Nr.	Tenzoriffer/Kapitelbezeichnung	Zeilennummer(n)	ggf. Originaltext	Hinweis/Änderungsvorschlag	Begründung	Spalte1
	Vorbemerkungen	-		Es muss bei allen Pflichten und vor allem bei allen Nachweisen darauf geachtet werden, dass keine unnötige Bürokratie aufgebaut wird. Zudem müssen bestehenden bürokratische Aufwände reduziert werden.	Bürokratieabbau ist eines der Kernziele der neuen Bundesregierung und muss auch im Bereich des IT-Sicherheitskatalog mit Nachdruck verfolgt werden. Jede Pflicht und vor allem jeder Nachweis über die Erfüllung einer Pflicht muss durch die "Brille" des Bürokratieabbaus gesehen werden. Insgesamt sollte sich mehr auf einzelne Stichproben statt auf eine (theoretische) allumfassende Kontrolle mit entsprechenden Zertifikaten etc. verlassen werden. Weiter muss eine bessere Abstimmung zwischen BNetzA und BSI sichergestellt werden, insbesondere im Bereich der Mehrspartenunternehmen. Prüfverfahren der Behörden sollten vereinheitlicht werden und Überschneidungen von Prüfungen soweit wie irgend möglich verhindert werden. Wo genau dies nötig und möglich ist, sollte Zusammen mit der Energiebranche geklärt werden.	
	Vorbemerkungen	-		Die IT-Sicherheitskataloge sollten nicht auf Basis der aktuell geltenden §11 Abs. 1a und 1b EnWG überarbeitet werden sondern erst auf Basis des neuen NIS2-Umsetzungsgesetzes.	Auf Grund der NIS2-Richtlinie müssen die unterschiedlichen Gesetze im Bereich der IT-Sicherheit noch angepasst werden, was insbesondere auch das EnWG betrifft. Hierdurch wird es zum einen dazu kommen, dass mehr Unternehmen in den Anwendungsbereich des Gesetzes fallen (insbesondere nicht nur Betreiber kritischer Energieanlagen, sondern auch Betreiber von Energieanlagen, wenn sie wichtige Einrichtungen sind, vgl. § 5c Abs. 2 EnWG-RegE). Zum anderen wird auch der Scope der Risikobetrachtung geändert: Bisher standen nur die kritischen Anlagen im Focus, zukünftig wird das gesamte Unternehmen in den Blick genommen. Richtig ist zwar, dass aktuell das NIS2-Umsetzungsgesetz nicht in der finalen Fassung vorliegt. Allerdings sind die Entwürfe des NIS2-Umsetzungsgesetzes der letzten Legislaturperiode bereits weit fortgeschritten und können problemlos als Basis der Überarbeitung dienen. Da die Kataloge erst zum 1.1.2027 gelten sollen (Zeile 45) und es bis dahin sicherlich eine Überarbeitung Fassung des EnWG (auf Grund des NIS2-Umsetzungsgesetz) existiert, sollte von einer vorherigen Überarbeitung der IT-Sicherheitskataloge abgesehen werden. Anderenfalls müssten die Kataloge erneut überarbeitet werden, bevor sie überhaupt in Kraft treten. Dies ist ein unnötiges bürokratisches Vorgehen und bindet unnötig Ressourcen der Wirtschaft und der Verwaltung. In der weiteren Kommentierung gehen wir allerdings davon aus, dass der IT-Sicherheitskatalog auf § 11 Abs. 1a und 1b EnWG gestützt wird. Vor diesem Hintergrund wird an verschiedenen Stellen aufgezeigt, dass die § 11 Abs. 1a und 1b EnWG keine hinreichende Ermächtigungsgrundlage für den hier vorgestellten IT-Sicherheitskatalog bieten.	
