bitkom

Stellungnahme

Juni 2026

Anforderungen nach § 39 Absatz 2 BSIG: Grundsätzliche Anforderungen im Nachweisverfahren (GAiN)

Zusammenfassung

Die Resilienz Kritischer Infrastrukturen gegenüber Cyberbedrohungen gewinnt angesichts der angespannten geopolitischen Lage, der fortschreitenden Digitalisierung und der zunehmenden Vernetzung von IT- und OT-Systemen weiter an Bedeutung. Gleichzeitig befindet sich der regulatorische Rahmen für Betreiber Kritischer Infrastrukturen in einem kontinuierlichen Wandel. Mit dem vorliegenden Entwurf der Version 2.2 der »Grundsätzlichen Anforderungen im Nachweisverfahren« (GAiN) verfolgt das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Ziel, die Anforderungen an die geänderten gesetzlichen Rahmenbedingungen anzupassen, bestehende Verfahren weiterzuentwickeln und die Rolle von Prüfungen und Zertifikaten im Nachweisverfahren näher zu konkretisieren.

Bitkom begrüßt die Möglichkeit, sich im Rahmen der Anhörung gemäß § 39 Absatz 2 BSIG zu dem Entwurf zu äußern. Als Branchenverband der deutschen Digitalwirtschaft vertritt Bitkom Unternehmen aller Größenordnungen, darunter zahlreiche Betreiber Kritischer Infrastrukturen, Anbieter digitaler Technologien sowie Prüf- und Sicherheitsdienstleister. Die Novellierung der GAiN auf Version 2.2 ist insgesamt ein wichtiger Schritt, um das Nachweisverfahren an die neue Rechtslage heranzuführen und zugleich praxisnäher auszugestalten. Positiv hervorzuheben sind insbesondere der erkennbare Ansatz zum Bürokratieabbau, etwa durch die Streichung mehrerer Anforderungen, die Reduzierung der Wiedervorlagepflicht für den Geltungsbereich bei Folgeprüfungen, die ausdrückliche Öffnung für die Interne Revision als prüfende Stelle sowie die erstmalige systematische Regelung der Verwendung bestehender Prüfungen und Zertifikate im Nachweisverfahren.

Entscheidend ist dabei, dass die Anforderungen des Nachweisverfahrens zu einer tatsächlichen Verbesserung der Cybersicherheit beitragen, ohne unnötige bürokratische Belastungen oder Doppelstrukturen zu schaffen. Bestehende Prüf- und

Zertifizierungsverfahren sollten dort, wo sie gleichwertige Sicherheitsnachweise ermöglichen, angemessen berücksichtigt werden. Gleichzeitig sind klare Anforderungen und eine konsistente Auslegung wichtige Voraussetzungen für Rechts- und Planungssicherheit bei Betreibern und prüfenden Stellen.

Zugleich besteht an mehreren Stellen Präzisierungs- und Korrekturbedarf, damit das mit der Novelle verfolgte Ziel einer Verschlankung und sinnvollen Anrechnung vorhandener Prüfungen in der Praxis tatsächlich erreicht wird. Dies betrifft insbesondere die vorgesehene Anrechnung bestehender Zertifikate: Wird diese an das Vorliegen eines gültigen, eignungsfestgestellten Branchenspezifischen Sicherheitsstandards gebunden, können Branchen ohne entsprechenden B3S faktisch von der Entlastungswirkung ausgeschlossen werden. Auch die Regelungen zur Unabhängigkeit konzernverbundener prüfender Stellen sollten funktional gefasst und an anerkannte Prüfungs- und Auditstandards anschlussfähig ausgestaltet werden.

Darüber hinaus sollte der Entwurf an einzelnen Stellen stärker auf Konsistenz und Praxistauglichkeit ausgerichtet werden. Dies gilt etwa für das Sprachregime, wenn Prüfberichte in deutscher oder englischer Sprache zulässig sind, Nachweisbestandteile jedoch grundsätzlich deutsch einzureichen sind. Ebenso sollte das Verhältnis der Vorgaben zu Risikoakzeptanz und Risikotransfer zur risikobasierten Steuerung und zu bestehenden Instrumenten der Praxis klarer gefasst werden. Auch beim 4-Augen-Prinzip sollte geprüft werden, ob starre zeitliche Vorgaben durch wirksamkeitsorientierte Kriterien ersetzt oder jedenfalls flexibilisiert werden können.

Vor diesem Hintergrund sollten insbesondere die Anrechnung bestehender Zertifikate praxistauglicher ausgestaltet, das Sprachregime vereinheitlicht, die Unabhängigkeitsanforderungen für Konzernstrukturen funktional gefasst und starre Vorgaben im Rahmen des 4-Augen-Prinzips flexibilisiert werden. Weitere Hinweise dienen der Präzisierung, der redaktionellen Bereinigung und der besseren Anschlussfähigkeit an den anerkannten Stand der Prüfungs- und Auditstandards.

Im Folgenden nimmt Bitkom zu den einzelnen Regelungsvorschlägen Stellung. Die Anmerkungen orientieren sich an der Struktur des Entwurfs und beziehen sich jeweils auf die entsprechenden Anforderungen und Regelungspunkte.

Kapitel 1: Grundlage

Die GAiN adressiert die Verfahrensebene, also die Frage, wie Prüfungen durchgeführt und Nachweise erbracht werden. Sie regelt hingegen nicht die konkrete Maßnahmenebene. Dass der Entwurf für die Maßnahmen auf §§ 30, 31 BSIG sowie die RUN verweist, ist daher sachgerecht. Für die Durchführung der Prüfungen selbst bleibt der Entwurf jedoch hinter dem etablierten Stand der Technik zurück, da er kaum Bezug auf anerkannte Audit- und Assurance-Standards nimmt.

Gerade auf der Verfahrensebene bestehen bereits einschlägige und bewährte Standards, die für eine nachvollziehbare, unabhängige und qualitätsgesicherte Prüfung herangezogen werden sollten. Dazu zählen insbesondere ISO/IEC 17021-1 mit Vorgaben zu Unparteilichkeit, Kompetenz und Unabhängigkeit, ISO/IEC 27006-1 zur Akkreditierung von ISMS-Zertifizierungen sowie ISO 19011 zur Auditierung von

Managementsystemen. Ebenfalls relevant sind ISAE 3000 (rev.) bzw. IDW PS 860 als Grundlage des C5-Testats, ISAE 3402 / IDW PS 951 sowie für die Interne Revision die Global Internal Audit Standards des IIA, IDW PS 983 und der DIIR-Revisionsstandard Nr. 3.

Zudem sollte klargestellt werden, wie Betreiber die prüfende Stelle zur Einhaltung der GAiN-Anforderungen verpflichten sollen. In der Praxis erfolgen Prüfungen und Zertifizierungen regelmäßig auf Grundlage bestehender Vertragswerke, AGB und Zertifizierungsbedingungen der prüfenden Stellen bzw. Konformitätsbewertungsstellen. Die GAiN sollte daher keine unklaren oder widersprüchlichen vertraglichen Pflichten erzeugen, sondern festlegen, dass die erforderliche Verpflichtung der prüfenden Stelle in geeigneter, nachweisbarer Form erfolgen kann, soweit dies mit den einschlägigen Prüf- und Zertifizierungsbedingungen vereinbar ist.

