

VORLAGE · TOMORIS TOOLBOX

IT-Inventar: Vorlage für Geräte, Software und Dienste

Felder, Beispiele und Prüfintervalle für Geräte, Server, Software, Cloud-Dienste und Daten, belegt mit CIS Controls v8.1, NIST CSF 2.0, BSI-Standard 200-2 und DVO (EU) 2024/2690

STAND

25.10.2026

UMFANG

PDF, 11 Seiten

ONLINE

tomoris.com/downloads/it-inventar-vorlage

AUF EINEN BLICK

6

Feldtabellen mit ausgefüllter Beispalspalte

IG1

CIS-Basisgruppe für alle: Safeguards 1.1, 1.2 und 2.1–2.3

3 Stufen

Schutzbedarf normal, hoch, sehr hoch (BSI 200-2)

Nr. 12.4

Inventarpflicht für NIS2-Einrichtungen (DVO (EU) 2024/2690)

FÜR WEN

- IT-Administration und IT-Leitung, die ein Inventar aufbauen oder bereinigen wollen
- IT-Dienstleister, die Kundenumgebungen übernehmen, dokumentieren und betreuen
- Geschäftsführung kleiner und mittlerer Unternehmen, die wissen will, welche IT sie besitzt und wer dafür verantwortlich ist
- Informationssicherheitsbeauftragte, die eine Strukturanalyse nach BSI-Standard 200-2 vorbereiten
- Wesentliche und wichtige Einrichtungen, die ihr Inventar nach NISG 2026 und DVO (EU) 2024/2690 führen müssen

WORUM ES GEHT

Nur was bekannt ist, lässt sich überwachen und schützen. Diese Vorlage gibt die Felder eines IT-Inventars vor: Geschäftsprozesse und Daten, Endgeräte und Netzwerkgeräte, Server und virtuelle Systeme, Software und Lizenzen sowie Cloud-Dienste und Dienstleister, je mit Mindest- und Empfehlungsfeldern und einem ausgefüllten Beispiel. Dazu kommen Schutzbedarf, Lebenszyklus bis zur Datenlöschung, Prüfintervalle und der Umgang mit nicht autorisierten Geräten und Programmen. Grundlage sind die CIS Controls v8.1, das NIST Cybersecurity Framework 2.0, der BSI-Standard 200-2 und für NIS2-Einrichtungen Anhang Nr. 12.4 der DVO (EU) 2024/2690.

Diese Vorlage ist an Ihr Unternehmen anzupassen: Felder, Gruppen, Intervalle und Zuständigkeiten hängen von Größe, Systemen und Geschäftsprozessen ab. Die Einstufung der Felder ist eine Empfehlung von TOMORIS auf Basis der genannten Standards; gesetzlich verbindlich ist nur, was als NIS2 gekennzeichnet ist, und nur für wesentliche und wichtige Einrichtungen. Sie ersetzt keine Rechtsberatung; maßgeblich ist der Gesetzestext in der jeweils geltenden Fassung.

Nutzung: Diese Vorlage dürfen Sie für den eigenen Gebrauch anpassen; weitergeben dürfen Sie sie nur in unveränderter Form.

INHALT

01	Wozu ein IT-Inventar dient und wie Sie es anlegen	3
02	Geschäftsprozesse und Daten	4
03	Endgeräte, Netzwerk- und IoT-Geräte	5
04	Server, virtuelle Systeme und Netz	6
05	Software und Lizenzen	6
06	Cloud-Dienste, SaaS und Dienstleister	7
07	Schutzbedarf und Lebenszyklus	8
08	Pflege und nicht autorisierte Funde	9
09	Quellen	11

01 —

Wozu ein IT-Inventar dient und wie Sie es anlegen

Was CIS, NIST und BSI unter einem Inventar verstehen, wann es Pflicht ist und wie Sie die Vorlage umsetzen.