	Tenzoriffer 3	24 - 26	Betreiber und Betriebsführer von Energieversorgungsnetzen und Betreiber und Betriebsführer von Energieanlagen haben den Abschluss des Zertifizierungsverfahrens durch Vorlage der jeweiligen Nachweisdokumente nachzuweisen	Die Pflichten der Betreiber und Betriebsführer müssen auf kritische Energieanlagen beschränkt werden.	Tenzoriffer 2 begrenzt die Pflichten (wie auch durch § 11 Abs. 1b EnWG vorgegeben) auf Betreiber von Energieanlagen, die nach der BSI-KritisVO als kritische Energieanlagen angesehen werden. Dies muss hier nachvollzogen werden.	
	Tenzoriffer 4	36 - 38	Tenzoriffer 4 ist wiederum nicht anzuwenden auf Energieversorgungsnetze, die nach der BSI-Kritisverordnung in der jeweils geltenden Fassung als Kritische Infrastruktur bestimmt wurden. Diese müssen weiterhin Tenzoriffer 1 einhalten.	Die Nichtanwendbarkeit muss sich auch auf die kritischen Energieversorgungsnetze beziehen.	Grund für die Nichtanwendbarkeit ist, dass keine Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb vorliegen. Hierbei handelt es sich um eine Tatbestandsvoraussetzung des § 11 Abs. 1a EnWG. Sind diese Tatbestandsvoraussetzungen nicht erfüllt besteht keine Ermächtigungsgrundlage um diese Betreiber überhaupt über die IT-Sicherheitskataloge zu erfassen.	
	Tenzoriffer 5	39 - 41	Betreiber und Betriebsführer von Energieversorgungsnetzen und Betreiber und Betriebsführer von Energieanlagen haben die in Anlage 3 genannten Maßnahmen umzusetzen. Es gelten die in Anlage 4 aufgeführten Begriffsbestimmungen.	Die Pflichten der Betreiber und Betriebsführer müssen auf kritische Energieanlagen beschränkt werden.	Die Ermächtigungsgrundlage für Betreiber von Energieanlagen zum Erlass des IT-Sicherheitskatalogs findet sich in § 11 Abs. 1b EnWG. Sie ist - im Gegensatz zu den Netzbetreibern in § 11 Abs. 1a EnWG - begrenzt auf Betreiber von Energieanlagen, die die Schwellenwerte der BSI-KritisVO erreichen. Es besteht somit keine Ermächtigungsgrundlage Betreiber von Energieanlagen unterhalb der Kritis-Schwelle zu regulieren.	
	Tenzoriffer 6	42 - 44	Betreiber und Betriebsführer von Energieversorgungsnetzen und Betreiber von Energieanlagen sind verpflichtet, der Bundesnetzagentur eine Ansprechperson für IT-Sicherheit zu benennen. Es gelten die in Anlage 3 aufgelisteten Regelungen zu Ansprechpersonen für IT-Sicherheit.	Die Pflichten der Betreiber und Betriebsführer müssen auf kritische Energieanlagen beschränkt werden.	Siehe Begründung zu Tenzoriffer 5	
	Anlage 1	82 - 85	Die Feststellung der Nichtanwendbarkeit kann nicht für Energieversorgungsnetze erfolgen, die nach der BSI-Kritisverordnung in der jeweils geltenden Fassung als Kritische Infrastruktur bestimmt wurden, und entbindet auch nicht von der Umsetzungspflicht der Tenzoriffern 5 und 6.	Die Nichtanwendbarkeit muss sich auch auf die kritischen Energieversorgungsnetze beziehen.	Siehe Begründung zu Tenzoriffer 4	

Anlage 1 Anlage 2	93 - 95 228 - 230	Basis des IT-Sicherheitskatalogs bilden stets die ISO/IEC-Normen in ihrer aktuellen, englischsprachigen Fassung. Soweit deutsche Übersetzungen der jeweils aktuellen ISO/IEC-Normen vorliegen, können diese als Arbeitsdokumente herangezogen werden.	Für Umstellungen auf neue Anforderungen müssen Übergangszeiten berücksichtigt werden, die sich so nicht in der Konsultationsfassung wiederfinden. Unklar ist auch, ob die nach der deutschen Fassung ausgerichtete ISMS umgestellt werden um den IT-Sicherheitskatalog einzuhalten Es sollte von der BNetzA eine übersetzte deutsche Fassung zur Verfügung gestellt werden	Bei der Verwendung der englischen Fassung können Übersetzungsfehler und firmeninterne Sprachbarrieren nicht ausgeschlossen werden. Die Verwendung der deutschen Fassung hat daher viele Vorteile im deutschsprachigen Raum. Die aktuelle Praxis, dass die deutsche Fassung als Grundlage dient und die englische Fassung verpflichtend anzuwenden ist, wenn nach der Übergangszeit noch keine deutsche Fassung vorliegt, hat sich aus unserer Sicht bewährt und sollte fortgeführt werden. Es macht wenig Sinn, wenn jedes Unternehmen selbst die englische Fassung ins Deutsche übersetzen muss, solange noch keine offizielle deutsche Übersetzung vorliegt.