Bei inhaltlichen Überschneidungen oder möglicher Unanwendbarkeit ist das BSI »unverzüglich« zu informieren und der Einzelfall vorzulegen; eine spätere Berufung auf die Unsicherheit soll »nicht zulässig« sein. Damit wird das Auslegungsrisiko vollständig auf Betreiber und Prüfteam verlagert, ohne eine Reaktionsfrist des BSI vorzusehen. In einem dreijährigen Nachweiszyklus mit fixem Stichtag nach § 39 Abs. 1 BSIG entsteht dadurch ein praktisches Terminrisiko.

Änderungsvorschlag: Es sollte in Kapitel 1 klargestellt werden, dass die Prüfungsdurchführung an den genannten anerkannten Audit-/Assurance-Standards auszurichten ist und die GAiN-Anforderungen diese ergänzen bzw. KRITIS-spezifisch konkretisieren. Zudem sollte präzisiert werden, in welcher geeigneten und nachweisbaren Form Betreiber prüfende Stellen zur Einhaltung der GAiN-Anforderungen verpflichten können, ohne Widersprüche zu bestehenden Vertrags-, AGB- oder Zertifizierungsbedingungen zu erzeugen.

Das BSI sollte eine angemessene Orientierungsfrist für eine Rückmeldung vorsehen und klarstellen, dass eine fristgerechte, dokumentierte Auslegung nach bestem Wissen nicht zu Lasten des Betreibers geht, solange das BSI nicht entschieden hat.

Kapitel 2: Prüfende Stelle und Prüfer

P.UP.01 & P.UP.02

P.UP.01 erklärt Stellen für ungeeignet, die »über geteilte Unternehmens- oder Konzernstrukturen mit dem Betreiber verbunden sind«. Damit sieht der Entwurf einen strukturellen Pauschalausschluss vor, der unabhängig davon greift, ob im konkreten Fall tatsächlich eine Gefährdung der Unabhängigkeit oder Unparteilichkeit besteht. Dies kann insbesondere in international aufgestellten Konzernen dazu führen, dass fachlich geeignete und organisatorisch hinreichend getrennte Prüf- oder Auditfunktionen ausgeschlossen werden, obwohl wirksame Vorkehrungen zur Vermeidung von Interessenkonflikten bestehen.

Der etablierte Stand der Technik setzt demgegenüber auf eine risikobasierte und funktionsbezogene Betrachtung. ISO/IEC 17021-1 verlangt die Identifikation, Analyse

und Behandlung von Interessenkonflikten, etwa durch das Verbot von Beratung und Auditierung desselben Gegenstands, klare Funktionstrennung, Weisungsunabhängigkeit in Prüfungsfragen sowie geeignete dokumentierte Safeguards. Konzernverbundene Stellen werden dabei nicht generell ausgeschlossen, sofern die Unparteilichkeit nachweislich gewahrt ist. Auch die EU-Abschlussprüferregulierung nach VO 537/2014 arbeitet mit konkreten Leistungsverboten, Unabhängigkeitsanforderungen und Rotation, nicht jedoch mit einem pauschalen Ausschluss aufgrund bloßer Konzernzugehörigkeit.

Der Entwurf geht damit über den Stand der Technik hinaus. Zugleich entsteht eine Wertungsinkonsistenz, da P.IR.01 die konzerninterne Interne Revision ausdrücklich zulässt. Diese Differenzierung sollte aufgelöst werden, indem nicht die gesellschaftsrechtliche Zugehörigkeit als solche, sondern die tatsächliche Sicherstellung von Unabhängigkeit, Unparteilichkeit und fachlicher Prüfungsqualität maßgeblich ist.

Für konzerninterne Einheiten sollte daher klargestellt werden, dass sie als hinreichend unabhängig gelten können, wenn organisatorische Trennung, Weisungsunabhängigkeit in Prüfungsfragen und ein anerkanntes Audit-Compliance-Rahmenwerk nachgewiesen sind, etwa auf Basis der Global Internal Audit Standards des IIA. Soweit für die Interne Revision nach P.IR.01 bzw. N.IR.01 ein Quality Assessment nach IDW PS 983 oder DIIR 3 als Wirksamkeitsnachweis verlangt wird, sollten zudem gleichwertige internationale QA-Verfahren, insbesondere externe IIA-Quality-Assessments, ausdrücklich anerkannt werden. Dies trägt der Praxis multinationaler Konzernstrukturen Rechnung und vermeidet parallele, rein national ausgerichtete Nachweisprozesse, ohne das Schutzniveau abzusenken.

Änderungsvorschlag: P.UP.01 und P.UP.02 sollten funktional statt strukturell gefasst werden. Unzulässig sollten nur solche Konstellationen sein, in denen die Unabhängigkeit oder Unparteilichkeit der prüfenden Stelle nicht durch geeignete, nachgewiesene Vorkehrungen sichergestellt werden kann. Eine bloße Unternehmens- oder Konzernzugehörigkeit sollte für sich genommen nicht zur Ungeeignetheit führen.

Konzernverbundene oder konzerninterne Stellen sollten als geeignet anerkannt werden können, wenn sie insbesondere folgende Voraussetzungen nachweisen:

- organisatorische und funktionale Trennung von beratenden, operativen oder umsetzungsverantwortlichen Einheiten,
- Weisungsunabhängigkeit in Prüfungs- und Bewertungsfragen,
- Ausschluss der Prüfung eigener Beratungs- oder Implementierungsleistungen,
- dokumentierte Verfahren zur Identifikation, Bewertung und Behandlung von Interessenkonflikten,
- ein anerkanntes Audit-Compliance- oder Qualitätssicherungsrahmenwerk, etwa auf Basis der Global Internal Audit Standards des IIA.

Ergänzend sollte bei P.IR.01 und N.IR.01 klargestellt werden, dass neben Quality Assessments nach IDW PS 983 oder DIIR 3 auch gleichwertige internationale QA-Verfahren, insbesondere externe Quality Assessments nach den Standards des IIA, als

Wirksamkeitsnachweis anerkannt werden können. Damit würde die Systematik von P.UP.01/P.UP.02 an die Logik von P.IR.01 angeglichen und zugleich eine praxistaugliche, international anschlussfähige und risikobasierte Nachweisführung ermöglicht.

P.UP.03

Die Leitung des Prüfteams muss spätestens nach drei Prüfzyklen wechseln, faktisch also nach neun Jahren, darf jedoch im Prüfteam verbleiben. Dieser Ansatz ist sachgerecht und mit dem Rotationsgedanken des Berufsrechts vergleichbar, etwa der externen Rotation des verantwortlichen Wirtschaftsprüfers grundsätzlich nach längstens zehn Jahren gemäß EU-VO 537/2014. Klärungsbedarf besteht allerdings beim Begriff »Prüfzyklus«.

Änderungsvorschlag: Die Regelung wird begrüßt; zugleich sollte die Definition »Prüfzyklus« (Bezug auf die anlagenbezogene Dreijahresperiode) klargestellt sowie um eine Übergangsregel für laufende Mandate ergänzt werden.

