Erklärung zur Anwendbarkeit (SoA)

Hinweis
Eine Zeile je Maßnahme aus Anhang A der ISO/IEC 27001:2022. Halten Sie je Zeile fest, ob die Maßnahme anwendbar ist, warum Sie sie aufnehmen (Risiko, Gesetz, Vertrag) oder warum nicht, wie weit sie umgesetzt ist (umgesetzt / teilweise umgesetzt / geplant / nicht umgesetzt) und wo der Nachweis liegt. Kurztitel und Erläuterungen sind eigene Worte; maßgeblich ist der Wortlaut Ihres lizenzierten Normexemplars.

ISO/IEC 27001:2022 Anhang A

A.5 Organisatorische Maßnahmen

Maßnahme	Worum es geht	Anwendbar	Begründung	Umsetzungsstand	Nachweis
A.5.1 Sicherheitsleitlinie und Themenrichtlinien	Alle Beteiligten sollen wissen, welche Sicherheitsregeln gelten und wer sie in Kraft gesetzt hat. Das Dach bildet eine kurze, von der Geschäftsführung unterschriebene Leitlinie; darunter regeln Themenrichtlinien einzelne Gebiete wie Zugriffe, Fernwartung oder Backup. Woran prüfen Sie es: Jede Richtlinie hat eine Freigabe, ein Datum der letzten Durchsicht und einen Nachweis, dass die Betroffenen sie kennen.				
A.5.2 Zuständigkeiten im ISMS festlegen	Für jede Sicherheitsaufgabe gibt es eine benannte Person, die sie übernommen hat. Typische Rollen im Mittelstand sind ISB, OT-Verantwortliche und Risikoeigentümer; eine RACI-Matrix zeigt auf einen Blick, wer entscheidet, wer mitarbeitet und wer informiert wird. Prüfen Sie, ob die Benennungen schriftlich vorliegen und die Personen davon wissen.				
A.5.3 Trennung von Aufgaben	Unverträgliche Tätigkeiten (Beantragen/Genehmigen, Ändern/Prüfen) trennen; in kleinen Teams kompensierende Kontrollen dokumentieren.				
A.5.4 Pflichten der Führungskräfte	Sicherheit gelingt nur, wenn Vorgesetzte sie vorleben und einfordern. Führungskräfte erklären ihrem Team die geltenden Regeln, achten im Alltag auf deren Einhaltung und sprechen Verstöße an. Woran prüfen Sie es: Unterweisungen sind dokumentiert, und Führungskräfte können die wichtigsten Regeln ihres Bereichs nennen.				
A.5.5 Behördenkontakte und Meldewege	Ansprechpartner und Meldewege zu Polizei (ZAC), BSI, Datenschutzaufsicht und ggf. NIS2-Meldestelle vorab festlegen.				
A.5.6 Kontakt zu Fachgruppen und Netzwerken	Mitgliedschaft in Branchen- oder Sicherheitsnetzwerken (z. B. Allianz für Cyber-Sicherheit, Verbände) pflegen, um Informationen auszutauschen.				

Maßnahme	Worum es geht	Anwendbar	Begründung	Umsetzungsstand	Nachweis
A.5.7 Bedrohungslage beobachten	Wer die aktuelle Gefährdungslage kennt, kann rechtzeitig reagieren. Legen Sie Quellen fest (BSI-Warnungen, Herstellerhinweise, ICS-Advisories, Branchennetzwerke), benennen Sie, wer sie sichtet, und halten Sie fest, welche Maßnahme aus einer relevanten Meldung folgt. Ein kurzer monatlicher Lagebericht an die Leitung macht die Arbeit sichtbar.				
A.5.8 Sicherheit in Projekten mitdenken	Sicherheitsanforderungen in jedes Projekt einbauen, z. B. per Checkliste bei Projektstart neuer Anlagen oder IT-Systeme.				
A.5.9 Bestandsverzeichnis Informationen und Systeme	Schützen kann man nur, was man kennt. Führen Sie ein Bestandsverzeichnis, das Informationsbestände, IT-Systeme und Anlagen der Produktion zusammen zeigt, und geben Sie jedem Eintrag eine verantwortliche Person. Woran prüfen Sie es: Neue und ausgemusterte Systeme tauchen zeitnah auf, und ein Abgleich mit Netzscan oder Lizenzportal findet keine großen Lücken.				
A.5.10 Nutzungsregeln für Informationen und Geräte	Beschäftigte brauchen klare Ansagen, was mit Firmengeräten und Informationen erlaubt ist und was nicht. Eine kurze Nutzungsrichtlinie regelt etwa private Nutzung, erlaubte Cloud- und KI-Dienste und den Umgang mit mobilen Geräten. Lassen Sie sich die Kenntnisnahme bestätigen und stimmen Sie Kontrollen mit Datenschutz und Betriebsrat ab.				
A.5.11 Rückgabe beim Ausscheiden	Beim Austritt oder Vertragsende Geräte, Schlüssel, Ausweise und Daten zurückfordern – per Checkliste im Austrittsprozess.				
A.5.12 Schutzklassen für Informationen	Nicht jede Information braucht denselben Schutz. Legen Sie wenige, gut verständliche Schutzklassen fest (zum Beispiel öffentlich, intern, vertraulich, streng vertraulich) und beschreiben Sie je Klasse, was das für Ablage, Weitergabe und Vernichtung bedeutet. Prüfen Sie, ob die Verantwortlichen ihre Informationen tatsächlich eingestuft haben.				
A.5.13 Schutzklasse sichtbar machen	Wer ein Dokument oder einen Datenträger in der Hand hat, soll sofort erkennen, wie schutzbedürftig der Inhalt ist. Bewährt sind Vermerke in Dokumentvorlagen, Labels in E-Mail und Office sowie Aufkleber auf Datenträgern. Stichprobe: Tragen vertrauliche Dokumente im Umlauf den passenden Vermerk?				
A.5.14 Sicherer Datenaustausch	Informationen sollen auch auf dem Weg zu Kunden, Lieferanten oder Behörden geschützt bleiben. Legen Sie fest, welche Wege je Schutzklasse erlaubt sind, etwa verschlüsselte E-Mail, ein Datenraum oder eine Austauschplattform für CAD-Daten, und regeln Sie den Austausch mit wichtigen Partnern vertraglich. Woran prüfen Sie es: Vertrauliche Daten gehen nicht unverschlüsselt per E-Mail oder über private Dienste hinaus.				
A.5.15 Zugriffsgrundsätze	Jede Person soll genau die Zugriffe haben, die ihre Aufgabe erfordert, nicht mehr. Halten Sie diese Grundsätze (Kenntnis nur bei Bedarf, geringste Rechte, Rollen statt Einzelrechte) in einer Richtlinie fest, die für Büro-IT und Produktion gleichermaßen gilt. Die technische Umsetzung beschreiben A.5.18 und A.8.3.				