Anlage 1 Anlage 2	128 - 133 264 - 270	Zu diesem Zweck muss jeder Netzbetreiber oder Betriebsführer ein Informationssicherheitsmanagementsystem nach ISO27001 mindestens für den nach Abschnitt B zu ermittelndem Geltungsbereich etablieren. Dieses Informationssicherheitsmanagementsystem muss der Netzbetreiber oder Betriebsführer anschließend von einer bei der Deutschen Akkreditierungsstelle nach dem Konformitätsbewertungsprogramm für den IT-Sicherheitskatalog nach § 11 1a EnWG akkreditierten Zertifizierungsstelle zertifizieren lassen.	Die Zertifizierung des betriebsgeführten Unternehmens ist überflüssig und sollte abgeschafft werden.	Bis zur "Mitteilung zur Zertifizierung nach IT-Sicherheitskatalog § 11 Abs. 1a und 1b EnWG im Fall einer Betriebsführung durch Dritte" musste das betriebsgeführte Unternehmen kein eigenes Zertifikat vorzeigen, sondern lediglich der Betriebsführer. Diese Zustand sollte wiederhergestellt werden. Es stellt einen unverhältnismäßigen Aufwand des betriebsgeführten Unternehmens dar, wenn dieses ein ISMS aufbauen und zertifizieren lassen muss, obwohl alle wesentlichen Assets bereits im Scope des Betriebsführers erfasst wurden. Hierbei handelt es sich um sinnlose bürokratische Mehraufwände, deren Abbau sich die neue Bundesregierung auf die Fahnen geschrieben hat. Sollte hierfür eine gesetzliche Änderung notwendig sein, so muss diese zügig angegangen werden. Hierfür sollte dringend ein enger Dialog mit der Energiebranche aufgenommen werden.
Anlage 1	146 - 148	Konsultationsfragen: Ist diese Trennung eindeutig? Können/sollten einzelne Systeme/Markrollen in den Geltungsbereich des Informationssicherheitsmanagementsystems integriert werden?	Die Trennung (Netzbetrieb / Messstellenbetrieb) ist aus unserer Sicht noch eindeutig eindeutig. Die Systeme/Markrollen sollten nicht in den Geltungsbereich des ISMS integriert werden. Für die Versorgungssicherheit ist es irrelevant, wenn beispielsweise die Abrechnungsmöglichkeit für 24 Stunden ausfällt. Es sollte jedoch eng überwacht werden, wo zukünftig Unklarheiten in der Abgrenzung auftauchen.	-
Anlage 1 Anlage 2	155 - 157 287 - 288	Für unmittelbar notwendige Systeme, ohne die die davon abhängigen Prozesse automatisch zum Erliegen kommen, dürfen keine Risiken akzeptiert werden	Die Forderung, dass „keine Risiken akzeptiert werden“ ist de facto nicht umsetzbar, da immer Risiken bestehen. Der Begriff des Prozesses muss definiert werden.	Die Risikoakzeptanz ist eine legitime und nicht wegdenkbare Methode zur Risikobehandlung. Nach Anwendung angemessener Behandlungsmaßnahmen verbleiben immer geringe Schadenspotenziale und Gefährdungen mit geringer Eintrittswahrscheinlichkeit und es besteht folglich immer ein Restrisiko. Es wird nur der Begriff des kritischen Prozesses definiert aber nicht der Begriff des Prozess selbst.
