Mehr Resilienz für Weltraumsysteme im Kontext europäischer Regularien

Interaktiver Workshop des ACS-Expertenkreises für Cybersicherheit im Weltraum

Bundesamt
für Sicherheit in der
Informationstechnik

Omnisecure, Berlin, 20. Januar 2026

Expertenkreis Cybersicherheit im Weltraum

Daten:

- Gegründet: November 2023
- Aktuell ca. 75 Mitglieder

Ziele:

- Austausch zwischen Behörden, Industrie und Forschungseinrichtungen in Deutschland zum Thema Cybersicherheit Weltraum
- Sensibilisierung für die Dringlichkeit des Themas
- Aufbau eines gemeinsamen Verständnisses von Sicherheitsanforderungen
- Einbringen national abgestimmter Positionen in internationale Standards

Kontakt und Publikationen:

Website Expertenkreis Cybersicherheit im Weltraum

Gemeinsam die Cybersicherheit von Weltraumsystemen stärken

Schwerpunkte Expertenkreis

PG-D
Identifizierung von Sicherheitsanforderungen

- Risiko-orientierter Ansatz über gesamten Lebenszyklus
- IT-Grundschutz-Profile, TRs

PG-I
Internationales, Standardisierung

- Unterstützung für und Austausch mit Gremien
- Einbringen in internationale Standards und Reviews

PG-Z
Zukunftstechnologien / Space 4.0

- Technologien, Entwicklungen, Geschäftsprozesse, Stakeholder

PG-R
Regulierung

- Mehrstufiges Zertifizierungsschema
- EU Space Act, NIS 2, CRA

PG-N
Nutzbarkeit

- Sensibilisierung, Motivation für CS in WR-Systemen
- Anwendung der Dokumente in Projekten

Was passiert heute?

EU Space Act

NIS 2

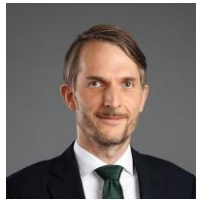
CER

CRA

Nationale Umsetzung

...

ÜBERBLICK und JURISTISCHE ANALYSE der regulatorischen Landschaft



Dr. Holger Kastler

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI

Informationssicherheit für Weltraumsysteme

Studie zur Kohärenz von EU Space Act, NIS 2, CRA, und EUCC

Version: 0.1
Datum: 13. Januar 2026

Synergien, Lücken, Überschneidungen?

IT-Grundschutz-profile

Technische Richtlinien

Prüfvor-schriften

Zertifizierungs-konzept

Mapping Bedrohungen, Anforderungen in Standards

...

Sascha Fankhänel

HOW TO – Nutzung der BSI-Anforderungspapiere zur effizienten, resilienten Umsetzung regulatorischer Anforderungen

Bundesgesetzblatt

Teil I

2025 Ausgegeben zu Bonn am 5. Dezember 2025 Nr. 301

Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

Vom 2. Dezember 2025

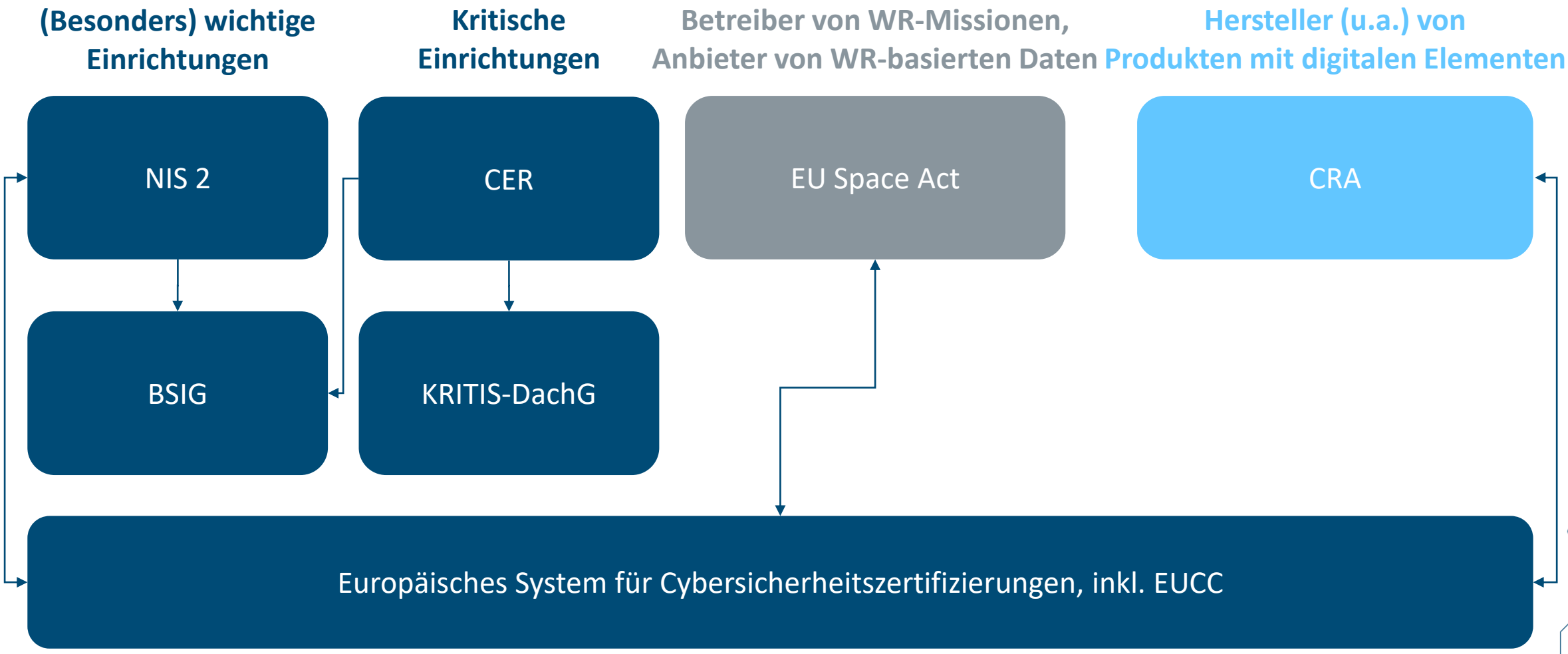
Der Bundestag hat das folgende Gesetz beschlossen:

