Checkliste: Security als Managementthema (IT/OT)

1. Verantwortung & Führung

- ☐ Security ist als **Managementverantwortung** klar benannt
- ☐ Zuständigkeiten für IT, OT und Security sind eindeutig geregelt
- ☐ Führungskräfte leben Security sichtbar vor
- ☐ Security ist Teil von Management- und Strategieentscheidungen

2. Strategie & Ziele

- ☐ Es existiert eine **IT/OT-Security-Strategie**
- ☐ Security-Ziele sind mit den **Geschäftszielen** abgestimmt
- ☐ Kritische Geschäfts- und Produktionsprozesse sind identifiziert
- ☐ Risikotoleranz ist definiert und dokumentiert

3. Risiko- & Entscheidungsmanagement

- ☐ Cyber-Risiken für IT *und* OT sind bekannt und bewertet
- ☐ Auswirkungen auf **Produktion, Safety und Verfügbarkeit** sind berücksichtigt
- ☐ Restrisiken werden bewusst akzeptiert und dokumentiert
- ☐ Management trifft Entscheidungen auf Basis verständlicher Risiko-Darstellungen

4. Organisation & Governance

- ☐ Klare Rollen, Prozesse und Eskalationswege existieren
- ☐ IT und OT arbeiten strukturiert zusammen (keine Silos)
- ☐ Relevante Richtlinien und Standards sind festgelegt
- ☐ Externe Dienstleister sind klar gesteuert und eingebunden

5. Ressourcen & Budget

- ☐ Ausreichendes Budget für IT/OT-Security ist eingeplant
- ☐ Qualifiziertes Personal steht zur Verfügung
- ☐ Zeit für Security-Maßnahmen ist realistisch berücksichtigt
- ☐ Security wird als **Daueraufgabe**, nicht als Projekt, verstanden

6. Schulung & Sicherheitskultur

☐ Zielgruppengerechte Schulungen existieren
☐ OT-Personal ist aktiv eingebunden
☐ Offene Melde- und Fehlerkultur wird gefördert
☐ Führungskräfte nehmen an Security-Maßnahmen teil

7. Incident & Krisenmanagement

☐ Es gibt Incident-Response-Pläne für IT und OT
☐ Rollen im Krisenfall sind klar definiert
☐ Krisen- und Notfallübungen werden durchgeführt
☐ Kommunikationswege intern und extern sind geklärt

8. Externe Experten & Kontrolle

☐ Externe Experten werden gezielt eingesetzt
☐ Empfehlungen sind verständlich und umsetzbar
☐ Unabhängige Reviews und Bewertungen finden statt
☐ Wissen wird intern gesichert und aufgebaut

9. Compliance & Regulierung

☐ Relevante gesetzliche Anforderungen sind bekannt (z. B. NIS2)
☐ Verantwortlichkeiten für Compliance sind klar
☐ Nachweise und Dokumentationen sind vorhanden
☐ Management kennt Haftungs- und Reputationsrisiken

10. Überprüfung & Weiterentwicklung

☐ Regelmäßige Reviews der Security-Lage finden statt
☐ Kennzahlen und Reifegrad werden beobachtet
☐ Lessons Learned aus Vorfällen werden umgesetzt
☐ Security-Strategie wird regelmäßig angepasst