Whitepaper

VANTUR
CONSULTING

Rechenzentrumsbetrieb

Vom Bauwerk zur Betriebssicherheit

Ein Praxisleitfaden zu Recht, Norm und Betrieb

DIN EN 50600, TSI.Standard vom TÜV Nord Cert, KRITIS und NIS2 im Tagesgeschäft

Inhalt

MANAGEMENT SUMMARY

Der Betrieb entscheidet, nicht nur der Bau

Rechenzentren werden heute nach höchsten technischen Standards geplant und errichtet. Zwischen 2022 und 2024 wuchs die installierte IT-Kapazität in Deutschland um rund 16 Prozent auf etwa 2.730 Megawatt. Getrieben von KI-Anwendungen, Cloud-Diensten und dem Bedarf an Colocation-Flächen. Der jährliche Stromverbrauch deutscher Rechenzentren liegt inzwischen bei rund 20 Milliarden Kilowattstunden.

Was in dieser Wachstumsgeschichte regelmäßig zu kurz kommt, ist der Betrieb. Die Organisation, Dokumentation und Verantwortungsstruktur, die aus einer technischen Anlage einen rechtssicheren, auditfähigen und wirtschaftlichen Dauerbetrieb macht.

Mit dem sogenannten Gefahrenübergang, dem Moment, in dem eine geprüfte Anlage an den Betreiber übergeben wird, beginnt eine umfassende Verantwortung für Sicherheit, für Verfügbarkeit, für Nachhaltigkeit und im Zweifel auch persönlich, im Sinne des Schutzes vor Organisationsverschulden.

> *„Der Bau ist fertig. Aber ist der Betrieb es auch?“ Diese Frage entscheidet heute über Zertifizierungsfähigkeit, Versicherungsschutz und Reputation eines Rechenzentrums.*

Dieses Whitepaper ordnet die wichtigsten Begriffe und Pflichten, von DIN EN 50600 über TSI.Standard und TÜV NORD CERT bis zu KRITIS und NIS2 und zeigt, welche Dokumente ein Betreiber tatsächlich braucht. Zudem macht es deutlich, warum Nachhaltigkeit längst kein Kür-, sondern ein Pflichtprogramm ist.

KAPITEL 1

Der Markt im Wandel: Wachstum mit Nebenwirkungen

Rechenzentren sind zum Rückgrat der Digitalisierung geworden. Cloud, Streaming, autonomes Fahren und insbesondere Künstliche Intelligenz treiben Rechenleistung und Flächenbedarf. Die Internationale Energieagentur (IEA) erwartet, dass sich der weltweite Stromverbrauch von Rechenzentren bis 2030 auf rund 945 Terawattstunden mehr als verdoppelt: Vergleichbar mit dem heutigen Verbrauch Japans.

Für Europa wird ein Anstieg auf über 150 TWh prognostiziert, das entspräche etwa fünf Prozent des europäischen Gesamtstromverbrauchs.

Gleichzeitig verändert sich der Markt strukturell:

- Hyperscaler mit latenzkritischen Anwendungen priorisieren die Nähe zu internationalen Internetknoten wie DE-CIX (Frankfurt) oder AMS-IX (Amsterdam).
- Enterprise-Betreiber gewichten Redundanz, Sicherheit und Betriebskosten stärker als reine Latenz.
- Edge-Rechenzentren wachsen deutlich zweistellig, weil Anwendungen wie Smart City, Industrie 4.0 und autonomes Fahren Datenverarbeitung näher am Entstehungsort erfordern.
- Strompreise, Netzentgelte und die Nähe zum Höchstspannungsnetz werden zum ebenso wichtigen Standortfaktor wie die Netzanbindung.

Die genannten Marken dienen ausschließlich der beispielhaften Einordnung von Hyperscalern und Infrastrukturakteuren im Marktumfeld.

Für Betreiber bedeutet das:

Standortentscheidung und Betriebskonzept sind kein einmaliger Akt, sondern ein fortlaufender Abgleich zwischen Nutzungszweck, Regulierung und Marktentwicklung. Ideale Standorte gibt es nicht – nur den besten Kompromiss für das jeweilige Geschäftsmodell.

KAPITEL 2

Vom Bauwerk zum Betrieb: Die Verantwortungslücke

Die Planung und Errichtung elektrotechnischer Anlagen erfolgt nach dem allgemein anerkannten Stand der Technik. Nach erfolgreicher Prüfung und Übergabe der Dokumentation an den Betreiber findet der sogenannte Gefahrenübergang statt: Ab diesem Zeitpunkt trägt der Betreiber die volle Verantwortung für den ordnungsgemäßen Betrieb und haftet bei Verstößen.