Inhaltsübersicht

Best Practices – Erhöhung der Rechtssicherheit und operativen Robustheit durch Standards

Europäisches Cybersicherheitsrecht – Überblick und juristische Analyse

Wer/was ist erfasst?



NIS-2-Richtlinie, NIS2UmsG und BSIG

NIS-2-Richtlinie:

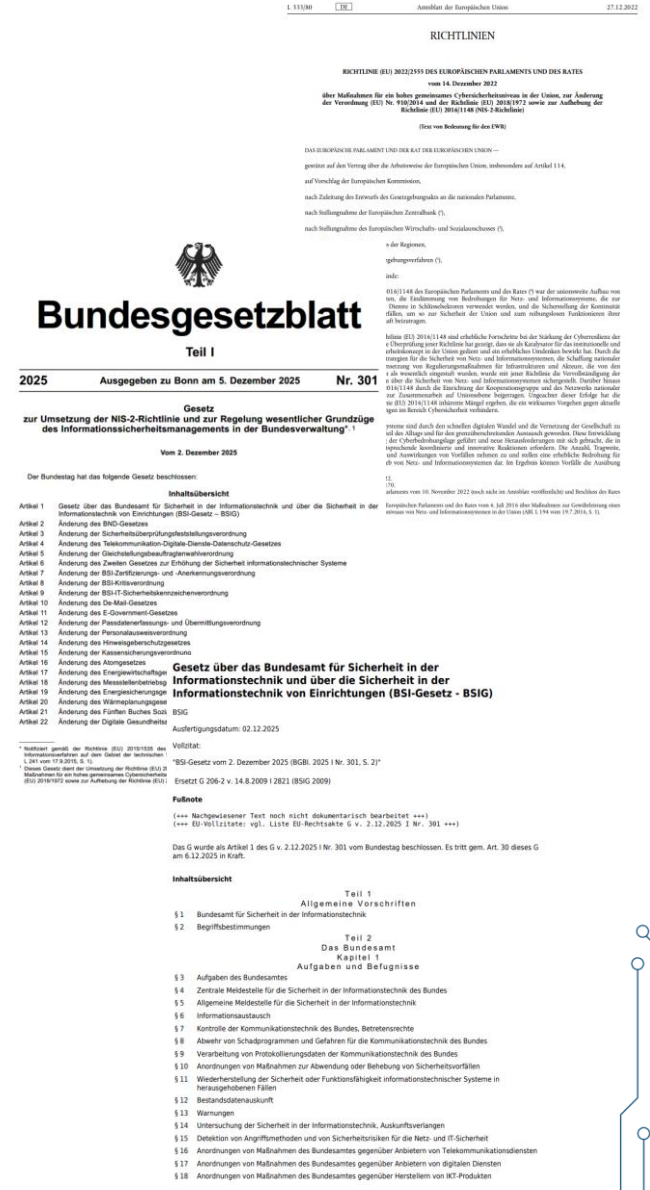
- Allgemeiner Rechtsrahmen für Netzwerk- und Informationssicherheit: Horizontale Mindestanforderungen an Cybersicherheit
- Anwendungsbereich: Einrichtungen in unterschiedlichen Industrien/Sektoren
  - Rechtliche Anforderungen sind davon unabhängig
  - Konkrete Risikobewertung ist von den spezifischen Risiken in dem betreffenden Sektor und der Einrichtung abhängig

Deutsches Umsetzungsgesetz (NIS2UmsG):

- (Artikel-)Gesetz, das gleichzeitig mehrere deutsche Gesetze ändert
  - BSIG
  - Andere Gesetze: TKG, EnWG, etc.

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSIG):

- Rechtsrahmen mit Mindestanforderungen an Cybersicherheit für wichtige und besonders wichtige Einrichtungen sowie für Betreiber kritischer Anlagen
- Risikomanagementmaßnahmen für Cybersicherheit wurden in Anlehnung an die NIS-2-Richtlinie umgesetzt.



