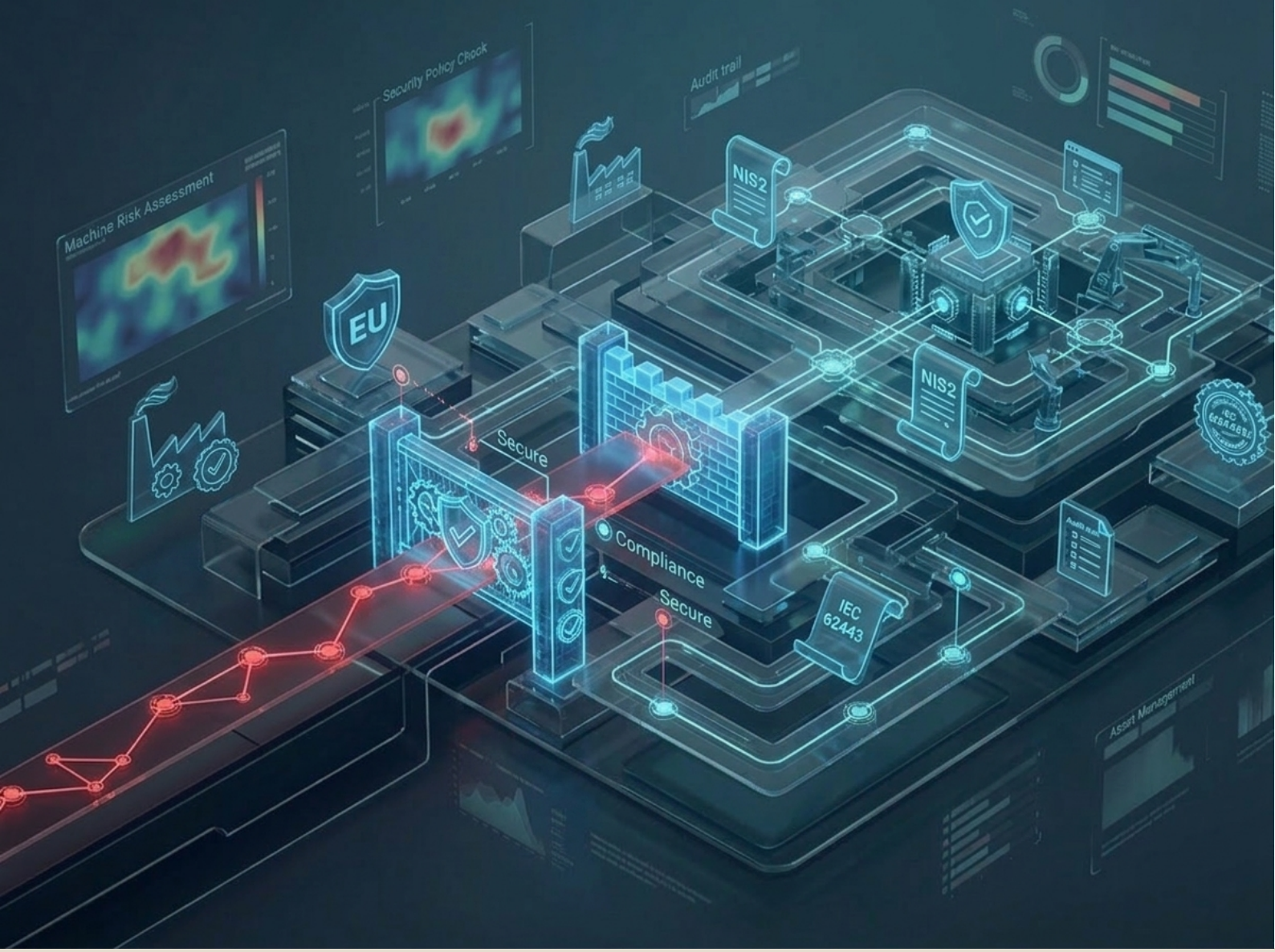

WHITE PAPER

Regulatorische Cybersicherheit im Maschinen- und Anlagenbau

Schweizer Perspektive:

Von ISG und IKT-Minimalstandard über PrSG/MaschV bis zu EU-Maschinenverordnung, NIS-2 und Cyber Resilience Act.

Schweizer und europäische Regulierungen verändern die Cybersicherheits-pflichten im Maschinen- und Anlagenbau grundlegend. Dieses White Paper zeigt aus Schweizer Perspektive, welche nationalen und EU-Vorschriften gelten, welche Fristen laufen und wie Sie mit einem integrierten Ansatz alle Anforderungen effizient erfüllen.

SecureComply GmbH | April 2026

SecureComply
Secure by Design. Compliant by Default.

Inhaltsverzeichnis

01 Executive Summary

Für Schweizer Maschinen- und Anlagenbauer definieren nationale und europäische Regulierungen die Cybersicherheitspflichten neu. Auf nationaler Ebene sind das Informationssicherheitsgesetz (ISG) mit Meldepflicht seit April 2025, der IKT-Minimalstandard des BWL, das Produktesicherheits-gesetz (PrSG) mit der Maschinenverordnung (MaschV) und das revidierte Datenschutzgesetz (revDSG) massgebend. Auf EU-Seite greifen die EU-Maschinenverordnung ab Januar 2027, der Cyber Resilience Act ab Dezember 2027 sowie NIS-2 und CER. Für Schweizer Unternehmen bedeutet dies:

Wer jetzt nicht handelt, riskiert nicht nur Bussgeld, sondern auch den Verlust von Kundenvertrauen und Marktzugang.

Die acht wichtigsten Regulierungen adressieren unterschiedliche Perspektiven. Sie beinhalten Produktsicherheit, Betreiberpflichten, Datenschutz, KI-Governance und physische Resilienz. Wer nur einzelne Anforderungen erfüllt, riskiert Lücken mit erheblichen rechtlichen und operativen Konsequenzen.

Schweizer Unternehmen im Maschinen- und Anlagenbau sind als Hersteller, Betreiber und Exporteure gleichzeitig von nationalen Schweizer Gesetzen und EU-Regulierungen betroffen. Wer in den EU-Markt exportiert, muss EU-Konformität nachweisen. Ein integrierter Compliance-Ansatz, der Schweizer und EU-Anforderungen verbindet, ist effizienter und nachhaltiger als isolierte Einzelmassnahmen.

Dieses White Paper gibt Ihnen einen kompakten, praxisorientierten Überblick über alle acht wichtigen Regulierungen. Es zeigt auf, was sie fordern, wen sie betreffen, bis wann Sie handeln müssen und was das konkret für Ihren Betrieb bedeutet.