Control 1 der CIS Controls v8.1 verlangt, alle Unternehmensgeräte aktiv zu verwalten, also zu inventarisieren, nachzuverfolgen und zu korrigieren: Endgeräte, Netzwerkgeräte, IoT-Geräte und Server, ob physisch, virtuell, per Fernzugriff oder in der Cloud angebunden. Ziel ist, genau zu wissen, was zu überwachen und zu schützen ist, und nicht autorisierte Geräte zu finden; Control 2 fordert dasselbe für Software. Im NIST Cybersecurity Framework 2.0 ist das die Kategorie Asset Management (ID.AM); ihre Unterkategorien greift diese Vorlage in den Abschnitten 02 bis 07 auf.

Für wesentliche und wichtige Einrichtungen ist das Inventar Pflicht: § 32 Abs. 4 lit. i NISG 2026 verlangt das Management von Anlagen. Für sie gilt der Anhang der DVO (EU) 2024/2690: für die in Art. 1 DVO genannten Anbieter wie Cloud- und verwaltete Dienste unmittelbar, für alle übrigen seit Oktober 2026 über § 2 NISV 2026. Nach Nr. 12.4 führen sie ein vollständiges, genaues, aktuelles und kohärentes Inventar ihrer Betriebsabläufe und Dienste sowie der Systeme und Werte, die sie unterstützen, und erfassen Änderungen nachvollziehbar. Für alle Unternehmen sind CIS, NIST und BSI anerkannte Empfehlungen; für NIS2-Einrichtungen ist zusätzlich der DVO-Anhang verbindlich.

Mustertext für den Geltungsbereich: „Das IT-Inventar umfasst alle Geräte, Systeme, Programme, Dienste und Daten von [Unternehmen] an den Standorten [Standorte], einschließlich Telearbeitsplätzen und der Cloud-Dienste laut Abschnitt 06. Verantwortlich ist [Name, Funktion], Vertretung [Name, Funktion].“

- Vorhandene Quellen nutzen: Übersichten zur Inventarisierung oder zum Konfigurationsmanagement (BSI-Standard 200-2, Kap. 8.1), Geräteverwaltung (MDM) und DHCP-Protokolle (CIS-Safeguards 1.1 und 1.4).
- Gruppen bilden: gleichartige Objekte mit gleichem Schutzbedarf zusammenfassen und die Anzahl vermerken (Kap. 8.1.1); für Wartung und Fehlersuche ist dennoch eine vollständige Erfassung der Systeme notwendig (Kap. 8.1.5). Auch nach Nr. 12.4.2 DVO richtet sich die Granularität nach dem Bedarf.
- Kennungen vergeben und verknüpfen: jedes Objekt eindeutig kennzeichnen, im BSI-Beispiel etwa GP002 für Prozesse und A003 für Anwendungen, und Anwendungen den Prozessen, Systeme den Anwendungen zuordnen (Kap. 8.1.2 bis 8.1.5).

Umsetzen lässt sich die Vorlage in einer Tabellenkalkulation, mit einem Tabellenblatt je Abschnitt 02 bis 06 und den Feldern als Spalten, oder in einem Inventarisierungswerkzeug (BSI-Standard 200-2, Kap. 8.1.3); automatische Erkennung sehen die CIS Controls ab Implementierungsgruppe IG2 vor (Safeguards 1.3 und 2.4). Spalte Mindestfeld: „ja“ heißt, die Quelle nennt das Feld als Mindestangabe (CIS „must“ oder „ensure“, BSI MUSS, SOLLTE oder „sollten“); „empfohlen“, sie nennt es nur bei Bedarf oder TOMORIS ergänzt es. Gesetzlich verpflichtend ist nur, was „(NIS2)“ trägt, und nur für NIS2-Einrichtungen. Werte in eckigen Klammern ersetzen Sie.

02

Geschäftsprozesse und Daten

Prozesse mit Verantwortlichen und Anwendungen, dazu die Daten mit Eigentümer, Aufbewahrung und Schutzbedarf.