P.UP.04

Das Prüfteam muss in seiner Gesamtheit über Audit-, Prüfverfahrens-, Informationssicherheits- sowie Sektor- und Branchenkompetenz verfügen. Die zusätzlich geforderte »Prüfverfahrenskompetenz für § 39 BSIG« bleibt jedoch undefiniert.

Für eine praxistaugliche Umsetzung sollten bestehende Kompetenzanforderungen aus ISO 19011 und ISO/IEC 27006-1 anrechenbar sein. Zugleich ist für Personalplanung und Qualifikationsnachweise Transparenz darüber erforderlich, welches Niveau und welche Nachweise für die zusätzliche Prüfverfahrenskompetenz erwartet werden.

Änderungsvorschlag: Ein Verweis auf eine konkretisierende Quelle (z. B. Orientierungshilfe/Anforderungsprofil) und eine Klarstellung, dass einschlägige Auditorenqualifikationen (z. B. ISO/IEC 27001 Lead Auditor) angerechnet werden können, sollte aufgenommen werden.

2.2 Anforderungen an die Interne Revision als prüfende Stelle

P.IR.01 & N.IR.01

Interne Revisionen dürfen abweichend von P.UP.01/02 als prüfende Stelle handeln, wenn ein wirksames Revisionssystem und die Einhaltung der IIA Global Internal Audit Standards nachgewiesen werden. Die Bestätigung soll über ein höchstens fünf Jahre altes Quality Assessment nach IDW PS 983 oder DIIR-Revisionsstandard Nr. 3 erfolgen.

Diese Öffnung ist begrüßenswert und steht im Einklang mit dem Three-Lines-Modell sowie der etablierten Combined-Assurance-Praxis. Klärungsbedürftig bleibt jedoch das Verhältnis zur fachlichen Mindestkompetenz nach P.UP.04, insbesondere mit Blick auf

IT-Sicherheits- und Branchenkompetenz, sowie zur organisatorischen Unabhängigkeit der Internen Revision vom jeweils geprüften Bereich.

Änderungsvorschlag: P.IR.01/N.IR.01 werden ausdrücklich unterstützt. Zugleich sollte der Verweis in N.IR.01 (richtig: § 39 Abs. 1 BSIG) korrigiert und klargestellt werden, dass die Kompetenzanforderungen nach P.UP.04 auch für die Interne Revision gelten und durch Hinzuziehung interner oder externer Fachexpertise erfüllbar sind.3 Prüfung und Nachweis

3.1 Allgemeine Anforderungen an die Nachweisprüfung

D.PA.02

D.PA.02 verlangt, dass alle Themenbereiche mit einer für das jeweilige Prüfobjekt geeigneten Prüfmethode und Prüfdauer betrachtet werden. Unklar bleibt jedoch, welche Prüfmethoden im Einzelnen zugrunde zu legen sind und nach welchen Kriterien ihre Eignung zu bestimmen ist. Ohne eine verbindliche oder zumindest klarstellende Definition besteht das Risiko unterschiedlicher Auslegungen durch prüfende Stellen. Dies kann die Vergleichbarkeit der Prüfnachweise beeinträchtigen und zusätzlichen Abstimmungsaufwand für Betreiber und Prüfteam erzeugen.

Änderungsvorschlag: D.PA.02 sollte um eine Definition oder Konkretisierung der zulässigen Prüfmethoden ergänzt werden. Das BSI sollte klarstellen, welche Prüfmethoden zugrunde gelegt werden können und nach welchen Kriterien deren Eignung für das jeweilige Prüfobjekt zu bestimmen ist.

D.PA.05

Relevante Risiken im Geltungsbereich dürfen nicht akzeptiert oder transferiert werden, soweit geeignete und wirksame technische und organisatorische Maßnahmen nach § 30 Abs. 1 Satz 1 BSIG möglich und ihre Umsetzung verhältnismäßig sind. Die KRITIS-spezifische Einschränkung ist im Grundsatz nachvollziehbar: Gebotene und verhältnismäßige Schutzmaßnahmen dürfen nicht durch Risikoakzeptanz oder Risikoverlagerung ersetzt werden.

Gleichzeitig kennen etablierte Ansätze der risikobasierten Steuerung, etwa ISO/IEC 27005 und ISO 31000, Risikoakzeptanz und Risikotransfer als legitime Optionen des Risikomanagements. Vor diesem Hintergrund sollte klarer abgegrenzt werden, dass die Anforderung nicht die risikobasierte Steuerung als solche einschränkt, sondern ausschließlich verhindern soll, dass erforderliche technische und organisatorische Maßnahmen unterbleiben.

Unklar bleibt zudem, wie der Begriff »relevante Risiken« zu verstehen ist. Die derzeitige Formulierung könnte so interpretiert werden, dass nur solche Risiken relevant sind, die durch Maßnahmen nach § 30 Abs. 1 Satz 1 und Satz 2 BSIG erfüllt bzw. mitigiert werden können. Dies würde den Begriff der Relevanz zu eng und potenziell zirkulär

fassen. Maßgeblich sollte vielmehr sein, ob ein Risiko einen hinreichenden Bezug zur Erbringung der kritischen Dienstleistung und zu den KRITIS-Schutzzielen aufweist.

Ebenfalls klarstellungsbedürftig ist der Begriff des »Transfers«. Es sollte ausgeschlossen werden, dass darunter pauschal auch Cyberversicherungen oder Auslagerungen verstanden werden. Beide Instrumente können sinnvolle ergänzende Elemente eines Risikomanagements sein. Sie dürfen jedoch nicht an die Stelle erforderlicher, geeigneter und verhältnismäßiger technischer und organisatorischer Maßnahmen treten.

Änderungsvorschlag: D.PA.05 sollte dahingehend klargestellt werden, dass sich das Verbot der Risikoakzeptanz oder des Risikotransfers ausschließlich auf Fälle bezieht, in denen dadurch gebotene, geeignete und verhältnismäßige technische und organisatorische Maßnahmen nach § 30 Abs. 1 Satz 1 BSIG unterlassen oder ersetzt würden.

Versicherungen, vertragliche Risikoverlagerungen und Auslagerungen sollten ausdrücklich als ergänzende Maßnahmen zulässig bleiben, soweit sie erforderliche technische und organisatorische Maßnahmen nicht ersetzen und die Verantwortung des Betreibers für die Einhaltung der gesetzlichen Anforderungen unberührt bleibt.

Zudem sollte der Begriff »relevante Risiken« präzisiert werden. Relevante Risiken sollten solche Risiken sein, die einen konkreten Bezug zur Erbringung der kritischen Dienstleistung haben und die Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit der hierfür erforderlichen informationstechnischen Systeme, Komponenten, Prozesse oder Daten wesentlich beeinträchtigen können. Die Relevanz sollte damit nicht allein daran anknüpfen, ob ein Risiko durch Maßnahmen nach § 30 Abs. 1 Satz 1 und Satz 2 BSIG mitigiert werden kann, sondern an seinem Bezug zur kritischen Dienstleistung und zu den KRITIS-Schutzzielen.