Regulierung	Frist	Adressiert	Kernbotschaft
EU-Maschinenverordnung 2023	Jan. 2027	Hersteller	Cybersicherheit als verbindliches Sicherheitsziel für Maschinenprodukte
Cyber Resilience Act (CRA)	11. Dez. 2027 (Meldepflichten ab Sep. 2026)	Hersteller	Schwachstellenmanagement, SBOM, ENISA-Meldungen für vernetzte Produkte
NIS-2-Richtlinie	Ab 2025/26 (DE Dez. 2025, AT Okt. 2026)	Betreiber	Risikomassnahmen, Meldepflichten, Managementhaftung ab 50 Mitarbeitenden
DSGVO / GDPR	Seit 2018	Alle	Schutz personenbezogener Daten, Bussgelder bis 4% des Jahresumsatzes
EU AI Act	Ab 2026/27	Hersteller & Betreiber	KI-Konformitätsanforderungen für sicherheitsrelevante Maschinenfunktionen
CER-Richtlinie	Ab 2024/25 (nationale Umsetzung läuft)	Betreiber	Physische Resilienz für Betreiber kritischer Infrastrukturen
IEC 62443	Laufend	Hersteller & Betreiber	Technischer Standard für OT/ICS-Sicherheit; Nachweis für NIS-2 und CRA
ISO 27001:2022	Laufend	Alle	ISMS-Standard; Nachweis für NIS-2; Kundenanforderung in der Industrie
ISG / IKT-Minimalstandard / revDSG (CH)	Seit Apr. 2025 (Bussen ab Okt. 2025)	Betreiber kritischer Infrastrukturen (CH)	24h-Meldepflicht bei Cyberangriffen; 106 Massnahmen basierend auf NIST CSF

02 Die neue Compliance-Realität

Produktionsanlagen sind vernetzt. Maschinen kommunizieren mit ERP-Systemen, mit der Cloud und mit anderen Maschinen. Engineering-Workstations sind Teil des Unternehmensnetzwerks. SPS-Systeme, die früher physisch isoliert betrieben wurden, sind heute über OT/IT-Grenzen hinweg erreichbar. Diese Vernetzung schafft Effizienz und gleichzeitig Angriffsfläche.

Die Reaktion des Gesetzgebers war unvermeidlich. Eine Welle neuer Regulierungen verpflichtet Hersteller und Betreiber, Cybersicherheit systematisch in ihre Produkte, Prozesse und Organisationsstrukturen zu integrieren.

Cyberangriffe auf Industrieunternehmen haben in Häufigkeit und Schadenswirkung massiv zugenommen. Laut IEA verdoppelten sich die Cyberangriffe auf Versorgungsunternehmen weltweit zwischen 2020 bis 2022 und verdoppelten sich 2023 erneut. In Deutschland stiegen die KRITIS-Meldungen an das BSI von 452 in den Jahren 2021/22 auf 726 in den Jahren 2023/24. In der Schweiz verzeichnete das BACS im zweiten Halbjahr 2023 eine Verdopplung der Cybervorfallsmeldungen gegenüber dem Vorjahr. Seit Einführung der Meldepflicht für kritische Infrastrukturen im April 2025 werden täglich Angriffe auf Schweizer KRITIS-Betreiber gemeldet (BACS Halbjahresbericht 2025/2).

Supply-Chain-Angriffe zeigen, dass Schwachstellen bei Lieferanten und Komponentenherstellern zu grossen Schäden beim Kunden führen. Laut ENISA Threat Landscape 2025 zählen Supply-Chain-Kompromittierungen zu den Top-Risiken für NIS-2-relevante Sektoren. Angreifer zielen gezielt auf Drittanbieter, weil deren Kompromittierung effektiver ist als der direkte Angriff auf gehärtete Industrieanlagen. Die globalen Kosten solcher Angriffe werden für 2025 auf 60 Milliarden USD geschätzt (Cybersecurity Ventures). Allein beim Kaseya-Vorfall 2021 waren über eine einzige kompromittierte Softwarekomponente zwischen 800 und 1’500 Unternehmen betroffen.

Die EU reagiert mit einem regulatorischen Rahmenwerk, das alle Glieder der Wertschöpfungskette erfasst.

Für den Maschinen- und Anlagenbau gilt:

Die Branche ist sowohl als Hersteller vernetzter Produkte als auch als Betreiber komplexer OT-Infrastrukturen in doppelter Weise von der neuen Regulatorik betroffen. Gleichzeitig steigen die Erwartungen der Industriekunden. ISO 27001-Zertifizierungen und IEC 62443-Nachweise werden zunehmend als Mindestanforderung in Ausschreibungen und Lieferantenqualifizierungen verlangt.

Die gute Nachricht ist, wer die regulatorischen Anforderungen systematisch angeht, baut gleichzeitig echte Widerstandsfähigkeit gegen Cyberangriffe auf und gewinnt Vertrauen bei Kunden und Partnern. Compliance und Sicherheit sind keine Gegensätze, sondern zwei Seiten derselben Medaille.

> **Fazit**
> Cybersicherheit ist keine IT-Frage mehr – sie ist eine unternehmerische Pflicht.
> NIS-2 macht die Geschäftsleitung persönlich haftbar (Art. 21, Art. 32), die EU-Maschinenverordnung erhebt Cybersicherheit zum verbindlichen Sicherheitsziel (Anhang III, Abschnitt 1.1.9 - "Schutz vor Verfälschung") und der Cyber Resilience Act verpflichtet Hersteller zur lebenslangen Sicherheitspflege ihrer Produkte.

03 EU-Maschinenverordnung 2023

Verordnung (EU) 2023/1230 – Ersetzt Maschinenrichtlinie 2006/42/EG
Schweizer Pendant: PrSG (SR 930.11) & MaschV (SR 819.14)

Verbindlich ab	Rechtsform	Betrifft
20. Januar 2027	EU-Verordnung (direkt anwendbar)	Alle Maschinenhersteller

Die EU-Maschinenverordnung ist der tiefgreifendste Wandel im Maschinenrecht seit Jahrzehnten. Sie integriert Cybersicherheit erstmals als verbindliches essentielles Sicherheitsziel, gleichrangig neben mechanischen und elektrischen Anforderungen. Maschinen müssen künftig so konstruiert sein, dass Cyberangriffe die Sicherheitsfunktionen nicht beeinträchtigen können.

Secure by Design ist damit keine Kür mehr, sondern gesetzliche Pflicht. In der Schweiz regelt das Produktesicherheitsgesetz (PrSG, SR 930.11) zusammen mit der Maschinenverordnung (MaschV, SR 819.14) die Maschinensicherheit. Die Schweiz hat sich im Rahmen des MRA (Mutual Recognition Agreement) verpflichtet, die wesentlichen Anforderungen der EU-Maschinenrichtlinie zu übernehmen. Die neue EU-Maschinenverordnung 2023/1230 mit ihren expliziten Cybersicherheitsanforderungen wird voraussichtlich auch in die Schweizer MaschV übernommen. Schweizer Hersteller, die in den EU-Raum exportieren, müssen die EU-MVO ab Januar 2027 direkt einhalten.

