Bundesnetzagentur

- Beschlusskammer 6 -
BK6-24-210-1

26.09.2025

Festlegungsverfahren

zur zukünftigen Aggregation und Abrechnung bilanzierungsrelevanter Daten (MaBiS-Hub) – Fokuspunkt Messwertverarbeitung und Pseudonymisierung (BK6-24-210-1)

- Öffentliche Konsultation IT-Leitlinien MaBiS-Hub -

Die Beschlusskammer 6 stellt neben den prozessualen Vorgaben auch IT-Leitlinien für den Aufbau des MaBiS-Hub zur öffentlichen Konsultation.

Zur Kommentierung der Ausführungen verwenden Sie bitte ausschließlich den entsprechenden Reiter der Excel-Konsultationsdatei.

Abkürzungen

AES	Advanced Encryption Standard
BA	Bilanzierungs- und Aggregierungsverantwortlicher
BCM	Business Continuity Management
BKV	Bilanzkreisverantwortlicher
DRP	Disaster Recovery Plans
IEC	Internationale Elektrotechnische Kommission
iMSys	Intelligentes Messsystem
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
LF	Lieferant
MaBiS	Marktregeln für die Durchführung der Bilanzkreisabrechnung Strom
MaKo	Marktkommunikation
MaLo	Marktlokation
MeLo	Messlokation
MB	Megabyte
MSB	Messstellenbetreiber
MV	Messwertverarbeiter
NB	Netzbetreiber
RPO	Recovery Point Objective
RPS	Requests per Second
RTO	Recovery Time Objective
SLA	Service Level Agreement
SLI	Service Level Indicator
SLO	Service Level Objectives
SMGW	Smart Meter Gateway
TLS	Transport Layer Security

Definitionen

Betriebsverfügbarkeit

Die Betriebsverfügbarkeit beschreibt den Anteil der geplanten Laufzeit, in der ein System tatsächlich betriebsbereit und nutzbar ist. Es werden sowohl ungeplante Ausfälle wie auch geplante Wartungs- und Instandhaltungsfenster berücksichtigt.

Kernsystem

Alle Systemteile, die direkten Einfluss auf die Verfügbarkeit der Funktion des Messwertverarbeiters (MV) und Bilanzierungs- und Aggregierungsverantwortlichen (BA) haben.

Unterstützende Systeme

Alle Systemteile, die den Komfort oder die Analyse beeinflussen, aber die die Funktionsfähigkeit des MV oder BA unberücksichtigt lassen. Hier sind beispielsweise Reporting Dashboards oder Analytics Prozesse zu nennen.

Service Level Agreement (SLA)

Ein SLA (Service Level Agreement) ist eine Vereinbarung zwischen Anbieter und Kunden über messbare Metriken wie Verfügbarkeit und Reaktionsfähigkeit. SLA enthalten formelle Verpflichtungen gegenüber den Kunden und legen die Konsequenzen dar, wenn diese Verpflichtungen nicht eingehalten werden.

Service Level Indicator (SLI):

Ein SLI (Service Level Indicator) misst die Einhaltung der vorgegebenen Zielwerte eines SLO. Die Messwerte müssen dabei mindestens die definierten Zielwerte erreichen oder besser sein.

SLO und SLI sind in Form eines Service Level Agreement (SLA) festzuhalten.

Service Level Objective (SLO):

Ein SLO (Service Level Objective) definiert einen Zielwert für eine bestimmte Metrik über eine bestimmte Zeit, welches den angestrebten Wert (z.B. Verfügbarkeit, Latenz) festlegt und damit eine konkrete Leistungsqualität eines IT-Services oder Systems definiert.

Technische Verfügbarkeit

Die Technische Verfügbarkeit definiert, wie lange das System für einen Zeitraum seine technische Funktionalität stabil aufrechterhält und keine Ausfälle aufweist. Dabei misst die technische Verfügbarkeit nur ungeplante Ausfallzeiten (wie z.B. Hardware-, Netzwerk- oder Softwarefehler).