L 333/80 DE Amtsblatt der Europäischen Union 27.12.2022

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)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 114,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme der Europäischen Zentralbank (1),

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses (2),

s der Regionen,

tgebungsverfahren (3),

inde:

016/1148 des Europäischen Parlaments und des Rates (4) war der unionsweite Aufbau von ten, die Einführung von Risikoregen für Netz- und Informationssysteme, die zur Dienste in Schlüsselsektoren verwendet werden, und die Sicherstellung der Kontinuität fällen, um so zur Sicherheit der Union und zum reibungslosen Funktionieren ihrer aft beizutragen.

hlinie (EU) 2016/1148 sind erhebliche Fortschritte bei der Stärkung der Cyberresilienz der e Überprüfung jener Richtlinie hat gezeigt, dass sie als Katalysator für das institutionelle und erheblichen Umfang gedient und als erhebliches Umbruchen bewirkt hat. Durch die trangten für die Sicherheit von Netz- und Informationssystemen, die Schaffung nationaler tsetzung von Regulierungsmaßnahmen für Infrastrukturen und Akteure, die von den s als wesentlich eingestuft wurden, wurde mit jener Richtlinie die Voraussetzung der e über die Sicherheit von Netz- und Informationssystemen sichergestellt. Darüber hinaus 016/1148 durch die Einrichtung der Kooperationsgruppe und des Netzwerks nationaler rer Zusammenarbeit auf Unionsebene beigetragen. Ungeachtet dieser Erfolge hat die sie (EU) 2016/1148 inhärente Mängel ergeben, die ein wirksames Vorgehen gegen aktuelle igen im Bereich Cybersicherheit verhindern.

ysteme sind durch den schnellen digitalen Wandel und die Vernetzung der Gesellschaft zu sid des Alltags und für den grenzüberschreitenden Austausch geworden. Diese Entwicklung r der Cyberbedrohungslage geführt und neue Herausforderungen mit sich gebracht, die in tsprechende koordinierte und innovative Reaktionen erfordern. Die Anzahl, Tragweite, und Auswirkungen von Vorfällen nehmen zu und stellen eine erhebliche Bedrohung für eb von Netz- und Informationssystemen dar. Im Ergebnis können Vorfälle die Ausübung

12.
(3) [illegible]
arlaments vom 10. November 2022 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates

Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines einsam von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

Bundesgesetzblatt

Teil I

2025 Ausgegeben zu Bonn am 5. Dezember 2025 Nr. 301

Gesetz
zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung*. [1]

Vom 2. Dezember 2025

Der Bundestag hat das folgende Gesetz beschlossen:

Inhaltsübersicht

Artikel 1 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz – BSIG)
Artikel 2 Änderung des BND-Gesetzes
Artikel 3 Änderung der Sicherheitsüberprüfungsfeststellungsverordnung
Artikel 4 Änderung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes
Artikel 5 Änderung der Gleichstellungsbeauftragtenwahlverordnung
Artikel 6 Änderung des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme
Artikel 7 Änderung der BSI-Zertifizierungs- und -Anerkennungsverordnung
Artikel 8 Änderung der BSI-Kritisverordnung
Artikel 9 Änderung der BSI-IT-Sicherheitskennzeichenverordnung
Artikel 10 Änderung des De-Mail-Gesetzes
Artikel 11 Änderung des E-Government-Gesetzes
Artikel 12 Änderung der Passdatenerfassungs- und Übermittlungsverordnung
Artikel 13 Änderung der Personalausweisverordnung
Artikel 14 Änderung des Hinweisgeberschutzgesetzes
Artikel 15 Änderung der Kassensicherungsverordnung
Artikel 16 Änderung des Atomgesetzes
Artikel 17 Änderung des Energiewirtschaftsgesetzes
Artikel 18 Änderung des Messstellenbetriebsgesetzes
Artikel 19 Änderung des Energiesicherungsgesetzes
Artikel 20 Änderung des Wärmeplanungsgesetzes
Artikel 21 Änderung des Fünften Buches Sozialgesetzbuch
Artikel 22 Änderung der Digitale Gesundheitsanwendungen-Verordnung

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz - BSIG)

Ausfertigungsdatum: 02.12.2025

Vollzitat:

"BSI-Gesetz vom 2. Dezember 2025 (BGBl. 2025 I Nr. 301, S. 2)"

Ersetzt G 206-2 v. 14.8.2009 I 2821 (BSIG 2009)

Fußnote

(+++ Nachgewiesener Text noch nicht dokumentarisch bearbeitet +++)
(+++ EU-Vollzitate; vgl. Liste EU-Rechtsakte G v. 2.12.2025 I Nr. 301 +++)

Das G wurde als Artikel 1 des G v. 2.12.2025 I Nr. 301 vom Bundestag beschlossen. Es tritt gem. Art. 30 dieses G am 6.12.2025 in Kraft.

Inhaltsübersicht

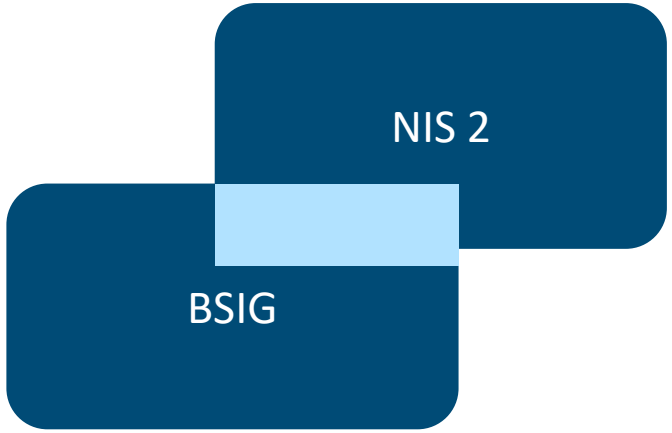
Teil 1
Allgemeine Vorschriften
§ 1 Bundesamt für Sicherheit in der Informationstechnik
§ 2 Begriffsbestimmungen