Zentrale Anforderungen

- Schutz der Sicherheitsfunktionen gegen unbefugte Verbindungen, Manipulationen und Cyberangriffe
- Keine unsicheren Standardkonfigurationen, keine Default-Passwörter, offene Ports oder unnötige Dienste
- Sichere Aktualisierbarkeit sicherheitsrelevanter Software über den gesamten Lebenszyklus
- Explizite Berücksichtigung von Cybersicherheitsrisiken in der Risikobeurteilung
- Erweiterte Konformitätsbewertung für Hochrisikoprodukte durch notifizierte Stelle

Fazit

Als Schweizer Maschinenhersteller tragen Sie ab Januar 2027 die volle Verantwortung für die Cybersicherheit Ihrer Produkte – sowohl für den EU-Export (EU-MVO) als auch zunehmend für den Schweizer Markt (PrSG/MaschV). Risikobeurteilungen, technische Dokumentation und interne Prozesse müssen jetzt angepasst werden. Das Schweizer MRA-Abkommen wird die Übernahme der Cybersicherheitsanforderungen beschleunigen.

Handlungsempfehlung

Starten Sie jetzt mit einer Cybersicherheits-Gap-Analyse Ihrer Produktlinie. Prüfen Sie die Konformität sowohl mit der EU-MVO 2023/1230 als auch mit dem Schweizer PrSG/MaschV. Integrieren Sie Secure-by-Design-Prinzipien in Ihre Engineering-Prozesse und berücksichtigen Sie die IEC 62443 als harmonisierten Standard.

04 Cyber Resilience Act

Verordnung (EU) 2024/2847 Cybersicherheit für Produkte mit digitalen Elementen

Vollständig ab	Meldepflichten	Betrifft
Dezember 2027	Ab September 2026	Hardware- & Software-Hersteller

Der Cyber Resilience Act schliesst eine kritische Lücke. Erstmals werden Hersteller gesetzlich verpflichtet, Schwachstellen in ihren vernetzten Produkten aktiv zu beheben, kostenlose Sicherheitsupdates bereitzustellen und bei ausgenutzten Schwachstellen innerhalb von 24 Stunden die europäische Cybersicherheitsbehörde ENISA zu informieren. Die Norm gilt für nahezu alle Hardware- und Softwareprodukte, von der SPS bis zum SCADA-System. Für Schweizer Hersteller, die Produkte in den EU-Markt liefern, wird der CRA zur Pflicht. Die Schweiz prüft derzeit die Übernahme über das MRA-Abkommen. Unabhängig davon müssen Schweizer Exporteure die CRA-Anforderungen erfüllen, um CE-Kennzeichnung und EU-Marktzugang zu behalten.

Zentrale Anforderungen

- Inverkehrbringen ohne bekannte, ausnutzbare Schwachstellen (Secure by Default)
- Software Bill of Materials (SBOM), vollständige Transparenz über alle Softwarekomponenten
- Kostenlose Sicherheitsupdates während der erwarteten Produktlebensdauer, mindestens jedoch 5 Jahre
- 24h-Erstmeldung an ENISA bei aktiv ausgenutzten Schwachstellen
- Koordinierte Schwachstellenoffenlegung (CVD-Policy) als Pflichtprozess

Fazit

Für OT-Komponentenhersteller und SPS/SCADA-Anbieter bedeutet der CRA eine fundamentale Erweiterung der Produktverantwortung: von der Erstlieferung hin zur lebenslangen Sicherheitspflege. SBOM und Vulnerability-Disclosure-Prozesse erfordern neue interne Strukturen.

Handlungsempfehlung

Bewerten Sie Ihre Produktpalette nach CRA-Risikostufen und starten Sie den Aufbau eines Schwachstellenmanagement-Prozesses und einer SBOM-Infrastruktur.

05 NIS-2-Richtlinie

Richtlinie (EU) 2022/2555 - Netz- und Informationssicherheit

Umsetzungsfrist	Grössenschwelle	Betrifft
Oktober 2024	Ab 50 Mitarbeitende Oder Umsatz > 10 mio€	Betreiber in 18+ Sektoren

NIS-2 ist die grösste Ausweitung des europäischen Cybersicherheitsrechts seit 2016 und trifft den Maschinenbau unmittelbar. Erstmals sind Unternehmen des verarbeitenden Gewerbes ab 50 Mitarbeitenden direkt adressiert. Die Anforderungen sind deutlich schärfer als die Vorgängerrichtlinie. Besonders brisant ist die explizite persönliche Haftung der Geschäftsleitung bei Verletzung der Aufsichtspflicht.

Die NIS-2-Richtlinie hätte bis Oktober 2024 in nationales Recht umgesetzt werden müssen. Tatsächlich verpassten 23 von 27 EU-Mitgliedstaaten diese Frist. Deutschland setzte NIS-2 im Dezember 2025 um (NIS2UmsuCG, ca. 29’500 betroffene Unternehmen), Österreich folgte mit dem NISG 2026 (Hauptpflichten ab Oktober 2026, ca. 4’000 Einrichtungen). Die Schweiz hat als Nicht-EU-Staat mit dem Informationssicherheitsgesetz (ISG, SR 128.1) und der seit April 2025 geltenden Meldepflicht für KRITIS-Betreiber einen eigenständigen, aber vergleichbaren Regulierungsansatz gewählt. Ergänzt wird dies durch den IKT-Minimalstandard des Bundesamtes für wirtschaftliche Landesversorgung (BWL) und die Cybersicherheitsverordnung (CSV), die zusammen das Schweizer Pendant zu NIS-2 bilden.

Zentrale Anforderungen

- Risikoanalyse, Incident Management und Business Continuity als Mindestanforderungen
- Supply-Chain-Sicherheit: Überprüfung und Bewertung aller sicherheitsrelevanten Lieferanten
- Meldepflicht bei erheblichen Vorfällen:
- 24h Erstmeldung
- 72h Detailbericht
- 30-Tage-Abschluss
- Haftung der Geschäftsleitung bedeutet Genehmigung und Überwachung der Sicherheitsmassnahmen
- Grundlegende Cyberhygiene wie MFA, Patch-Management, Zugangskontrolle, Verschlüsselung

Fazit

Für mittelständische Maschinenbauunternehmen ist NIS-2 die unmittelbarste regulatorische Pflicht. Die Kombination aus technischen Anforderungen, Meldepflichten und persönlicher Managementhaftung erfordert ein strukturiertes, dokumentiertes Sicherheitsprogramm.