D.PA.06

Im Nachweis nach § 39 Abs. 1 BSIG müssen Audits, Prüfungen und Zertifizierungen nach § 61 Abs. 1 BSIG sowie Nachweise nach § 61 Abs. 3 BSIG, die als bwE auf Anordnung erstellt wurden, nicht berücksichtigt werden. Die Trennung zwischen dem KRITIS-Nachweis nach § 39 BSIG und den bwE-Auditpflichten nach § 61 BSIG ist grundsätzlich hilfreich und schafft Abgrenzungsklarheit. Aus Betreibersicht wäre jedoch ergänzend eine wechselseitige Anrechenbarkeit wünschenswert, soweit inhaltsgleiche Anforderungen bereits geprüft wurden. Dies würde Doppelprüfungen vermeiden, ohne das Sicherheitsniveau abzusenken.

Änderungsvorschlag: Es sollte ausdrücklich erlaubt werden, dass inhaltlich überschneidende Ergebnisse aus § 61-Prüfungen auf freiwilliger Basis als Nachweisbestandteil verwendet werden dürfen.

3.2 Prüfgrundlage & 3.5 Dokumentation des Geltungsbereiches

Der Entwurf adressiert den zunehmenden Einsatz von Systemen der Künstlichen Intelligenz in kritischen Anlagen bislang nicht ausdrücklich. KI-Komponenten finden

sich heute unter anderem in Systemen zur Angriffserkennung und im Security-Monitoring, etwa bei anomaliebasierter Detektion oder SIEM/SOAR, in der Netz- und Anlagensteuerung, in der vorausschauenden Instandhaltung sowie in der Betrugs- und Missbrauchserkennung. Solche Systeme erweitern die Angriffsfläche, etwa durch Datenmanipulation, Model Poisoning, Prompt Injection oder fehlende Robustheit und Erklärbarkeit, und begründen neue Abhängigkeiten, die für die Nachweisprüfung relevant sind.

Für eine sachgerechte Einordnung sind insbesondere die EU-KI-Verordnung sowie einschlägige KI-Sicherheits- und Management-Standards maßgeblich. Der AI Act stuft KI als Sicherheitskomponente im Betrieb kritischer digitaler Infrastruktur als Hochrisiko-Anwendungsfall ein; daneben bieten ISO/IEC 42001, ISO/IEC 23894, ISO/IEC 22989, das NIST AI Risk Management Framework und der BSI-Kriterienkatalog AIC4 relevante Bezugspunkte. Eine maßvolle Verankerung in der GAiN würde Konsistenz zwischen KRITIS-Nachweis und KI-Compliance schaffen, ohne neue materielle Pflichten zu begründen.

Dabei sollte klargestellt werden, dass die GAiN keine über §§ 30/31 BSIG und den AI Act hinausgehenden KI-Pflichten schafft, sondern lediglich die Sichtbarkeit relevanter KI-Systeme im Nachweisverfahren sicherstellt. Bereits vorhandene KI-Governance-Artefakte, etwa KI-Inventare, Risikomanagement nach Art. 9 AI Act oder Konformitätsdokumentation, sollten als Nachweisbestandteile wiederverwendbar gemacht werden.

Änderungsvorschlag: Angeregt wird, in der GAiN eine schlanke, klarstellende Verankerung des Themas vorzunehmen: (1) Aufnahme der KI-Nutzung in die Dokumentation des Geltungsbereichs (siehe B.5a), (2) Berücksichtigung KI-spezifischer Risiken und Standards in der Prüfgrundlage (siehe B.9a) und (3) Anrechenbarkeit KI-bezogener Konformitätsnachweise im Rahmen von Abschnitt 3.6 (siehe B.13). Eine Doppelregulierung gegenüber dem AI Act ist dabei ausdrücklich zu vermeiden; Ziel ist Transparenz und Wiederverwendbarkeit vorhandener Nachweise.

D.PG.01–P.PG.04

Die Prüfgrundlage muss vier Ebenen abdecken: Basisanforderungen, KRITIS-spezifische, sektorspezifische und betreiberspezifische Anforderungen. Ein eignungsfestgestellter B3S darf nach D.PG.03 nicht alleinige Prüfgrundlage sein. Diese Schichtung ist grundsätzlich nachvollziehbar und entspricht der Logik etablierter Standards wie ISO/IEC 27001, ergänzt um KRITIS-spezifische, sektorspezifische und betreiberspezifische Konkretisierungen.

Unklar bleibt jedoch das Zusammenspiel mit N.BG.02. Nach D.PG.01 müssen Basisanforderungen anerkannten Standards entsprechen. Vor diesem Hintergrund ist nicht nachvollziehbar, weshalb Zertifikate künftig nur noch dann als Bestandteil des Nachweises verwendet werden dürfen, wenn ein B3S besteht. Dies könnte die Nutzung eines B3S faktisch verpflichtend machen, obwohl ein B3S grundsätzlich nicht verpflichtend sein soll.

Anerkannte internationale Sicherheitsstandards und Zertifizierungsschemata sollten als Bestandteil der Prüfgrundlage herangezogen werden können, sofern sie das nach

§§ 30, 31 BSIG geforderte Schutzniveau adressieren. Dies gilt insbesondere für ISO/IEC 27001 sowie vergleichbare branchenspezifische oder internationale Sicherheits- und Prüfschemata. Gerade in internationalen Konzern- und Lieferkettenstrukturen können bestehende Zertifizierungen und Prüfungen effizient eingebunden, Doppelprüfungen vermieden und regelmäßige Überprüfungen gestärkt werden.

Soweit KI-Systeme für die kritische Dienstleistung eingesetzt werden, sollten zudem einschlägige KI-spezifische Sicherheits- und Managementanforderungen berücksichtigt werden. Dazu zählen insbesondere Anforderungen an Robustheit, Daten- und Modellintegrität, Nachvollziehbarkeit, Monitoring und Lieferkette. Diese können auf der betreiber- bzw. sektorspezifischen Ebene der Prüfgrundlage abgebildet werden, etwa anhand von ISO/IEC 42001, ISO/IEC 23894, BSI AIC4 oder, soweit anwendbar, der VO (EU) 2024/1689.

Entscheidend sollte daher nicht sein, ob ein B3S verwendet wird, sondern ob die Prüfgrundlage vollständig, nachvollziehbar und prüffähig dokumentiert ist. Die Vollständigkeit einer selbst erstellten oder ergänzten Prüfgrundlage nach P.PG.04 sollte anhand einer transparenten Zuordnung der jeweiligen Anforderungen zu den vier Ebenen nachgewiesen werden.

Änderungsvorschlag: Es sollte klargestellt werden, wie D.PG.03 und N.BG.02 zusammenspielen. Ein B3S sollte als geeigneter, aber nicht zwingender Bestandteil der Prüfgrundlage verstanden werden. Zertifikate und anerkannte internationale Standards sollten unabhängig vom Bestehen eines B3S berücksichtigt werden können, sofern sie das geforderte Schutzniveau adressieren und die relevanten Anforderungen nachvollziehbar abdecken.