Genau an dieser Schnittstelle entsteht in der Praxis regelmäßig eine Lücke. Die bauliche und technische Seite ist hervorragend dokumentiert, doch es fehlt ein Rahmenwerk, das festlegt, wer im Betrieb wofür verantwortlich ist, welche Prüfungen wann fällig sind und wie im Ernstfall reagiert wird. Diese Lücke ist der eigentliche Ansatzpunkt für Betreiberberatung.

Warum das mehr als Formalie ist

- **Rechtssicherheit**: Arbeitsschutzgesetz, Betriebssicherheitsverordnung und DGUV-Vorschriften verlangen eine dokumentierte Gefährdungsbeurteilung als Grundlage jeder Entscheidung.
- **Versicherungsschutz**: Feuerschutzklauseln wie SK3602 verpflichten zu jährlichen Prüfungen durch anerkannte Sachverständige. Ohne Nachweis drohen gekürzte oder verweigerte Leistungen.
- **Zertifizierungsfähigkeit**: Audits von Zertifizierungsanbietern (z. B. TÜV NORD CERT) und DIN EN 50600 Audits prüfen explizit, ob Betriebsprozesse gelebt und nicht nur beschrieben werden.
- **Persönliche Haftung**: Ohne benannte, befähigte Personen und dokumentierte Prüfroutinen drohen Organisationsverschulden und im Schadensfall persönliche Konsequenzen für Verantwortliche.

KAPITEL 3

Der Rechenzentrums-Kompass: Begriffe und Normen

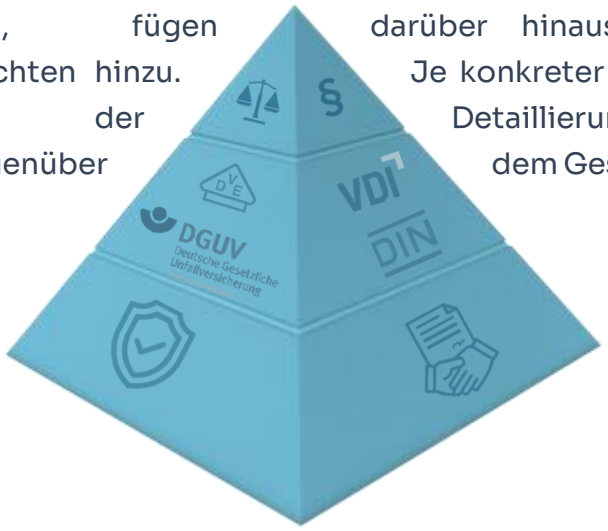
Kaum ein Betreiber kennt alle relevanten Regelwerke im Detail und muss es auch nicht. Entscheidend ist, die Zusammenhänge zu verstehen und zu wissen, wo im eigenen Betrieb Handlungsbedarf besteht. Die folgende Übersicht ordnet die wichtigsten Begriffe.

Begriff	Bedeutung für den Betrieb
DIN EN 50600 / ISO/IEC 22237	Internationale Normenreihe für Planung, Bau und Betrieb von Rechenzentren. Teil 3-1 regelt Informationen für Management und Betrieb und ist Grundlage für jedes Betriebsführungshandbuch.
TSI.STANDARD	Kriterienkatalog vom TÜV NORD CERT zur Prüfung und Zertifizierung von Rechenzentren, kombiniert mit DIN EN 50600. Level 1 – 4 beschreiben den Redundanzgrad, analog zu den klassischen Tier-Stufen.
KRITIS	**Krit**ische **I**nfra**s**trukturen im Sinne des BSI-Gesetzes Energie, Wasser, IT/TK u. a. Rechenzentren ab bestimmter Größe fallen darunter und unterliegen besonderen Nachweis- und Meldepflichten.
NIS2	EU-Richtlinie zur **N**etz- und **I**nformations**s**icherheit ist über das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) seit 6. Dezember 2025 in deutsches Recht überführt. Erweitert den Kreis betroffener Unternehmen deutlich und verschärft die Nachweis-, Melde- und Haftungspflichten für Betreiber.
ArbSchG / BetrSichV / TRBS	Arbeitsschutzgesetz, Betriebssicherheitsverordnung und Technische Regeln Betriebssicherheit. Verpflichten den Betreiber zu Gefährdungsbeurteilung, Prüfkonzept und einer „zur Prüfung befähigten Person“ (EFK).