Teil 2
Das Bundesamt
Kapitel 1
Aufgaben und Befugnisse
§ 3 Aufgaben des Bundesamtes
§ 4 Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes
§ 5 Allgemeine Meldestelle für die Sicherheit in der Informationstechnik
§ 6 Informationsaustausch
§ 7 Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte
§ 8 Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes
§ 9 Verarbeitung von Protokollierungsdaten der Kommunikationstechnik des Bundes
§ 10 Anordnungen von Maßnahmen zur Abwendung oder Behebung von Sicherheitsvorfällen
§ 11 Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen
§ 12 Bestandsdatenauskunft
§ 13 Warnungen
§ 14 Untersuchung der Sicherheit in der Informationstechnik, Auskunftsverlangen
§ 15 Detektion von Angriffsmethoden und von Sicherheitsrisiken für die Netz- und IT-Sicherheit
§ 16 Anordnungen von Maßnahmen des Bundesamtes gegenüber Anbietern von Telekommunikationsdiensten
§ 17 Anordnungen von Maßnahmen des Bundesamtes gegenüber Anbietern von digitalen Diensten
§ 18 Anordnungen von Maßnahmen des Bundesamtes gegenüber Herstellern von IKT-Produkten

NIS 2 & BSIG – Cybersicherheits-Risikomanagement

Mindestanforderungen
Art. 21 Abs. 2 NIS-2-Richtlinie <> § 30 Abs. 2 BSIG

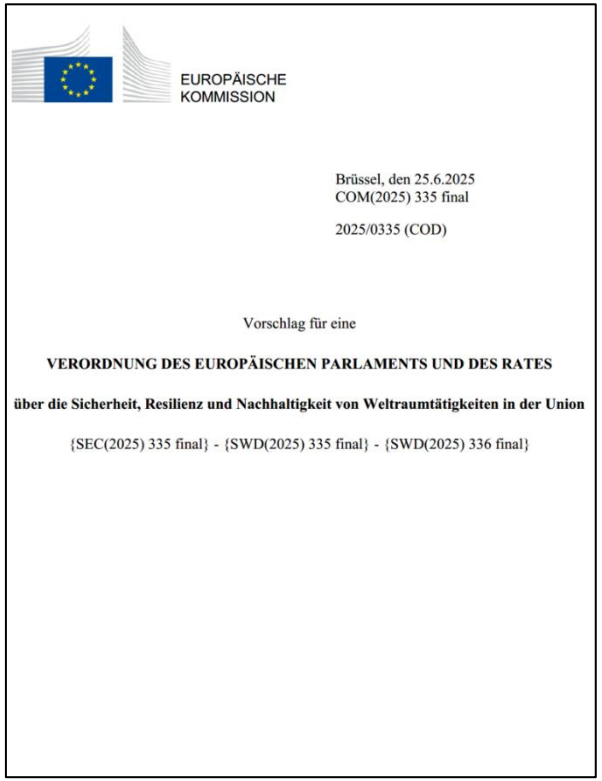
1. Risikoanalyse
2. Bewältigung von Sicherheitsvorfällen
3. BCM und Krisenmanagement
4. Lieferkettensicherheit
5. Schwachstellenmanagement
6. Wirksamkeitsbewertungen
7. Cyberhygiene und Schulungen
8. Kryptografie und Verschlüsselung
9. Personalsicherheit, Zugriffskontrolle und Anlagenmanagement
10. MFA, Authentifizierung, gesicherte Kommunikation



EU Space Act (Entwurf)

Entwurf vom 25. Juni 2025: Eigene Anforderungen an Resilienz der Weltrauminfrastruktur und Risikomanagement für Cybersicherheit gemäß Artikel 75-95 EUSA

- Risikomanagement einschließlich Risikobewertungen
- Leitungsverantwortung, Personalsicherheit
- Zugangsrechte
- Prävention und Schutz, auch vor Sicherheitsvorfällen
- Kryptografie und Verschlüsselung
- BCM einschließlich Backup-Management
- Prüfprogramm für die Netz- und Informationssysteme, Pen Tests
- Umgang mit Sicherheitsvorfällen, Krisenmanagement
- Meldung erheblicher Sicherheitsvorfälle
- Schulungen
- Lieferkettensicherheit



EUROPÄISCHE
KOMMISSION

Brüssel, den 25.6.2025
COM(2025) 335 final

2025/0335 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über die Sicherheit, Resilienz und Nachhaltigkeit von Weltraumtätigkeiten in der Union

{SEC(2025) 335 final} - {SWD(2025) 335 final} - {SWD(2025) 336 final}

EU Space Act (Entwurf)

Entwurf vom 25. Juni 2025: Verhältnis zu NIS-2-Richtlinie und CER-Richtlinie

Verhältnis NIS-2-Richtlinie und EU Space Act:
Für *wichtige und wesentliche Einrichtungen* gemäß NIS-2-Richtlinie gilt:
>> Im Hinblick auf Risikomanagementmaßnahmen geht EU Space Act als speziellerer Rechtstakt der NIS-2-Richtlinie mit ihren sektorunabhängigen, horizontalen Mindestanforderungen vor (Art. 75 Abs. 1 EUSA)
>> Im Übrigen ist eine Anwendung der NIS-2-Richtlinie aber nicht ausgeschlossen