Recovery Time Objective (RTO):

Das Recovery Time Objective ist die maximale zulässige Zeitspanne bis zur Wiederherstellung der Betriebsbereitschaft nach Ausfall des Systems, von Systemkomponenten, -diensten, -prozessen, & -funktionen.

Inhaltsverzeichnis

1. Übergreifende Anforderungen 5
   1.1. Technische Gesamtanforderungen 5
2. Performance 6
   2.1. Reaktions- und Antwortzeiten 6
   2.2. Anfragenverarbeitung 6
3. Verfügbarkeit 6
   3.1. Technische Verfügbarkeit 6
   3.2. Betriebsverfügbarkeit 6
   3.3. Backups & Disaster Recovery 7
4. Skalierbarkeit und Erweiterbarkeit 7
   4.1. Technische Voraussetzungen 7
   4.2. Neue Funktionen und Services 8
   4.3. Verhalten bei Last 8
5. IT- und Datensicherheit 8
   5.1. Strategische Ebene: Sicherheitsrahmen und Governance 8
   5.2. Operative Maßnahmen: Sicherheitsmanagement und Prozesse 9
   5.3. Technische Umsetzung: Schutzmaßnahmen und Infrastruktur 9
   5.4. Qualitätssicherung und Kontrolle 10
6. Wartbarkeit und Dokumentation 10
   6.1. Modulare Strukturierung des Quellcodes 10
   6.2. Dokumentationsanforderungen 10
   6.3. Testkonzept 10
7. Betrieb und Support 11
8. Revisionssicherheit und Auditierung 11
   8.1. Revisionssicherheit 11
   8.2. Auditierung 11
9. Monitoring und Reporting 12
   9.1. Technisches Monitoring 12
   9.2. Reporting an die Bundesnetzagentur 12
   9.3. Technischer Statusbericht für Marktteilnehmer 12
10. Release- und Change Management 13
   10.1. Release Management 13
   10.2. Change Management 13
   10.3. Revisionssichere Ablage 13

1. Übergreifende Anforderungen

- Der MaBiS-Hub ist von technischer Seite so zu dimensionieren, dass er perspektivisch die anwachsende Anzahl von Stamm- und Abrechnungsdaten (siehe Anhang) als auch die von der Bundesnetzagentur festgelegten prozessualen Anforderungen performant abbilden kann
- Dabei soll die Performance entsprechend den Anforderungen skalieren und nicht im ersten Schritt die perspektivischen Volumina erfüllt werden
- Der Messwertverarbeiter und der Bilanzierungs- und Aggregierungsverantwortliche des MaBiS-Hub halten ihre Daten separat und kommunizieren diese nur über Schnittstellen und die festgelegten Prozesse

1.1. Technische Gesamtanforderungen

- **Softwareentwicklung und Quellcode**
  - Verwendung von **offenen Programmiersprachen** mit breiter Community-Unterstützung (z. B. Java, Python, Go)
- **Open Source**
  - Der vollständige Quellcode der Anwendung ist unter einer anerkannten Open-Source-Lizenz (z. B. Apache 2.0) zu veröffentlichen
  - Offene Bereitstellung und Pflege von Dokumentationen und Schnittstellen-Spezifikationen
- **Einsatz von KI-Tools**
  - KI-Tools zur Unterstützung des gesamten Entwicklungsprozesses (von der Anforderungserhebung und -spezifizierung über die technische Spezifizierung, Codegenerierung, Tests bis zur Dokumentation) sind zulässig, wenn Datenschutzkonformität sichergestellt ist (z.B. keine Datenübertragung in Nicht-EU-Drittländer) und generierte Inhalte manuell überprüft und dokumentiert werden
  - Softwareentwickler behalten die ausschließliche Verantwortung für den KI-produzierten und eingecheckten Quellcode
- **ACID-Prinzipien als Systemgrundlage**
  - Anwendung des ACID-Modells (Atomicity, Consistency, Isolation, Durability) auf alle transaktionsbasierten Prozesse
  - Das ACID-Prinzip ist übergreifend für Datenverarbeitung, Aggregation, Bilanzierung und Archivierung verpflichtend einzuhalten
- **Schnittstellenmanagement**
  - Standardisierte, dokumentierte APIs (z.B. REST mit OpenAPI-Spezifikation)
  - Verwendung offener Datenstandards und Formate (z.B. JSON, XML) unter Berücksichtigung der von der EDI@Energy vorgegebenen Datenformate und Standards
  - Unterstützung von Schnittstellen für andere Hubs / Plattformen (Interoperabilität)
- **Datenmanagement**
  - Nutzung eines kanonischen Datenmodells zur Harmonisierung der Datenflüsse