Maßnahme	Worum es geht	Anwendbar	Begründung	Umsetzungsstand	Nachweis
A.5.16 Lebenszyklus von Identitäten	Jede Aktion im System soll sich einer Person oder einem bekannten technischen Konto zuordnen lassen. Regeln Sie, wie Konten angelegt, geändert und gelöscht werden, und halten Sie Ausnahmen wie Sammelkonten an Bedienpanels bewusst fest. Woran prüfen Sie es: Es gibt keine aktiven Konten ausgeschiedener Personen und keine Konten ohne zuständige Person.				
A.5.17 Umgang mit Authentisierungsdaten	Passwörter, Token und Schlüssel dürfen nicht in falsche Hände geraten. Geben Sie Regeln für Ausgabe, Aufbewahrung und Wechsel vor, stellen Sie einen Passwortmanager bereit und ersetzen Sie voreingestellte Passwörter an Anlagen vor der Inbetriebnahme. Prüfen Sie stichprobenartig, ob Zugangsdaten offen auf Zetteln oder in Dateien liegen.				
A.5.18 Rechtevergabe und Rezertifizierung	Rechte entstehen nur auf Antrag mit Freigabe und verschwinden wieder, wenn sie nicht mehr gebraucht werden. Die verantwortlichen Personen bestätigen in festen Abständen, ob die vergebenen Rechte noch passen; bei Austritt oder Wechsel werden Rechte zeitnah entzogen. Woran prüfen Sie es: Antrag und Freigabe sind nachvollziehbar, und die letzte Rezertifizierung ist dokumentiert.				
A.5.19 Lieferantenrisiken steuern	Lieferanten mit Zugang zu Ihren Daten, Systemen oder Anlagen bringen eigene Risiken mit. Teilen Sie sie nach Bedeutung ein, legen Sie je Stufe fest, welche Sicherheitsnachweise Sie erwarten, und berücksichtigen Sie das schon bei der Auswahl. Ein Lieferantenverzeichnis mit Einstufung und Datum der letzten Bewertung macht den Stand prüfbar.				
A.5.20 Sicherheitsklauseln in Lieferverträgen	Was im Vertrag steht, lässt sich später einfordern. Vereinbaren Sie mit wichtigen Lieferanten je nach Leistung zum Beispiel Regeln für Fernwartung, Fristen für die Meldung von Vorfällen, Vertraulichkeit und das Recht, Nachweise anzufordern oder zu prüfen. Prüfen Sie, ob die Verträge kritischer Lieferanten diese Punkte enthalten.				
A.5.21 Herkunft und Versorgung von IT-Komponenten	Risiken aus Hard-/Software-Lieferketten betrachten, z. B. Herkunft von Komponenten, Update-Versorgung, SBOM bei Anlagen.				
A.5.22 Lieferantenleistung im Blick behalten	Ein guter Vertrag nützt wenig, wenn niemand hinschaut, ob er eingehalten wird. Bewerten Sie kritische Lieferanten in festen Abständen anhand von Störungen, Berichten oder Zertifikaten und prüfen Sie Änderungen an deren Leistungen, bevor Sie sie übernehmen. Ergebnis und Folgen der Bewertung gehören ins Lieferantenverzeichnis.				
A.5.23 Cloud-Dienste auswählen, betreiben, verlassen	Auswahl, Nutzung, Konfiguration und Ausstieg aus Cloud-Diensten regeln – inkl. geteilter Verantwortung mit dem Anbieter.				