Verhältnis CER-Richtlinie und EU Space Act:
Für *kritische Einrichtungen* gemäß CER-Richtlinie gilt:
>> CER-Richtlinie findet neben dem EU Space Act Anwendung
>> Nationales Recht, das die CER-Richtlinie umsetzt oder damit zusammenhängt (insbesondere KRITIS-DachG, indirekt auch BSIG, BSI-KritisV) ist neben dem EU Space Act anwendbar und von den Betreibern kritischer Anlagen zu beachten
>> Besondere Anforderungen an Risikomanagementmaßnahmen von Betreibern kritischer Anlagen: insbesondere Systeme zur Angriffserkennung (§ 31 Abs. 2 BSIG)

EU Space Act (Entwurf)

Entwurf vom 5. Dezember 2025: Art. 75 und 75a EUSA

- Verhältnis zu NIS-2-Richtlinie (Art. 75 Abs. 1 EUSA) – Parallelität
- Verhältnis zu CER-Richtlinie (Art. 75 Abs. 2 EUSA) – Parallelität

- Cybersicherheitsanforderungen für wichtige und wesentliche Einrichtungen gemäß NIS-2-RL:
  - Durchführungsrechtsakt der Kommission
  - Mindestens Anforderungen gemäß Art. 21 Abs. 2 NIS-2-Richtlinie

  >> Auf den ersten Blick: Synergie / Vereinheitlichung der Cybersicherheitsanforderungen

  >> Aber: Inhalt des KOM-Rechtsakts entscheidend, kann auch darüber hinausgehen

- Cybersicherheitsanforderungen für sonstige Betreiber von Weltraummissionen oder Anbieter von weltraumbasierten Daten, inkl. Drittlandsbetreiber und -anbieter, internationale Organisationen und EU-Betreiber von unionseigenen Ressourcen (Art. 75a):
  - Spezifische Cybersicherheits-Anforderungen (Art. 75a Abs. 4 EUSA)
  - Anforderungen ähneln jedoch aktuell stark den Anforderungen an NIS-2-Richtlinie

  >> Unklar, warum Anforderungen strukturell anders sein sollen, sich dann aber doch annähern (ohne identisch zu sein)

Cyberresilienz-Verordnung (CRA)

Einheitlicher EU-Rechtsrahmen für Cybersicherheitsanforderungen an Produkte mit digitalen Elementen (PDE)

- CRA ist in Kraft, produktbezogene Cybersicherheits-Anforderungen gelten aber erst ab dem **11. Dezember 2027**
- PDE sind in verschiedene **Stufen** (normal, wichtig, kritisch) und **Klassen** eingeteilt: **Wichtige PDE** (z.B. Identitätsmanagement, Firewalls), **Kritische PDE** (z.B. Hardwaregeräte mit Sicherheitsboxen)
- CRA gilt für **Hersteller,** Distributoren, Importeure, Händler

>> Hauptverantwortung während gesamten Lebenszyklus beim Hersteller.

- Lieferanten und Unterlieferanten: indirekt betroffen, da der Hersteller zur **Lieferkettensicherheit** verpflichtet ist.

Ausgewählte Cybersicherheitsanforderungen an die Eigenschaften von PDE und Behandlung von Schwachstellen:

- Sichere Standardkonfiguration (*security by default*)
- Schwachstellenmanagement einschließlich regelmäßige Sicherheitsaktualisierungen
- Zugriffskontrolle (IAM)
- Verschlüsselung
- Datenintegrität, Datenminimierung
- Verfügbarkeit wesentlicher Funktionen, Minimierung negativer Auswirkungen auf andere Geräte
- Möglichst geringe Angriffsflächen (*security by design*)