2. Performance

Eine hohe Systemperformance muss reibungslose Abläufe, kurze Antwort- und Reaktionszeiten und eine positive Nutzererfahrung sicherstellen.

2.1. Reaktions- und Antwortzeiten

- **Allgemein:**
  - Überwachung und Dokumentation der vorgegebenen Zielwerte als Messgröße
  - Monitoring und Reporting der Reaktions- und Antwortzeiten
  - Bei Zielwertverstößen sind automatisierte technische und prozessuale Mechanismen und Maßnahmen zur kontinuierlichen Zielerreichung umzusetzen
- **Service Level Objectives (SLO)**
  - End-to-End Latenzbudget (Perzentile): P50=100ms, P95=500ms, P99=1000ms
  - Systemauslastungsgrenzen
    - CPU-Auslastung: P99 ≤ 80%
    - RAM-Auslastung: P99 ≤ 80%

2.2. Anfragenverarbeitung

- Hauptlasten des Datenempfangs ergeben sich aus den Fristen aus der Festlegung „Wechselprozesse im Messwesen Strom Teil 2 – Fokus Übermittlung von Werten“
- Anfragenverarbeitung ≥ 1.000 gleichzeitige API-Aufrufe pro Sekunde (RPS)
- Für API-Anfragen/-Antworten ist die Payload (Body) auf
  - 2MB maximal beschränkt
  - Wo Komprimierungsalgorithmen einsetzbar sind, sind diese zwingend zu verwenden

3. Verfügbarkeit

- Die technische Verfügbarkeit (ausschließlich ungeplante Ausfälle) ist als Monatsmittelwert vorgegeben
- Die Betriebsverfügbarkeit (ungeplante + geplante Ausfälle) ist als Jahresmittelwert vorgegeben
- Ein Monitoring der Verfügbarkeiten ist im Reporting zu berücksichtigen (siehe Kapitel 9)

3.1. Technische Verfügbarkeit

- SLO Technische Verfügbarkeit:
  - Kernsystem: ≥99,95% (max. ~22min Downtime pro Monat)
  - Unterstützende Systeme: ≥97% (max. ~22h Downtime pro Monat)

3.2. Betriebsverfügbarkeit

- SLO Betriebsverfügbarkeit:
  - Kernsystem: ≥99,68%: (technische Verfügbarkeit + 24h (geplante) Downtime pro Jahr)
  - Unterstützende Systeme: ≥95% (technische Verfügbarkeit + 175h (geplante) Downtime pro Jahr)
- Geplante Downtime ist als Gesamtbudget für ein Jahr zu verstehen und kann verteilt werden
  - Kernsystem: Max. zulässige geplante Downtime pro Tag 8h

    - Unterstützende System: Max. zulässige geplante Downtime 48h

- Wartungsarbeiten und damit verbundene Einschränkungen sind 7 Tage vor Durchführung anzukündigen, sofern diese an Wochenenden durchgeführt werden
- Wartungsarbeiten und damit verbundene Einschränkungen sind 14 Tage vor Durchführung anzukündigen, sofern diese an einem Werktag durchgeführt werden müssen