Anlage 1 Anlage 2	199 - 202	Konsultationsfragen: Wie kann der Nachweis über die Identifikation der kritischen Prozesse so gestaltet werden, dass transparent wird, welche Prozesse warum nicht ins ISMS aufgenommen wurden? Können/müssen die Auditoren in die Erstellung dieses Nachweises eingebunden werden?	Es sollte nichts am bisherigen Prozess geändert werden. Üblicherweise wird die Identifikation der kritischen Prozesse bereits mit dem Auditor abgestimmt. Dieser bestätigt durch seine Prüfung auf Grundlage der DIN ISO/IEC 27001, dass diese Identifikation korrekt vorgenommen wurde.	-
Anlage 1 Anlage 2	203 - 204 330 - 331	Anlagenbetreiber müssen ihre Nachweisdokumente digital bei der Bundesnetzagentur über das Postfach it-sicherheitskatalog@bnetza.de einreichen.	Einführung einer flexiblen Formulierung, die die Verwendung alternativer und ggf. auch sicherer Austauschwege zukünftig ermöglicht bzw. nicht ausschließt	Der Übermittlungsweg per E-Mail gilt in Sicherheitskreises als unsicher und entspricht nicht mehr dem Stand der Technik. Alternative Übermittlungswege, wie z.B. über Meldeportale oder geschützte Austauschverzeichnisse, sollten auch in Anbetracht der sich weiterentwickelnden Sicherheitspraktiken grundsätzlich möglich sein. Im besten Falle richtet die BNetzA eine grundsätzlich sicherere Möglichkeit nach dem Stand der Technik so schnell wie möglich ein.
Anlage 1 Anlage 2	184 - 186 312 - 314	Neben den Schnittstellen zwischen den vorgenannten Teilplänen müssen Schnittstellen Systemen, die keine kritischen Systeme sind, im Netzstrukturplan klar gekennzeichnet und in einer Übersicht definiert werden.	Dieser Satz macht grammatikalisch noch keinen Sinn und muss angepasst werden.	
Anlage 1 Anlage 2 Anlage 3	140 277 348 - 350			Die Anlage 4 sollte die die Begriffe „Ausfalltoleranz“ und „notwendige Wiederanlaufzeit“ definieren und in Beziehung zueinander stellen
Anlage 3	337 - 340	Neben den zertifizierungspflichtigen, risikobasierten Maßnahmen nach Anlage 1 oder Anlage 2 als notwendigem Mindeststandard zur IT-Sicherheit, haben Betreiber für ihre übrigen Systeme allgemein anerkannte, verhältnismäßige Maßnahmen nach dem Stand Technik zur Erhöhung der Cybersicherheit zu ergreifen.	Die Pflichten für die "übrigen Systeme" müssen gestrichen werden.	Die Ermächtigungsgrundlage für Betreiber von Energieanlagen zum Erlass des IT-Sicherheitskatalogs findet sich in § 11 Abs. 1a und 1b EnWG. Sie ist begrenzt auf "Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind". Die "übrigen Systeme" sind nicht für einen sicheren Netzbetrieb notwendig und sind deshalb bisher nicht in den IT-Sicherheitskatalogen erfasst. Es existiert also bisher keine Ermächtigungsgrundlage um auch die "übrigen Systeme" über die IT-Sicherheitskataloge zu regulieren. Im übrigen ist unklar, wie in Mehrspartenunternehmen (also z.B. einem Unternehmen, das sowohl Energie- als auch Wasseranlagen betreibt) die Pflichten aus EnWG und BSI bzw. die Zuständigkeiten von BNetzA und BSI abgegrenzt werden.