Mapping gesetzlicher Cybersicherheits-Anforderungen

Anforderung	EUSA (i.d.F.v. 25.6.2025) (Art. 76–95)	BSIG (i.d.F.v. 5.12.2025) (§§ 28-42)	CRA (Art. 13 i.V.m. Anhang I)
Risikomanagementsystem (ISMS / RMS)	Verpflichtung zur Einrichtung, Umsetzung und Aufrechterhaltung eines risikobasierten Managementsystems über den gesamten Missions- und Lebenszyklus hinweg (Art. 76 Abs. 1, 5, 6)	Verpflichtung zu risikobasierten Maßnahmen nach dem Stand der Technik (§ 30 Abs. 1 u. 2); besondere Pflichten für KRITIS (§ 31)	Verpflichtung zur Durchführung einer Cybersicherheits-Risikobewertung als Grundlage aller Produktanforderungen (Art. 13 Abs. 2)
Governance / Verantwortung der Leitung	Leitungsorgan haftet für Umsetzung und Überwachung der Maßnahmen (Art. 77 Abs. 1)	Geschäftsleitung ist für Umsetzung und Überwachung verantwortlich (§ 38 Abs. 1)	Hersteller trägt Gesamtverantwortung für Konformität (Art. 13 Abs. 1)
Identitäts- und Zugangsmanagement	Verpflichtung zu IAM-Protokollen (Art. 81 Abs. 1)	Zugriffskontrolle und MFA verpflichtend (§ 30 Abs. 2 Nr. 10, 11)	Schutz vor unbefugtem Zugriff verpflichtend (Anhang I Nr. 1 d)
Kryptographie und Schlüsselmanagement	Detaillierte Vorgaben inkl. Ende-zu-Ende-Authentifizierung (Art. 85)	Pflicht zu Konzepten für kryptographische Verfahren (§ 30 Abs. 2 Nr. 8)	Verschlüsselung als zentrale Sicherheitsmaßnahme (Anhang I Nr. 1 e)
Backup und Recovery	Pflicht zu Backup- und Wiederherstellungsstrategien (Art. 86)	Pflicht zu Backup und Notfallwiederherstellung (§ 30 Abs. 2 Nr. 4)	Sicherstellung der Verfügbarkeit nach Vorfällen (Anhang I Nr. 1 h)
Business Continuity / Krisenmanagement	Verpflichtende Reaktions- und Wiederherstellungspläne (Art. 87)	Bestandteil der Risikomanagementmaßnahmen (§ 30 Abs. 2 Nr. 3)	Mittelbar durch Verfügbarkeits- und Updatepflichten sowie gemäß Anhang I Nr. 1 h)
Tests und Prüfungen	Verpflichtendes Prüf- und Testprogramm (Art. 88)	Nachweis- und Prüfpflichten (§§ 35–37)	Regelmäßige Sicherheitsüberprüfungen (Anhang I Nr. 2)
Schulungen und Awareness	Verpflichtende Schulungen (Art. 89)	Schulungs- und Sensibilisierungspflichten (§ 30 Abs. 2 Nr. 8)	Nicht ausdrücklich
Incident- und Schwachstellenmanagement	Meldepflichten und Incident-Handling-Prozesse (Art. 78 Abs. 1 c) und Art. 91, 93)	Melde-, Nachweis- und Informationspflichten (§ 32)	Umfassendes Vulnerability-Management inkl. SBOM (Art. 14, Anhang I Teil II Ziffer 1)
Lieferketten-Risikomanagement	Verpflichtender Lieferketten-Risikomanagement-Rahmen (Art. 92, Anhang VII Nr. 6)	Pflicht zur Berücksichtigung der Lieferkette (§ 30 Abs. 2 Nr. 4)	Hersteller haftet für Cybersicherheit entlang der Lieferkette (CRA fokussiert auf SBOM)

Europäisches System für Cybersicherheitszertifizierung

Rechtsakt zur Gründung der Europäischen Cybersicherheitsagentur (ENISA) stellt Grundlage dar für Einführung europäischer Schemata für Cybersicherheitszertifizierung

- **EUCC: EU-Schema auf der Grundlage Gemeinsamer Kriterien** (*Common Criteria*), gilt für Produkte der Informations- und Kommunikationstechnik
- Gegenstand einer Zertifizierung können sein:
  - **IKT-Produkt**
  - **IKT-Dienst**
  - **IKT-Prozess**
  - **verwalteter Sicherheitsdienst**
- Die Zertifizierung erfolgt *grundsätzlich* **auf freiwilliger Basis**.
- Soweit IKT-Produkte, IKT-Dienste, IKT-Prozesse, und/oder verwaltete Sicherheitsdienste zertifiziert wurden, gilt die **Vermutung**, dass diese den Anforderungen des angewandten Schemas, d.h. des EUCC, genügen.

Mögliche Synergien:

>> In Art. 27 CRA, Art. 24 NIS-2-Richtlinie, und Art. 85 Abs. 4 EUSA ist vorgesehen, Zertifizierung und Erfüllung rechtlicher Anforderungen zu verknüpfen (vorbehaltlich nationaler Regelungen und KOM-Rechtsakte).

>> § 30 Abs. 6 BSIG: (Besonders) wichtige Einrichtungen dürfen bestimmte IKT-Produkte, -Dienste und Prozesse nur verwenden, wenn diese über eine Cybersicherheitszertifizierung gemäß europäischer Schemata verfügen.

>> Einrichtungs-bezogene Cybersicherheitsanforderungen sind damit aber nicht erfasst.

Bisherige Ergebnisse in Arbeitsthesen

1. EU Space Act (Erster Entwurf der Kommission) enthält bislang die detailliertesten Resilienz- und Cybersicherheitsanforderungen.
2. Spezifische Anforderungen sind grundsätzlich gerechtfertigt durch Besonderheiten im Sektor Weltraum.
3. Mindestanforderungen durch NIS-2-Richtlinie führen tendenziell zu unterschiedlichen Schutzniveaus in den EU-Mitgliedstaaten.
4. National höhere Anforderungen dienen der Cybersicherheit, sind aber potenziell negativ für die wirtschaftlichen Akteure in diesen Mitgliedstaaten.
5. Einheitlicher, sektorspezifischer Rechtsrahmen für Cybersicherheit im Weltraumbereich wäre daher sinnvoll.
6. Ermöglichung entweder durch eigenständigen EU-Rechtsakt und spezifischen Durchführungsrechtsakten (Erster Vorschlag EUSA) ODER durch Nutzung europäischer Standards, die die technischen und organisatorischen Maßnahmen enthalten und die Vermutung enthalten, dass bei deren Erfüllung auch die gesetzlichen Anforderungen (EUSA, NIS 2, BSIG, CRA) erfüllt sind.
7. EU-Schemata mit einheitlichen Cybersicherheitsanforderungen können helfen, die teils parallel existierenden gesetzlichen Anforderungen zu erfüllen und die Erfüllung durch Zertifizierung nachzuweisen; hierfür bedarf es geeigneter Schemata und entsprechender KOM-Rechtsakte / nationaler Rechtsakte, die diese als anerkennen und die Erfüllungsvermutung für die gesetzlichen Anforderungen statuieren.