3.3. Backups & Disaster Recovery

- Disaster Recovery Plans (DRP) sind zu erstellen, umzusetzen, kontinuierlich zu testen und zu überprüfen in Bezug auf
    - Szenarien: Systemkomplettausfall, Sicherheitsvorfall, Rechenzentrumsausfall
- Tests sind zu dokumentieren und auszuwerten (kontinuierliche Verbesserung)
- Notfall- & Kommunikationspläne sind zu erstellen und mind. halbjährlich zu testen

- **Backups:**

    - Grundlegend:
        - Anwendung 3-2-1 Prinzip für alle vollständigen Backups: 3 gesamt, 2 auf unterschiedlichen Medien am gleichen Ort und 1 Backup an einem anderen Ort (Georedundanz)
        - Backups sind, unter Berücksichtigung der aktuell geltenden Best-Practice-Vorgaben des Bundesverbands IT-Sicherheit, zu verschlüsseln und vor unbefugten Zugriffen zu schützen
    - Durchführung:
        - Viertelstündliche Snapshots, Aufbewahrungszeit 1 Tag
        - Tägliche inkrementelle Backups, Aufbewahrungszeit 7 Tage
        - Wöchentlich vollständige Backups, Aufbewahrungszeit 30 Tage
        - Monatlich vollständige Backups werden 12 Monate lang aufbewahrt
    - Test und Verifizierung
        - Funktions- und Backuptests des/der Systems(e) sind halbjährlich durchzuführen und zu protokollieren
    - Backup-Protokolle von vollständigen Backups sind zu erstellen

- **Wiederherstellungszeit**

        - Zulässige Zeitspanne bis zur Wiederherstellung bei Ausfall von Systemkomponenten, -diensten, -prozessen, & -funktionen als Recovery Time Objective (RTO):
        - Kernsysteme: ≤ 22min
        - Unterstützende Systeme: ≤ 2h

4. Skalierbarkeit und Erweiterbarkeit

4.1. Technische Voraussetzungen

- Cloud-native, mandantenfähige und containerisierte Architektur
- Unterstützung von horizontaler und vertikaler Skalierung
- Nutzung standardisierter Plattformtechnologien (z. B. Kubernetes, OpenShift)
- Lose Kopplung der Komponenten zur Verbesserung von Wartbarkeit und Erweiterbarkeit

4.2. Neue Funktionen und Services

- **Systemarchitektur ist modular und erweiterbar ausgelegt:**
  - Neue Funktionen sollen als eigenständige Module ergänzt werden können
  - Keine tiefgreifenden Änderungen am bestehenden Kernsystem erforderlich
- **Erweiterbarkeit betrifft etwa:**
  - Neue Verarbeitungstypen (z.B. zusätzliche Bilanzierungsverfahren)
  - Neue Datenquellen und Schnittstellen (z.B. andere Hubs, Plattformen)
  - Anpassung an gesetzliche oder regulatorische Änderungen ohne Re-Design

4.3. Verhalten bei Last

- **Horizontale und vertikale Skalierbarkeit:**
  - Es müssen beliebig viele Instanzen von Services im Live-Betrieb möglich sein
  - Dynamische Ressourcenanpassung bei Lastspitzen (Auto-Scaling)
  - Services und Dienste müssen stateless bereitgestellt werden, um eine maximale horizontale Skalierung gewährleisten zu können
- **Leistungsfähigkeit insbesondere garantiert bei:**
  - Stark steigendem Transaktionsvolumen von Messwerten
  - Hohem Änderungsaufkommen von Stammdatenänderungen
  - Hinzufügen neuer Marktteilnehmer
  - Ausfällen von einzeln Komponenten bis zu Rechenzentren
- **Kein Funktionsverlust oder Systemabbruch bei:**
  - Erhöhter Datenfrequenz
  - Gleichzeitigen Aggregations- und Analyseprozessen
  - Ausfall der zugrunde liegend Hardwareinfrastruktur (z.B. Rechenzentren)