Anlage 3	337 - 340	Neben den zertifizierungspflichtigen, risikobasierten Maßnahmen nach Anlage 1 oder Anlage 2 als notwendigem Mindeststandard zur IT-Sicherheit, haben Betreiber für ihre übrigen Systeme allgemein anerkannte, verhältnismäßige Maßnahmen nach dem Stand Technik zur Erhöhung der Cybersicherheit zu ergreifen.	Die Begriffe "Cybersicherheit" und "IT-Sicherheit" sollten in den Begriffsbestimmungen definiert werden	Es werden die Begriffe Cybersicherheit und IT-Sicherheit nicht abgegrenzt genau verwendet. So wird in Zeile 61-63 Cybersicherheit als Ziel festgelegt.
Anlage 3	340 - 343	Bei der Bewertung der Verhältnismäßigkeit dieser Maßnahmen sind das Ausmaß der Risikoexposition, die Größe des Betreibers beziehungsweise des Betriebsführers und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, gebührend zu berücksichtigen.	Bei der Bewertung der Verhältnismäßigkeit der Maßnahmen sind die Größe des Betreibers beziehungsweise des Betriebsführers sowie das Niveau der bewerteten Informationssicherheitsrisiken angemessen zu berücksichtigen	„Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere“ ist faktisch die Definition von Risiko. Die Risikoexposition wiederum ist eine Eingangsgröße für das Risiko. Beide Aspekte können deshalb in dem Begriff der "Informationssicherheitsrisiken" aufgehen.
Anlage 3	344 - 354	-	Klarstellung, dass sich BCM nur auf den zertifizierten Geltungsbereich und nur auf die kritischen Prozesse / Systeme bezieht.	Der Begriff Betriebsfähigkeit lässt, ohne weitere Erläuterung, einen großen Interpretationsspielraum und könnte sich auf das Unternehmen im Allgemeinen beziehen, die geforderten BIA und RIA wiederum (Zeile 348-351) beziehen sich nur auf den zertifizierten Geltungsbereich, die weiteren Punkte (Zeilen 352-354) sind wiederum ohne konkreten Bezug (bzw. fehlt hier ggf. eine Ergänzung, dass Notfallpläne, Krisenkommunikation und Notfallübungen auf Basis der BIA und RIA abgeleitet werden sollen.“)
Anlage 3	351	Eine Risikoanalyse basierend auf der Risikoabschätzung nach Anlage 1 oder Anlage 2,	Klärung, ob Risikoabschätzung etwas anderes ist als die Risikoanalyse	In Anlage 1 ist bereits eine Risikoanalyse für die kritischen Prozesse nach ISO 27001 gefordert
Anlage 3	366 - 368	Bei der Bestimmung des Ansprechpartners sind – soweit einschlägig – die Vorschriften des Sicherheitsüberprüfungsgesetzes (SÜG) und der Sicherheitsüberprüfungsfeststellungsverordnung (SÜFV) zu beachten.	Dieser Hinweis könnte so verwirrend, sein da im Regelfall keine Sicherheitsüberprüfung vorgeschrieben bzw. möglich ist. Es sollte eine entsprechende Klarstellung erfolgen oder darauf hingewirkt werden, dass die Möglichkeiten einer Sicherheitsüberprüfung erweitert werden.	Die Möglichkeiten der Sicherheitsüberprüfung sind im Moment nicht ausreichend. Bereits jetzt hat der Bund die Pflicht, bestimmte Personen auch im nichtöffentlichen Bereich (also in der Privatwirtschaft) einer Sicherheitsüberprüfung zu unterziehen. Dies gilt beispielsweise für Teile von Übertragungsnetzbetreibern oder Verteilnetzbetreibern, da sie eine lebenswichtige Einrichtung darstellen können (vgl. § 1 Abs. Abs. 4, 5; 2 Abs. 1 Sicherheitsüberprüfungsgesetz; § 16 Sicherheitsüberprüfungsfeststellungsverordnung). Allerdings besteht auch außerhalb des in § 16 Sicherheitsüberprüfungsfeststellungsverordnung genannten Leitstellenbetriebs teilweise ein Bedürfnis (potentielle) Mitarbeiter einer Sicherheitsüberprüfung unterziehen zu lassen. Besondere Probleme bestehen, falls die Anforderungen an die Bedeutung der Einrichtung nach § 16 Sicherheitsüberprüfungsfeststellungsverordnung nicht erreicht werden. In einem solchen Fall erklärt sich der Bund für nicht zuständig für die Sicherheitsüberprüfung und die Länder können diese teilweise nicht anbieten. Es kann allerdings auch unterhalb der Anforderungen des § 16 Sicherheitsüberprüfungsfeststellungsverordnung ein Bedürfnis für eine Sicherheitsüberprüfung von Personen im sicherheitsrelevanten Bereich geben.
