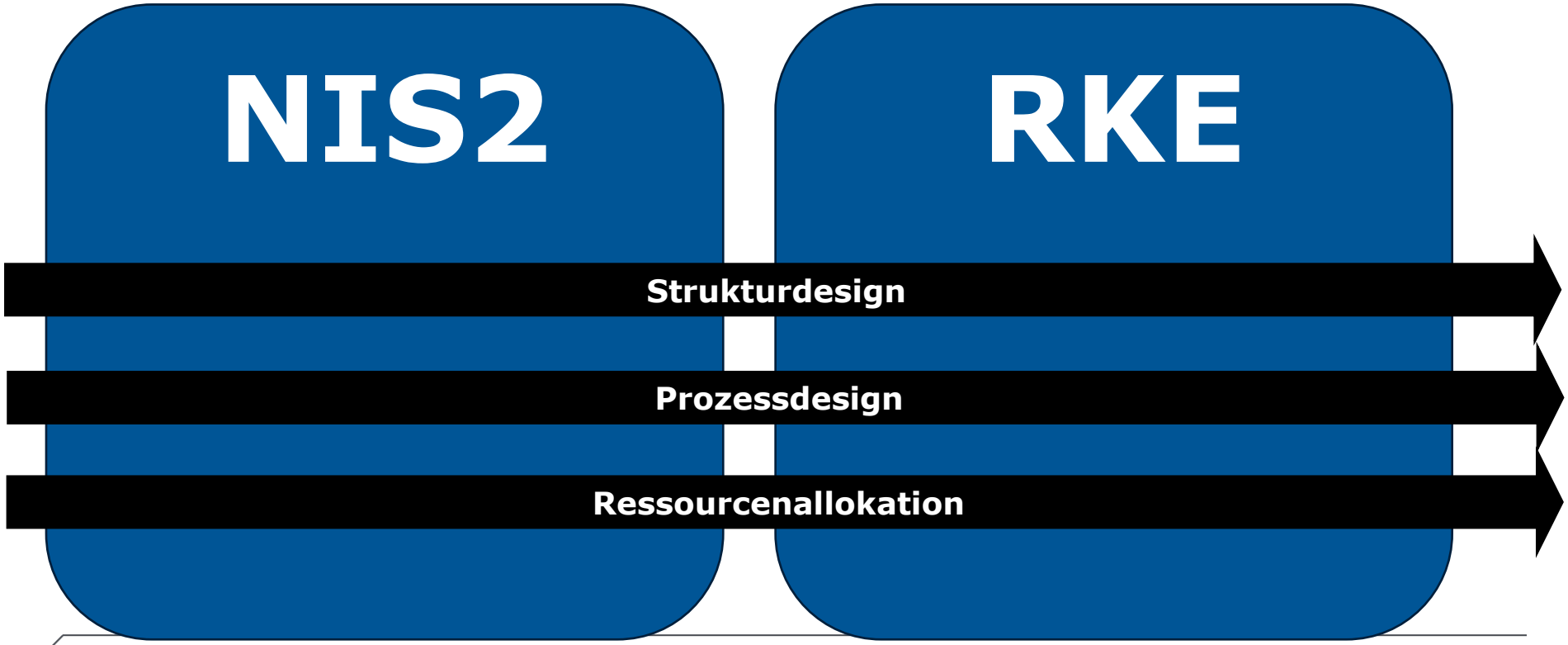
(Text von Bedeutung für den EWR)

NIS2

Zeitstrahl


I. Sicherheitsarchitektur
Okt 24
Nationale legistische Umsetzung NIS2 und RKE
Juli 26
Ermittlung kritische Einrichtungen
Jun 27
Erfüllung Anforderung Art. 13 (1) a-f
2024
2025
2026
2027
2028
Nationale Risiko-bewertung
Jän 26
Zustellung Bescheid an kritische Einrichtungen
Aug 26
II. Bestandsaufnahme Art. 13 a-f [b!] & Ableitung Maßnahmen
III. Umsetzung (B-T-O-P) – [B!,T!]