Maßnahme	Worum es geht	Anwendbar	Begründung	Umsetzungsstand	Nachweis
A.5.24 Vorfallbereitschaft	Wenn ein Vorfall eintritt, soll niemand erst überlegen müssen, wer was tut. Legen Sie Rollen, Meldewege, Eskalationsstufen und eine aktuelle Kontaktliste vorab fest und denken Sie Szenarien für die Produktion mit, etwa den Ausfall einer Linie. Woran prüfen Sie es: Der Ablauf ist beschrieben und wurde mindestens einmal geübt.				
A.5.25 Einstufung gemeldeter Ereignisse	Nicht jede Meldung ist ein Vorfall, aber jede verdient eine Entscheidung. Legen Sie Kriterien fest, nach denen gemeldete Ereignisse eingestuft werden, zum Beispiel betroffene Systeme, Schutzklasse der Daten oder Auswirkung auf die Produktion. Halten Sie die Entscheidung mit Begründung fest, damit sie später nachvollziehbar ist.				
A.5.26 Vorfälle bewältigen	Im Ernstfall zählt, den Schaden schnell zu begrenzen und den Betrieb sicher wieder aufzunehmen. Halten Sie für häufige Szenarien wie Ransomware oder kompromittierte Konten kurze Ablaufpläne bereit, die Eindämmen, Bereinigen und Wiederanlauf abdecken. Dokumentieren Sie während der Bearbeitung, was wann entschieden wurde.				
A.5.27 Nachbereitung von Vorfällen	Jeder Vorfall zeigt eine Schwachstelle, die sich schließen lässt. Besprechen Sie nach relevanten Vorfällen im Team, was gut lief, was nicht und warum, und übertragen Sie die Erkenntnisse in Maßnahmen, Risikobewertung oder Schulung. Woran prüfen Sie es: Aus den Nachbesprechungen sind Maßnahmen mit Termin und Verantwortlichen entstanden.				
A.5.28 Sicherung von Beweismitteln	Spuren eines Angriffs sind schnell verwischt, etwa durch einen Neustart oder eine Neuinstallation. Legen Sie vorab fest, wer Protokolle, Datenträger und Systemabbilder sichert, wie die Übergabe dokumentiert wird und wann ein externer Forensikpartner hinzukommt. So bleiben Beweise auch für Versicherung, Behörden oder Gericht verwertbar.				
A.5.29 Schutz im Notbetrieb	Im Notbetrieb wird improvisiert, und gerade dann entstehen Lücken. Planen Sie, welche Schutzmaßnahmen auch während einer Störung gelten müssen, zum Beispiel keine ungesicherten Notzugänge und kein Abschalten der Protokollierung, und welche Ersatzlösungen dafür bereitstehen. Prüfen Sie in Notfallübungen, ob das eingehalten wird.				
A.5.30 Wiederanlauf von IT und OT	Wiederanlaufziele (RTO/RPO) für IT- und OT-Systeme ableiten, Notfallpläne erstellen und regelmäßig testen.				
A.5.31 Rechtskataster und Vertragspflichten	Sie sollen jederzeit wissen, welche Gesetze, Vorschriften und Verträge Sicherheitspflichten für Sie begründen. Ein Rechtskataster listet sie mit Fundstelle, Bedeutung für Ihr Unternehmen und zuständiger Person, etwa DSGVO, NIS2, Kundenverträge und Exportkontrolle. Prüfen Sie es mindestens jährlich und bei neuen Gesetzen oder Großkunden.				

