Checkliste: Wirksamkeitsprüfung von Policies (inkl. PDCA-Ansatz)

Ein Informationssicherheits-Managementsystem (ISMS) ist nur wirksam, wenn Policies nicht nur dokumentiert, sondern auch im Alltag verstanden, umgesetzt und überprüft werden. Die folgende Checkliste unterstützt Sie bei der Bewertung der Wirksamkeit. Sie orientiert sich am PDCA-Zyklus (Plan–Do–Check–Act), der als Grundlage für kontinuierliche Verbesserung dient.

Was bedeutet PDCA?
Der PDCA-Zyklus (Plan – Do – Check – Act) ist ein bewährtes Modell zur kontinuierlichen Verbesserung:

- Plan: Maßnahmen planen (z. B. Erstellung oder Aktualisierung einer Policy)
- Do: Maßnahmen umsetzen (z. B. Policy kommunizieren, Schulungen durchführen)
- Check: Umsetzung überprüfen (z. B. interne Audits, Feedback, Tests)
- Act: Korrigieren und verbessern (z. B. Policy anpassen, Prozesse optimieren)

 https://www.linkedin.com/in/jonas-zerer https://zerer-its.de

Checkliste nach PDCA-Struktur

PLAN

- ☐ Ist die Policy dokumentiert und aktuell?
- ☐ Deckt die Policy relevante Risiken und regulatorische Anforderungen ab?
- ☐ Sind Verantwortlichkeiten und Ziele klar definiert?
- ☐ Wurde die Policy in den übergeordneten ISMS-Kontext eingebunden?

DO

- ☐ Wurde die Policy allen relevanten Mitarbeitern zugänglich gemacht?
- ☐ Gab es Kommunikationsmaßnahmen?
- ☐ Wurden Mitarbeiterschulungen durchgeführt?
- ☐ Sind externe Partner/Dienstleister in die Policy einbezogen, sofern notwendig?

CHECK

- ☐ Wird regelmäßig geprüft, ob die Policy angewendet wird?
- ☐ Gibt es Nachweise (z. B. Schulungsprotokolle, Awareness-Tests, Auditberichte)?
- ☐ Wurde die Policy in den letzten 12 Monaten überprüft?
- ☐ Sind Abweichungen oder Lücken dokumentiert worden?

ACT

- ☐ Wurden Korrekturmaßnahmen definiert, wenn Lücken festgestellt wurden?
- ☐ Wurden Policies bei Bedarf angepasst oder erweitert?
- ☐ Gibt es ein etabliertes Verfahren, um Feedback aus der Praxis in Verbesserungen umzusetzen?
- ☐ Werden Lessons Learned aus Audits oder Vorfällen in die nächste Planungsphase übernommen?

Dokumentieren Sie nicht nur die Existenz einer Policy, sondern auch deren gelebte Anwendung. Nutzen Sie den PDCA-Zyklus als festen Bestandteil Ihres ISMS, um kontinuierlich sicherzustellen, dass Richtlinien wirksam, aktuell und alltagstauglich sind.