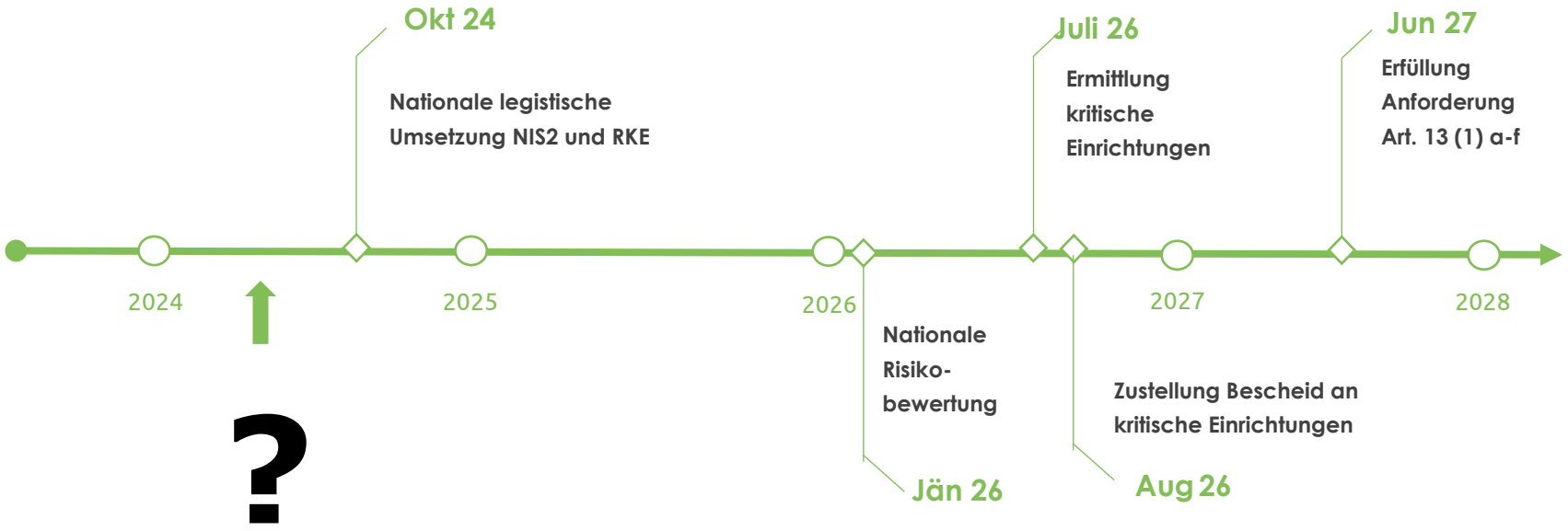
Eine Organisation – eine Sicherheit



Case Study 2 - Vorgehensmodell risikobasierter Ansatz Physische Sicherheit

1. Identifikation der kritischen Infrastrukturen
2. Ermittlung des Täterprofils und der Täterqualität
3. (Objektbezogene) Bestandsaufnahme Physische Sicherheit
4. Resilienzanalyse Physische Sicherheit
5. Risikobasierte Ableitung der Maßnahmen

Zeitstrahl


Okt 24
Nationale legistische Umsetzung NIS2 und RKE
Juli 26
Ermittlung kritische Einrichtungen
Jun 27
Erfüllung Anforderung Art. 13 (1) a-f
2024
2025
2026
2027
2028
?
Nationale Risiko-bewertung
Jän 26
Zustellung Bescheid an kritische Einrichtungen
Aug 26

Falsche Zusammenfassung

1. Da RKE und NIS 2 von EU-Kommission zueinander abgestimmt und zeitgleich verabschiedet wurden, sind diese integriert zu sehen
2. In der RKE gibt es neben der Anforderung der Physischen Sicherheit weitere Anforderungen wie die personelle Sicherheit, etc. die ebenfalls integriert zu sehen sind.
3. Eine Vorbereitung für NIS2 ist gut, eine Vorbereitung für RKE ist auch gut, ein Ansatz, der beides abdeckt ist aber am besten.

DANKE FÜR IHRE AUFMERKSAMKEIT!

FH-Prof. Dr. Martin Langer
T: +43 1 606 68 77 2151
E: martin.langer@fh-campuswien.ac.at

https://www.fh-campuswien.ac.at/studium-weiterbildung/aktuell/news-und-events/campus-lectures-sicherheit-im-fokus-eine-spionin-und-ein-spion-erzaehlen.html