Informations-sicherheitsleitlinie

Die Leitlinie beschreibt die Informationssicherheitspolitik von Stromnetz Berlin.

Stromnetz Berlin

Inhaltsverzeichnis

Abbildungsverzeichnis

Präambel

Als Betreiberin des Stromverteilnetzes stellt Stromnetz Berlin eine für die Gesellschaft kritische Infrastruktur bereit. Daraus ergeben sich nicht nur erhöhte regulatorische Anforderungen, sondern auch eine besondere Verantwortung. Der Betrieb und die Weiterentwicklung des Berliner Stromverteilnetzes sowie der dafür notwendigen Prozesse hängen in hohem Maße von der Stabilität und Sicherheit der eingesetzten IT- und OT-Systeme ab. Dabei ist die Sicherstellung der Informationssicherheit von zentraler Bedeutung und umfasst den nachhaltigen Schutz der Verfügbarkeit, Integrität und Vertraulichkeit von Informationen, Prozessen, Systemen, Anwendungen und Dienstleistungen, die für den Geschäftsbetrieb von Stromnetz Berlin erforderlich sind.

Angesichts zunehmender Bedrohungen im Cyberraum, der notwendigen Digitalisierung der Netzinfrastruktur für die Energiewende sowie regulatorischer Änderungen ist es notwendig, Informationssicherheit als ganzheitliche Aufgabe im gesamten Unternehmen und allen Bereichen von Stromnetz Berlin zu verstehen. Die strukturierte Umsetzung der Informationssicherheit bei Stromnetz Berlin erfolgt durch den Betrieb eines Informationssicherheitsmanagementsystem (ISMS), welches auf einer einheitlichen und verbindlichen Informationssicherheitsstrategie basiert und einem kontinuierlichen Verbesserungsprozess unterliegt.

Für den Erfolg des Managementsystems ist ein ausgewogenes Verhältnis zwischen akzeptierten Vorgaben, einer aktiven Steuerung und Awareness innerhalb von Stromnetz Berlin erforderlich. Dies setzt ein nachhaltiges Commitment der Geschäftsführung und der obersten Leitungsebene von Stromnetz Berlin voraus.

Regelungen

Diese Leitlinie regelt als führendes Dokument die Informationssicherheit von Stromnetz Berlin. Sie gibt einen strategischen Überblick über die Gesamtstruktur des Managementsystems (ISMS) inklusive der definierten Rollen und Verantwortlichkeiten. Die Leitlinie definiert die Ziele an die Informationssicherheit und erklärt, wie diese die Unternehmensziele von Stromnetz Berlin unterstützen. Die Umsetzung der Informationssicherheitsleitlinie bei Stromnetz Berlin orientiert sich unter anderem an folgenden regulatorischen Rahmenbedingungen:

- NIS2-Umsetzungsgesetz (NIS2) zur Umsetzung der EU NIS2-Richtlinie in Deutschland
- Energiewirtschaftsgesetz (EnWG) für Sicherheitsvorgaben an Energienetzbetreiber
- Messstellenbetriebsgesetz (MsbG) für Sicherheitsvorgaben zum Betrieb intelligenter Messsysteme
- BSI-Gesetz (BSIG) für Sicherheitsvorgaben an Einrichtungen und Betreiber kritischer Anlagen
- Kritis-Verordnung (KritisV) für Festlegungen für Betreiber kritischer Anlagen
- IT-Sicherheitskatalog (IT-SiKat) der Bundesnetzagentur für Energienetzbetreiber