Der Zusammenhang zwischen Geschäftsprozessen und Anwendungen muss immer dargestellt werden (BSI-Standard 200-2, Kap. 8.1.3). Erfassen Sie Hauptprozesse mit ihren wichtigsten Teilprozessen; fehlen Beschreibungen, helfen Geschäftsverteilungspläne oder kurze Workshops mit den Fachverantwortlichen (Kap. 8.1.2). Für personenbezogene Daten ist das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO ein Startpunkt, mit Zwecken, Datenkategorien, Empfängern, Drittlandübermittlungen und wenn möglich Löschfristen (vgl. Kap. 8.1.2).

Geschäftsprozesse und Daten zum Ausfüllen (BSI-Standard 200-2, Kap. 8.1.2; CIS-Safeguards 3.1, 3.2, 3.4 und 3.5)

FELD	WAS EINTRAGEN	BEISPIEL	MINDESTFELD?
Kennung	eindeutige Nummer oder Kürzel	GP003	ja, BSI 8.1.2
Name, Beschreibung	Prozess oder Fachaufgabe	Auftragsabwicklung	ja, BSI 8.1.2; DVO 12.4.2 (NIS2)
Verantwortlich	Person oder Fachabteilung	[Name], Vertrieb	ja, BSI 8.1.2
Anwendungen	benötigte Anwendungen	A001 ERP, A002 E-Mail	ja, BSI 8.1.2; DVO 12.4.2 (NIS2)
Daten	Datenkategorien	Kundendaten (in A001, C002)	ja, CIS 3.2
Dateneigentümer	verantwortliche Person	[Name], Vertrieb	ja, CIS 3.1
Sensibilität	Einstufung nach Ihrem Schema	vertraulich	ja, CIS 3.1
Aufbewahrung, Löschung	Mindest- und Höchstdauer, Verfahren	[Frist] bis [Frist], Löschlauf	ja, CIS 3.4, 3.5
Schutzbedarf	Vertraulichkeit, Integrität, Verfügbarkeit; NIS2 auch Authentizität	hoch, hoch, hoch	ja, BSI 8.2.3; DVO 12.1.2 (NIS2)

Im Dateninventar stehen nach CIS mindestens die sensiblen Daten; es wird mindestens jährlich geprüft (Safeguard 3.2, IG1). Was wann zu löschen ist, regeln nach BSI die Fachverantwortlichen je Geschäftsprozess, unter Beachtung gesetzlicher Aufbewahrungsfristen und bei personenbezogenen Daten abgestimmt mit dem oder der Datenschutzbeauftragten (CON.6.A1).

03

Endgeräte, Netzwerk- und IoT-Geräte

Mindestfelder nach CIS-Safeguard 1.1 und BSI-Standard 200-2 für Notebooks, Smartphones, Drucker, Switches und vernetzte Geräte.

Erfassen Sie alle Geräte, die Daten speichern oder verarbeiten können, auch solche, die regelmäßig mit Ihrem Netz verbunden sind, ohne unter Ihrer Kontrolle zu stehen (CIS-Safeguard 1.1). Leicht übersehen werden Netzdrucker, TK-Anlagen, Gebäudesteuerung, Warnmelder oder mitgebrachte Smartwatches; das BSI rät, die Räume nach Geräten abzugehen, die Strom brauchen und vernetzt sein könnten (BSI-Standard 200-2, Kap. 8.1.5 und 8.1.7).

Endgeräte und Netzwerkgeräte zum Ausfüllen (CIS-Safeguard 1.1, BSI-Standard 200-2, Kap. 8.1.4 und 8.1.5)