D.PG.01, D.PG.02 und P.PG.04 sollten klarstellen, dass internationale, anerkannte Sicherheitsstandards und -schemata als Bestandteil der Prüfgrundlage herangezogen werden können. Voraussetzung sollte sein, dass sie Anforderungen nach §§ 30, 31 BSIG abbilden und verbleibende Lücken durch KRITIS-spezifische, sektorspezifische oder betreiberspezifische Ergänzungen geschlossen werden.

Für den Einsatz von KI-Systemen sollte in D.PG.01 klargestellt werden, dass einschlägige KI-Sicherheits- und Managementanforderungen, etwa nach ISO/IEC 42001, ISO/IEC 23894 oder BSI AIC4, in der Prüfgrundlage zu berücksichtigen sind, soweit sie für die kritische Dienstleistung relevant sind. Eine eigenständige KI-Prüfmethodik sollte damit nicht eingeführt, sondern die bestehende Prüfgrundlagenlogik lediglich um die KI-Dimension geschärft werden.

Ergänzend sollte das BSI eine Hilfestellung oder Vorlage in Form eines Mapping-Schemas bereitstellen. Dieses sollte dokumentieren, welche Basisanforderungen, KRITIS-spezifischen, sektorspezifischen und betreiberspezifischen Anforderungen durch B3S, ISO/IEC 27001, KI-bezogene Standards, weitere Zertifizierungen oder zusätzliche Maßnahmen abgedeckt werden. Dadurch würde die Prüfgrundlage praxistauglich, international anschlussfähig und prüffähig ausgestaltet, ohne den B3S faktisch verpflichtend zu machen.

3.3 Prüfung nach dem 4-Augen-Prinzip

D.4A.01 & D.4A.02

Bestimmte Prüfungssachverhalte sind im 4-Augen-Prinzip zu prüfen. Nach D.4A.02 Nr. 4 sollen beide Prüfer hierfür etwa gleiche zeitliche Ressourcen einsetzen; für keinen Prüfer darf der Zeitanteil zwei Drittel der summierten Prüfzeit überschreiten.

Die Trennung von Prüfungsdurchführung und Qualitätskontrolle entspricht grundsätzlich dem Stand der Technik, etwa nach ISO/IEC 17021-1 sowie der auftragsbegleitenden Qualitätssicherung im Berufsrecht. Eine starre, minutengenaue Zwei-Drittel-Zeitgrenze ist jedoch unüblich, schwer revisionssicher nachzuweisen und kann fachlich kontraproduktiv sein. Dabei sollte klar zwischen denjenigen Prüfungssachverhalten, die tatsächlich im 4-Augen-Prinzip zu prüfen sind, und der zeitlichen Gesamtverteilung innerhalb der Nachweisprüfung unterschieden werden. Für die im 4-Augen-Prinzip erfassten Sachverhalte sollte maßgeblich sein, dass diese jeweils durch mindestens zwei geeignete Prüfer eigenständig und substanziell beurteilt werden. Prozentuale Zeitanteile sind hierfür nur begrenzt aussagekräftig und können insbesondere bei Prüfteams mit mehr als zwei Personen zu Fehlsteuerungen führen. Soweit zeitliche Obergrenzen oder Orientierungswerte vorgesehen werden, sollten diese daher nicht als Bestandteil der 4-Augen-Prüfung einzelner Sachverhalte verstanden werden, sondern allenfalls als gesondertes Plausibilitätskriterium für die Gesamtverteilung der Prüfaufwände.

Änderungsvorschlag: Nr. 4 sollte klar zwischen den im 4-Augen-Prinzip zu prüfenden Sachverhalten und der zeitlichen Gesamtverteilung der Prüfung unterscheiden und als Wirksamkeits-/Soll-Kriterium gefasst werden: Maßgeblich ist nicht eine annähernd gleiche zeitliche Ressourcenzuordnung, sondern dass die betreffenden Sachverhalte von mindestens zwei geeigneten Prüfern eigenständig und substanziell beurteilt werden; prozentuale Zeitanteile sollten hierfür nicht entscheidend sein. Die Zwei-Drittel-Grenze sollte allenfalls als Orientierung für die Gesamtverteilung der Prüfaufwände formuliert werden (»soll regelmäßig nicht überschreiten«).

3.4 Dokumentation des Prüfergebnisses

D.PE.03 i. V. m. N.BN.02 / N.BN.05

Der Entwurf enthält widersprüchliche Sprachvorgaben: Während der Prüfbericht nach D.PE.03 und der Geltungsbereich nach N.BN.05 auf Deutsch oder Englisch vorliegen dürfen, verlangt N.BN.02 die Einreichung aller Bestandteile des Nachweises in deutscher Sprache. Für international nach ISO/IEC 27001 oder über ein C5-Testat geprüfte Unternehmen liegen die zugrunde liegenden Nachweise jedoch regelmäßig auf Englisch vor. Der Widerspruch erzeugt zusätzlichen Übersetzungsaufwand ohne erkennbaren Sicherheitsgewinn.

Änderungsvorschlag: Vereinheitlichung des Sprachregimes: Deutsch oder Englisch sollten durchgängig für alle Nachweisbestandteile zugelassen werden, mindestens jedoch für ausdrücklich zugelassene Ausnahmen wie Anlage PD.A sowie für

referenzierte Zertifikate und Testate. N.BN.02 sollte entsprechend an D.PE.03 und N.BN.05 angeglichen werden.

D.PE.12

Die Anforderung verlangt, dass der Betreiber die Mängelliste um einen Umsetzungsplan ergänzt. Dies ist sachgerecht, da die Verantwortung für die Mängelbehebung beim Betreiber liegt. In der Praxis legen prüfende Stellen jedoch häufig Vorschläge für Maßnahmen, Fristen oder Priorisierungen bei; teilweise wird dies von Betreibern erwartet.

Unklar bleibt, ob solche Vorschläge künftig ausgeschlossen sein sollen oder zulässig bleiben, sofern Entscheidung und Umsetzung beim Betreiber verbleiben. Zudem sollte das Verhältnis zu D.PE.10 klargestellt werden, da die Mängelliste dort Teil des Prüfberichts ist, D.PE.12 aber auf eine Bereitstellung durch den Betreiber abstellt.

Änderungsvorschlag: D.PE.12 sollte klarstellen, dass der Umsetzungsplan in der Verantwortung des Betreibers liegt. Zugleich sollte geregelt werden, ob prüfende Stellen oder beratende Dritte Vorschläge beisteuern dürfen, ohne die Unabhängigkeit der Prüfung zu beeinträchtigen. Außerdem sollte präzisiert werden, ob der Betreiber die Mängelliste aus dem Prüfbericht, eine um den Umsetzungsplan ergänzte Fassung oder beide Fassungen bereitzustellen hat.

D.PE.13

D.PE.13 sollte durch eine praxisnahe Ausfüllhilfe flankiert werden. Gerade bei der Mängelliste ist eine einheitliche Dokumentation wichtig, um Vergleichbarkeit, Nachvollziehbarkeit und eine effiziente Bearbeitung durch Betreiber, Prüfstellen und BSI zu gewährleisten.