Begriff	Bedeutung für den Betrieb
DGUV Vorschrift 1 + 3	Unfallverhütungsvorschriften der Berufsgenossenschaften. Vorschrift 3 regelt Wiederholungsprüfungen elektrischer Anlagen. Basis für die klassische 4-Jahres-Prüffrist.
DIN VDE 0105-100 / 0100-600	Regeln zum Betrieb bzw. zur Prüfung elektrischer Anlagen. DIN VDE 0105-100 erlaubt bei nachweislich dauerhafter Überwachung (z. B. RCM-Sensoren) den Verzicht auf das Abschalten zur Isolationsmessung.
CSRD / EU-Taxonomie	**C**orporate **S**ustainability **R**eporting **D**irective. Ursprünglich ab 2025 für einen wachsenden Unternehmenskreis vorgesehen; durch das EU-Omnibus-Paket wurden die Schwellenwerte deutlich angehoben und die Berichtspflicht auf 2028 (Geschäftsjahr 2027) verschoben. Für Rechenzentrumsbetreiber bleibt vor allem die Lieferkettenwirkung relevant.
EnEfG	**En**ergie**ef**fizienz**g**esetz verpflichtet Betreiber seit 2024 zur Abwärmeerfassung und -nutzung sowie zu PUE-Grenzwerten (Neubauten ≤ 1,2 ab 1.7.2026; Bestand ≤ 1,5 ab 2027, ≤ 1,3 ab 2030), zu 100 % bilanziellem Grünstrombezug ab 2027 sowie zur Meldung an das Rechenzentrumsregister.
SDC-Zertifizierung (TÜV Rheinland)	**S**ustainable **D**ata **C**enter: ganzheitliche Nachhaltigkeitsbewertung in elf Dimensionen, eingeordnet in die Effizienzklassen A – G.

Die Normenpyramide: Gesetz, Richtlinie, Vertrag

Gesetze wie das Arbeitsschutzgesetz oder die Betriebssicherheitsverordnung geben den verbindlichen Rahmen vor. Richtlinien und technische Regeln (TRBS, DGUV-Vorschriften, DIN-VDE-Normen) konkretisieren, wie dieser Rahmen in der Praxis umzusetzen ist. Verträge, etwa technische Anschlussbedingungen mit dem Energieversorger oder die Feuerschutzklausel in der Gebäudeversicherung, fügen darüber hinaus wirtschaftliche und vertragliche Pflichten hinzu. Je konkreter die Ebene, desto höher meist der Detaillierungsgrad, aber die Verbindlichkeit gegenüber dem Gesetz bleibt in jeder Ebene bestehen.



KAPITEL 4

Die vier Säulen des sicheren Rechenzentrumsbetriebs

Säule 1 — Verfügbarkeit und Redundanz

Verfügbarkeit ist die zentrale Kennzahl jedes Rechenzentrums. Die klassischen Tier-Stufen des Uptime Institute und die TSI.Standard Level beschreiben, wie redundant Strom- und Kühlpfade ausgelegt sind und ob Wartung im laufenden Betrieb möglich ist (Concurrently Maintainable). Beide Systeme folgen jedoch eigenen Bewertungslogiken und sind trotz ähnlicher Grundidee nicht eins zu eins gleichzusetzen. Die folgende Tabelle bildet die Referenzwerte des Uptime Institute ab.

Stufe	Redundanzprinzip	Erwartete Verfügbarkeit	Ausfallzeit / Jahr
Tier I	Ein Pfad, kaum Redundanz	99,6826 %	≈ 28,8 Std.
Tier II	Ein Pfad, einige Redundanzen	99,7489 %	≈ 22 Std.
Tier III	Mehrere Pfade, wartbar im Betrieb	99,9817 %	≈ 1,6 Std.
Tier IV	Vollständig fehlertolerant	99,9949 %	≈ 26,3 Min.

Ziel eines modernen Betriebskonzepts ist es, keinen Einzelausfallpunkt zuzulassen (No Single Point of Failure) und jedes technische Gewerk im Vollbetrieb isolieren und warten zu können.