5. IT- und Datensicherheit

5.1. Strategische Ebene: Sicherheitsrahmen und Governance

- Die Umsetzung muss die relevanten Gesetze und Richtlinien, insbesondere NIS2-Gesetz, IT-Sicherheitsgesetz 2.0, DSGVO, EU AI Act, EU Data Act berücksichtigen
- Umsetzung berücksichtigt die Empfehlungen der Handreichung „Stand der Technik“ des Bundesverband IT-Sicherheit in der jeweils aktuell geltenden Fassung
- Zertifizierung MaBiS-Hub gem. ISO/IEC 27001 auf Basis BSI IT-Grundschutz
- Etablierung eines **ISMS** (ISO/IEC 27001, BSI 200-1 bis 200-3), u.a.:
  - Verpflichtende Einführung und Pflege eines vollständigen ISMS
    - Definition von Schutzbedarfskategorien (vertraulich, kritisch, normal)
    - Regelmäßige Risikoanalysen und -bewertungen, in jedem Fall immer vor geplanten Änderungen am IT-Verbundsystem sowie bei neuerkannten Bedrohungsszenarien
  - Dokumentation aller sicherheitsrelevanten Prozesse (technisch + organisatorisch)
  - Klare Regelung aller Rollen, Verantwortlichkeiten, Eskalationsprozesse
  - Einrichtung eines BCM gemäß BSI 200-4
- **Etablierung einer wirksamen Data Governance**
  - Weitreichende Definition und Dokumentation der Datennutzungsprozesse (Zugriffe, Weiterverarbeitung, Archivierung, Löschung)
  - Klassifikation der Daten und Einrichtung eines Datenlebenszyklusmanagements
  - Protokollierung aller datenschutzrelevanten Vorgänge (Privacy Audit Trail)

    - Schaffung einer automatisierten Datenexportfunktion bis auf Basis Messstellen-granularer Datensätze zur Erfüllung der Vorgaben des EU AI Acts
- Berücksichtigung von Sicherheitsaspekten von Beginn an in Architektur, Entwicklung, Betrieb (Security „by Design“):
    - Einhaltung von Zero-Trust-Prinzipien bei der Integration: restriktive und kontrollierte Integration von Code in produktive Systeme
    - Einrichtung eines effektiven Abhängigkeitsmanagements, insb. Anfertigung und Pflege einer Software Bill of Materials für alle eingesetzten 3rd-Party Software-Module, -Bibliotheken, etc.
    - Definition von Security Policies und Contribution Guidelines
    - Verwendung von Signaturen und Hashes, die stets dem aktuellen Stand der Technik genügen müssen (aktuell SHA-2)

5.2. Operative Maßnahmen: Sicherheitsmanagement und Prozesse

- Anfertigung eines (Fach-)Sicherheitskonzepts nach Standard 200-2 BSI und regelmäßige Aktualisierung; dabei insbesondere bereits in der Konzeptionsphase Feststellung des Schutzbedarfs auf Basis des Architekturkonzepts für Ableitung des Schutzbedarfsniveaus
- Etablierung Incident-Response-Prozesse und Notfallpläne inkl. Erstellung interner und externer Informationsketten
- Einrichtung eines effektiven Sicherheits-Patches- und Schwachstellenmanagements gem. der aktuell geltenden Handreichung „Stand der Technik“ des Bundesverbands IT-Sicherheit e.V.