Handlungsempfehlung

Prüfen Sie Ihre NIS-2-Einstufung (wesentlich oder wichtig), implementieren Sie die 10 Mindest-massnahmen und etablieren Sie einen Incident-Response-Prozess mit klaren Meldewegen.

Schweizer Perspektive:

ISG und IKT-Minimalstandard

Die Schweiz ist als Nicht-EU-Staat nicht direkt an NIS-2 gebunden, hat aber mit dem Informationssicherheitsgesetz (ISG, SR 128.1), der Cybersicherheitsverordnung (CSV) und dem IKT-Minimalstandard ein eigenständiges, zunehmend verbindliches Regulierungsrahmenwerk aufgebaut. Für Schweizer Maschinen- und Anlagebauer ist dieses Rahmenwerk unmittelbar relevant. Dies sowohl als Betreiber kritischer Infrastrukturen als auch als Zulieferer für KRITIS-Sektoren wie Energie, Wasser, Transport und Lebensmittelproduktion. Das Bundesamt für Cybersicherheit (BACS, ehemals NCSC) koordiniert die Umsetzung und betreibt die zentrale Meldeplattform Cyber Security Hub.

ISG-Meldepflicht (seit April 2025)

Seit dem 1. April 2025 müssen Betreiber kritischer Infrastrukturen Cyberangriffe innerhalb von 24 Stunden nach Entdeckung dem Bundesamt für Cybersicherheit (BACS) melden. Betroffen sind Unternehmen der Energieversorgung, Trinkwasserversorgung, Transportunternehmen, Spitäler, Cloud-Anbieter und Rechenzentren sowie Kantons- und Gemeindeverwaltungen. Seit Oktober 2025 sind Bussen bis CHF 100’000 möglich, wenn einer behördlichen Meldeanordnung nicht Folge geleistet wird.

IKT-Minimalstandard

Der IKT-Minimalstandard wurde vom Bundesamt für wirtschaftliche Landesversorgung (BWL) auf Basis des NIST Cybersecurity Framework (CSF) entwickelt und umfasst rund 130 konkrete Massnahmen, gegliedert in die fünf Kernfunktionen: Identifizieren (ID), Schützen (PR), Erkennen (DE), Reagieren (RS) und Wiederherstellen (RC). Er definiert ein messbares Mindestniveau für die Cybersicherheit und wird sektorspezifisch konkretisiert. Für den Maschinen- und Anlagenbau sind insbesondere die Bereiche Asset Management (ID.AM), Zugangskontrolle (PR.AC), Datensicherheit (PR.DS) und Incident Response (RS.RP) von zentraler Bedeutung. Das BWL stellt ein kostenloses Assessment-Tool (Excel-basiert) zur Verfügung, mit dem Unternehmen ihren Reifegrad messen und Lücken identifizieren können. Der Reifegrad wird auf einer Skala von 0 bis 5 gemessen, wobei Stufe 3 als angemessenes Schutzniveau für die meisten Industrieunternehmen gilt.

Strom	Gas	Wasser / Fernwärme
Verbindlich seit Juli 2024	Verbindlich seit Juli 2025	Empfohlen (noch nicht verbindlich)

Relevanz für den Maschinenbau

- Maschinenbauer, die an Schweizer KRITIS-Betreiber (Energie, Wasser, Transport, Lebensmittelproduktion, Gesundheitswesen) liefern, werden durch Lieferantenanforderungen indirekt an den IKT-Minimalstandard gebunden. Die CSV verschärft diese Anforderungen zusätzlich
- Der IKT-Minimalstandard mappt direkt auf ISO 27001 und NIST CSF 2.0. Unternehmen mit ISO 27001:2022-Zertifizierung erfüllen den Grossteil der Anforderungen bereits. Die rund 130 Massnahmen lassen sich systematisch auf die 93 Controls des ISO 27001 Annex A abbilden
- Die ISG-Meldepflicht folgt dem gleichen Muster wie NIS-2 (24h-Erstmeldung an BACS via Cyber Security Hub, 72h-Detailmeldung). Ein gemeinsamer Incident-Response-Prozess deckt sowohl die Schweizer ISG-Pflicht als auch die EU NIS-2-Anforderungen ab
- Eine politische Initiative zur Ausweitung des IKT-Minimalstandards auf weitere Sektoren ist im Parlament hängig. Die Verbindlichkeit wird voraussichtlich zunehmen. Zudem wird erwartet, dass die Cybersicherheitsverordnung (CSV) in einer nächsten Revision erweiterte Melde- und Sorgfaltspflichten für weitere Branchen einführt

Fazit

Für Schweizer Maschinenbauunternehmen bildet die Kombination aus ISG-Meldepflicht, Cybersicherheitsverordnung (CSV) und IKT-Minimalstandard das nationale Äquivalent zu NIS-2. Wer ein ISMS nach ISO 27001 betreibt und die IEC 62443-Anforderungen für OT-Sicherheit umsetzt, erfüllt gleichzeitig den IKT-Minimalstandard weitgehend.

Das Mapping ist klar:
ISO 27001 Annex A deckt die Identify- und Protect-Funktionen ab, IEC 62443 ergänzt die OT-spezifischen Detect- und Respond-Anforderungen. Der integrierte Ansatz zahlt sich hier besonders aus und schafft gleichzeitig die Basis für EU-Konformität.

Handlungsempfehlung

Prüfen Sie, ob Ihre Kunden unter die ISG-Meldepflicht fallen und ob der IKT-Minimalstandard für Ihren Sektor bereits verbindlich ist. Nutzen Sie das kostenlose BACS-Assessment-Tool, um Ihren Reifegrad zu messen. Registrieren Sie sich auf dem Cyber Security Hub des BACS für den Informationsaustausch. Planen Sie die Implementierung der rund 130 Massnahmen des IKT-Minimalstandards entlang der fünf NIST-CSF-Kernfunktionen und priorisieren Sie die OT-relevanten Massnahmen für Ihre Maschinensteuerungen und Netzwerke.

06 DSGVO / GDPR

Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung
Schweizer Pendant: revDSG (SR 235.1)

In Kraft	Schweiz	Betrifft
Seit Mai 2018	revDSG seit Sep. 2023	Alle Organisationen

Die DSGVO ist nicht neu, bleibt aber hochrelevant und wird in Industrieumgebungen zunehmend komplex. Für Schweizer Unternehmen gilt seit dem 1. September 2023 das revidierte Datenschutzgesetz (revDSG, SR 235.1), das sich stark an der DSGVO orientiert und den Datenschutz in der Schweiz auf ein vergleichbares Niveau hebt. Vernetzte Maschinen mit Condition Monitoring, Smart-Factory-Anwendungen und Mitarbeiterüberwachungssysteme generieren kontinuierlich personenbezogene Daten. Das revDSG bringt neue Pflichten wie die Datenschutz Folgenabschätzung, erweiterte Informationspflichten und Meldepflichten bei Verletzungen der Datensicherheit (Meldung an EDÖB innert 72 Stunden). Wer EU-Kunden bedient, unterliegt zusätzlich der DSGVO.

Zentrale Anforderungen

- Rechtsgrundlage, Zweckbindung und Datenminimierung für jede Verarbeitung personenbezogener Daten
- Technische und organisatorische Massnahmen (TOMs): Verschlüsselung, Zugangskontrolle, Pseudonymisierung
- Datenpannen-Meldung an Aufsichtsbehörde innerhalb von 72 Stunden nach Bekanntwerden
- Datenschutz-Folgenabschätzung (DSFA) bei Verarbeitungen mit hohem Risiko
- Auftragsverarbeitungsverträge (AVV) mit allen Dienstleistern und Cloud-Anbietern

Fazit

Für Schweizer Maschinenbauunternehmen erzeugen vernetzte Produktionssysteme, Mitarbeiterdaten aus MDE-Systemen und KI-Anwendungen sowohl revDSG- als auch DSGVO-Pflichten. Das Verarbeitungsverzeichnis ist unter dem revDSG ebenso Pflicht wie unter der DSGVO. Regelmässige Datenschutzschulungen, klare Prozesse bei Datenpannen (Meldung an EDÖB und ggf. EU-Aufsichtsbehörde) und die Ernennung eines Datenschutzbeauftragter (DSB) sind unverzichtbar. Beim revDSG gibt es keine Pflicht zur Ernennung eines DSB (anders als DSGVO!). Schweizer Unternehmen profitieren davon, dass ein einheitliches Datenschutz-Management-System beide Regulierungen gleichzeitig abdecken kann.

Handlungsempfehlung

Führen Sie ein aktuelles Verarbeitungsverzeichnis gemäss revDSG Art. 12 und DSGVO Art. 30. Überprüfen Sie Ihre TOMs regelmässig (revDSG Art. 8, DSGVO Art. 32) und stellen Sie sicher, dass alle Auftragsverarbeiter durch Auftragsverarbeitungsverträge (AVV) vertraglich eingebunden sind, die alle Anforderungen nach revDSG Art. 9, DSGVO Art. 28 erfüllen. Prüfen Sie, ob Ihre Datenübermittlungen ins Ausland den Anforderungen des revDSG (Art. 16-17) entsprechen.

07 EU AI Act

Verordnung (EU) 2024/1689 – KI-Verordnung

Schweizer Kontext: Keine eigene KI-Regulierung, aber Relevanz über EU-Export

Vollständig ab	Hochrisiko-KI	Betrifft
August 2026/27	Maschinenprodukte 2027	Hersteller und Betreiber

Der EU AI Act ist das erste umfassende KI-Gesetz der Welt und trifft den Maschinenbau an einem neuralgischen Punkt. KI-Systeme, die als Sicherheitskomponenten von Maschinen fungieren, etwa in der Qualitätssicherung, der vorausschauenden Wartung oder bei kollaborativen Robotern, gelten per Definition als Hochrisiko-KI. Damit unterliegen sie strengen Anforderungen an Dokumentation, Transparenz, Datenqualität und menschliche Überwachung.

Zentrale Anforderungen

- Inventarisierung und Risikoklassifizierung aller eingesetzten KI-Systeme
- Risikomanagement über den gesamten KI-Lebenszyklus mit kontinuierlicher Überwachung
- Vollständige technische Dokumentation vor dem Inverkehrbringen
- Automatisches Logging und Rückverfolgbarkeit von KI-Entscheidungen (Audit Trail)
- Robustheit gegen Cyberangriffe und Adversarial Attacks (Art. 15)

Fazit

Maschinenhersteller und -integratoren, die KI für sicherheitsrelevante Funktionen einsetzen, müssen Konformitätsnachweise erbringen, auch wenn die KI-Technologie von Drittanbietern stammt. Die Verbindung von AI Act und EU-Maschinenverordnung macht eine frühzeitige Planung unerlässlich.

Handlungsempfehlung

Erstellen Sie ein KI-Inventar, klassifizieren Sie alle Systeme nach Risikoklasse und prüfen Sie, welche Systeme Hochrisiko-Anforderungen unterliegen.

08 CER-Richtlinie

Richtlinie (EU) 2022/2557 - Resilienz kritischer Einrichtungen

Umsetzungsfrist	Fokus	Schwesterrichtlinie
Oktober 2024	Physische Resilienz	NIS-2 (Cyber)

Die CER-Richtlinie gilt für Betreiber kritischer Einrichtungen in 11 Sektoren (u.a. Energie, Verkehr, Wasser, Gesundheit, Lebensmittel). Sie ergänzt NIS-2 um die physische Dimension der Resilienz. Während NIS-2 die Cyberresilienz adressiert, schreibt CER den Schutz kritischer Einrichtungen vor physischen Bedrohungen vor, wie Naturkatastrophen, Terrorismus, Sabotage und hybride Angriffe, die physische und digitale Vektoren kombinieren.

Relevanz für Maschinenhersteller

- Direkt: Wenn der Hersteller selbst als kritische Einrichtung eingestuft wird (selten)
- Indirekt: Wenn Kunden (z.B. Kraftwerke, Wasserwerke) kritische Einrichtungen sind und vertragliche CER-Anforderungen stellen (Lieferkettensicherheit, Produktresilienz)

Zentrale Anforderungen

- Umfassende Risikoanalyse wie physische, Cyber- und Hybridbedrohungen berücksichtigen
- Präventionsmassnahmen wie Zugangskontrolle, Perimeterschutz, Sicherheitsüberprüfung von Personal
- Formalisierter Resilienzplan mit Massnahmen, Verantwortlichkeiten und Testzyklen
- Business Continuity Management (BCM) und Wiederherstellungsprozesse
- Meldepflicht erheblicher Störungen an die zuständige nationale Behörde ohne unnötige Verzögerung (Art. 11). Anders als NIS-2 gibt es keine feste 24/72-Stunden-Frist, aber zeitnahe Meldung ist erforderlich.

Fazit

Für Hersteller von Maschinen für Energieanlagen, Wasserwerke, Lebensmittelproduktion oder Verkehrsinfrastruktur ist eine Prüfung, ob Ihre Kunden als kritische Einrichtung eingestuft werden, wichtig. Erwarten Sie vertragliche Anforderungen zur Lieferkettensicherheit, Produktresilienz und Unterstützung bei der Resilienzplanung Ihrer Kunden.

Schweiz-spezifischer Hinweis:
Die CER-Richtlinie gilt nicht direkt in der Schweiz. Schweizer Unternehmen sind betroffen, wenn sie EU-Niederlassungen haben oder EU-kritische Einrichtungen beliefern. In der Schweiz gilt die Nationale Strategie zum Schutz kritischer Infrastrukturen (SKI), die ähnliche, aber weniger formalisierte Anforderungen stellt.

Handlungsempfehlung

- Prüfen Sie, ob Ihre Kunden als kritische Einrichtungen nach CER eingestuft werden
- Analysieren Sie vertragliche CER-Anforderungen (Lieferkettensicherheit, Produktresilienz)
- Integrieren Sie physische Resilienz in Ihr ISMS (ISO 27001) und implementieren Sie ISO 22301 (BCM)
- Führen Sie hybride Risikoanalysen durch, die Cyber- und physische Bedrohungen kombinieren
- Etablieren Sie koordinierte Prozesse mit NIS-2 (gemeinsames Incident Management, Meldewesen)

09 IEC 62443

Internationale Normenfamilie - Industrial Cybersecurity für IACS

Status	Zertifizierung	Anerkennung
Freiwillig (starke Präsumption)	Durch akkreditierte Stellen	NIS-2, EU-MVO, CRA

IEC 62443 ist der technische Goldstandard für OT-Cybersicherheit in industriellen Automatisierungs- und Steuerungssystemen. Die Normenfamilie ist zwar nicht direkt gesetzlich verbindlich, aber sie ist de facto die anerkannte Methode für den Nachweis der Konformität mit NIS-2, EU-Maschinenverordnung und dem Cyber Resilience Act. Für Maschinenbauunternehmen, die im industriellen B2B-Umfeld tätig sind, wird eine IEC 62443-Zertifizierung zunehmend zur Kundenanforderung.

Die IEC 62443 definiert vier Security Levels (SL 1–4), die Schutzanforderungen je nach Angreifertyp abstufen und setzt auf Netzwerksegmentierung durch Zones & Conduits.

Sieben Foundational Requirements bilden das Fundament: von Identifikation und Zugriffskontrolle über Systemintegrität und Datenvertraulichkeit bis hin zu Ereignisreaktion und Ressourcenverfügbarkeit.

Die Normenreihe gliedert sich in System-Sicherheitsanforderungen (3-3), einen Secure Development Lifecycle für Hersteller (4-1), technische Anforderungen auf Komponentenebene (4-2) und ein Cyber Security Management System für Anlagenbetreiber (2-1).

Fazit

IEC 62443 bietet den methodischen Rahmen, um OT-Sicherheitsanforderungen strukturiert umzusetzen und nachzuweisen. Die Norm wird von Regulierungsbehörden und Kunden gleichermassen als Referenz herangezogen.
Die EU-Maschinenverordnung verweist auf IEC 62443 als harmonisierten Standard für den Nachweis der Cybersicherheit (Anhang III, 1.1.9), der CRA akzeptiert IEC 62443-4-1 als Konformitätsnachweis für den Secure Development Lifecycle und NIS-2 nennt IEC 62443 explizit als geeignete Massnahme für die OT-Sicherheit.
Für Schweizer Unternehmen deckt eine IEC 62443-Zertifizierung gleichzeitig wesentliche Anforderungen des IKT-Minimalstandards ab, insbesondere in den Bereichen Schützen (PR) und Erkennen (DE). In Kombination mit ISO 27001 entsteht ein durchgängiges IT/OT-Sicherheitsmanagement. Dies ist der effizienteste Weg, um alle regulatorischen Anforderungen gleichzeitig zu adressieren.

Handlungsempfehlung

Bewerten Sie Ihre OT-Systeme nach IEC 62443-Zonen und Security Levels und definieren Sie das erforderliche Security Level (SL-T) für jede Zone. Priorisieren Sie die Zertifizierung nach IEC 62443-4-1 (Secure Development Lifecycle) für Ihre Produktentwicklung. Dies wird zunehmend zur Voraussetzung in Kundenausschreibungen, insbesondere im Energie-, Wasser- und Transportsektor. Nutzen Sie IEC 62443-3-3 für die Systemebene und IEC 62443-4-2 für die Komponentenebene als Leitfaden. Für Schweizer Unternehmen empfiehlt sich, die Ergebnisse der Zonenbewertung direkt mit dem IKT-Minimalstandard-Assessment zu verknüpfen, um Doppelarbeit zu vermeiden.

10 ISO/IEC 27001:2022

Internationaler Standard - Informationssicherheitsmanagement (ISMS)

Revision	Übergangsfrist	Zertifizierbar
Oktober 2022	Abgelaufen (Okt. 2025)	Ja, alle Branchen

ISO 27001 ist die methodische Basis für ein unternehmensweites Informationssicherheits-managementsystem (ISMS). Die Version 2022 bringt 11 neue Kontrollen, die moderne Bedrohungen wie Cloud-Sicherheit, Bedrohungsintelligenz und Data Leakage Prevention adressieren. Eine ISO 27001-Zertifizierung ist heute in vielen Industriebranchen eine faktische Marktzugangsvoraus-setzung und deckt einen wesentlichen Teil der NIS-2-Anforderungen methodisch ab.

Zentrale Anforderungen

- Risikobasierter Ansatz

  ISMS-Scope festlegen, Risikobeurteilung durchführen (Identifikation, Analyse, Bewertung)
  Risikobehandlungsplan erstellen und Statement of Applicability (SoA) dokumentieren

- 93 Controls in 4 Themengruppen (Annex A)

  Organisatorisch (37): Policies, Risikomanagement, Lieferanten, Incident Response
  Personal (8): Screening, Awareness, Vertraulichkeit
  Physisch (14): Zutrittskontrolle, Perimeterschutz, Gerätesicherheit
  Technologisch (34): Zugriffskontrolle, Verschlüsselung, Logging, Backup

- 11 neue Controls in Version 2022

  Threat Intelligence (5.7), Cloud Security (5.23), ICT Readiness for BCM (5.30)
  Data Leakage Prevention (8.12), Secure Coding (8.28), Configuration Management (8.9)
  Data Masking (8.11), Web Filtering (8.23), Monitoring Activities (8.16)

- PDCA-Zyklus (Klauseln 4-10)

  Plan: Kontext, Führung, Risikoplanung, Sicherheitsziele
  Do: Ressourcen, Kompetenz, Awareness, Betrieb
  Check: Monitoring, interne Audits, Managementbewertung
  Act: Nichtkonformitäten, Korrekturmaßnahmen, kontinuierliche Verbesserung

- Zertifizierung

  Stage 1/2 Audit durch akkreditierte Stelle
  Zertifikat gültig 3 Jahre, jährliche Überwachungsaudits
  Übergangsfrist 2013 → 2022: Abgelaufen (31. Oktober 2025)

Fazit

ISO 27001 ist die effektivste Einzelinvestition in Compliance-Reichweite. Eine Zertifizierung stärkt das Kundenvertrauen, erleichtert den NIS-2-Nachweis erheblich und deckt gleichzeitig die DSGVO/revDSG-Anforderungen an technische und organisatorische Massnahmen (TOMs) systematisch ab.
Für Schweizer Unternehmen bildet ISO 27001 zudem die methodische Brücke zum IKT-Minimalstandard. Die 93 Controls des Annex A lassen sich direkt auf die 106 Massnahmen des IKT-Minimalstandards abbilden, insbesondere in den Kernfunktionen Identifizieren (ID) und Schützen (PR).
In Kombination mit IEC 62443 entsteht ein durchgängiges IT/OT-Sicherheitsmanagement, das sowohl die Unternehmens-IT als auch die Produktions- und Maschinensteuerungsebene abdeckt.
Bestehende 2013-Zertifikate mussten bis Oktober 2025 auf Version 2022 umgestellt sein. Wer dies versäumt hat, muss eine Neuzertifizierung durchlaufen.

Handlungsempfehlung

Starten Sie mit einer Gap-Analyse gegen ISO 27001:2022, unter besonderer Berücksichtigung der 11 neuen Controls (Threat Intelligence, Cloud Security, Data Leakage Prevention, Secure Coding).
Der ISMS-Aufbau dauert typischerweise 6 bis 9 Monate. Ein Zertifizierungsaudit ist innerhalb von 12 bis 18 Monaten realistisch.
Definieren Sie den ISMS-Scope so, dass er sowohl IT- als auch OT-Systeme einschliesst. Dies erleichtert die spätere IEC 62443-Integration erheblich.
Nutzen Sie parallel das BACS-Assessment-Tool, um den IKT-Minimalstandard-Reifegrad zu messen und die ISO 27001-Implementierung gezielt auf die noch offenen Punkte auszurichten.
Wählen Sie eine Zertifizierungsstelle, die sowohl ISO 27001 als auch IEC 62443 prüfen kann, um Audit-Synergien zu nutzen.

11 Synergien und Überschneidungen

Die acht Regulierungen adressieren unterschiedliche Perspektiven, Produktsicherheit, Betreiberpflichten, Datenschutz, KI-Governance und physische Resilienz. Sie wirken aber nicht isoliert voneinander. Viele Anforderungen überschneiden sich inhaltlich, und eine einzelne Massnahme kann mehrere regulatorische Pflichten gleichzeitig erfüllen. Wer diese Synergien gezielt nutzt, reduziert den Implementierungsaufwand erheblich und baut gleichzeitig ein robustes, durchgängiges Sicherheitsmanagement auf.

Synergie-Matrix: Welche Massnahme erfüllt welche Regulierung?

Die folgende Matrix zeigt, welche konkreten Sicherheitsmassnahmen Anforderungen aus mehreren Regulierungen gleichzeitig erfüllen. Je mehr Treffer eine Massnahme erzielt, desto höher ist ihr Effizienzpotenzial für Ihre Compliance-Strategie.

Massnahme	MVO	CRA	NIS-2	DSGVO	AI Act	CER	IEC 62443	ISO 27001	IKT Min.	Treffer
Risikomanagement / Risikobeurteilung	✓	✓	✓	✓	✓	✓	✓	✓	✓	9/9
Incident Response & Meldeprozesse	–	✓	✓	✓	–	✓	✓	✓	✓	7/9
Secure Development Lifecycle (SDL)	✓	✓	–	–	✓	–	✓	–	–	4/9
Supply-Chain-Sicherheit / Lieferantenbew.	–	✓	✓	✓	–	–	✓	✓	–	5/9
Schwachstellenmanagement & Patching	✓	✓	✓	–	–	–	✓	✓	✓	6/9
Netzwerksegmentierung (Zones & Conduits)	–	–	✓	–	–	✓	✓	✓	✓	5/9
Zugangskontrolle & Authentifizierung	✓	✓	✓	✓	–	✓	✓	✓	✓	8/9
Logging, Monitoring & Audit Trail	–	✓	✓	✓	✓	–	✓	✓	✓	7/9
Business Continuity Management (BCM)	–	–	✓	–	–	✓	✓	✓	✓	5/9
Technische Dokumentation & Nachweise	✓	✓	–	✓	✓	–	✓	✓	✓	7/9
Schulungen & Awareness	–	–	✓	✓	–	–	–	✓	✓	4/9
SBOM & Softwaretransparenz	–	✓	–	–	✓	–	✓	–	–	3/9
Verschlüsselung & Datenschutz	–	✓	✓	✓	–	–	✓	✓	✓	6/9
Physischer Schutz & Perimetersicherheit	–	–	–	–	–	✓	✓	✓	–	3/9

✓ = Regulierung stellt explizite Anforderung an diese Massnahme

Lesebeispiel: Risikomanagement wird von allen 9 Rahmenwerken gefordert (9/9 Treffer)

Die wichtigsten Synergie-Paare

Bestimmte Regulierungen ergänzen sich besonders gut. Wer diese Paare gemeinsam implementiert, vermeidet doppelte Assessments, konsolidiert Prozesse und spart Ressourcen:

Synergie-Paar	Gemeinsamer Nutzen
ISO 27001 + IEC 62443	Das ISMS nach ISO 27001 liefert das Managementsystem, IEC 62443 die OT-spezifischen technischen Kontrollen. Zusammen ergeben sie ein durchgängiges IT/OT-Sicherheitsmanagement und decken den Grossteil der NIS-2-Anforderungen methodisch ab.
NIS-2 + CER-Richtlinie	NIS-2 adressiert die Cyber-Resilienz, CER die physische Resilienz. Beide fordern Risikoanalysen, Meldepflichten und BCM. Ein koordinierter Ansatz vermeidet doppelte Assessments und nutzt gemeinsame Governance-Strukturen.
EU-MVO + Cyber Resilience Act	Beide fordern Secure by Design für vernetzte Produkte. Die EU-MVO fokussiert auf Sicherheitsfunktionen, der CRA auf Schwachstellenmanagement und SBOM. Ein gemeinsamer SDL-Prozess erfüllt beide Anforderungen.
CRA + IEC 62443-4-1	IEC 62443-4-1 definiert den Secure Development Lifecycle für OT-Komponenten. Wer nach IEC 62443-4-1 zertifiziert ist, erfüllt wesentliche CRA-Anforderungen an Produktsicherheit automatisch (Vermutungswirkung).
DSGVO + NIS-2	Beide fordern technische und organisatorische Massnahmen, Incident-Meldeprozesse und Risikobewertungen. TOMs, die für die DSGVO implementiert wurden, decken viele NIS-2-Anforderungen ab. Die Meldeprozesse können konsolidiert werden.
EU AI Act + EU-MVO	KI-Systeme als Sicherheitskomponenten von Maschinen unterliegen beiden Regulierungen. Eine integrierte Konformitätsbewertung vermeidet Doppelarbeit bei Risikoanalyse, Dokumentation und Zertifizierung.
ISG/IKT-Minimalstandard + ISO 27001	Die 93 Controls des ISO 27001 Annex A decken den Grossteil der 106 Massnahmen des IKT-Minimalstandards ab, insbesondere in den Kernfunktionen Identifizieren und Schützen. Eine ISO 27001-Zertifizierung bildet damit die effizienteste Grundlage für die IKT-Minimalstandard-Konformität. Der ISG-Meldeprozess (24h an BACS) lässt sich nahtlos in das ISO 27001 Incident-Management (A.5.24–A.5.28) integrieren.
revDSG + DSGVO	Das revDSG orientiert sich stark an der DSGVO. Ein einheitliches Datenschutz-Management-System deckt beide Regulierungen gleichzeitig ab. Verarbeitungsverzeichnis, DSFA-Prozess, Meldepflichten (72h an EDÖB bzw. EU-Aufsichtsbehörde) und TOMs können konsolidiert geführt werden.

Effizienzgewinn durch integrierten Ansatz

Unsere Erfahrung zeigt
Unternehmen, die Compliance-Anforderungen isoliert angehen, investieren bis zu 40% mehr Ressourcen als nötig. Ein integrierter Ansatz aufgebaut auf ISO 27001 als methodische Basis, ergänzt um IEC 62443 für OT-Sicherheit, adressiert den Grossteil aller Regulierungen und des IKT-Minimalstandards mit einem gemeinsamen Massnahmenset.

Drei Massnahmen mit der höchsten Synergie-Wirkung

- Risikomanagement (9/9)
- Zugangskontrolle (8/9)
- Incident Response (7/9)

Ausblick - Digital Product Passport (DPP)

Der Digital Product Passport (DPP) ist Teil der Ecodesign for Sustainable Products Regulation (ESPR), die im Juli 2024 in Kraft getreten ist. Ab 2027 soll jedes in der EU verkaufte Produkt schrittweise eine digitale Identität erhalten, die Informationen zu Zusammensetzung, Umweltfussabdruck und Konformitätsstatus enthält. Das zentrale EU-DPP-Register wird ab Mitte 2026 operativ. Erste rechtliche Pflichten gelten ab Februar 2027 für Batterien, danach folgen weitere Produktkategorien bis 2030.

Der DPP ist primär eine Nachhaltigkeits- und Transparenzregulierung und keine Cybersicherheitsvorschrift im engeren Sinne. Für den Maschinenbau ergeben sich dennoch wichtige Berührungspunkte:

- Die EU-Maschinenverordnung fordert ab 2027 die digitale Bereitstellung von Dokumentation. Dies bedeutet ein natürlicher Brückenschlag zum DPP.
- SBOM-Anforderungen aus dem CRA und Produkttransparenz aus dem DPP ergänzen sich zu einem durchgängigen digitalen Produktdossier
- DPP-Plattformen müssen selbst Cybersicherheitsanforderungen erfüllen. Datenintegrität, Zugriffsschutz und Manipulationssicherheit der Produktdaten werden zur Pflicht.
- Supply-Chain-Transparenz aus NIS-2 und Lieferantendaten aus dem DPP können in gemeinsamen Systemen konsolidiert werden.

Fazit
Der DPP ist für Maschinenbauer kein unmittelbarer Compliance-Treiber, wird aber ab 2027 zunehmend relevant. Unternehmen, die bereits digitale Dokumentation nach EU-MVO und SBOM-Prozesse nach CRA aufbauen, schaffen gleichzeitig die Grundlage für eine spätere DPP-Konformität.
Eine frühzeitige Berücksichtigung in der IT-Architektur vermeidet spätere Nachrüstkosten.

Empfohlene Implementierungsreihenfolge

Basierend auf der Synergie-Analyse empfehlen wir eine vierstufige Vorgehensweise:

- Erstens

  Den Aufbau eines ISMS nach ISO 27001:2022 als methodische Grundlage. Dieses adressiert bereits die meisten organisatorischen Anforderungen aller Regulierungen. Parallel dazu den IKT-Minimalstandard-Reifegrad mit dem BACS-Assessment-Tool messen und die ISO 27001-Implementierung gezielt auf offene Punkte ausrichten.

- Zweitens

  Die Erweiterung um IEC 62443 für OT-spezifische Kontrollen und den Secure Development Lifecycle. Damit sind die technischen Anforderungen von EU-Maschinenverordnung, CRA und NIS-2 weitgehend abgedeckt.

- Drittens

  Die Integration von DSGVO/revDSG-TOMs und AI-Act-Konformität in das bestehende Managementsystem. Für Schweizer Unternehmen bedeutet dies: ein einheitliches Datenschutz-Management, das sowohl revDSG als auch DSGVO abdeckt.

- Viertens

  Die Prüfung der CER-Anforderungen für physische Resilienz und die Einrichtung des ISG-Meldeprozesses (24h-Erstmeldung an BACS), sofern Ihr Unternehmen oder Ihre Kunden als kritische Einrichtung eingestuft sind.

Ihr Weg zur Compliance mit SecureComply

SecureComply GmbH ist ein auf die Fertigungsindustrie spezialisiertes Cybersicherheits-Beratungsunternehmen mit Sitz in der Schweiz. Unser Ansatz verbindet IT- und OT-Sicherheit in einem durchgängigen, vierstufigen Programm, von der initialen Analyse bis zur erfolgreichen Zertifizierung.

Wir sprechen die Sprache der Industrie. Keine generischen Beratungskonzepte, sondern branchenerprobte Methoden, zertifizierte Experten und messbarer Sicherheitsfortschritt für Unternehmen ab 50 Mitarbeitenden.

Unser Team vereint langjährige Erfahrung aus IT-Sicherheit, Operational Technology und industrieller Automatisierung. Wir verstehen die Besonderheiten von Produktionsumgebungen: Verfügbarkeit geht vor, Legacy-Systeme sind Realität, und der Engineering-Prozess muss weiterlaufen, auch während der Sicherheitsimplementierung.

ISO 27001	**IEC 62443**	**NIS-2 & EU-MVO**
Wir führen Sie sicher zur Zertifizierung	OT-Sicherheit nach internationalem Standard	Regulatorische Compliance nachweisbar

SecureComply
Secure by Design. Compliant by Default.

Jetzt Beratungsgespräch vereinbaren

Wir analysieren Ihre aktuelle Compliance-Lage und zeigen Ihnen, welche Regulierungen für Sie relevant sind und wie Sie diese effizient erfüllen.

info@securecomply.ch - www.securecomply.ch