Zudem sollte D.PE.13 klarstellen, dass nicht jeder festgestellte Sicherheitsmangel automatisch zur Reduktion eines Reife- oder Umsetzungsgrades führen muss. Maßgeblich sollte eine nachvollziehbare Bewertung im Einzelfall sein, insbesondere nach Schwere, Reichweite und tatsächlicher Auswirkung des Mangels auf das geprüfte Kriterium. Geringfügige Mängel sollten daher nicht zwingend zur Nicht-Erreichung eines Reife- oder Umsetzungsgrades führen, sofern die Bewertung transparent begründet und dokumentiert wird.

Änderungsvorschlag: Die Ausfüllhilfe zur Mängelliste sollte um ein Beispiel zu D.PE.13 ergänzt werden. Dieses sollte zeigen, wie die relevanten Angaben zur Bewertung, Maßnahme, Fristsetzung und zum Umsetzungsstand nachvollziehbar einzutragen sind.

D.PE.13 sollte klarstellen, dass geringfügige Sicherheitsmängel nicht zwingend zu einer Reduktion eines Reife- oder Umsetzungsgrades führen, sofern dies im Einzelfall nachvollziehbar begründet wird. Die Ausfüllhilfe zur Mängelliste sollte um ein Beispiel ergänzt werden, das zeigt, wie Bewertung, Maßnahme, Fristsetzung, Umsetzungsstand und Auswirkungen auf Reife- oder Umsetzungsgrade transparent zu dokumentieren sind.

3.5 Dokumentation des Geltungsbereiches

N.DG.01 & N.DG.02

Die Dokumentation des Geltungsbereichs nach Anlage PD.A erfasst gemäß N.DG.01 Prozesse, Systeme, Komponenten, Schnittstellen und durch Dritte betriebene Teile, adressiert den Einsatz von KI-Systemen jedoch nicht ausdrücklich. Werden KI-Systeme für die kritische Dienstleistung eingesetzt, etwa KI-gestützte Angriffserkennung, Netz- und Anlagensteuerung oder vorausschauende Instandhaltung, sind deren Existenz, Funktion, Datenflüsse und externe Abhängigkeiten im Geltungsbereich derzeit nicht zwingend transparent.

Eine klare Darstellung der KI-Nutzung im Geltungsbereich ist erforderlich, da KI-Komponenten eigene Schutzbedarfe, Trainings- und Inferenzdaten, Modell- und Lieferkettenabhängigkeiten sowie spezifische Bedrohungen wie Datenmanipulation, Model Poisoning, Adversarial Inputs, Prompt Injection oder fehlende Robustheit und Erklärbarkeit mit sich bringen. Dies entspricht der Logik der Geltungsbereichs-Kriterien G05 zu maßgeblichen Systemen, Komponenten und Applikationen, G08 zu Schnittstellen sowie G10 zu durch Dritte betriebenen Teilen und ist anschlussfähig an die KI-Inventarisierung nach dem AI Act sowie an ISO/IEC 42001.

Soweit kein KI-System im Geltungsbereich eingesetzt wird, sollte analog zu N06 für Wartungsschnittstellen ein kurzer schriftlicher Vermerk genügen.

Änderungsvorschlag: N.DG.01 sollte um ein Kriterium ergänzt werden, etwa: »G14: Im Geltungsbereich für die kritische Dienstleistung eingesetzte KI-Systeme sind erkennbar und nachvollziehbar beschrieben, einschließlich Zweck/Funktion, Einbettung in Prozesse, maßgeblicher Datenflüsse (Trainings-/Inferenzdaten), Modell- und Dienstleisterabhängigkeiten sowie der jeweiligen Rolle des Betreibers (Anbieter/Betreiber im Sinne der VO (EU) 2024/1689).« Ergänzend sollte der Netzstrukturplan (N.DG.02) KI-relevante Komponenten und ihre externen KI-Schnittstellen kenntlich machen (z. B. neues Kriterium »N13: KI-Systeme und KI-bezogene externe Schnittstellen sind im Netzstrukturplan erkennbar oder in den schriftlichen Ergänzungen beschrieben.«). Die Anforderung ist bewusst dokumentations- und transparenzorientiert zu halten, ohne den Prüfumfang materiell auszuweiten.

N.DG.02 (N12)

Aus dem Netzstrukturplan muss nach N12 ersichtlich sein, welche Netzabschnitte und KRITIS-relevanten IT-Komponenten durch Systeme zur Angriffserkennung überwacht werden; nicht überwachte Bereiche sind entsprechend zu kennzeichnen. Dies knüpft sachgerecht an die Pflicht zum Einsatz von Systemen zur Angriffserkennung im Rahmen der Maßnahmen nach §§ 30/31 BSIG an. Soweit die Angriffserkennung selbst KI-gestützt erfolgt, sollte zugleich die Transparenz der KI-Nutzung berücksichtigt werden. Bei großen und dynamischen Umgebungen, insbesondere in Cloud- oder OT-Strukturen, stößt eine granulare Darstellung im statischen Netzstrukturplan jedoch an praktische Grenzen.

Änderungsvorschlag: Ergänzend sollten alternative gleichwertige Darstellungsformen (tabellarische Zuordnung, logische Sichten, Referenz auf Asset-/CMDB-Auszüge) ausdrücklich zugelassen werden, sofern Nachvollziehbarkeit und Vollständigkeit gewahrt bleiben.

3.6 Verwendung anderer Prüfungen und Zertifikate

N.BG.01, N.BG.05 & N.BG.08

Die Anforderungen an das Prüfteam sind teilweise so weit gefasst, dass sie in der Praxis zu einer vollständigen erneuten Prüfung bereits zertifizierter Kontrollen führen können. Damit würde die Anrechnung bestehender Zertifikate nur begrenzt entlasten. Sachgerecht wäre eine risikobasierte und stichprobenorientierte Delta-Prüfung. Diese sollte insbesondere prüfen, ob der Zertifizierungsumfang die für die kritische Dienstleistung relevanten Teile der Anlage umfasst, der zugrunde liegende Standard geeignet ist und verbleibende Lücken gezielt geschlossen werden.

Änderungsvorschlag: N.BG.01, N.BG.05 und N.BG.08 sollten klarstellen, dass bestehende Zertifizierungen nicht vollständig neu zu prüfen sind. Das Prüfteam sollte risikobasiert und stichprobenorientiert prüfen, ob der Scope passt, das Schutzniveau adressiert wird und identifizierte Lücken durch gezielte Zusatzprüfungen geschlossen werden. Eine vollständige Neuprüfung sollte nur in begründeten Ausnahmefällen erfolgen.

N.BG.02

Die Öffnung für bestehende Zertifikate und Testate, etwa ISO/IEC 27001, ISO 27001 auf Basis IT-Grundschutz, C5 oder andere Prüfzertifikate, ist grundsätzlich zu begrüßen. Sie kann bestehende Audit- und Zertifizierungsprozesse einbinden, Doppelprüfungen vermeiden und den Nachweisaufwand reduzieren.