Maßnahme	Worum es geht	Anwendbar	Begründung	Umsetzungsstand	Nachweis
A.5.32 **Lizenzen und Know-how-Schutz**	Fremde Rechte wahren und eigenes Wissen schützen gehören zusammen. Führen Sie Lizenzen zentral, verhindern Sie die Installation nicht lizenzierter Software und kennzeichnen Sie eigenes Know-how wie Konstruktionen oder Rezepturen als schutzwürdig. Ein jährlicher Abgleich von Lizenzbestand und Installationen zeigt, ob es passt.				
A.5.33 **Nachweise sicher aufbewahren**	Nachweise wie Protokolle, Verträge, Prüfberichte oder Freigaben müssen auch Jahre später noch vollständig und unverändert vorliegen. Legen Sie je Art fest, wo sie liegen, wer darauf zugreifen darf und wie lange sie aufbewahrt werden, und sorgen Sie dafür, dass sie über diese Zeit gesichert und lesbar bleiben. Stichprobe: Lässt sich ein älterer Nachweis schnell finden, und ist er unversehrt?				
A.5.34 **Datenschutz im ISMS**	Datenschutz und Informationssicherheit greifen ineinander und sollten nicht getrennt geplant werden. Binden Sie die Person, die den Datenschutz verantwortet, in Risikobewertung und Maßnahmen ein und verknüpfen Sie Verarbeitungsverzeichnis und Bestandsverzeichnis. Woran prüfen Sie es: Datenschutzanforderungen tauchen in Richtlinien und Risikoregister des ISMS auf.				
A.5.35 **Blick von außen auf das ISMS**	Wer das eigene ISMS betreibt, übersieht leicht Schwächen. Lassen Sie es deshalb in geplanten Abständen und bei größeren Änderungen von Personen prüfen, die nicht selbst daran mitgearbeitet haben, etwa durch ein externes Audit oder einen Penetrationstest. Ergebnisse und Folgemaßnahmen gehören in die Managementbewertung.				
A.5.36 **Regeltreue im Alltag prüfen**	Regeln wirken nur, wenn sie im Alltag eingehalten werden. Prüfen Sie das regelmäßig auf drei Wegen: Führungskräfte schauen in ihrem Bereich hin, der ISB zieht Stichproben, und technische Prüfungen zeigen Abweichungen bei Konfigurationen. Gefundene Abweichungen werden wie Nichtkonformitäten behandelt.				
A.5.37 **Schriftliche Betriebsanweisungen**	Wichtige Abläufe sollen auch dann funktionieren, wenn die erfahrene Person fehlt. Schreiben Sie die Schritte für Backup, Wiederherstellung, Benutzerverwaltung oder den Neustart einer Anlage so auf, dass eine fachkundige Vertretung sie ausführen kann. Prüfen Sie, ob die Anweisungen aktuell sind und dort liegen, wo man sie im Ernstfall braucht.				

A.6 Personenbezogene Maßnahmen

Maßnahme	Worum es geht	Anwendbar	Begründung	Umsetzungsstand	Nachweis
A.6.1 **Überprüfung von Bewerbenden**	Vertrauen in neue Mitarbeitende soll auf geprüften Angaben beruhen, nicht allein auf einem guten Eindruck. Legen Sie je nach Sensibilität der Stelle fest, welche rechtlich zulässigen Prüfungen erfolgen, etwa Zeugnisse, Referenzen oder bei besonderen Rollen ein Führungszeugnis. Dokumentieren Sie, dass die Prüfung vor Arbeitsbeginn stattgefunden hat.				

Maßnahme	Worum es geht	Anwendbar	Begründung	Umsetzungsstand	Nachweis
A.6.2 Sicherheitspflichten im Arbeitsvertrag	Wer bei Ihnen arbeitet, soll von Anfang an wissen, welche Sicherheitspflichten mit der Stelle verbunden sind. Nehmen Sie diese Pflichten, etwa Vertraulichkeit, Einhaltung der Richtlinien und Meldung von Vorfällen, in den Arbeitsvertrag oder eine Zusatzvereinbarung auf. Prüfen Sie, ob die aktuelle Vertragsvorlage das abdeckt und auch für Leiharbeitskräfte gilt.				
A.6.3 Sicherheitswissen aufbauen	Beschäftigte sollen Gefahren erkennen und richtig handeln können. Planen Sie Schulungen nach Zielgruppe, vom kurzen E-Learning im Büro über Unterweisungen in der Schichtübergabe bis zu Fachschulungen für Administration und Automatisierung. Woran prüfen Sie es: Teilnahmequoten sind nachgewiesen, und Phishing-Übungen zeigen Fortschritt.				
A.6.4 Umgang mit Regelverstößen	Einen fairen, mit HR und Betriebsrat abgestimmten Prozess für den Umgang mit Regelverstößen festlegen.				
A.6.5 Austritt und Rollenwechsel	Mit dem letzten Arbeitstag enden nicht alle Pflichten. Erklären Sie beim Austritt oder Wechsel, welche Pflichten weiter gelten, zum Beispiel Vertraulichkeit, und lassen Sie sich das bestätigen. Zugleich werden Rechte, die nicht mehr gebraucht werden, über den Austritts- oder Wechselprozess entzogen.				
A.6.6 Geheimhaltung vertraglich absichern	Bevor vertrauliche Informationen das Haus verlassen, sollte schriftlich geregelt sein, was der Empfänger damit tun darf. Nutzen Sie geprüfte Muster für Beschäftigte, Dienstleister und Partner, führen Sie eine Übersicht der abgeschlossenen Vereinbarungen und passen Sie die Muster an, wenn sich Ihr Schutzbedarf ändert. Stichprobe: Liegt für aktuelle Projekte mit Externen eine Vereinbarung vor?				
A.6.7 Homeoffice und mobiles Arbeiten	Regeln für Homeoffice und mobiles Arbeiten festlegen (VPN, Bildschirmsperre, Umgang mit Ausdrucken).				
A.6.8 Einfache Meldewege für Mitarbeitende	Je früher jemand eine Auffälligkeit meldet, desto kleiner bleibt der Schaden. Sorgen Sie für einen einfachen, allen bekannten Weg, etwa eine Telefonnummer, ein Postfach oder einen Melde-Button, und danken Sie für jede Meldung, auch für Fehlalarme. Woran prüfen Sie es: Beschäftigte können auf Nachfrage sagen, wie sie etwas melden.				