FELD	WAS EINTRAGEN	BEISPIEL	MINDESTFELD?
Kennung	eindeutig, etwa der Hostname	NB-0042	ja, CIS 1.1, BSI 8.1.4
Typ und Funktion	Geräteart und Aufgabe	Notebook	ja, BSI 8.1.4
Modell	Hersteller, Modell, Seriennummer	[Modell], SN [Nummer]	empfohlen (TOMORIS)
Plattform	Hardware und Betriebssystem	Windows 11 Pro	ja, BSI 8.1.4
Standort	Gebäude und Raum oder mobil	mobil, [Ort]	ja, BSI 8.1.4
Netzadressen	MAC-Adresse, IP falls statisch	MAC [Adresse]	ja, CIS 1.1
Schnittstellen	WLAN, Bluetooth, Mobilfunk	WLAN, LTE	ja, BSI 8.1.4
Eigentümer	Verantwortliche, Abteilung, Nutzende	[Name], Vertrieb	ja, CIS 1.1, BSI 8.1.5
Administration	Person oder Dienstleister	IT-Betrieb	ja, BSI 8.1.4
Netzzulassung	darf ins Netz?	ja, seit [Datum]	ja, CIS 1.1
Status	in Betrieb, Test, Planung, ausgemustert	in Betrieb	ja, BSI 8.1.5
Schutzbedarf	aus den Anwendungen (Abschnitt 07)	hoch	ja, BSI 8.2.4

Für Mobilgeräte helfen MDM-Werkzeuge (CIS 1.1). Wechseldatenträger wie USB-Sticks oder Sicherungsdaten-träger erfassen Sie als Gruppe, soweit sie Daten mit Mindestschutzbedarf tragen (BSI-Standard 200-2, Kap. 8.1.3); NIS2-Einrichtungen brauchen dafür ein Konzept (Anhang Nr. 12.3 DVO (EU) 2024/2690).

04

Server, virtuelle Systeme und Netz

Server und virtuelle Maschinen mit Zuordnung zum Host, dazu Netzplan, Außenanbindungen und Räume.

Server und virtuelle Systeme zum Ausfüllen (BSI-Standard 200-2, Kap. 8.1.4 und 8.1.5)

FELD	WAS EINTRAGEN	BEISPIEL	MINDESTFELD?
Kennung	Hostname oder Nummer	SRV-ERP01	ja, BSI 8.1.4
Typ und Funktion	etwa Datenbankserver für A001	Datenbankserver	ja, BSI 8.1.4
Plattform	physisch oder virtuell, Betriebssystem	VM, Windows Server	ja, BSI 8.1.4
Host	physischer Host, Cluster, Cloud	HV-HOST02	ja, BSI 8.1.4
Anwendungen	Kennungen der Anwendungen	A001	ja, BSI 8.1.5
Standort	Gebäude, Raum, Rechenzentrum	Serverraum [Raum]	ja, BSI 8.1.4
Netzanbindung	Netzsegment und Netzadresse	VLAN 20, 10.0.20.15	ja, BSI 8.1.4
Administration	Person oder Dienstleister	[Dienstleister]	ja, BSI 8.1.4
Status	in Betrieb, Test, Planung	in Betrieb	ja, BSI 8.1.5
Schutzbedarf	Maximum der Anwendungen, Kumulation und Verteilung beachten	hoch	ja, BSI 8.2.2, 8.2.4

Die Zuordnung virtueller Systeme zu ihren physischen Hosts muss nachvollziehbar sein (BSI-Standard 200-2, Kap. 8.1.4). Der Netzplan zeigt IT-Systeme, Netzkomponenten und Netzverbindungen samt VLANs und VPNs sowie Außenanbindungen mit Anbieter und Art der Leitung, etwa MPLS, Mietleitung oder VPN. CIS verlangt ab IG2 Architekturdiagramme mit jährlicher Prüfung (Safeguard 12.4), NIS2-Einrichtungen dokumentieren ihre Netzarchitektur verständlich und aktuell (Anhang Nr. 6.7.2 lit. a DVO (EU) 2024/2690). Erfassen Sie auch Räume mit Systemen oder schutzbedürftigen Informationen samt Akten (Kap. 8.1.8).

05

Software und Lizenzen

Zugelassene Software mit Version, Lizenz, Supportende und Verantwortlichen nach CIS-Safeguards 2.1 und 2.2 und BSI APP.6.A9.