Anlage 4	393 - 395	Konsultationsfragen: Ist hier eine explizite Abgrenzung zwischen Lieferanten/Dienstleistern hilfreich? Falls ja, wie kann die Grenze zwischen Lieferanten/Dienstleistern und Betriebsführern trennscharf beschrieben werden?	Eine explizite Abgrenzung zwischen Lieferanten/Dienstleistern und Betriebsführern ist sinnvoll, da es in der Praxis häufig zu Unsicherheiten/Begriffunklarheiten kommt, wie ein beauftragtes Unternehmen einzuschätzen ist. Dies hat auch praktische Auswirkungen, da beispielsweise Betriebsführer ein eigenes Zertifikat brauchen nach IT-Sicherheitskatalog, Lieferanten/Dienstleister dagegen lediglich über vertraglichen Vereinbarungen gebunden werden (bzw. ggf. zukünftig über den Cyber Resilience Act). Ein erster Ansatz zur Abgrenzung wäre wie folgt: - Ein Betriebsführer ist verantwortlich für die Steuerung des gesamten Betriebs. Er agiert damit faktisch wie der Eigentümer im alltäglichen Geschäft. -Ein Lieferant/Dienstleister ist lediglich verantwortlich für einen bestimmten Bereich des Betriebs. Ihm werden auch im alltäglichen Geschäft Weisungen vom Betreiber erteilt. Ggf. können aber auch die Abgrenzungskriterien für die „Betreibereigenschaft“ herangezogen werden (vgl. § 1 Abs. 1 Nr. 2 BSI-Kritisverordnung).	
Anlage 4	454 - 457	3. Verteil- und Übertragungsnetzbetreiber: Konsultationsfrage: Wie kann die Pflicht zur Sicherstellung der Versorgungssicherheit basierend auf gesetzlichen Pflichten analog zu den Vorgaben für die Gruppe 1 und 2 konkretisiert werden?	Versorgungssicherheit bedeutet die kontinuierliche Sicherstellung der Sicherheit und Zuverlässigkeit des Elektrizitäts-/Gasversorgungssystems in der jeweiligen Regelzone bzw. im jeweiligen Netz. Hierzu gehört, Gefährdungen und Störungen der Sicherheit und Zuverlässigkeit des Elektrizitäts-/Gasversorgungssystems zu beseitigen. Dies erfolgt durch netz- und marktbezogene Maßnahmen (§§ 13 Abs. 1, 14 Abs. 1, 16 Abs. 1, 16a EnWG). Sollten diese nicht ausreichen, um die Gefährdung oder Störung zu beseitigen, sind Netzbetreiber berechtigt und verpflichtet, sog. Notfallmaßnahmen zu ergreifen (§§ 13 Abs. 2, 14 sowie §§ 16 Abs. 2, 16a EnWG).	
Anlage 4	463 -	-	Klarstellung erforderlich, was mit Funktionen gemeint ist.	Es ist unklar, ob hiermit kritische Funktionen gemeint sind (vgl. Zeile 419 - 421). Zudem ist unklar, was mit den einzelnen Spalten gemeint ist. Was ist insbesondere der Infrastrukturbetrieb?