A.7 Physische Maßnahmen

Maßnahme	Worum es geht	Anwendbar	Begründung	Umsetzungsstand	Nachweis
A.7.1 Sicherheitszonen auf dem Gelände	Ein Gelände ist leichter zu schützen, wenn klar ist, wo welcher Schutz gilt. Teilen Sie es in Zonen ein, etwa öffentlicher Bereich, Bürogebäude, Produktion, Serverraum und Leitstand, und beschreiben Sie, wie die Grenzen gesichert sind. Ein Lageplan mit eingezeichneten Zonen ist ein guter Nachweis.				

Maßnahme	Worum es geht	Anwendbar	Begründung	Umsetzungsstand	Nachweis
A.7.2 Zutrittskontrolle und Besuchende	Nur wer berechtigt ist, soll in die jeweilige Zone gelangen. Steuern Sie den Zutritt über Schlüssel- oder Ausweissysteme, melden Sie Besuchende an und begleiten Sie sie in geschützten Bereichen. Woran prüfen Sie es: Die Liste der Zutrittsberechtigungen ist aktuell, und ausgegebene Schlüssel sind nachvollziehbar.				
A.7.3 Schutz sensibler Räume	Räume mit sensiblen Informationen oder Technik (z. B. Konstruktion, Leitstand) angemessen sichern.				
A.7.4 Gelände- und Raumüberwachung	Gelände und kritische Räume überwachen, z. B. mit Einbruchmeldeanlage, Videotechnik (Betriebsrat einbinden) oder Wachdienst.				
A.7.5 Gebäudegefahren und Naturereignisse	Feuer, Wasser, Hitze oder Sturm können Technik und Unterlagen ebenso zerstören wie ein Angriff. Bewerten Sie, welche dieser Gefahren an Ihren Standorten realistisch sind, auch mit Blick auf zunehmende Wetterextreme, und schützen Sie wichtige Räume entsprechend, zum Beispiel mit Brandmeldern, Wassersensoren oder erhöhter Aufstellung. Die Bewertung gehört ins Risikoregister.				
A.7.6 Regeln in geschützten Zonen	Regeln für Tätigkeiten in Sicherheitsbereichen festlegen, z. B. Begleitpflicht für Fremdfirmen im Serverraum.				
A.7.7 Nichts liegen lassen, Bildschirm sperren	Clean-Desk- und Clear-Screen-Regeln einführen – auch an Terminals und HMIs in der Produktion.				
A.7.8 Geschützte Aufstellorte für Technik	Wo ein Gerät steht, entscheidet mit darüber, wie gut es geschützt ist. Stellen Sie Server, Netzkomponenten und Steuerungen so auf, dass Staub, Feuchtigkeit, Stöße und neugierige Finger fernbleiben, zum Beispiel in abschließbaren Schränken oder eigenen Räumen. Stichprobe: Stehen offene Schaltschränke oder Netzwerkschränke in frei zugänglichen Bereichen?				
A.7.9 Geräte unterwegs	Laptops, mobile Geräte und Service-Notebooks außerhalb des Betriebs schützen (Verschlüsselung, Transportregeln).				
A.7.10 Wechseldatenträger und USB	Umgang mit USB-Sticks und Wechselmedien regeln – Freigabe, Verschlüsselung, Schleusen-PC für die Produktion.				
A.7.11 Strom, Kühlung, Netzanbindung	Ohne Strom, Kühlung und Netzanbindung stehen auch gut geschützte Systeme still. Ermitteln Sie, welche Systeme auf eine unterbrechungsfreie Versorgung angewiesen sind, und sichern Sie sie etwa mit USV, Notstrom oder redundanter Klimatisierung ab. Woran prüfen Sie es: Die Ersatzversorgung wird regelmäßig unter Last getestet, und die Ergebnisse sind dokumentiert.				

Maßnahme	Worum es geht	Anwendbar	Begründung	Umsetzungsstand	Nachweis
A.7.12 Leitungen und Kabelwege schützen	Ein beschädigtes oder angezapftes Kabel kann ganze Bereiche lahmlegen oder Daten preisgeben. Führen Sie Leitungen möglichst geschützt, etwa in Kabelkanälen oder Doppelböden, trennen Sie Strom- und Datenleitungen, wo es nötig ist, und deaktivieren Sie ungenutzte Netzwerkdosen in Hallen und Besprechungsräumen. Ein aktueller Kabel- und Dosenplan hilft bei der Prüfung.				
A.7.13 Wartung von Geräten und Anlagen	Gut gewartete Technik fällt seltener aus, und die Wartung selbst darf keine Hintertür öffnen. Planen Sie Wartungen nach den Vorgaben der Hersteller, begleiten oder protokollieren Sie Einsätze von Fremdfirmen und prüfen Sie Geräte, die zur Reparatur außer Haus waren, bevor sie wieder ans Netz gehen. Ein Wartungsplan mit erledigten Terminen dient als Nachweis.				
A.7.14 Datenträger vor Abgabe löschen	Datenträger vor Entsorgung oder Weitergabe sicher löschen oder vernichten – mit Nachweis des Dienstleisters.				