Nach CIS-Safeguard 2.1 (IG1) dokumentiert das Softwareinventar jede lizenzierte Software mit Titel, Hersteller, erstem Installations- oder Nutzungsdatum und geschäftlichem Zweck, wo angebracht auch mit URL, App-Store, Version, Bereitstellungsweg, Außerbetriebnahme und Lizenzanzahl. Das Bestandsverzeichnis nach BSI zeigt, auf welchen Systemen Software unter welcher Lizenz läuft, und soll anlassbezogen aktualisiert werden, insbesondere bei jeder Installation (APP.6.A9). Standardsoftware wie E-Mail und Büroprogramme erfassen Sie als Paket (BSI-Standard 200-2, Kap. 8.1.3).

Software und Anwendungen zum Ausfüllen (CIS-Safeguards 2.1 bis 2.3, BSI APP.6.A9)

FELD	WAS EINTRAGEN	BEISPIEL	MINDESTFELD?
Kennung	Nummer der Anwendung	A001	ja, BSI 8.1.3
Titel, Hersteller	Produktname und Hersteller	[ERP-Software], [Hersteller]	ja, CIS 2.1
Zweck	geschäftlicher Zweck, Prozesse	Aufträge, GP003	ja, CIS 2.1
Installiert seit	erste Installation oder Nutzung	[TT.MM.JJJJ]	ja, CIS 2.1
Version, Bereitstellung	Version, Installationsweg, URL	[Version], Softwareverteilung	empfohlen, CIS 2.1
Systeme	wo installiert	SRV-ERP01, 25 Clients	ja, APP.6.A9
Lizenz	Lizenzart, Anzahl, Laufzeit	25 Benutzer, bis [Datum]	ja, APP.6.A9
Support	unterstützt ja oder nein, Support bis	ja, bis [MM/JJJJ]	ja (Status), CIS 2.2; Datum empfohlen
Status	zugelassen, Ausnahme, nicht zugelassen, außer Betrieb	zugelassen	ja, CIS 2.2, 2.3
Verantwortlich	Verantwortliche und Benutzergruppen	[Name]; Vertrieb	ja, BSI 8.1.3
Konfiguration	Abweichung vom Standard	keine	ja, APP.6.A9

Zugelassen ist nach CIS-Safeguard 2.2 nur Software, die der Hersteller noch unterstützt; ist sie unverzichtbar, dokumentieren Sie eine Ausnahme mit ausgleichenden Maßnahmen und Annahme des Restrisikos. Lizenzen sollen Einsatzzweck und Vertrag entsprechen und den gesamten Nutzungszeitraum abdecken (APP.6.A9). NIS2-Einrichtungen legen beim Erwerb sicherheitsrelevanter IKT-Produkte und -Dienste Anforderungen an Sicherheitsupdates über die gesamte Lebensdauer oder an den Ersatz nach Supportende fest (Anhang Nr. 6.1.1 und 6.1.2 lit. b DVO (EU) 2024/2690).

06

Cloud-Dienste, SaaS und Dienstleister

Anbieter, Vertrag, Datenstandort, Verantwortliche und Admin-Konten je Dienst sowie das Verzeichnis der Dienstleister.

Jeder Cloud-Dienst braucht eine Service-Definition, und die Verantwortungsbereiche zwischen Anbieter und Unternehmen müssen klar abgegrenzt und dokumentiert sein (Basis-Anforderungen OPS.2.2.A3 und A4); alle geplanten und genutzten Cloud-Dienste sollen dokumentiert werden (OPS.2.2.A3). Im Vertrag soll stehen, wo der Anbieter die Leistung erbringt, wie Daten sicher gelöscht werden und wie gekündigt wird (OPS.2.2.A9). CIS-Safeguard 15.1 (IG1) verlangt ein Dienstleisterinventar mit Klassifizierung und interner Ansprechperson, Safeguard 5.1 ein Kontoinventar samt Admin-Konten.