5.3. Technische Umsetzung: Schutzmaßnahmen und Infrastruktur

- **Technisch-organisatorische Maßnahmen** (TOMs)
    - Ergreifung und Dokumentation von technischen und organisatorischen Maßnahmen (TOM) für den Informationsverbund gem. Handreichung „Stand der Technik“ des Bundesverbands IT-Sicherheit e.V. (jeweils aktuelle Fassung)
- **Identity & Access Management** (IAM)
    - Verwendung der SM-PKI als Authentifizierung der Marktteilnehmer
    - Einsatz von 2FA / MFA bei besonders schützenswerten Bereichen (beispielsweise im Administrationsbereich des Betreibers)
- **Berechtigungsmanagement**
    - Zentrale Verwaltung und Auditierung aller Berechtigungen
    - Erstellung und Umsetzung eines Rollen- und Attribut-basierten Berechtigungskonzepts für den Zugriff auf Systemteile und Daten des MaBiS-Hub; dabei Regelung und Umsetzung von Onboarding- / Offboarding-Prozessen sowie Delegationsfähigkeit und Nachvollziehbarkeit von Rollenvergaben
- **Verschlüsselung**
    - Kryptoagile Gestaltung des Systems, insb. durch Vorbereitung des Einsatzes von Post-Quanten-sicheren Verfahren
    - Die verwendeten Verschlüsselungsverfahren müssen stets dem aktuellen Stand der Technik entsprechen und sowohl die Anforderungen des BSI IT-Grundschutz-Kompendiums Baustein CON.1 als auch die Vorgaben der DSGVO erfüllen
    - Ende-zu-Ende-Verschlüsselung aller Datenübertragungen
    - Nutzung der SM-PKI Zertifikate für die Verschlüsselung
    - Verschlüsselung ruhender Daten (aktueller Standard ist AES-256)
- **Monitoring**

- Einrichtung von Systemen zur effektiven Angriffserkennung (Intrusion Detection System, IDS) und -verhinderung (Intrusion Prevention System, IPS)

5.4. Qualitätssicherung und Kontrolle

- Jährliche externe Security Audits
- Risikoanalysen und Updates hinsichtlich Anlass, Turnus und Inhalt gem. Zertifizierungsbedingungen
- Mindestens jährliche Durchführung externer Penetrationstests
- Code Reviews sicherheitskritischer Module
- Sicherheitsanalysen bei jeder wesentlichen Systemänderung
- Ergebnisse inkl. Maßnahmenumsetzung sind an BNetzA zu kommunizieren

6. Wartbarkeit und Dokumentation

6.1. Modulare Strukturierung des Quellcodes

- Klare Trennung von Fachlogik, Infrastruktur, Schnittstellen und technischen Hilfsklassen
- Einhaltung von Modularitätsprinzipien: kleine, wiederverwendbare, klar abgegrenzte Komponenten
- Verwendung von standardisierten Frameworks und Architekturmustern (z.B. MVC, Microservices)
- Hohe Lesbarkeit und Kommentierung des Codes
- Rückverfolgbarkeit der Fachlogik durch sprechende Methodennamen, strukturierte Module und Dokumentationen

6.2. Dokumentationsanforderungen

- Lebende Systemdokumentation in einem zentralen, versionierten Repository (z.B. GitLab, Confluence)
    - Zielgruppenorientierte Dokumentation:
        - **Anwenderdokumentation** (Nutzer, Marktpartner)
        - **Betriebsdokumentation** (Systemadministration, IT-Operations)
        - **Entwicklerdokumentation** (Modulstruktur, Codebeispiele, API)
- Automatisierte Dokumentation technischer Schnittstellen mittels OpenAPI-Spezifikation
    - Bereitstellung für alle Datenzulieferer und Marktpartner
    - Versionierung und Änderungsverfolgung

6.3. Testkonzept

- Definition und Pflege eines umfassenden Testkonzepts für:
    - **Unit-Tests** (Modul-/Funktionslogik)
    - **Integrationstests** (Systemverhalten, Schnittstellen)
    - **End-to-End-Tests** (Nutzerprozesse)
    - **Last- und Performancetests** (bei Releases und Simulationen)
- Einsatz von automatisierten Testroutinen (CI/CD)
- Testabdeckung in % als Kennzahl für das Reporting

7. Betrieb und Support

- Bereitstellung eines technischen 2nd Level Supports und eines 3rd Level Supports für Energiemarktteilnehmer
- Kein Clearing von fehlerhaften Messwerten, keine Klärung prozessualer Abwicklungsfragen
- **Erreichbarkeit**
  - Servicezeiten: 24/7
  - Kanäle: Ticketsystem
- **Reaktionszeiten (erste Rückmeldung)**
  - Gestaffelt nach Priorität/Kritikalität
  - Blocker: < 15 Minuten
  - Kritisch: < 1 Stunde
  - Normal: < 8 Stunden
  - Niedrig: < 24 Stunden
- **Lösungszeiten:**
  - Gestaffelt nach Priorität/Kritikalität
  - Blocker: < entsprechend RTO
  - Kritisch: < 8 Stunden
  - Normal: < 3 Tage
  - Niedrig: < 5 Tage