Säule 2 — Rechtssicherheit und Betreiberverantwortung

Das Arbeitsschutzgesetz verpflichtet den Arbeitgeber, alle notwendigen Maßnahmen für Sicherheit und Gesundheit der Beschäftigten zu ergreifen. Die Betriebssicherheitsverordnung konkretisiert dies für Arbeitsmittel und Anlagen: Gefährdungsbeurteilung, Festlegung von Prüfart, Prüfumfang und Prüffristen sowie die Benennung „zur Prüfung befähigter Personen". In der Praxis meist Elektrofachkräfte mit einschlägiger Ausbildung und aktueller Praxiserfahrung.

Die DGUV Vorschrift 3 konkretisiert daraus die bekannten Wiederholungsprüfungen elektrischer Anlagen. Besonders relevant für Rechenzentren:

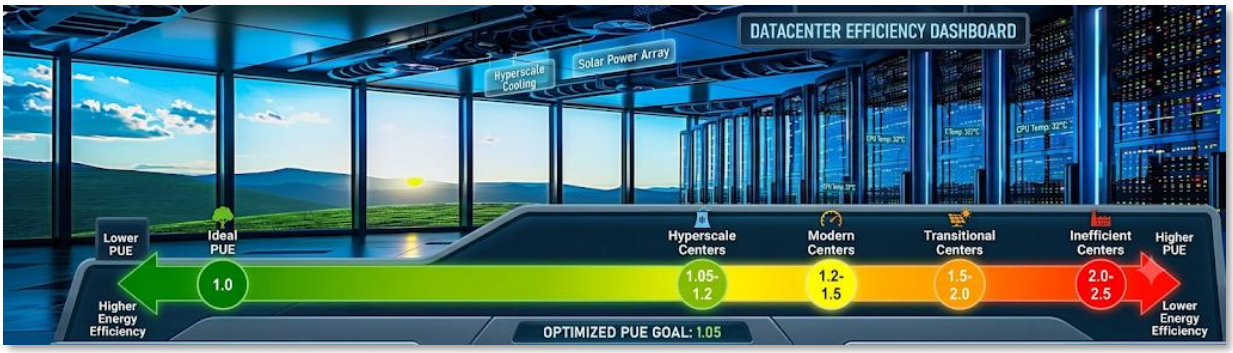
Anlage / Betriebsmittel	Prüffrist	Prüfer
Elektrische Anlagen, ortsfest	4 Jahre	Elektrofachkraft
… in Betriebsstätten besonderer Art (DIN VDE 0100 Gruppe 700)	1 Jahr	Elektrofachkraft
Fehlerstrom-Schutzeinrichtungen (stationär)	6 Monate	Benutzer
Bei dauerhafter RCM-/Isolationsüberwachung	Verlängerung/Aussetzung möglich	EFK + Messtechnik

> *Ein Betreiber muss nicht zwingend abschalten, um zu prüfen. DIN VDE 0105-100 erlaubt bei dauerhafter Überwachung – etwa per Differenzstromsensoren (RCM) nach DIN EN 62020 – die Aussetzung der klassischen Isolationsmessung, ohne die Prüfpflicht selbst aufzuheben.*

Diese Ausnahmeregelung ist für den unterbrechungsfreien 24/7/365-Betrieb von zentraler Bedeutung: Sie verbindet gesetzliche Prüfpflicht mit wirtschaftlicher Realität. Vorausgesetzt, das Managementsystem dahinter ist sauber dokumentiert.

Säule 3 — Nachhaltigkeit als Compliance-Aufgabe

Nachhaltigkeit ist längst kein freiwilliges Zusatzthema mehr. Die Corporate Sustainability Reporting Directive (CSRD) verpflichtet, nach der Anhebung der Schwellenwerte und der Verschiebung der Berichtswellen durch das EU-Omnibus-Paket, ab dem Geschäftsjahr 2027 einen kleineren, aber weiterhin wachsenden Kreis großer Unternehmen zu nicht-finanzieller Berichterstattung – auch Rechenzentrumsbetreiber entlang der Lieferkette bleiben mittelbar betroffen. Das Energieeffizienzgesetz (EnEfG) verlangt seit 2024 die Erfassung und teilweise Nutzung von Abwärme sowie konkrete PUE-Grenzwerte (Neubauten ≤ 1,2 ab 1.7.2026, Bestand ≤ 1,5 ab 2027 und ≤ 1,3 ab 2030) und ab 2027 einen bilanziell vollständig grünen Strombezug, nicht, wie mitunter verkürzt dargestellt, „klimaneutrale Neubauten": Rechenzentren werden dadurch energieeffizienter, aber nicht klimaneutral. Die EU-Taxonomie ergänzt Offenlegungspflichten zu Umweltkennzahlen.