Cloud- und SaaS-Dienste zum Ausfüllen (BSI OPS.2.2, CIS-Safeguards 5.1 und 15.1)

FELD	WAS EINTRAGEN	BEISPIEL	MINDESTFELD?
Dienst	Bezeichnung, Zweck, Status	C001 E-Mail, in Nutzung	ja, OPS.2.2.A3
Anbieter	Anbieter und Kontaktstelle	[Anbieter], [Kontakt]	ja, CIS 15.1; DVO 5.2 (NIS2)
Vertrag, Ausstieg	Laufzeit, Kündigung, Datenrückgabe	bis [Datum], Export, Löscherbestätigung	empfohlen, OPS.2.2.A9, A14
Leistung	Service-Definition, Verantwortung	Anlage [X] zum Vertrag	ja, OPS.2.2.A3, A4
Datenstandort	Ort der Leistungserbringung	[EU, Region]	empfohlen, OPS.2.2.A9
Klassifizierung	Einstufung von Dienst und Daten	kritisch, Daten hoch	ja, CIS 15.1
Verantwortlich	interne Ansprechperson	[Name], IT-Leitung	ja, CIS 15.1
Admin-Konten	Konten mit Adminrechten	[Name], [Name]	ja, CIS 5.1

NIS2-Einrichtungen führen zusätzlich ein Verzeichnis ihrer direkten Anbieter mit Kontaktstellen und bereitgestellten IKT-Produkten und -Diensten (Anhang Nr. 5.2 DVO (EU) 2024/2690).

07

Schutzbedarf und Lebenszyklus

Schutzbedarf je Eintrag nach BSI-Standard 200-2 und die Felder von der Beschaffung bis zur Datenlöschung.

Der BSI-Standard 200-2 kennt drei Schutzbedarfskategorien: „normal“, wenn die Schadensauswirkungen begrenzt und überschaubar sind, „hoch“, wenn sie beträchtlich sein können, und „sehr hoch“, wenn sie ein existenziell bedrohliches, katastrophales Ausmaß erreichen können (Kap. 8.2.1). Bewerten Sie Vertraulichkeit, Integrität und Verfügbarkeit getrennt. IT-Systeme erben den Schutzbedarf der Anwendungen, die auf ihnen laufen oder deren Daten sie transportieren; laufen viele Anwendungen auf einem System, kann er steigen (Kumulationseffekt), bei Redundanz oder nur unwesentlichen Teilen einer Anwendung sinken (Verteilungseffekt). Der Gesamtschutzbedarf ist das Maximum der Grundwerte und zu begründen (Kap. 8.2.2 und 8.2.4).

NIS2-Einrichtungen ordnen allen Anlagen und Werten eine Klassifizierungsstufe zu, die auf Vertraulichkeits-, Integritäts-, Authentizitäts- und Verfügbarkeitsanforderungen beruht; ergänzen Sie dafür die Authentizität als vierten Wert (Anhang Nr. 12.1.2 lit. b DVO (EU) 2024/2690). Ihr Konzept deckt den Lebenszyklus von Erwerb, Verwendung, Speicherung und Transport bis zur Entsorgung ab (Nr. 12.2.2). Das BSI sieht vor dem Einsatz Prüf- und Genehmigungsverfahren und Bestandsverzeichnisse vor (ORP.1.A8); beim Austritt sind alle Geräte einzuziehen (ORP.2.A2). NIS2-Einrichtungen dokumentieren dann Abgabe, Rückgabe oder Löschung der Geräte und Daten, die das Personal verwahrt; ist das nicht möglich, dürfen diese nicht mehr auf ihre Systeme zugreifen (Nr. 12.5).

Lebenszyklusfelder zum Ausfüllen, für alle Geräte aus den Abschnitten 03 und 04

FELD	WAS EINTRAGEN	BEISPIEL	MINDESTFELD?
Beschafft, Garantie	Datum, Beleg, Garantie bis, Prüfung vor Einsatz	[Datum], Rechnung [Nr.], bis [Datum]	empfohlen, ORP.1.A8
Ausgabe	an wen, Datum, Bestätigung	[Name], [Datum]	empfohlen (TOMORIS)
Rückgabe	bei Austritt: Datum, entgegenge- nommen von	[Datum], [Name]	ja für Geräte des Personals, ORP.2.A2; DVO 12.5 (NIS2)
Löschung	Verfahren nach CON.6.A12, Nachweis	Schlüssel gelöscht, Protokoll [Nr.]	ja (Verfahren), CON.6.A12; Nachweis empfohlen
Entsorgt am	Datum und Entsorger	[Datum], [Entsorger]	empfohlen (TOMORIS)