- **Incident- und Problemmanagement**
  - Umsetzung eines strukturierten, ISO 20000-kompatiblen Prozesses
  - Automatisierte Erkennung von Incidents über Monitoring
- **Error-Handling**
  - Zentrale Fehlerbehandlung mit:
    - Maschinell auswertbarer Protokollierung
    - Fehlertyp-Klassifikation (technisch / fachlich / extern)
    - Verlinkung zu Handlungsanweisungen (Knowledge Base)

8. Revisionssicherheit und Auditierung

8.1. Revisionssicherheit

- Alle systemrelevanten Vorgänge (z.B. Datenverarbeitung, Rollenvergabe, Wertbildung) müssen vollständig, nachvollziehbar und unveränderbar dokumentiert werden
- Unveränderbarkeit der Logs (z.B. durch WORM-Speicherung, digitale Signaturen)
- Zeitstempelung aller Aktionen im Format UTC mit Zeitzone bzw. Sommer- und Winterzeit
- Versionierung aller Stammdaten
- Aufbewahrungsfristen entsprechend der gesetzlichen Vorgaben
- Dokumentation von:
  - Änderungen an Stamm- und Bewegungsdaten, Berechnungsformeln, Konfigurationen
  - Zugriffs- und Änderungsrechten

8.2. Auditierung

- **Zentrales Audit-Frameworks:**
  - Prüfung auf Einhaltung von Sicherheits-, Datenschutz- und Abrechnungsanforderungen
  - Audit-Logs zu jeder Interaktion mit sensiblen oder sicherheitsrelevanten Systemteilen
- **Auditfähige Protokollierung:**
  - Nutzer- und Systemzugriffe (Login, Rollenwechsel, API-Calls)

    - Änderungen an Berechnungslogiken, Konfigurationen, Stammdaten / Nachweis über die Regulatorik-konforme Abrechnungslogik
    - Bearbeitung von Werten (z.B. Korrekturen, Reklamationen, Ersatzwertbildung)
    - Prozessdurchläufe (z.B. Aggregationen, Abrechnungsdurchläufe)
- **Zugriff auf Auditdaten:**
    - Nur für berechtigte Rollen (z.B. Revisionsstelle, BNetzA, Betreiber)
    - Möglichkeit zum Export revisionsrelevanter Protokolle (z.B. PDF, JSON, XML)
- **Interne und externe Audits:**
    - Jährliche interne System- und Sicherheitsüberprüfungen oder anlassbezogen bei Vorfällen
    - Unterstützung externer Audits durch Dritte (z.B. Wirtschaftsprüfer, Datenschutzaufsicht, BNetzA)
    - Dokumentierte Auditpläne, Auditberichte und Maßnahmenverfolgung

9. Monitoring und Reporting

9.1. Technisches Monitoring

- Zentrale Überwachung der Systemlandschaft:
    - Infrastrukturressourcen (CPU, RAM, Speicher, Netzwerk)
    - Verfügbarkeit und Status von Services, Schnittstellen und Datenbankverbindungen
    - API-Antwortzeiten, Fehlerhäufigkeiten, Queues
    - Nutzerzugriffe
- Echtzeit-Alarme bei Überschreitung der festgelegten Kennzahlen an Betreiber und BNetzA
- Speicherung technischer Monitoringdaten für mindestens 12 Monate
- Verknüpfung mit Incident- und Eskalationsmanagement
- Revisionssicher, speicherbar und auswertbar

9.2. Reporting an die Bundesnetzagentur

- Format: Standardisierte, revisionssichere Reports (z.B. maschinenlesbar + signiertes PDF)