A.8 Technologische Maßnahmen

Maßnahme	Worum es geht	Anwendbar	Begründung	Umsetzungsstand	Nachweis
A.8.1 Verwaltete Endgeräte	Laptops, Smartphones und Tablets zentral verwalten (Geräteverwaltung), Datenträger verschlüsseln, Bildschirmsperre und automatische Updates erzwingen und verlorene Geräte aus der Ferne sperren oder löschen können. Nachweis: Bericht der Geräteverwaltung mit dem Anteil verwalteter, verschlüsselter und aktueller Geräte.				
A.8.2 Administratorrechte	Administrative Rechte nur an benannte Personen vergeben, getrennte persönliche Admin-Konten ohne E-Mail und Internet nutzen, Notfallkonten versiegelt aufbewahren und jede Anmeldung protokollieren. Nachweis: Liste der privilegierten Konten mit Datum der letzten Überprüfung, bewährt halbjährlich.				
A.8.3 Technische Durchsetzung der Berechtigungen	Zugriffe technisch so einschränken, wie es das Berechtigungskonzept vorsieht: Rechte über Rollen, Freigaben auf Dateiablagen nach Abteilung, vertrauliche Bereiche gesondert geschützt. Nachweis: Rollenmodell und Stichprobe, dass die eingestellten Rechte dem Konzept entsprechen.				
A.8.4 Schutz von Quellcode und SPS-Programmen	Quellcode, Skripte und SPS-Programme in einer Versionsverwaltung führen, Schreibzugriff auf das Projektteam beschränken und Änderungen einer Person zuordnen. Auch bei Integratoren sicherstellen, dass Sie die aktuellen Quellprojekte erhalten.				
A.8.5 Starke Anmeldeverfahren	Mehrfaktor-Anmeldung für alle Zugänge aus dem Internet, Cloud-Dienste, E-Mail und Administration einsetzen; Passwörter lang statt kompliziert, Sperre nach Fehlversuchen, keine Standardpasswörter. Nachweis: Konfigurationsexport oder Bericht des Identitätsdienstes mit der MFA-Abdeckung und begründeten Ausnahmen.				

Maßnahme	Worum es geht	Anwendbar	Begründung	Umsetzungsstand	Nachweis
A.8.6 Auslastung und Kapazitätsplanung	Auslastung von Servern, Speicher, Netzen und Cloud-Diensten überwachen, Schwellwerte mit Alarm festlegen und Erweiterungen rechtzeitig planen. Volle Speicher sind eine häufige Ursache für ausgefallene Sicherungen und fehlende Protokolle.				
A.8.7 Abwehr von Malware	Zentral verwaltete Schutzsoftware mit Verhaltenserkennung auf allen geeigneten Systemen, E-Mail-Filter und gesperrte Makros aus dem Internet. Wo der Anlagenhersteller keine Schutzsoftware freigibt: Anwendungs-Whitelist, Schleusen-PC für USB-Datenträger und Netztrennung. Nachweis: Statusbericht der Schutzsoftware und Liste der Ausnahmen.				
A.8.8 Schwachstellen- und Patchmanagement	Schwachstellen über Inventarabgleich, Herstellerhinweise und Scanner erkennen, nach Schweregrad und Ausnutzung priorisieren und in festen Fristen beheben (bewährt: 7, 30, 90 und 180 Tage). Für nicht patchbare OT-Systeme befristete Ausnahmen mit kompensierenden Maßnahmen im Risikoregister führen. Nachweis: Auswertung offener Schwachstellen nach Alter und Schweregrad.				
A.8.9 Sichere Standardkonfiguration	Für jeden Systemtyp eine sichere Standardkonfiguration festlegen (z. B. nach CIS Benchmarks oder BSI IT-Grundschutz), zentral ausrollen und Abweichungen regelmäßig prüfen. Konfigurationen von Netzkomponenten und Steuerungen sichern und nach Änderungen vergleichen.				
A.8.10 Löschfristen und Löschwege	Für jede Datenart Aufbewahrungsfrist und Löschweg festlegen, auch in Sicherungen, Archiven und bei Cloud-Anbietern. Datenträger und Geräte vor Entsorgung, Reparatur oder Rückgabe sicher löschen oder nach DIN 66399 vernichten lassen. Nachweis: Löschprotokolle und Vernichtungsnachweise.				
A.8.11 Echtdaten maskieren	In Test-, Schulungs- und Analyseumgebungen keine echten Personal- oder Kundendaten verwenden; wo Echtdaten nötig sind, Namen und Kennungen maskieren oder pseudonymisieren und die Freigabe dokumentieren.				
A.8.12 Abflusswege für Daten absichern	Schützenswerte Informationen wie Konstruktionsdaten bestimmen und die Abflusswege absichern: USB-Datenträger beschränken, private Cloud-Speicher sperren, vertrauliche Anhänge nur an freigegebene Empfänger, Datenaustausch über eine protokollierte Plattform. Technische Überwachung mit Datenschutz und Betriebsrat abstimmen.				
A.8.13 Backup und Wiederherstellungstest	Sicherungskonzept aus Wiederanlaufzeit und maximal tolerierbarem Datenverlust der Prozesse ableiten, 3-2-1-1-0-Regel mit mindestens einer unveränderbaren oder offline gelagerten Kopie, Sicherungssystem mit eigenen Zugangsdaten. SPS-Programme und Anlagenkonfigurationen nach jeder Änderung mitsichern. Nachweis: Protokoll des letzten vollständigen Wiederherstellungstests mit Zeitmessung.				