Nach N.BG.02 ist die Anrechnung jedoch nur möglich, wenn ein einschlägiger, eignungsfestgestellter und gültiger B3S besteht. Diese Voraussetzung ist nicht nachvollziehbar. Für einzelne KRITIS-Anlagenkategorien existiert kein B3S; in anderen Fällen sind B3S nicht frei verfügbar. Betreiber ohne passenden B3S würden damit faktisch von der Anrechnung ausgeschlossen. Dies konterkariert das Entlastungsziel und kann die Nutzung eines B3S faktisch verpflichtend machen.

Besonders problematisch ist dies für Mehrspartenbetreiber mit einem einheitlichen, zertifizierten ISMS. Unterschiedliche B3S enthalten teils unterschiedlich formulierte Anforderungen, etwa zu Bedrohungskategorien, Schwachstellen oder Gefährdungen, ohne dass hierfür stets eine sachliche Differenzierung aus den jeweiligen Geschäftsfeldern erkennbar ist. Eine einheitliche Risikomanagement-Methodik wird dadurch unnötig erschwert.

Auch C5-Type-2-Testate nach ISAE 3000 bzw. IDW PS 860 sollten ausdrücklich als Nachweisbestandteil berücksichtigt werden können. Sie sind insbesondere für Cloud- und IT-Dienstleistungen etabliert und enthalten eine prüferische Bewertung über

einen Berichtszeitraum. Klarstellungsbedürftig ist dabei, wie Feststellungen, Ausnahmen oder Einschränkungen im Testat im Rahmen des Nachweises zu bewerten sind.

Änderungsvorschlag: N.BG.02 sollte gestrichen oder so gefasst werden, dass bestehende Zertifikate und Testate auch ohne einschlägigen B3S angerechnet werden können. Maßgeblich sollte sein, ob Scope, Statement of Applicability, Prüfgegenstand und Prüftiefe geeignet sind, das nach §§ 30, 31 BSIG geforderte Schutzniveau und die Anforderungen der Prüfgrundlage nach D.PG.01 ff. für die kritische Dienstleistung abzubilden.

Für Mehrspartenbetreiber sollte eine einheitliche, am geforderten Schutzniveau ausgerichtete Prüf- und Nachweissystematik ermöglicht werden. Ein BSI-Mapping der KRITIS- bzw. RUN-Anforderungen gegen anerkannte Standards und Schemata, insbesondere ISO/IEC 27001 Annex A, ISO 27001 auf Basis IT-Grundschutz und C5-Kriterien, könnte hierfür eine geeignete Grundlage bilden.

Ergänzend sollte ausdrücklich geregelt werden, dass C5-Type-2-Testate nach ISAE 3000 bzw. IDW PS 860 als Nachweisbestandteil herangezogen werden können. Dabei sollte beschrieben werden, wie Feststellungen, Ausnahmen oder Einschränkungen zu berücksichtigen und gegebenenfalls durch Zusatzprüfungen oder Maßnahmen zu adressieren sind.

N.BG.07

Die Vorgabe, dass die letzte Prüfung höchstens zwölf Monate zurückliegen darf, kann mit ISO/IEC 27001- und C5-Type-2-Zyklen grundsätzlich vereinbar sein. In der Praxis kann sie jedoch zusätzlichen Timing-Druck erzeugen und mit internationalen Zertifizierungs- und Auditzyklen kollidieren. Zudem bleibt unklar, auf welches Datum abgestellt wird: Prüfungshandlung, Bericht, Testat oder Zertifikat. Ohne Klarstellung entstehen Unsicherheiten bei der Einplanung und Verwendung bestehender Nachweise.

Änderungsvorschlag: N.BG.07 sollte klarstellen, welches Datum maßgeblich ist. Zudem sollte eine angemessene Toleranz oder Öffnungsklausel für planbare abweichende Zertifizierungszyklen vorgesehen werden, etwa 18 bis 36 Monate mit jährlichen Überwachungsaudits, sofern ein aktueller Sicherheitsstatus hinreichend dokumentiert ist.

N.BG.10

Soweit im Rahmen der Verwendung bestehender Prüfungen und Zertifikate zusätzliche Maßnahmen erforderlich werden, sollte klar zwischen Bewertung und Umsetzung unterschieden werden. Aufgabe des Prüfteams sollte es sein, verbleibende Lücken nachvollziehbar festzustellen und zu bewerten. Die Festlegung und Ausgestaltung zusätzlicher Maßnahmen sollten hingegen in der Verantwortung des Betreibers liegen. Andernfalls bestünde das Risiko, dass das Prüfteam über seine Prüfrolle hinaus in eine umsetzungs- oder beratungsähnliche Verantwortung gedrängt wird.

Änderungsvorschlag: N.BG.10 sollte klarstellen, dass das Prüfteam verbleibende Lücken im Rahmen einer Delta-Prüfung feststellt und bewertet, die Festlegung und Ausgestaltung zusätzlicher Maßnahmen jedoch in der Verantwortung des Betreibers liegt.

3.7 Berücksichtigung alter Mängelliste in Prüfung und Nachweis

D.AM.02, D.AM.03, D.AM.04 & N.AM.03

Nicht abgeschlossene Sicherheitsmängel aus dem Vornachweis sind in die aktuelle Mängelliste nach PE.A zu überführen; die IDs sollen dabei mit dem Präfix »ALT-[JAHR]-« unter Beibehaltung der bisherigen ID und Jahreszahl gebildet werden. Die durchgängige Rückverfolgbarkeit offener Mängel über mehrere Prüfzyklen entspricht guter Auditpraxis, insbesondere dem Follow-up nach ISO 19011.

Zugleich sollte vermieden werden, dass dieselbe Pflicht zur Übernahme nicht behobener Sicherheitsmängel sowohl in D.AM.03 als auch in N.AM.03 doppelt geregelt wird. Soweit D.AM.03 die inhaltliche Pflicht zur Überführung alter offener Mängel beschreibt, sollte N.AM.03 diese Pflicht lediglich hinsichtlich Format, Kennzeichnung und Nachweisführung konkretisieren. Soweit D.AM.03 die inhaltliche Pflicht zur Überführung alter offener Mängel beschreibt, sollte N.AM.03 diese Pflicht lediglich hinsichtlich Format, Kennzeichnung und Nachweisführung konkretisieren.

Geplante Maßnahmen aus einem kontinuierlichen Verbesserungsprozess sollten dabei nicht pauschal als Sicherheitsmängel behandelt und in die Mängelliste übernommen werden. In die Mängelliste sollten nur solche KVP-Maßnahmen aufgenommen werden, die auf einen konkret festgestellten Sicherheitsmangel zurückgehen oder dessen Behebung dokumentieren. Reine Verbesserungsmaßnahmen ohne festgestellten Mangel sollten hiervon abgegrenzt werden. Bei der Nutzung anderer Prüfungen nach D.AM.04 ist eine Herkunftskennzeichnung sinnvoll, führt jedoch zu zusätzlichem Dokumentationsaufwand.