Der PUE-Wert (Power Usage Effectiveness) bleibt eine wichtige, aber unvollständige Kennzahl: Er sagt nichts über Stromherkunft, CO2-Fußabdruck oder Wiederverwertbarkeit von Hardware aus.

Zertifizierungen wie das Sustainable-Data-Center-Label (SDC) von TÜV Rheinland bewerten deshalb ganzheitlich, von Standort und Bauweise über IT-Infrastruktur, Elektro- / Klimatechnik bis zu Abwärmenutzung, Wasserverbrauch, THG-Bilanzierung und Prozessqualität und ordnen den Betrieb in Effizienzklassen A bis G ein.

- **Kurzfristig**: PUE und Energieverbrauch erfassen und benchmarken, erste CO2-Bilanz (Scope 1–3), Quick-Wins wie Freikühlung und Leckagevermeidung.
- **Mittelfristig**: Abwärmenutzung prüfen, ESG-Strategie mit Zielpfaden, CSRD-Reporting vorbereiten.
- **Langfristig**: Rechenzentren nach Nachhaltigkeitskriterien modernisieren, Kreislaufwirtschaft (Refurbishment, Recycling), Zertifizierung gezielt einsetzen.

Säule 4 — Wirtschaftlichkeit und Bewirtschaftungsmodell

Wie ein Rechenzentrum bewirtschaftet wird, hängt stark vom Betreibertyp ab. Colocation-Betreiber steuern Sicherheit und technische Verfügbarkeit meist mit eigenem Fachpersonal und definieren Leistungen für Dritte.

Hyperscaler vergeben die Bewirtschaftung häufiger an spezialisierte Dienstleister, weil der Betrieb nicht zum Kerngeschäft zählt.

Enterprise-Betreiber integrieren das Rechenzentrum oft in ein unternehmensweites Facility Management, das nicht auf Rechenzentren spezialisiert ist – hier ist externe Expertise besonders wertvoll.

Über alle Betreibertypen hinweg gilt:

Der Anteil des Energieverbrauchs durch Gebäudetechnik ist in modernen Rechenzentren von rund 50 Prozent (2010) auf etwa 25 Prozent gesunken. Ein Effizienzgewinn, der ohne professionelle Dienstleistersteuerung kaum zu erreichen ist. Gleichzeitig verschärft der Fachkräftemangel die Auswahl geeigneter Partner.

APLEONA

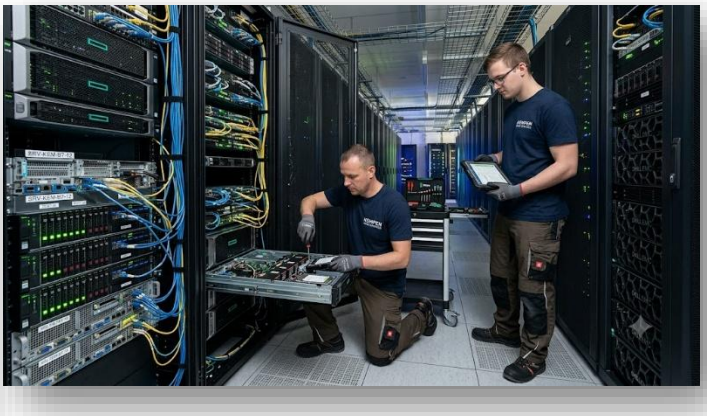
WISAG

Piepenbrock seit 1913

SPIE STRABAG

Dienstleistungssteuerung

Professionalisierung



KAPITEL 5

Die Dokumente, die jedes Rechenzentrum wirklich braucht

> *Wer Betrieb erst ab dem Go-Live denkt, plant das Ausfallrisiko bereits mit. Maximale RZ-Verfügbarkeit braucht die betriebliche Perspektive ab Tag eins der Planung.*

Viele der oben genannten Anforderungen laufen in der Praxis in wenigen zentralen Dokumenten zusammen. Sie sind kein Selbstzweck, sondern das Bindeglied zwischen High-End-Infrastruktur und dem Menschen, der sie betreibt.

Betriebsführungshandbuch

Das zentrale Dokument, das alle relevanten Betriebsprozesse festhält: Inbetriebnahme, Wartung und Instandhaltung, Störungs- und Zwischenfallmanagement, Modernisierung, Dokumentations- und Berichtswesen, Sicherheits- und Risikomanagement. Es ist ausdrücklich ein lebendes Dokument, das im Betrieb fortgeführt und regelmäßig angepasst wird – kein einmalig erstelltes Konzept.