Maßnahme	Worum es geht	Anwendbar	Begründung	Umsetzungsstand	Nachweis
A.8.14 Redundante Auslegung kritischer Systeme	Systeme, deren Ausfall nicht tolerierbar ist, redundant auslegen (zweite Leitung, Cluster, zweites Netzteil, zweiter Standort) und die Umschaltung regelmäßig erproben. Redundanz ersetzt keine Sicherung, denn gelöschte oder verschlüsselte Daten werden mit gespiegelt.				
A.8.15 Protokolle sammeln und schützen	An- und Abmeldungen samt Fehlversuchen, Rechteänderungen, Admin-Aktionen, Konfigurationsänderungen, Funde der Schutzsoftware, Verbindungen zwischen Zonen und Fernwartungssitzungen protokollieren, zentral sammeln und vor Veränderung schützen. Aufbewahrung bewährt: 90 Tage durchsuchbar, 6 bis 12 Monate archiviert, abgestimmt mit dem Datenschutz.				
A.8.16 Alarmierung bei Auffälligkeiten	Wenige, gut abgestimmte Alarmregeln mit klarer Zuständigkeit festlegen (z. B. viele Fehlanmeldungen, Admin-Anmeldung nachts, neue Verbindung ins Produktionsnetz, gelöschte Sicherungen) und regelmäßige Auswertungen dokumentieren. In der Produktion bewährt: passives Mitlesen des Netzverkehrs an einer Spiegelschnittstelle.				
A.8.17 Einheitliche Systemzeit	Alle Systeme einschließlich Netzkomponenten und Steuerungen mit einer gemeinsamen, verlässlichen Zeitquelle synchronisieren, Protokolle in einer einheitlichen Zeitzone speichern und Abweichungen melden. Ohne einheitliche Zeit lassen sich Vorfälle kaum rekonstruieren.				
A.8.18 Mächtige Admin-Werkzeuge	Werkzeuge, die Sicherheitsmechanismen umgehen oder Systeme tief verändern können (Admin-Werkzeuge, Debugger, Scanner, Engineering-Software für Steuerungen), nur auf dafür vorgesehenen Systemen installieren, auf benannte Personen beschränken und die Nutzung nachvollziehbar machen.				
A.8.19 Freigegebene Software	Benutzern keine Installationsrechte geben, Software nur aus einem freigegebenen Katalog verteilen und neue Programme nach Prüfung von Herkunft, Lizenz und Sicherheit freigeben. Auf Servern und Bedienstationen nur über das Änderungsmanagement installieren.				
A.8.20 Netzkomponenten und Netzplan	Netzkomponenten sicher konfigurieren und verwalten (Verwaltung nur aus einem Admin-Netz, keine Standardpasswörter, aktuelle Firmware), einen aktuellen Netzplan führen und Übergänge zwischen IT und OT über Firewalls mit dokumentierten Regeln kontrollieren. Nachweis: Netzplan und Regelwerk mit Datum der letzten Durchsicht.				
A.8.21 Anforderungen an Netzanbieter	Sicherheitsanforderungen an Internet-, VPN- und Standortverbindungen festlegen und mit den Anbietern vereinbaren (Verfügbarkeit, Verschlüsselung, Meldung von Störungen und Vorfällen). Leistung und Störungsberichte regelmäßig auswerten.				
A.8.22 Netzzonen und Segmentierung	Netze nach Schutzbedarf in Zonen teilen, mindestens Büro-IT, Produktionsnetz, DMZ für Übergänge, Gastnetz und ein Verwaltungsnetz für Administratoren. Verbindungen zwischen Zonen nur ausdrücklich erlaubt; die Zonen- und Übergangslogik der IEC 62443 ist dafür eine gute Grundlage.				