Informationssicherheitsstrategie

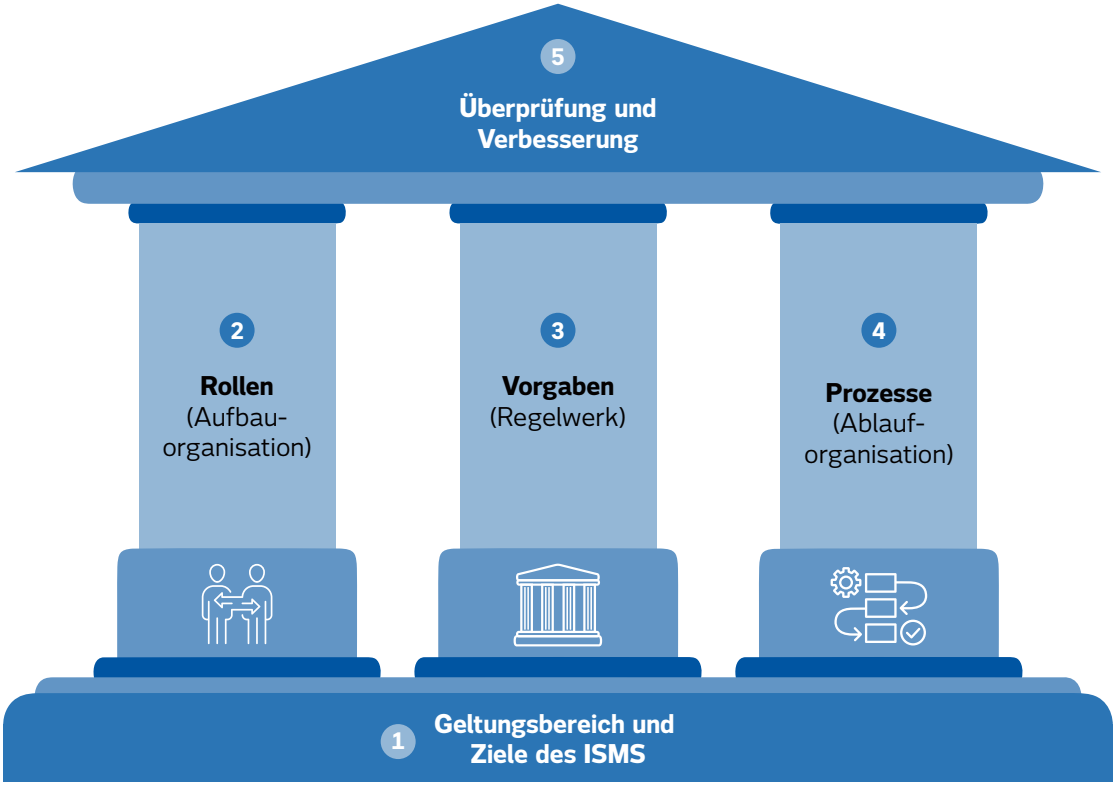

Abbildung 1: ISMS von Stromnetz Berlin

Stromnetz Berlin steuert Informationssicherheit über ein strukturiertes Managementsystem (ISMS). Das ISMS bildet den Rahmen für den zuverlässigen und sicheren Betrieb von Geschäftsprozessen, Informationen, Prozessen und Systemen von Stromnetz Berlin und besteht aus fünf Kernelementen:

1. Ziele und Geltungsbereich sind das Fundament: Sie definieren das angestrebte Sicherheitsniveau in den Unternehmensbereichen von Stromnetz Berlin sowie die zu erreichenden Sicherheitsziele.

2. Verbindliche Vorgaben (Regelwerk) legen darauf aufbauend Stromnetz Berlinweite, einheitliche Regeln im Umgang mit Informationen und dem sicheren Betrieb von Systemen fest.

3. Prozesse (Ablauforganisation) beschreiben, wie Informationssicherheit im Arbeitsalltag praktisch umgesetzt und gesteuert wird.

4. Rollen und Verantwortlichkeiten (Ablauforganisation) stellen sicher, dass Zuständigkeiten eindeutig geregelt sind.

5. Regelmäßige Überprüfungen und Verbesserungsinitiativen stellen eine kontinuierliche Weiterentwicklung des ISMS sicher.