Notfallhandbuch

Definiert Eskalationspfade, Zuständigkeiten und Sofortmaßnahmen für den Ernstfall, von Stromausfall bis Cybervorfall. Je klarer die Reaktionsketten vorab dokumentiert sind, desto geringer die Reaktionszeit im Ernstfall und desto besser die Verteidigungsposition gegenüber Aufsicht und Versicherer.

Betreiberkonzept

Beschreibt Rollen und Verantwortlichkeiten: Wer trägt welche Betreiberpflicht, welche Leistungen werden intern erbracht, welche extern beschafft. Häufig in Anlehnung an DIN EN 15221 und das Funktions- und Leistungsmodell nach RealFM strukturiert.

Wartungs- und Instandhaltungskonzept

Legt fest, welche Anlagen wie häufig präventiv, zustandsorientiert oder korrektiv instandgehalten werden, in Anlehnung an DIN EN 13306 und ISO 55001. Zustandsüberwachung (z. B. Schwingungsanalyse, Thermographie, Isolationsüberwachung) ermöglicht dabei, gesetzliche Prüffristen ohne Betriebsunterbrechung einzuhalten.

SOPs und EOPs

Standard Operating Procedures und Emergency Operating Procedures übersetzen die genannten Konzepte in konkrete, Schritt-für-Schritt-Arbeitsanweisungen für das Personal vor Ort. Die eigentliche Übersetzung von Norm in Handlung.

> *Ein Betriebsführungshandbuch ohne gelebte SOPs ist Papier. SOPs ohne dokumentiertes Betreiberkonzept sind Kür ohne Pflicht. Erst im Zusammenspiel entsteht Auditfähigkeit.*

KAPITEL 6

KRITIS und NIS2: neue Pflichten, neue Reichweite

Kritische Infrastrukturen, Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation, unterliegen besonderen Anforderungen an physische Sicherheit, IT-Sicherheit und Notfallmanagement. Rechenzentren ab einer bestimmten Größenordnung fallen explizit darunter.

Mit dem NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG), seit 6. Dezember 2025 in Kraft, hat der Gesetzgeber diesen Rahmen erheblich verschärft: Der Kreis betroffener Unternehmen wächst deutlich über die bisherigen KRITIS-Betreiber hinaus, Melde- und Nachweispflichten werden strenger, und die Verantwortung der Geschäftsleitung für IT- und Betriebssicherheit wird explizit gemacht. Für Betreiber bedeutet das:

- Physische Sicherheit: Zutrittskontrollen, Schutz vor Einbruch, Vandalismus und Naturkatastrophen müssen dokumentiert und nachweisbar sein.
- IT-Sicherheit: Abwehr von Cyberangriffen und unbefugtem Zugriff wird Teil der Betreiberpflicht, nicht nur der IT-Abteilung.
- Notfallmanagement: Erprobte Krisenpläne und regelmäßige Übungen werden zur Nachweispflicht, nicht zur Kür.
- Zertifizierte Sicherheit: Nachweisbare Standards, etwa nach ISO 27001, gewinnen an Bedeutung als Beleg gegenüber Aufsichtsbehörden.

Kriterium	KRITIS	NIS2
RECHTSGRUNDLAGE	• Nationales deutsches Recht (BSI-Gesetz, Verordnung)	• EU-Richtlinie, Umsetzung in nationale Gesetze
GELTUNGSBEREICH	• Betreiber Kritischer Infrastrukturen mit definierten Schwellenwerten	• Wesentliche und wichtige Einrichtungen in definierten Sektoren
BETROFFENHEITS-PRÜFUNG	• Anlagen- und versorgungs-bezogone Schwellenwerte	• Unternehmensgröße (Mitarbeitter, Umsatz/ Bilanzsumme) + Sektor
ADRESSAT	• Eng gefasst (systemrelevante Betreiber)	• Deutlich ausgeweitet, viele mittelständ Unternehmen betroffen
SEKTOREN	• Energie, Wasser, Gesundheit, Transport, Emährung, Finanzwesen, ITK u.a.	• Erweiterte Liste inkl. IT-Dienstleister, digitale Industrie, Abfallwintschaft, Forschung u.a.
FOKUS DER ANFORDERUNGEN	• Schutz kritischer Anlagen und IT-Systeme	• Ganzheitliches Cyber Risikamagement and Governance

Wer heute ein Betriebsführungshandbuch, ein Notfallkonzept und ein Betreiberkonzept sauber aufgesetzt hat, ist für NIS2 in weiten Teilen bereits vorbereitet, die Regelwerke ergänzen sich, statt sich zu widersprechen.