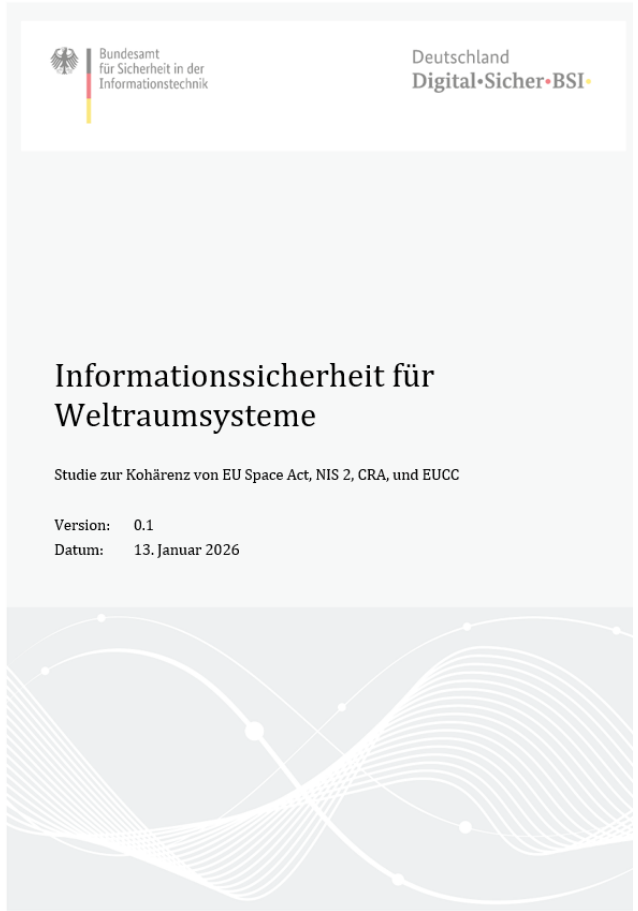
*Alternativ oder ergänzend gibt es schon heute **Technische Richtlinien** und **Schutzprofile** des BSI, die die aktuelle Lücke füllen können.*

HOW TO – Operative Nutzung der BSI-Dokumente

Anleitung zur effizienten Umsetzung gesetzlicher / regulatorischer Anforderungen

Mapping der einzelnen Anforderungen in den BSI-Dokumenten mit den gesetzlichen und regulatorischen Anforderungen

- **Anlagen** zur Studie
- Aktuell im **Entwurfsstadium**
- Zur **Veröffentlichung** geplant, abrufbar über Website Expertenkreis Cybersicherheit im Weltraum (Link via QR Code)



IT-Grundschutz-Profil und Technische Richtlinie

Dokumente direkt von bsi.de:

Frage:
Können die Dokumente zur Rechtsicherheit beitragen?

Vom abstrakten Paragraphen zum konkreten Handeln

Gesetzliche Anforderung (BSIG)	TR-03184-1/2 Maßnahmen - Profile	Konformität
Anforderungen an besonders wichtige und wichtige Einrichtungen:		
§ 30 Abs. 1 Nr. 1: Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik	Kap.6 Risikobehandlung von Gefährdungen, Kap. 5 (Schutzbedarfsfeststellung), Kap. 10.4 Risikomanagement	[++] Erfüllt
§ 30 Abs. 1 Nr. 2: Maßnahmen zur Bewältigung von Sicherheitsvorfällen	BM8, BM19, BM59, DER.1, DER.2.1	[+] Erfüllt
§ 30 Abs. 1 Nr. 3: Aufrechterhaltung des Betriebs, wie Backup-Management und Wiedererstellung nach einem Notfall, und Kr		[++] Erfüllt*
§ 30 Abs. 1 Nr. 4: Sicherheit der Lieferkette einsch sicherheitsbezogener Aspekte der Beziehungen z oder Diensteanbietern		[+] Teilweise erfüllt
§ 30 Abs. 1 Nr. 5: Sicherheitsmaßnahmen bei Erw Wartung von informationstechnischen Systemen, Prozessen, einschließlich Management und Offen		[++] Erfüllt
§ 30 Abs. 1 Nr. 6: Konzepte und Verfahren zur Bev von Risikomanagementmaßnahmen im Bereich d Informationstechnik		[++] Erfüllt
§ 30 Abs. 2 Nr. 7: Grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sich Informationstechnik		[++] Erfüllt
§ 30 Abs. 1 Nr. 8: Konzepte und Prozesse für den kryptographischen Verfahren		[++] Erfüllt
§ 30 Abs. 1 Nr. 9: Erstellung von Konzepten für die die Zugriffskontrolle und für die Verwaltung von und -Prozessen		[++] Erfüllt
§ 30 Abs. 1 Nr. 10: Verwendung von Lösungen zur Authentifizierung oder kontinuierlichen Authenti Sprach-, Video- und Textkommunikation sowie ge Notfallkommunikationssysteme innerhalb der Einrichtung	BM45, ORP.4	[+] Teilweise erfüllt*
Zusätzliche Anforderungen an Betreiber kritischer Anlagen:		
§ 31 Abs. 2: Einsatz von Systeme zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen.	BM59	[o]*

§ 30 Abs. 1 Nr. 2: Maßnahmen zur **Bewältigung von Sicherheitsvorfällen**

§ 30 Abs. 1 Nr. 3: **Aufrechterhaltung des Betriebs**, wie Backup-Management und **Wiederherstellung nach einem Notfall, und Krisenmanagement**