Berichtsinhalte	**Frequenz**
Verfügbarkeiten und Ausfallzeiten (inkl. geplanter Wartungen)	Monatlich
Nachweis von Penetrationstests	Jährlich
Ergebnisse von Audits und damit verbundener Umsetzungsmaßnahmen	Jährlich
Fristentreue und Datenqualität bei Datenanlieferung von Stamm- und Bewegungsdaten	Nach näherer Maßgabe BNetzA
Beschwerdehäufigkeit je Marktteilnehmer	Nach näherer Maßgabe BNetzA
Nachweis von End-to-End Tests	Anlassbezogen
Erhebliche IT-Störungen (§ 8b Abs. 4 BSIG)	Anlassbezogen
Erheblicher Sicherheitsvorfall (NIS2)	Anlassbezogen
Sonstige auf Anforderungen BNetzA beizutragende Inhalte	Anlassbezogen

9.3. Technischer Statusbericht für Marktteilnehmer

- Aufbau und Zurverfügungstellung einer Status Page, über die Marktteilnehmer Informationen zur historischen (90 Tage) und aktuellen technischen Verfügbarkeit abrufen können

10. Release- und Change Management

10.1. Release Management

- **Definition von Release-Arten**:
  - **Major Release**: Neue Hauptfunktionen, potenziell breaking changes
  - **Minor Release**: Erweiterungen, neue Schnittstellen, keine Abwärtsinkompatibilität
  - **Patch Release / Hotfix**: Fehlerbehebung oder sicherheitskritische Aktualisierungen
- **Versionierungs-System**:
  - Verwendung des **semantischen Versionierungs-Schemas** (Versionsnummer von MAJOR.MINOR.PATCH)
  - Alle Releases müssen eindeutig dokumentiert und Changelog-geführt werden
- **Rollout-Strategie**:
  - Vorabbereitstellung auf Testumgebungen
  - Einhaltung definierter Release-Zyklen (z.B. quartalsweise)
  - Bereitstellung von:
    - Release Notes
    - Migration Guides
    - Testszenarien
- **Rollback-Konzept**:
  - Alle Releases müssen rücksetzbar sein (Rollback oder Hotfix-Fallback). Daten müssen entsprechend aus letztem Snapshot / Sicherheitspunkt wiederhergestellt werden
  - Validierte Snapshots und Sicherungspunkte als technischer Rückhalt
- **Vorlaufzeiten:**
  - Neue Releases müssen den Marktpartner mit folgender Mindestvorlaufzeit angekündigt werden:
    - Major Release: mind. 3 Monate
    - Minor Release: mind. 8 Wochen
    - Patches: mind. 2 Tage
    - Hotfix: keine

10.2. Change Management

- **Veränderungskategorien**:
  - Standard-Changes: Geplante, risikoarme Änderungen mit Freigabeprozess
  - Emergency-Changes: Dringende Korrekturen (z.B. Sicherheitslücken, Systemausfall)
  - Signifikante Changes: Änderungen mit fachlicher Auswirkung, z.B. Datenstruktur, Algorithmus
- **Change-Request-Verfahren**:
  - Jeder Änderungsbedarf wird als Change Request (CR) dokumentiert:
    - Beschreibung, Auswirkung, Verantwortlicher, Prüfdatum
    - Bewertung von Risiken, Testbedarf und Kommunikationsmaßnahmen
  - CRs werden durch ein Change Advisory Board (CAB) geprüft und freigegeben
- **Testpflicht vor Produktivsetzung**:
  - Jeder Change durchläuft abgestufte Tests (Unit, Integration, UAT)
  - Erfolgsnachweise in Form von Testprotokollen
  - Nur dokumentierte, geprüfte und freigegebene Changes dürfen deployed werden

10.3. Revisionssichere Ablage

- Alle CRs, Entscheidungsprotokolle, Testdokumente und Abnahmeprotokolle werden:
  - Versioniert und revisionssicher abgelegt