Maßnahme	Worum es geht	Anwendbar	Begründung	Umsetzungsstand	Nachweis
A.8.23 Web- und DNS-Filter	Zugriffe auf schädliche und unerwünschte Webseiten über einen Webfilter oder DNS-Filter sperren und Uploads zu privaten Cloud-Speichern unterbinden. Produktionssysteme sollten keinen direkten Internetzugang haben.				
A.8.24 Verschlüsselung und Schlüsselverwaltung	Festlegen, wo verschlüsselt oder signiert wird (Datenträger, Übertragung, Sicherungen, gespeicherte Passwörter, Fernwartung), Mindeststandards nach dem Stand der Technik (z. B. BSI TR-02102) vorgeben, unsichere Verfahren abschalten und Schlüssel sowie Zertifikate über ihren ganzen Lebenszyklus verwalten, einschließlich Wiederherstellung und Widerruf.				
A.8.25 Sicherheit in jeder Entwicklungsphase	Sicherheit in jede Phase eigener Entwicklung einbauen: Anforderungen und Bedrohungsanalyse vor dem Start, sichere Programmierung, Tests vor der Freigabe, Pflege der Softwarekomponenten. Das gilt auch für Steuerungssoftware; Hersteller von Produkten mit digitalen Elementen müssen das zusätzlich nach dem Cyber Resilience Act nachweisen.				
A.8.26 Sicherheit im Lastenheft	Sicherheitsanforderungen festlegen, bevor Anwendungen oder Anlagen entwickelt oder beschafft werden, z. B. als Anhang zum Lastenheft: persönliche Konten, MFA für Fernzugriff, Protokollierung, Updates über die Nutzungsdauer, Komponentenliste, dokumentierte Ports.				
A.8.27 Architekturgrundsätze	Architekturgrundsätze wie Defense in Depth, geringste Rechte, sichere Standardeinstellungen und Zonenmodell schriftlich festlegen und bei Entwürfen von Systemen, Netzen und Anlagen nachweisbar anwenden, z. B. in einer kurzen Architekturprüfung.				
A.8.28 Programmierregeln und Code-Review	Programmierregeln festlegen (z. B. nach OWASP), Änderungen von einer zweiten Person prüfen lassen, statische Codeanalyse und Prüfung der Fremdkomponenten auf bekannte Schwachstellen automatisieren. Für SPS-Programme eine eigene Programmierrichtlinie mit Kommentierung und Freigabe.				
A.8.29 Sicherheitstests vor Inbetriebnahme	Sicherheit vor der Inbetriebnahme testen: automatische Tests bei Software, Penetrationstests für exponierte Systeme, bei Anlagen eine Sicherheitsprüfung in Werks- und Baustellenabnahme (FAT/SAT) mit Prüfung auf Standardpasswörter, offene Dienste und Fernzugänge.				
A.8.30 Externe Entwickler und Integratoren	Externe Entwicklung und Integratoren über Sicherheitsanforderungen im Vertrag, Nachweise (Testberichte, Komponentenliste), kontrollierten Zugang zu Ihren Systemen und eine Abnahme mit Übergabe aller Programmstände und Konten steuern.				
A.8.31 Entwicklung, Test und Betrieb getrennt halten	Entwicklung, Test und Betrieb trennen; Entwicklerinnen und Entwickler haben im Betrieb keine Schreibrechte. Änderungen an Steuerungen zuerst an einer Simulation oder Ersatzsteuerung testen, wo das möglich ist.				

Maßnahme	Worum es geht	Anwendbar	Begründung	Umsetzungsstand	Nachweis
A.8.32 Kontrollierte Änderungen	Änderungen an IT- und OT-Systemen beantragen, nach Risiko und Auswirkung bewerten, testen, freigeben, mit Rückfallplan umsetzen und dokumentieren. Standardänderungen vorab genehmigen, Notfalländerungen nachträglich dokumentieren. Nachweis: Änderungsprotokoll mit Stichprobe.				
A.8.33 Umgang mit Testdaten	Testdaten bewusst auswählen und schützen; Echtdaten in Testsystemen nur ausnahmsweise, mit Freigabe, maskiert oder pseudonymisiert und befristet. Testumgebungen mit Echtdaten so schützen wie den Betrieb.				
A.8.34 Prüfungen ohne Betriebsstörung	Technische Prüfungen wie Penetrationstests, Schwachstellenscans oder Audits an laufenden Systemen planen, Umfang und Zeitfenster mit den Verantwortlichen abstimmen und Zugänge der Prüfer befristen. In der Produktion aktive Scans nur nach Absprache und in geplanten Stillständen.				

Über diese Vorlage

Vorlagenversion 1.0-b993bc0e
Stand der Inhalte 26.09.2026
Herausgeber Erstellt mit Complass, https://complass.eu

Rechtsgrundlage (Stand): ISO/IEC 27001:2022 und ISO/IEC 27001:2022/Amd 1:2024 (Originaltext)

Diese Vorlage ist keine Rechtsberatung. Sie ersetzt nicht die Prüfung, welche Anforderungen für Ihr Unternehmen gelten, und garantiert kein Prüfungs- oder Zertifizierungsergebnis.

Lizenz: Creative Commons Namensnennung 4.0 International (CC BY 4.0). Sie dürfen die Vorlage verwenden, ändern und weitergeben, auch kommerziell, wenn Sie die Quelle nennen. Namensnennung: „Vorlage: Complass (complass.eu), CC BY 4.0“. https://creativecommons.org/licenses/by/4.0/deed.de