Änderungsvorschlag: In der BSI-Formatvorlage (PE.A) sollten entsprechende Felder (Herkunft, ALT-ID, Behebungsphase) verbindlich vorgesehen werden. Zugleich sollten D.AM.02, D.AM.03 und N.AM.03 systematisch gestrafft und redaktionell aufeinander abgestimmt werden, um kleinteilige oder doppelte Vorgaben zur Übernahme nicht behobener Sicherheitsmängel in die aktuelle Mängelliste zu vermeiden. Soweit D.AM.03 die inhaltliche Pflicht zur Überführung alter offener Mängel beschreibt, sollte N.AM.03 diese Pflicht lediglich hinsichtlich Format, Kennzeichnung und Nachweisführung konkretisieren. Zudem sollten D.AM.02, D.AM.03 und N.AM.03 so aufeinander abgestimmt werden, dass die Pflicht zur Übernahme nicht behobener Sicherheitsmängel nur einmal inhaltlich geregelt und anschließend lediglich hinsichtlich Format, Kennzeichnung und Nachweisführung konkretisiert wird. D.AM.04 sollte klarstellen, dass geplante Maßnahmen aus einem kontinuierlichen Verbesserungsprozess nur dann in die Mängelliste aufzunehmen sind, wenn sie auf einen konkret festgestellten Sicherheitsmangel zurückgehen oder dessen Behebung dokumentieren.

3.8 Vorlagen für Bestandteile eines Nachweises nach § 39 Absatz 1 BSIG

N.BN.01

Für alle Nachweisdokumente sind die einschlägigen BSI-Formulare und Vorlagen zu verwenden; die jeweils aktuelle Version wird durch das BSI veröffentlicht, einschließlich etwaiger Übergangsfristen. Die verpflichtende Nutzung standardisierter Vorlagen für Nachweisdokument, Mängelliste und Prüfgrundlage nach N.BN.01, N.BN.07 und N.BN.09 ist im Sinne der Vergleichbarkeit und Prüfbarkeit grundsätzlich sinnvoll. Einheitliche Formate können den Aufwand für Betreiber, Prüfstellen und eingebundene Dienstleister senken.

Wichtig ist jedoch, dass die Vorlagen möglichst langfristig stabil bleiben und Änderungen planbar erfolgen. Kurzfristige Anpassungen ohne angemessene Übergangsfrist können laufende Prüfungen, Nachweiserstellungen sowie interne Prozesse und Schnittstellen erheblich beeinträchtigen. Dies gilt insbesondere, wenn Betreiber und Lieferanten strukturierte Datenflüsse, interne Freigabeprozesse oder Tool-Schnittstellen auf die BSI-Vorlagen ausrichten.

Zudem sollten die Vorlagen nicht nur als Dokumentformate, sondern soweit möglich auch in strukturierten, maschinenlesbaren Formaten bereitgestellt werden, insbesondere für Mängellisten. Dies würde die Weiterverarbeitung, Qualitätssicherung und Nachverfolgung von Feststellungen erleichtern.

Änderungsvorschlag: Für neue oder geänderte BSI-Vorlagen sollte eine angemessene Mindest-Übergangsfrist vorgesehen werden, etwa sechs Monate. Versionsstände sollten eindeutig gekennzeichnet und Änderungen nachvollziehbar dokumentiert werden.

Ergänzend sollten strukturierte, maschinenlesbare Formate bereitgestellt werden, insbesondere für Mängellisten und andere wiederkehrend auszuwertende Nachweisinhalte. Soweit künftig Felder zur KI-Dokumentation ergänzt werden, sollten diese in die Vorlagen für Anlage PD.A aufgenommen und ebenfalls versioniert sowie maschinenlesbar ausgestaltet werden.

N.BN.05

Anlage PD.A ist bei Folgeprüfungen nur noch beizufügen, wenn sich signifikante Änderungen ergeben haben. Das ist eine sinnvolle Entlastung für Betreiber und Prüfstellen. Unbestimmt bleibt jedoch der Begriff »signifikant«. Mit Blick auf die Transparenz der KI-Nutzung sollte klargestellt werden, dass die Einführung oder wesentliche Änderung von KI-Systemen im Geltungsbereich als signifikante Änderung gilt.

Änderungsvorschlag: Der Begriff »signifikante Änderungen« sollte konkretisiert werden (z. B. neue Standorte, wesentliche Architektur-/Schnittstellenänderungen, Wechsel wesentlicher Dienstleister sowie Einführung oder wesentliche Änderung eingesetzter KI-Systeme).

Kapitel 4: Inkrafttreten

Die Anforderungen gelten grundsätzlich bereits; abweichend treten lediglich N.BG.01 bis N.BG.10 zum 01.01.2027 in Kraft. Die spätere Inkraftsetzung der Zertifikatsregelung ist sachgerecht, da sie Betreibern und Prüfstellen Zeit zur Umstellung gibt. Für die übrigen, bereits geltenden Anforderungen fehlt jedoch eine Übergangsregelung für laufende oder bereits begonnene Prüfungen. Eine etwaige KI-Dokumentationspflicht sollte zudem zeitlich auf die Anwendungsfristen des AI Act abgestimmt werden, um Doppelaufwand und Friktionen bei der Umsetzung zu vermeiden.

Änderungsvorschlag: Eine Übergangsregel sollte vorgesehen werden, wonach für bereits begonnene Nachweisprüfungen die zum Prüfungsbeginn geltende GAiN-Fassung angewandt werden darf (Vertrauensschutz), und um Klarstellung der maßgeblichen Stichtagsbetrachtung.

Redaktionelle Hinweise

Feststellung: Im Entwurf finden sich mehrere redaktionelle Punkte, die vor Festlegung korrigiert werden sollten.

Textstelle	Anmerkung
Änderungshistorie	Zeile zu Version 2.2 enthält kein Datum.
Kapitel 2	Überschrift »Prüfende Stelle und Prüfer« vs. Inhaltsverzeichnis »Prüfende Stelle und Prüfende« – einheitliche, geschlechtsneutrale Bezeichnung empfohlen.
N.IR.01	Verweis »§ 39a Absatz 31 BSIG« existiert nicht; gemeint ist § 39 Abs. 1 BSIG.
P.UP. 03	Leerzeichen in der Kennung (sollte »P.UP.03« lauten).
D.PA.06	Tippfehler »des Bundeamtes« → »des Bundesamtes«.
Überschrift 3.6	Inhaltsverzeichnis nennt »Verwendung von bestehenden Prüfungen und Zertifikaten«, der Fließtext »Verwendung anderer Prüfungen und Zertifikate«

Textstelle	Anmerkung
N.BG.04	Die Formulierung sollte sprachlich überprüft und eindeutig gefasst werden. Insbesondere sollte geprüft werden, ob die derzeitige Negation bzw. die Satzkonstruktion mit »ob« die intendierte Aussage zutreffend wiedergibt oder redaktionell angepasst werden muss.
Definition »Prüfbericht«	Der zweite Satz der Definition scheint unvollständig zu sein und sollte redaktionell vervollständigt bzw. sprachlich bereinigt werden.

Änderungsvorschlag: Die nachstehend gelisteten Punkte sollten korrigiert bzw. sprachlich eindeutig gefasst werden.

Bitkom vertritt mehr als 2.300 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 700 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Felix Kuhlenkamp | Leiter Sicherheit
T +49 30 27576-279 | f.kuhlenkamp@bitkom.org

Verantwortliches Bitkom-Gremium

AK Informationssicherheit