Mindestverfahren nach CON.6.A12 (Auszug): unverschlüsselte wiederbeschreibbare Datenträger vollständig mit Zufallswerten überschreiben, verschlüsselte durch sicheres Löschen des Schlüssels; eingebaute Datenträger etwa in Druckern über die Gerätefunktion löschen, sonst ausbauen und löschen oder nach E-3 bzw. H-3 vernichten; Smartphones und IoT-Geräte auf Werkseinstellung setzen, bei IoT danach alle Zugangsdaten ändern; Papier nach P-3, optische Datenträger nach O-3 vernichten (ISO/IEC 21964-2). Externe Entsorger müssen mindestens Ihre internen Anforderungen erfüllen (CON.6.A11).

08

Pflege und nicht autorisierte Funde

Prüfintervalle laut CIS, BSI und DVO, Zuständigkeiten und der Ablauf für Geräte und Software, die nicht im Inventar stehen.

Prüfintervalle laut Quelle (CIS mit Implementierungsgruppe, BSI, DVO)

WAS	WIE OFT	QUELLE
Geräte- und Softwareinventar prüfen und aktualisieren	mindestens halbjährlich und nach wesentlichen Änderungen	CIS 1.1, 2.1, IG1
Nicht autorisierte Geräte behandeln	wöchentlich	CIS 1.2, IG1
Herstellerunterstützung der Software prüfen	mindestens monatlich	CIS 2.2, IG1
Nicht autorisierte Software prüfen	monatlich oder öfter	CIS 2.3, IG1
Dateninventar prüfen, sensible Daten zuerst	mindestens jährlich	CIS 3.2, IG1
Aktive Konten auf Berechtigung prüfen	mindestens vierteljährlich	CIS 5.1, IG1
Dienstleisterinventar prüfen	jährlich oder bei wesentlichen Änderungen	CIS 15.1, IG1
Softwarebestand nachtragen	anlassbezogen, insbesondere bei Installation	BSI APP.6.A9

Inventar prüfen, Änderungsverlauf dokumentieren regelmäßig

DVO Nr. 12.4.3 (NIS2)

CIS definiert „bi-annually“ im Glossar der Controls v8.1 als „every six months“; nach wesentlichen Änderungen, etwa einem Hardwaretausch oder einer Übernahme, ist die Prüfung zu wiederholen. Empfehlung von TOMORIS: Änderungen zusätzlich laufend eintragen, bei Beschaffung, Ausgabe, Rückgabe und Entsorgung. Die DVO nennt keine Frist, sondern verlangt eine regelmäßige Überprüfung.

Zuständigkeiten zum Ausfüllen (Aufteilung als Empfehlung von TOMORIS, Intervalle laut Tabelle oben)

AUFGABE	ZUSTÄNDIG	VERTRETUNG	INTERVALL
Inventar führen, Änderungen nachtragen	_____	_____	laufend
Funde nicht autorisierter Geräte behandeln	_____	_____	wöchentlich (CIS 1.2)
Abgleich mit Geräteverwaltung, Lizenzen, Supportstatus	_____	_____	monatlich (CIS 2.2, 2.3)
Cloud-Dienste, Verträge, Admin-Konten prüfen	_____	_____	vierteljährlich (CIS 5.1)
Gesamtprüfung und Freigabe durch die Leitung	_____	_____	halbjährlich (CIS 1.1, 2.1)

