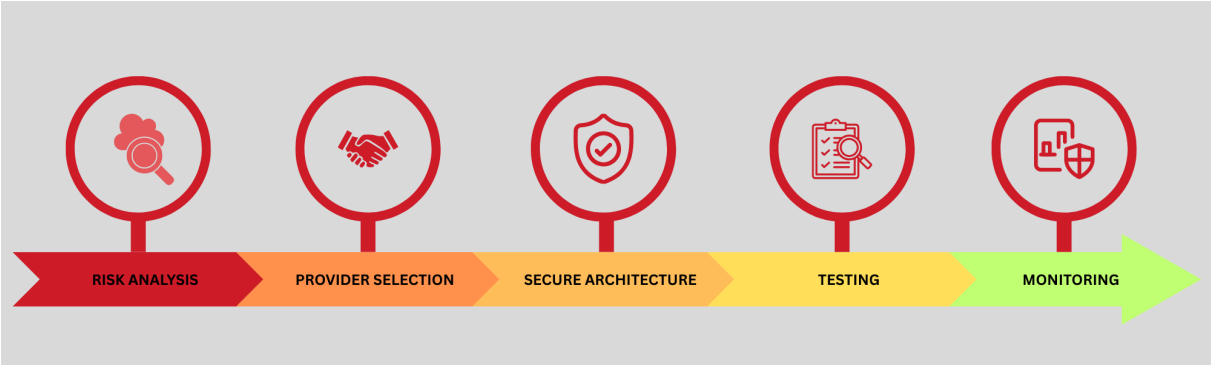

✅ Checkliste: Security by Design bei Einführung eines Cloud-Dienstes

Ziel: Sicherheit bewusst von Beginn an planen, bewerten und verankern – nicht nachträglich.

---

1. Risikoanalyse – Sicherheit als Ausgangspunkt

- Analysieren Sie bereits in der Bedarfsphase: **Welche Bedrohungsszenarien** könnten auftreten?
- Klassifizieren Sie alle geplanten Daten nach **Vertraulichkeit, Integrität und Verfügbarkeit**.
- Legen Sie **Schutzziele** für jede Datenkategorie fest.
- **Security by Design Fokus:** Denken Sie frühzeitig in Schutzklassen und Sicherheitszielen, nicht erst in Reaktionen auf Vorfälle.

---

2. Anbieterprüfung – Sicherheit als Auswahlkriterium

- Bewerten Sie Cloud-Anbieter nicht nur nach Kosten, sondern gezielt nach **Sicherheitsarchitektur** und **Compliance-Niveau**.
- Prüfen Sie, ob der Anbieter:
  - **Ende-zu-Ende-Verschlüsselung** anbietet,
  - **Zero Trust-Prinzipien** unterstützt,
  - **regelmäßige Penetrationstests** durchführt,
  - **Zertifikate wie ISO 27001 oder SOC 2** besitzt.
- **Security by Design Fokus:** Sicherheit muss ein **zwingendes Entscheidungskriterium** bei der Anbieterauswahl sein – nicht ein Bonus.

---

3. Sicherheitsarchitektur entwickeln – Sicherheit verankern

- Entwerfen Sie eine Cloud-Architektur, die:

    - **Minimale Berechtigungen** (Least Privilege) standardmäßig nutzt,
    - **Mandantentrennung** konsequent berücksichtigt,
    - **Monitoring und Auditing** ab Tag 1 integriert.
- Definieren Sie Rollenmodelle so, dass **Fehlkonfigurationen schwer möglich sind**.
- **Security by Design Fokus:** Sicherheitsmechanismen müssen **fest in der Architektur eingebaut sein**, nicht optional nachrüstbar.

---

4. Sicherheitstests und Abnahmekriterien – Sicherheit als Freigabevoraussetzung

- Führen Sie Schwachstellenscans und Sicherheitstests **vor jedem Go-Live** durch.
- Setzen Sie ein **Security Acceptance Test (SAT)** als zwingende Voraussetzung für Produktivschaltungen.
- Dokumentieren Sie getestete Sicherheitsfeatures und Konfigurationen verbindlich.
- **Security by Design Fokus:** Keine Freigabe neuer Dienste ohne nachgewiesene Umsetzung der Sicherheitsanforderungen.

---

5. Betrieb und kontinuierliche Verbesserung – Sicherheit dauerhaft einplanen

- Richten Sie ein **kontinuierliches Schwachstellenmanagement** ein.
- Planen Sie **regelmäßige Audits und Überprüfungen** von Cloud-Konfigurationen.
- Führen Sie **Security-Awareness-Schulungen** für alle Nutzer und Administratoren verpflichtend ein.
- **Security by Design Fokus:** Sicherheit ist ein **lebendiger, fortlaufender Prozess** – nicht ein einmaliges Projekt.