Normative Grundlage des ISMS ist der internationale Standard ISO/IEC 27001:2022, ergänzt um die regulatorisch notwendigen Anforderungen an einen Energienetzbetreiber. Ergänzend dienen Best Practices des Bundesamts für Sicherheit in der Informationstechnik (BSI) als Orientierungshilfe. Das ISMS bewertet Sicherheitsmaßnahmen risikoorientiert auf Basis eines identifizierten Schutzniveaus und setzt diese in der Organisation um. Das Risikomanagement des ISMS erfasst Risiken systematisch, bewertet und behandelt diese durch geeignete Maßnahmen und schafft Transparenz gegenüber der Leitungsebene von Stromnetz Berlin. Die Gesamtverantwortung für die Umsetzung, Weiterentwicklung und ständige Verbesserung des ISMS liegt bei der Geschäftsführung und dem ISMS-Steering-Committee.

Geltungsbereich

Das ISMS von Stromnetz Berlin erstreckt sich auf alle Geschäftsprozesse, darin verarbeitete und gespeicherte Informationen, eingesetzte IT- und OT-Komponenten und deren Betrieb sowie alle Arbeitsplätze, Standorte und mobilen Komponenten von Stromnetz Berlin, unabhängig vom Einsatzort. Die verschiedenen, definierten Geltungsbereiche (Scopes) im ISMS von Stromnetz Berlin legen dafür jeweils die konkret geltenden Regelungen abhängig vom Schutzniveau und den regulatorischen Anforderungen fest. Die Sicherheitsvorgaben des ISMS sind für die Geschäftsführung, alle Organisationsbereiche, Führungskräfte und Mitarbeitende von Stromnetz Berlin sowie für externe Partner, Dienstleister und sonstige Akteure, die im Auftrag von Stromnetz Berlin Tätigkeiten ausführen oder Zugriff auf Informationen von Stromnetz Berlin haben, verbindlich.

Ziele

Ziel des ISMS ist ein angemessenes und wirksames Sicherheitsniveau innerhalb von Stromnetz Berlin. Ein solches Sicherheitsniveau ist notwendig, um die Versorgungssicherheit der Berliner Bevölkerung zu gewährleisten, berechtigte Erwartungen von Mitarbeitenden und Stakeholder*innen zu erfüllen sowie gesetzlichen und regulatorischen Vorgaben nachzukommen. Das ISMS gewährleistet den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und trägt damit unmittelbar zur Sicherheit der kritischen Dienstleistung und der Geschäftsprozesse bei Stromnetz Berlin bei. Aus diesen übergeordneten Zielen leiten sich folgende operative Sicherheitsziele des ISMS ab:

1. Aktive Förderung der Transparenz von Informationssicherheitsrisiken

2. Festlegung klarer Rollen und Verantwortlichkeiten für alle Prozesse des ISMS und Integration des ISMS und seiner Vorgaben in alle Prozesse und Projekte bei Stromnetz Berlin

3. Einhaltung aller gesetzlichen, vertraglichen und regulatorischen Anforderungen an die Informationssicherheit, denen Stromnetz Berlin unterliegt

4. Aufbau und Befähigung einer unternehmensweiten Organisation für die Informationssicherheit

5. Entwicklung eines unternehmensweiten Bewusstseins und Akzeptanz für die Informationssicherheit

6. Fortlaufende Weiterentwicklung der Wirksamkeit des ISMS und Beibehaltung eines angemessenen Reifegrads des ISMS und seiner Sicherheitsmaßnahmen.

Organisation

Rollen

Die Gesamtverantwortung für die Informationssicherheit liegt bei der Geschäftsführung von Stromnetz Berlin. Zur Erreichung der Sicherheitsziele legt die Geschäftsführung eine Organisationsstruktur für die Informationssicherheit fest und stattet deren Rollen und Gremien mit den notwendigen Ressourcen und klar definierten Verantwortlichkeiten aus.

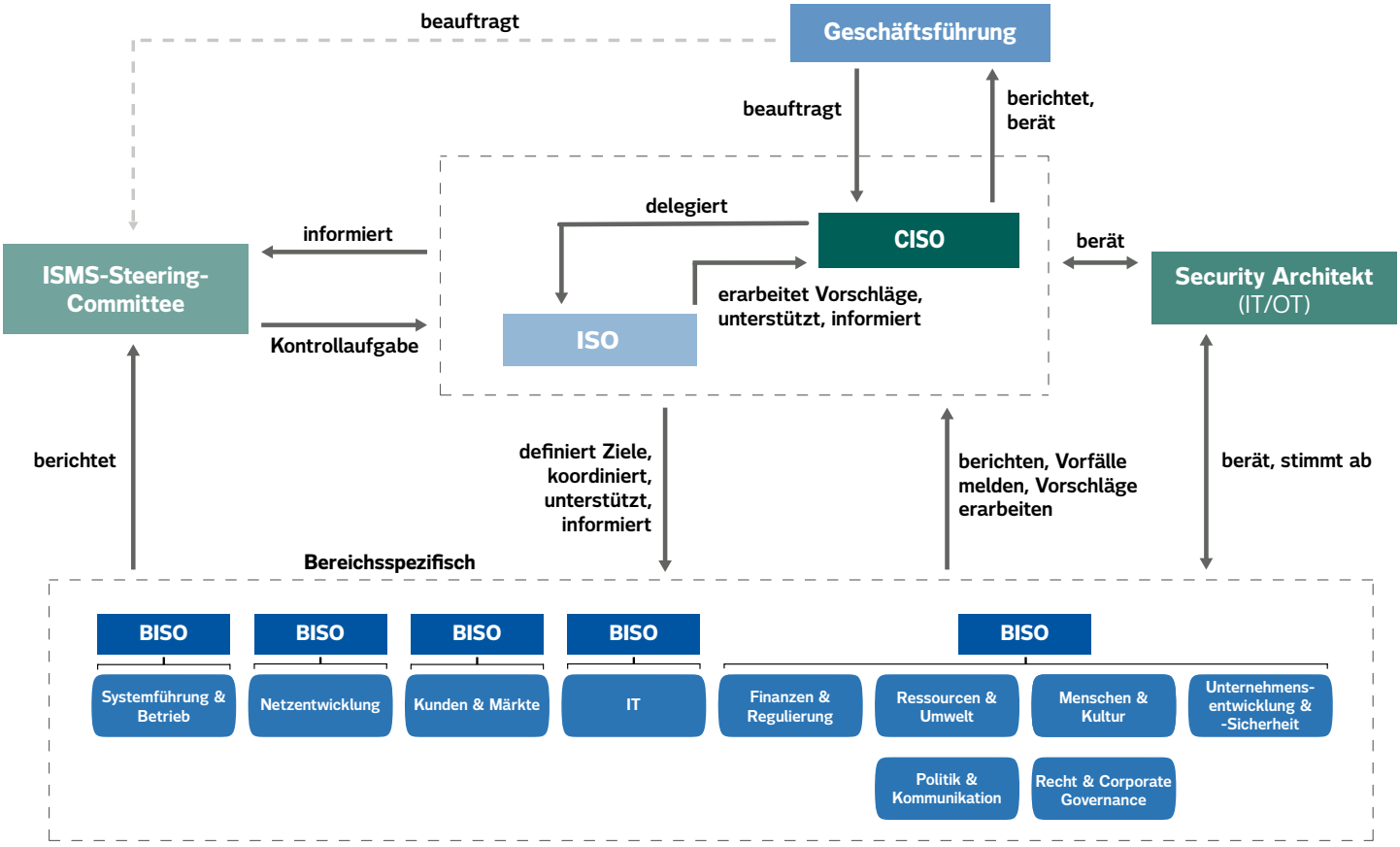

Abbildung 2: ISMS-Organisation von Stromnetz Berlin

Die Organisationsstruktur des ISMS beinhaltet folgende Rollen:

1. Die **Geschäftsführung** legt die übergeordneten Ziele für die Informationssicherheit fest und beauftragt den Chief Information Security Officer (CISO) mit der Umsetzung des ISMS.

2. Das **ISMS-Steering-Committee** übernimmt die operative Aufsicht über den Umsetzungsstand des ISMS und ist mit entscheidungsbefugten Vertreter*innen aller Bereiche besetzt. Dies stellt sicher, dass die Informationssicherheit in allen Unternehmensbereichen berücksichtigt wird.

3. Der **Chief Information Security Officer (CISO)** trägt die Umsetzungsverantwortung für die Informationssicherheit und berichtet regelmäßig an die Geschäftsführung. Er steuert den Betrieb des ISMS.

4. Der **Information Security Officer (ISO)** unterstützt die strategischen Prioritäten des CISO, koordiniert die operative Steuerung des ISMS und berichtet regelmäßig an den CISO.

5. Die **Business Information Security Officers (BISO)** verzahnen Informationssicherheit mit den Bereichen und Geschäftsprozessen von Stromnetz Berlin als Bindeglied zwischen CISO und der jeweiligen Bereichsleitung. Die BISOs sorgen dafür, dass zentrale Vorgaben und Prozesse in ihren Zuständigkeitsbereich übersetzt und integriert werden. Sie berichten direkt an den CISO und die jeweilige Bereichsleitung.

Die Konkretisierung der Rollen erfolgt in nachgelagerten ISMS-Dokumenten.

Vorgaben

Das ISMS hat für die Definition seiner Vorgaben eine adressatengerechte, hierarchische Regelungsstruktur definiert (ISMS-Framework). Alle Dokumente des ISMS-Frameworks unterliegen einer regelmäßigen Revision und Aktualisierung.