Ergänzend zur digitalen Sicherheit nach NIS2 gilt seit dem 17. März 2026 das KRITIS-Dachgesetz, das die europäische CER-Richtlinie (EU 2022/2557) über die Resilienz kritischer Einrichtungen in deutsches Recht überführt. Es schafft erstmals einen bundeseinheitlichen Rahmen für den physischen Schutz kritischer Infrastrukturen, Rechenzentren eingeschlossen, mit eigenen Registrierungs-, Risikoanalyse- und Resilienzpflichten.

Für Colocation- und Rechenzentrumsbetreiber mit Kunden aus dem Finanzsektor kommt zudem die Verordnung über die digitale operationale Resilienz im Finanzsektor (DORA) ins Spiel: Sie gelten dort seit Anfang 2025 unmittelbar als IKT-Drittdienstleister mit eigenen Nachweis- und Mitwirkungspflichten gegenüber ihren Finanzkunden.

KAPITEL 7

ITIL im Rechenzentrum: Betrieb als Servicemanagement

Neben den baulich-technischen und rechtlichen Rahmenbedingungen bildet das IT-Servicemanagement nach ITIL 4 das operative und strategische Fundament für einen verlässlichen Rechenzentrumsbetrieb. ITIL 4 löst die früheren starren Lebenszyklen (ITIL v3) ab und stellt das flexible Service Value System (SVS) in den Mittelpunkt. Dieses System transformiert eingehende Anforderungen (Demand) dynamisch in messbaren Nutzen (Value) für den Kunden und das Unternehmen.

Für eine ganzheitliche Betriebsführung berücksichtigt ITIL 4 stets die vier Dimensionen des Service Managements:

- **Organisationen und Menschen**: Klare Rollen, Kompetenzen und Betriebskulturen im RZ-Team.
- **Informationen und Technologie**: Die technische Infrastruktur, Monitoring-Tools und Automatisierungen.
- **Partner und Lieferanten**: Einbindung von Hardware-Herstellern, Wartungsdienstleistern und Carrier-Anbindungen.
- **Wertströme und Prozesse**: Schlanke, aufeinander abgestimmte Abläufe von der Bereitstellung bis zum Incident-Handling.

Innerhalb der flexiblen Wertschöpfungskette (Service Value Chain) sichern vor allem die zentralen Management-Praktiken den stabilen Tagesbetrieb bei kontinuierlich hohen Verfügbarkeitsanforderungen:

- **Incident Management:** Schnelle, strukturierte Reaktion auf Störungen zur frühestmöglichen Wiederherstellung des Normalbetriebs.
- **Change Enablement:** Rationale, kontrollierte und nachvollziehbare Steuerung von Anpassungen an der RZ-Infrastruktur zur Minimierung von Ausfallrisiken.
- **Problem Management:** Systematische Ursachenanalyse (Root Cause Analysis), um wiederkehrende technische Störungen nachhaltig zu eliminieren.
- **Service Level Management:** Transparente Definition, Überwachung und Steuerung der vereinbarten Qualitäts- und Verfügbarkeitsparameter (SLA/OLA).
- **Continual Improvement:** Die fortlaufende Optimierung von Prozessen, Systemen und Sicherheitsstandards als fest verankerter Grundsatz.

Durch diese integrative Sichtweise schlägt ITIL 4 die Brücke zwischen der hochkomplexen technischen RZ-Infrastruktur, einem aktiven Risikomanagement und der tatsächlichen Wertschöpfung für die Fachbereiche und Endkunden.

KAPITEL 8

Standort- und Bewirtschaftungsentscheidungen

Die Wahl des Standorts bleibt ein Kompromiss zwischen Latenz, Flächenverfügbarkeit, Stromversorgung und Nachhaltigkeit.

Hyperscaler priorisieren die Nähe zu internationalen Internetknoten, Enterprise-Betreiber legen mehr Wert auf Redundanz, Sicherheit und Betriebskosten. Wachsende Bedeutung gewinnen auch Empfehlungen zum Mindestabstand redundanter Standorte (inzwischen 200 statt früher 5 Kilometer) sowie die Verfügbarkeit von Grünstrom und Netzkapazität.