- Erkennen: Geräte und Software, die nicht im Inventar stehen, finden sich in Netzscans, DHCP-Protokollen, Geräteverwaltung oder Softwareinventur; das BSI rät zu regelmäßigen Netzscans nach nicht zuzuordnenden Geräten (BSI-Standard 200-2, Kap. 8.1.7), CIS zu Erkennungswerkzeugen ab IG2 (Safeguards 1.3 bis 1.5, 2.4).
- Zuordnen: klären, wem Gerät oder Software gehört und wofür sie gebraucht wird; erst mit Inventar und Fachbereichen abgleichen, dann entfernen (Empfehlung von TOMORIS).
- Entscheiden: Geräte aus dem Netz entfernen, Fernzugang verweigern oder in Quarantäne setzen (CIS 1.2) oder zulassen und inventarisieren; Software entfernen oder eine dokumentierte Ausnahme erteilen (CIS 2.3).
- Dokumentieren: Fund, Entscheidung, Zuständige und Datum festhalten, Ausnahmen befristen (Empfehlung von TOMORIS); NIS2-Einrichtungen erfassen Änderungen im Inventar nachvollziehbar (Anhang Nr. 12.4.1 DVO (EU) 2024/2690).

Funde und Ausnahmen zum Ausfüllen

DATUM	FUND	ENTSCHEIDUNG	ZUSTÄNDIG, BEFRISTET BIS
[TT.MM.JJJJ]	unbekanntes Gerät, MAC [Adresse], Besprechungsraum	Quarantäne, Klärung mit [Abteilung]	_____
_____	_____	_____	_____

Technisch verhindern lässt sich nicht genehmigte Software mit Allowlisting (CIS-Safeguard 2.5, IG2; NIST PR.PS-05); NIS2-Einrichtungen schützen ihre Systeme vor nicht genehmigter Software (Anhang Nr. 6.9 DVO (EU) 2024/2690).

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

KOSTENLOS PRÜFEN

NIS2-Betroffenheitscheck

tomoris.com/tools/nis2-check

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

09

Quellen

Alle Aussagen sind belegt. Gesetzestexte gelten in der jeweils geltenden Fassung.

- CIS Critical Security Controls Navigator v8.1 (Safeguards im Wortlaut, mit Implementierungsgruppen)**
Safeguards 1.1 bis 1.5, 2.1 bis 2.5, 3.1, 3.2, 3.4, 3.5, 5.1, 12.4, 15.1, gelesen am 25.10.2026
www.cisecurity.org/controls/cis-controls-navigator
- CIS Critical Security Controls Version 8.1 (August 2024), Dokument zum Download auf der CIS-Seite zu v8.1**
Control 1 und 2 (Überblick), Glossar „Bi-annually“, S. A3
www.cisecurity.org/controls/v8-1
- NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29 (Februar 2024)**
Anhang A: Kategorie ID.AM und Unterkategorie PR.PS-05
nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- BSI-Standard 200-2 IT-Grundschutz-Methodik, Version 1.0 (Oktober 2017)**
Kap. 8.1 Strukturanalyse (8.1.1 bis 8.1.8), 8.2.1 bis 8.2.4
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Sta...
- BSI IT-Grundschutz-Kompendium, Edition 2023 (Gesamt-PDF)**
ORP.1.A8, ORP.2.A2, CON.6.A1, A11, A12, OPS.2.2.A3, A4, A9, A14, APP.6.A9
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- NISG 2026, BGBl. I Nr. 94/2025, geltende Fassung im RIS**
§ 32 Abs. 4 lit. i, Fassung vom 25.10.2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- NISV 2026, BGBl. II Nr. 290/2026**
§ 2, kundgemacht am 1.10.2026
www.ris.bka.gv.at/eli/bgbl/II/2026/290
- Durchführungsverordnung (EU) 2024/2690, Anhang**
Nr. 5.2, 6.1.2, 6.7.2, 6.9, 12.1.2, 12.2.2, 12.3, 12.4 und 12.5
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/deu
- Verordnung (EU) 2016/679 (DSGVO), Art. 30**
Art. 30 Abs. 1 Verzeichnis von Verarbeitungstätigkeiten
eur-lex.europa.eu/eli/reg/2016/679/oj/deu