§ 30 Abs. 1 Nr. 4: **Sicherheit der Liefer**kette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern

Vorfallbehandlung (§ 30 Abs. 1 Nr. 2)

- **Detektion: BM8 (IDS/IPS Systeme)** Einsatz von Host- oder Netzwerk-Intrusion Detection/ Prevention Systemen (signaturbasiert oder Anomalie basiert)

- **Analyse: BM19 (Regelmäßiges Prüfen von Logginginformationen/-protokollen)**
  Implementierung und Umsetzung der entsprechenden Prozesse zu Art und Häufigkeit des Auditings sowie toolgestütze Überprüfung und Auswertung von Logginginformationen im Rahmen des Auditings

- **Reaktion: BM59 (SIEM/SOC)**
  Zentrales Incident Management& Resonse (SIEM/SOC) angelehnt an IT-Grundschutz DER.1 gemäß BM59.

Geschäftskontinuität (§ 30 Abs. 1 Nr. 3)

- **Resilienz: BM16 (Redundanzsystem)**
  Sicherstellung der Verfügbarkeit und Funktionsfähigkeit z.B. auch durch Wiederherstellung von Datenbeständen

- **Planung: BM22 (Notfallkonzept)**
  Beachtung des BSI 200-4 Standards; gelebte Umsetzung des Konzepts z.B. durch sensibilisieren des Personals

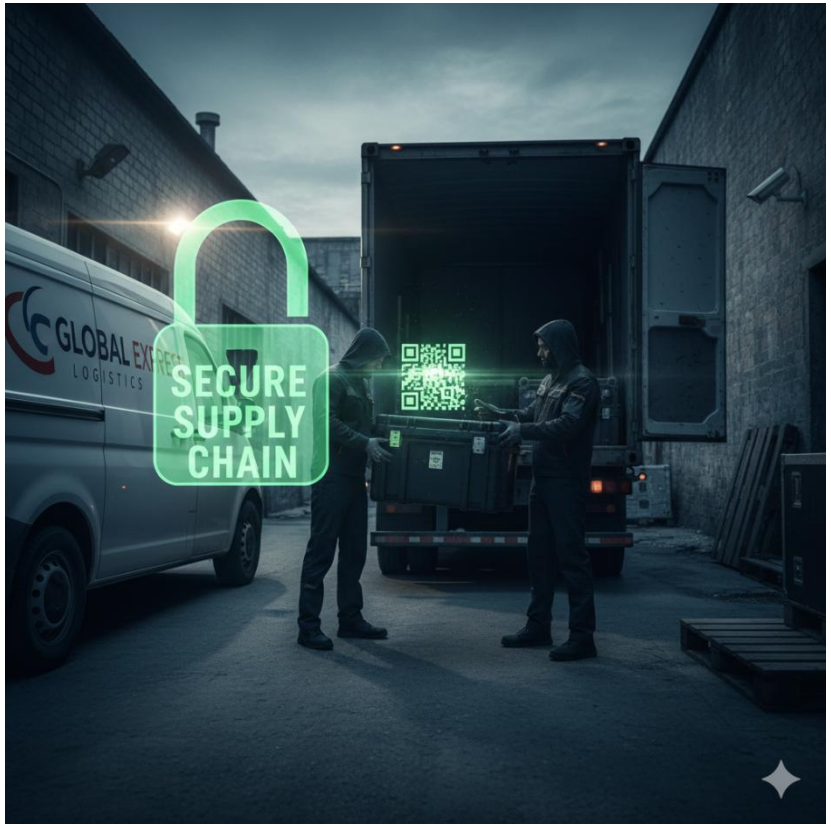
- **Ziel:** Einhaltung definierter Wiederherstellungszeiten für den Betrieb.

Lieferkettensicherheit (§ 30 Abs. 1 Nr. 4)

- **Produktprüfung: BM5 (Software-Integritätscheck)**
  Sicherstellung der Integrität durch technische Maßnahmen (z.B. Hashsumme) und organisatorische Maßnahmen (z.B. versiegelte Briefe, persönliche Übergabe) sowie Auditierung der Zulieferer

- **Lieferantenprüfung: BM36 (Softwarelieferanten prüfen)**
  Überprüfung der Software-Lieferkette z.B. VS-Belehrung

- **Logistik: BM32 (Vertrauenswürdiger Transport)**
  Sicherstellung vertrauenswürdiger Transporte durch Sicherheitsüberprüfungen des Personals



Zusammenfassung– Vom Paragraphen zum konkreten Handeln

Herausforderung:

- „vage Gesetzestexte“
- „Komplexität“
- „Unklare Prüfungsziele“

Lösung?

- Fundament der Compliance
- Schutzbedarfsfeststellung als Hebel
- Präzision durch Profil und TR
- „Audit-Readiness“

→ Die Profile und TR machen Cybersicherheit im Weltraumsektor messbar und prüfbar

Fragen?

Kontakt

Dr. Holger A. Kastler

holger.kastler@dlapiper.com

DLA Piper
Maximilianstr. 2
80539 München

Sascha Fankhänel

sascha.fankhaenel@jade-hs.de

Jade Hochschule
Friedrich-Paffrath-Str. 101
26386 Wilhelmshaven

Dr. Johanna Niecknig

johanna.niecknig@bsi.bund.de
xprt-space@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87

53175 Bonn

www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

Follow us: