


Informationssicherheitspolitik und IS-Ziele

Kapitel 5.2 und 6.2 – Anforderungen, Rahmenkonzept und Praxisbeispiele

Revision 01

Template Change History

Version	Date	Author	Change description
1.0	25.02.2026	Markus Steinmetz	Dokument erstellt

Inhaltsverzeichnis

1.	Übersicht.....	3
1.1	Zweck.....	3
1.2	Begriffe und Definitionen.....	3
1.3	Abkürzungen	3
1.4	Referenzdokumente.....	4
2.	Kapitel 5.2 – Informationssicherheitspolitik.....	5
2.1	Normative Anforderungen	5
2.2	Ziele in der Politik: Direkt oder als Rahmen?	5
2.3	Mindestinhalt eines Rahmens für IS-Ziele in der Politik.....	6
2.4	Typische Struktur einer IS-Politik (Praxisvorlage).....	7
3.	Kapitel 6.2 – Informationssicherheitsziele.....	8
3.1	Normative Anforderungen	8
3.2	SMART-Kriterien als Qualitätsrahmen	9
4.	Beispielziele nach Kapitel 6.2	10
4.1	Zugriffskontrolle / Identitätsmanagement	10
4.2	Verfügbarkeit / Business Continuity	10
4.3	Security Awareness & Schulung.....	11
4.4	Schwachstellenmanagement / Patch Management	11
4.5	Sicherheitsvorfallsmanagement	12
4.6	Lieferanten- und Supply-Chain-Sicherheit	12
4.7	Risikomanagement / Restrisiko	13
5.	Verhältnis Kap. 5.2 zu Kap. 6.2 und Audit-Hinweise.....	14
5.1	Zusammenhang der Kapitel	14
5.2	Empfohlene Dokumentationsstruktur für IS-Ziele	14
5.3	Häufige Audit-Findings	15
	ANNEX – IS-Zieleregister (Empfohlene Struktur)	16

1. Übersicht

1.1 Zweck

Dieses Dokument beschreibt die normativen Anforderungen an die Informationssicherheitspolitik (Kap. 5.2) und die Informationssicherheitsziele (Kap. 6.2) der ISO 27001:2022. Es enthält den Rahmen für die Ableitung von IS-Zielen, praxisnahe Beispielziele sowie Hinweise für die Audit-Praxis.

1.2 Begriffe und Definitionen

Begriff	Definition
IS-Politik	Formales Statement des Top-Managements zur Ausrichtung und den Grundsätzen der Informationssicherheit (Kap. 5.2).
IS-Ziel	Messbares, SMART-konformes Ziel abgeleitet aus der IS-Politik und der Risikobeurteilung (Kap. 6.2).
CIA-Triade	Vertraulichkeit (Confidentiality), Integrität (Integrity), Verfügbarkeit (Availability) – die drei Grundsatzprinzipien.
KVP	Kontinuierlicher Verbesserungsprozess – verbindliche Anforderung gemäß ISO 27001 (Kap. 5.2(d), 10).
ISMS	Informationssicherheits-Managementsystem.

1.3 Abkürzungen

Abkürzung	Bedeutung
ISMS	Information Security Management System / Informationssicherheits-Managementsystem
CIA	Confidentiality, Integrity, Availability
KPI	Key Performance Indicator / Kennzahl
CISO	Chief Information Security Officer
RBAC	Role-Based Access Control / Rollenbasierte Zugriffskontrolle

Abkürzung	Bedeutung
RTO	Recovery Time Objective / Wiederherstellungsziel (Zeit)
CVSS	Common Vulnerability Scoring System
NC	Nonconformity / Nichtkonformität (Major / Minor)
SLA	Service Level Agreement
KVP	Kontinuierlicher Verbesserungsprozess

1.4 Referenzdokumente

Referenz	Bezeichnung / Ausgabe
[ISO27001]	ISO/IEC 27001:2022 – Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheits-Managementsysteme – Anforderungen
[ISO27002]	ISO/IEC 27002:2022 – Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmaßnahmen

2. Kapitel 5.2 - Informationssicherheitspolitik

2.1 Normative Anforderungen

Kapitel 5.2 der ISO 27001:2022 verpflichtet das Top-Management zur Festlegung einer Informationssicherheitspolitik. Die Politik muss folgende Anforderungen erfüllen:

Anforderung	Normtext (sinngemäß)	Ausprägung
(a) Angemessenheit	Der Art der Organisation angemessen	Berücksichtigung von Branche, Größe, Kontext und Risikoprofil
(b) Ziele oder Rahmen	Enthält IS-Ziele oder einen Rahmen für deren Festlegung	Direkte Ziele oder Verweis auf Kap. 6.2-Prozess
(c) Compliance-Verpflichtung	Verpflichtung zur Erfüllung anwendbarer Anforderungen	Gesetzliche, regulatorische und vertragliche Pflichten
(d) KVP-Verpflichtung	Verpflichtung zur kontinuierlichen Verbesserung des ISMS	Expliziter Verbesserungsauftrag an das Management
Dokumentation	Als dokumentierte Information vorliegen	Schriftliche Freigabe durch Top-Management
Kommunikation	Innerhalb der Organisation kommuniziert	Mitarbeiter müssen die Politik kennen
Verfügbarkeit	Für interessierte Parteien verfügbar (soweit angemessen)	Kunden, Behörden, Auditoren auf Anfrage

2.2 Ziele in der Politik: Direkt oder als Rahmen?

Die Norm lässt bewusst zwei Optionen offen und gibt keine inhaltlich vorgeschriebenen Ziele vor:

Option	Beschreibung	Typischer Anwendungsfall
Ziele direkt enthalten	Die Politik benennt konkrete, messbare Ziele	Kleine Organisationen mit überschaubarem ISMS
Rahmen für Ziele	Die Politik definiert Prinzipien, Kriterien und Vorgaben, nach denen Ziele in Kap. 6.2 abgeleitet werden	Mittlere und große Organisationen; Ziele in separatem Dokument

In der Praxis dominiert der Rahmen-Ansatz: Die IS-Politik bleibt strategisch und stabil (1–3 Jahre), während operative Ziele gemäß Kap. 6.2 jährlich oder anlassbezogen aktualisiert werden.

2.3 Mindestinhalt eines Rahmens für IS-Ziele in der Politik

Damit die IS-Politik als gültiger Rahmen im Sinne von Kap. 5.2 (b) anerkannt wird, sollte sie mindestens folgende Elemente adressieren:

Schutzbedarfsprinzipien: Bezug auf die CIA-Triade (Vertraulichkeit, Integrität, Verfügbarkeit) als leitende Grundprinzipien

Risikobasierte Ableitung: Aussage, dass Ziele auf Basis der Risikobeurteilung und -behandlung gemäß Kap. 6.1 festgelegt werden

Compliance-Verankerung: Bezug auf gesetzliche, regulatorische und vertragliche Anforderungen (z. B. DSGVO, ISO/SAE 21434, IEC 62443)

Governance und Verantwortung: Benennung, wer für Festlegung und Überwachung der Ziele zuständig ist (z. B. CISO, IS-Beauftragter)

Review-Zyklus: Wann und wie werden Ziele überprüft und im Management Review bewertet?

2.4 Typische Struktur einer IS-Politik (Praxisvorlage)

Abschnitt	Inhalt
1. Geltungsbereich und Zweck	Scope des ISMS; Schutzobjekte; Zielsetzung des Dokuments
2. Top-Management-Statement	Formelles Bekenntnis der Geschäftsleitung zur Informationssicherheit
3. Schutzprinzipien (CIA)	Vertraulichkeit, Integrität, Verfügbarkeit als Leitprinzipien
4. Rahmen für IS-Ziele	Ableitung aus Risikobeurteilung; Messbarkeit; Verantwortlichkeit; Review-Turnus
5. Verpflichtung zur Compliance	Auflistung relevanter Anforderungsquellen
6. Verpflichtung zur kont. Verbesserung	Expliziter KVP-Auftrag; Verknüpfung mit Management Review
7. Kommunikation und Verfügbarkeit	Verteilerwege; Zugänglichkeit für interessierte Parteien
8. Freigabe	Datum, Unterschrift, nächstes Review-Datum

3. Kapitel 6.2 - Informationssicherheitsziele

3.1 Normative Anforderungen

Kapitel 6.2 legt fest, welche formalen Eigenschaften IS-Ziele aufweisen müssen und was für jedes Ziel zu planen ist:

Eigenschaft	Anforderung (Kap. 6.2)
Konsistenz	Ziele müssen mit der IS-Politik übereinstimmen
Messbarkeit	Ziele müssen messbar sein (soweit praktikabel)
Anforderungsberücksichtigung	Relevante IS-Anforderungen (Risiken, Compliance, interessierte Parteien) einbeziehen
Überwachung	Fortschritt bei der Erreichung der Ziele muss überwacht werden
Kommunikation	Ziele müssen kommuniziert werden
Aktualisierung	Ziele müssen bei Bedarf aktualisiert werden
Dokumentation	Ziele müssen als dokumentierte Information vorliegen

Für jedes Ziel muss zusätzlich geplant werden:

Was wird getan? (konkrete Maßnahme oder Aktivität)

Welche Ressourcen werden benötigt? (Budget, Personal, Werkzeuge)

Wer ist verantwortlich? (benannte Verantwortliche)

Bis wann wird es abgeschlossen? (Termin / Meilensteine)

Wie werden die Ergebnisse bewertet? (KPI, Messmethode, Nachweise)

3.2 SMART-Kriterien als Qualitätsrahmen

Kriterium	Bedeutung im ISMS-Kontext	Prüffrage für den Auditor
S – Spezifisch	Konkreter Bezug zu Asset, Prozess oder Kontrollbereich	Ist klar, was genau erreicht werden soll?
M – Messbar	KPI, Prozentsatz, Anzahl, Zeitwert, Schwellenwert	Kann der Fortschritt quantifiziert werden?
A – Akzeptiert	Von Management und Verantwortlichen getragen	Ist Commitment der Führung dokumentiert?
R – Realistisch	Ressourcen und Zeitrahmen sind vorhanden	Sind Budget und Kapazität eingeplant?
T – Terminiert	Klares Zieldatum oder Review-Zyklus	Gibt es einen definierten Fälligkeitstermin?

4. Beispielziele nach Kapitel 6.2

Die folgenden Beispiele zeigen praxisnahe, SMART-konforme IS-Ziele gegliedert nach typischen Ziel- und Kontrollbereichen.

4.1 Zugriffskontrolle / Identitätsmanagement

Ziel: Bis Q4 2026 wird ein rollenbasiertes Zugriffskonzept (RBAC) für alle kritischen Systeme eingeführt. Die Anzahl unbefugter Zugriffe auf kritische Systeme wird dadurch um mindestens 80 % gegenüber dem Vorjahreswert reduziert.

Element	Inhalt
Maßnahme	Einführung RBAC, Überarbeitung Berechtigungsmatrix, Rezertifizierung aller privilegierten Accounts
Ressourcen	3 PT/Monat IT-Sicherheit, IAM-Tool-Lizenz (Budget: 15.000 EUR)
Verantwortlich	CISO / IT-Leiter
Termin	31.12.2026
Bewertung / KPI	Monatliche Auswertung der SIEM-Logs; Anzahl Zugriffsverletzungen; Audit-Nachweis

4.2 Verfügbarkeit / Business Continuity

Ziel: Ab 01.01.2027 beträgt die maximale ungeplante Ausfallzeit kritischer IT-Dienste (Tier 1) weniger als 4 Stunden je Vorfall (RTO < 4h). Die Verfügbarkeit dieser Dienste liegt bei mindestens 99,5 % pro Quartal.

Element	Inhalt
Maßnahme	Redundanzkonzept für Tier-1-Dienste, Test der Notfallwiederherstellung (halbjährlich), BCP-Aktualisierung
Ressourcen	Infrastrukturbudget, BC-Manager (0,5 FTE)
Verantwortlich	IT-Betrieb / BC-Manager
Termin	Q2 2026 (Konzept), Q4 2026 (Test), laufend ab 01.01.2027
Bewertung / KPI	Auswertung Incident-Tickets; RTO-Messung im DR-Test; Verfügbarkeits-Report

4.3 Security Awareness & Schulung

Ziel: Bis 31.12.2026 haben mindestens 95 % aller Mitarbeitenden (inkl. Externe mit Systemzugang) die jährliche IS-Pflichtschulung erfolgreich abgeschlossen. Die Phishing-Klickrate sinkt im Vergleich zum Vorjahrestest um mindestens 30 %.

Element	Inhalt
Maßnahme	E-Learning-Pflichtschulung (LMS), jährliche Phishing-Simulation, Awareness-Kampagne
Ressourcen	LMS-Plattform, IS-Beauftragter (Koordination), Phishing-Testtool
Verantwortlich	IS-Beauftragter / HR
Termin	Schulungsabschluss jährlich bis 31.12., Phishing-Test Q2 und Q4
Bewertung / KPI	Schulungsabschlussquote aus LMS; Klickrate aus Phishing-Report

4.4 Schwachstellenmanagement / Patch Management

Ziel: Ab sofort werden kritische Schwachstellen (CVSS-Score $\geq 9,0$) innerhalb von 72 Stunden nach Bekanntwerden gepatcht oder durch dokumentierte Mitigationsmaßnahmen kompensiert. Für High-Schwachstellen (CVSS 7,0–8,9) gilt eine Frist von 14 Tagen.

Element	Inhalt
Maßnahme	Vulnerability-Scanner (monatlich), Patch-Prozess mit SLA-Definition, Ausnahmemanagement
Ressourcen	Vulnerability-Management-Tool, Patch-Teams IT-Infrastruktur
Verantwortlich	IT-Sicherheit / Systemadministration
Termin	Prozess-Einführung Q1 2026, laufend
Bewertung / KPI	Patch-Compliance-Rate (%); Anzahl Overdue-Patches; Zeit bis Patch (MTTR)

4.5 Sicherheitsvorfallsmanagement

Ziel: 90 % aller gemeldeten Sicherheitsvorfälle werden innerhalb von 24 Stunden nach Meldung initial bewertet und klassifiziert. Major Incidents (Klasse P1) werden innerhalb von 4 Stunden eskaliert.

Element	Inhalt
Maßnahme	Incident-Response-Prozess aktualisieren, SIEM-Alerting konfigurieren, IR-Team schulen
Ressourcen	SIEM/SOAR-Plattform, IR-Team (6 Personen on-call)
Verantwortlich	SOC-Leiter / CISO
Termin	Q2 2026 (Prozess), laufend
Bewertung / KPI	Bewertungsquote aus Ticket-System; Eskalationszeit (Mean Time to Escalate)

4.6 Lieferanten- und Supply-Chain-Sicherheit

Ziel: Bis Q3 2026 werden alle kritischen Lieferanten (Tier 1) einer Informationssicherheitsbewertung nach dem internen Supplier-Security-Framework unterzogen. Lieferanten ohne akzeptables Sicherheitsniveau erhalten bis Q4 2026 einen verbindlichen Maßnahmenplan.

Element	Inhalt
Maßnahme	Lieferantenkritikalitätsbewertung, IS-Fragebögen versenden, On-Site-Assessments für Top-10-Lieferanten
Ressourcen	Einkauf + IS-Beauftragter, Supplier-Assessment-Tool
Verantwortlich	Einkaufsleiter / IS-Beauftragter
Termin	Bewertung Q3 2026, Maßnahmenpläne Q4 2026
Bewertung / KPI	% bewerteter kritischer Lieferanten; Anzahl offener Maßnahmenpläne

4.7 Risikomanagement / Restrisiko

Ziel: Nach Abschluss der jährlichen Risikobehandlung liegt das Restrisiko aller als „Hoch“ klassifizierten Risiken unterhalb des definierten Risikoakzeptanzlevels. Nicht akzeptable Restrisiken werden dem Top-Management zur expliziten Entscheidung vorgelegt.

Element	Inhalt
Maßnahme	Jährliche Risikobeurteilung, Risikobehandlungsplan aktualisieren, Statement of Applicability überprüfen
Ressourcen	Risikomanagement-Tool (GRC), IS-Beauftragter (5 PT/Jahr)
Verantwortlich	IS-Beauftragter / Risikokomitee
Termin	Jährlich bis Q1 (nach Management Review)
Bewertung / KPI	Anzahl Hoch-Risiken oberhalb Akzeptanzlevel; Behandlungsquote (%)

5. Verhältnis Kap. 5.2 zu Kap. 6.2 und Audit-Hinweise

5.1 Zusammenhang der Kapitel

Dimension	Kap. 5.2 – IS-Politik	Kap. 6.2 – IS-Ziele
Ebene	Strategisch / normativ	Operativ / messbar
Frage	"Was wollen wir sein und wie gehen wir vor?"	"Was wollen wir konkret erreichen?"
Funktion	Rahmen und Leitprinzipien vorgeben	Konkrete KPIs, Termine, Verantwortliche
Stabilität	Stabil (typisch 1–3 Jahre)	Dynamisch (jährlich oder anlassbezogen)
Freigabe	Top-Management (schriftlich)	Verantwortliche + Management Review
Dokumentform	Politikdokument (1–3 Seiten)	Zieltabelle / Maßnahmenprogramm

5.2 Empfohlene Dokumentationsstruktur für IS-Ziele

Bewährte Spalten einer IS-Zieltabelle (Kap. 6.2-Dokument):

Ziel-ID	Zielbeschreibung	KPI/Messgröße	Zielwert	Verantw.	Ressourcen	Termin
IS-Z-001	Reduktion unbef. Zugriffe um 80 %	Anzahl Zugriffsverletzungen	–80 % gg. Vorjahr	CISO	IAM-Tool	Q4 2026
IS-Z-002	RTO < 4h für Tier-1-Dienste	Gemessene RTO im DR-Test	< 4h / 99,5 % Verf.	IT-Leiter	Redundanzinfra	Q4 2026
Ziel-ID	Termin	Status	Nachweis			
IS-Z-001	Q4 2026	In Umsetzung	SIEM-Report			
IS-Z-002	Q4 2026	Geplant	DR-Testprotokoll			

5.3 Häufige Audit-Findings

Finding-Typ	Typischer Befund	Referenz
Major NC	IS-Politik enthält keinerlei Bezug zu Zielen – weder direkt noch als Rahmen	Kap. 5.2 (b)
Major NC	Keine Verpflichtung zu Compliance oder KVP erkennbar	Kap. 5.2 (c)/(d)
Major NC	IS-Ziele sind nicht dokumentiert oder nicht messbar	Kap. 6.2
Minor NC	Rahmen in der Politik vorhanden, aber keine erkennbare Verbindung zu dokumentierten Zielen	Kap. 5.2/6.2
Minor NC	Ziele nicht kommuniziert oder nicht mit dem Management Review verknüpft	Kap. 6.2 / 9.3
Minor NC	Politik nicht vom Top-Management freigegeben oder veraltet	Kap. 5.2
Observation	Ziele im Rahmendokument vorhanden, aber keine klare Messmethodik beschrieben	Kap. 6.2
Observation	Ziele rein qualitativ formuliert ohne quantifizierbare KPIs	Kap. 6.2

Hinweis für Auditoren: Fehlende Messbarkeit oder rein qualitative Ziele ohne Bewertungsmechanismus sind klassische Minor Nonconformities in Stage-2-Audits. Die Verknüpfung der Ziele mit dem Management Review (Kap. 9.3) und der kontinuierlichen Verbesserung (Kap. 10) wird ebenfalls geprüft.

ANNEX - IS-Zieleregister (Empfohlene Struktur)

Empfohlene Spalten eines IS-Zieleregisters gemäß Kap. 6.2:

Ziel-ID	Zielbeschreibung	KPI/Messgröße	Zielwert	Verantwortlich	Ressourcen
IS-Z-001	Reduktion unbef. Zugriffe um 80 %	Anzahl Zugriffsverletzungen	–80 % gg. Vorjahr	CISO	IAM-Tool (15 TEUR)
IS-Z-002	RTO < 4h für Tier-1-Dienste	Gemessene RTO im DR-Test	< 4h / 99,5 %	IT-Leiter	Redundanzinfra
IS-Z-003	Schulungsabschlussquote ≥ 95 %	Quote aus LMS	≥ 95 % aller MA	IS-Beauftragter	LMS-Plattform
IS-Z-004	Krit. Schwachstellen in 72h gepatcht	Patch-Compliance-Rate	100 % (CVSS ≥ 9)	IT-Sicherheit	Vuln.-Mgmt-Tool
IS-Z-005	90 % Incidents in 24h bewertet	Bewertungsquote	≥ 90 %	SOC-Leiter	SIEM/SOAR
IS-Z-006	Alle Tier-1-Lieferanten bewertet	% bewerteter Lieferanten	100 % Tier-1	Einkaufsleiter	Assessment-Tool
IS-Z-007	Alle Hoch-Risiken unter Akzeptanzlevel	Anzahl Hoch-Risiken > Level	0	IS-Beauftragter	GRC-Tool

Ziel-ID	Termin	Status	Nachweis
IS-Z-001	Q4 2026	In Umsetzung	SIEM-Report
IS-Z-002	Q4 2026	Geplant	DR-Testprotokoll
IS-Z-003	31.12.2026	Geplant	LMS-Report
IS-Z-004	laufend	Geplant	Scan-Report
IS-Z-005	Q2 2026	Geplant	Ticket-Report
IS-Z-006	Q3 2026	Geplant	Assessment-Report
IS-Z-007	Q1 jährlich	Geplant	Risikoregister

===== DOKUMENTENDE =====