Für die Bewirtschaftung selbst zeigt sich ein klarer Trend: Immer mehr Auftraggeber konzentrieren sich auf die strategische Betriebssteuerung und vergeben operative wie taktische Facility Services an spezialisierte externe Partner. Entscheidend ist dabei nicht der Preis allein, sondern der Nachweis der Kompetenz – sowohl des Unternehmens als auch des eingesetzten Personals vor Ort.

Quelle: H2 2025 EMEA Data Centre Market Report von Cushman & Wakefield

Checkliste zur Selbstbewertung

Die folgenden Fragen verdichten die zentralen Themen dieses Whitepapers zu einer schnellen Standortbestimmung für Eigentümer, Betreiber und Asset-Manager:

- ☐ Gibt es ein aktuelles, gelebtes Betriebsführungshandbuch oder nur ein einmalig erstelltes Konzept?
- ☐ Ist eine Gefährdungsbeurteilung vorhanden, aktuell und mit benannten befähigten Personen hinterlegt?
- ☐ Sind Prüffristen bekannt, terminiert und, wo möglich, durch Managementsystem und Messtechnik verlängerbar?
- ☐ Existiert ein Notfallhandbuch mit klaren Eskalationspfaden und regelmäßigen Übungen?
- ☐ Ist die Organisation NIS2-/KRITIS-fähig aufgestellt, inklusive IT-Sicherheit und Meldewegen?
- ☐ Haben wir eine aktuelle CO2-Bilanz (Scope 1–3) und einen PUE-Wert im Marktvergleich?
- ☐ Nutzen oder planen wir die Verwertung von Abwärme?
- ☐ Ist unser Strombezug zu einem wesentlichen Anteil erneuerbar?
- ☐ Ist unsere Dienstleistersteuerung auf dem aktuellen Stand von Markt und Technik?
- ☐ Sind wir auf ein Audit eines Zertifizierungsanbieters (z. B. TÜV NORD CERT) oder ein DIN EN 50600-Audit heute vorbereitet, oder nur „historisch gewachsen“?

> *Wer bei mehr als zwei dieser Fragen zögert, hat keinen akuten Notfall, aber eine klare Prioritätenliste für den nächsten Betriebsführungs-Check.*

KAPITEL 10

Wie Vantur Consulting unterstützt

Vantur Consulting verbindet die Eigentümerperspektive mit operativer Umsetzbarkeit – für Immobilien ebenso wie für Rechenzentren. Unser Leistungsbild für den Rechenzentrumsbetrieb:

Betriebsführungshandbuch

Erstellung normkonformer Handbücher nach DIN EN 50600 und den Kriterienkatalogen gängiger Zertifizierungsanbieter (z. B. TSI.STANDARD von TÜV NORD CERT), als Grundlage für Zertifizierung und Tagesbetrieb, nicht als Aktenordner fürs Regal.

Notfall- und Betreiberkonzept

SOPs, EOPs, Eskalationspfade und klare Verantwortlichkeiten für den Ernstfall – rechtssicher nach KRITIS und NIS2 aufgesetzt.

Wartungs- und Instandhaltungskonzept

Präventive und zustandsorientierte Instandhaltung in Anlehnung an DIN EN 13306 und ISO 55001, für maximale Verfügbarkeit ohne unnötige Betriebsunterbrechungen.

Zertifizierungsbegleitung

Vorbereitung und Begleitung von Audits bei Zertifizierungsanbietern (z. B. TÜV NORD CERT) und von DIN-EN-50600-Audits bis zur erfolgreichen Zertifizierung, inklusive Auditsimulation und Dokumentenprüfung.

Betriebskosten- und Nachhaltigkeitsberatung

Benchmarking von FM-Kosten, PUE-Optimierung und Vorbereitung auf CSRD-Reporting und SDC-Zertifizierung, damit Nachhaltigkeit vom Compliance-Risiko zum Wettbewerbsvorteil wird.

FAZIT

Betrieb ist keine Nebensache

Rechenzentren werden nach höchsten technischen Standards gebaut. Ob sie diesen Anspruch über Jahre halten, entscheidet sich nicht im Bauplan, sondern im Betrieb. In klaren Verantwortlichkeiten, gelebten Prozessen, nachweisbarer Nachhaltigkeit und einer Dokumentation, die im Audit und im Ernstfall gleichermaßen trägt.

Die gute Nachricht: Die dafür nötigen Bausteine sind bekannt, normiert und erprobt. Es braucht keine Neuerfindung, sondern einen Partner, der Norm, Recht und Betrieb in ein handhabbares System übersetzt.