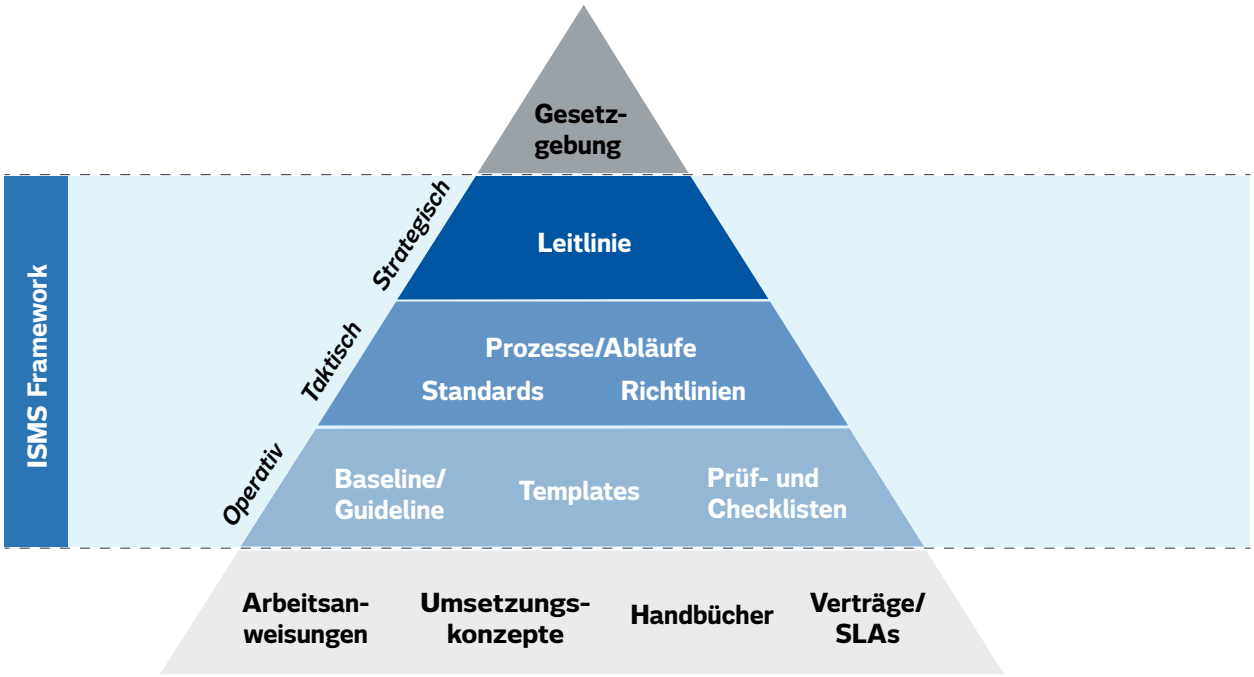

Abbildung 3: ISMS-Framework

Das ISMS-Framework besteht aus den folgenden drei Regelungsebenen:

	Dokumententyp	Freigabe durch	Kommunikation
Ebene 1	Informationssicherheitsleitlinie der SNB	Geschäftsführung	Organisationsweite Veröffentlichung (Internet, Intranet)
Ebene 2	Richtlinien (für alle verbindlich)	ISMS-SC	Organisationsweite Veröffentlichung (ISMS-Sharepoint)
	Standards (für spezifische Zielgruppen)	CISO	
Ebene 3	Prozesse	CISO	
	Umsetzungskonzepte wie Betriebshandbücher, Handlungshilfen, Templates, Ergänzende Dokumentationen	Systemverantwortliche, BISOs, Fachabteilung	Kommunikation an betroffene Bereiche oder Personen

Tabelle 1: ISMS-Framework

Zusätzlich zu den Vorgabedokumenten existieren Umsetzungs- und Nachweisdokumente (z. B. Reports, Dokumentationen, Protokolle). Diese Dokumente sind nicht Bestandteil des ISMS-Frameworks und dienen als Nachweis für die Umsetzung von definierten Sicherheitsmaßnahmen.

Prozesse

Um die Vorgaben und Methoden des Managementsystems im Betrieb von Stromnetz Berlin wirksam umsetzen zu können, etabliert das ISMS Stromnetz Berlinweite Prozesse. Diese ISMS-Prozesse stellen die Arbeitsweise der ISMS-Organisation und entsprechende Schnittstellen zu weiteren relevanten Bereichen und Projekten dar. Alle Prozesse haben eindeutige Rollen und Verantwortlichkeiten innerhalb des ISMS.

Kontinuierliche Verbesserung

Zur kontinuierlichen Verbesserung des Managementsystems überprüft Stromnetz Berlin das ISMS regelmäßig auf Angemessenheit, Eignung und Wirksamkeit mit dem Ziel, den Reifegrad des Managementsystems fortlaufend zu verbessern. Die Geschäftsführung und das ISMS-Steering-Committee sind aktiv in den Verbesserungsprozess eingebunden und unterstützen die kontinuierliche Verbesserung durch Aufsicht und Support. Die regelmäßige Überprüfung wird durch Stromnetz Berlin in einem organisationsweiten Auditprogramm geplant und gesteuert. Identifizierte Abweichungen in den Überprüfungen werden durch die ISMS-Organisation bewertet, dokumentiert und fließen in einen jährlichen Managementbericht und Verbesserungsmaßnahmen zusammen. Regelmäßige Reports an das ISMS-Steering-Committee stellen dafür die notwendige Transparenz sicher. Stromnetz Berlin wird neben internen Audits ebenfalls regelmäßig, wie regulatorisch gefordert, durch externe Prüfer auditiert. Diese externen Audits überprüfen die Konformität des Managementsystems und seiner Kontrollen (Maßnahmen) gegenüber regulatorisch geforderten nationalen und internationalen Standards.

Stromnetz Berlin GmbH
Eichenstraße 3a
12435 Berlin

info@stromnetz-berlin.de
www.stromnetz.berlin

Dezember 2025