

Drei wichtige Maßnahmen im Rahmen eines ISO 27001/NIS Audits

Robert Jamnik, Head of
Audit Services, CIS



Wiederkehrende Themen



- Nachweise



- Risikomanagement



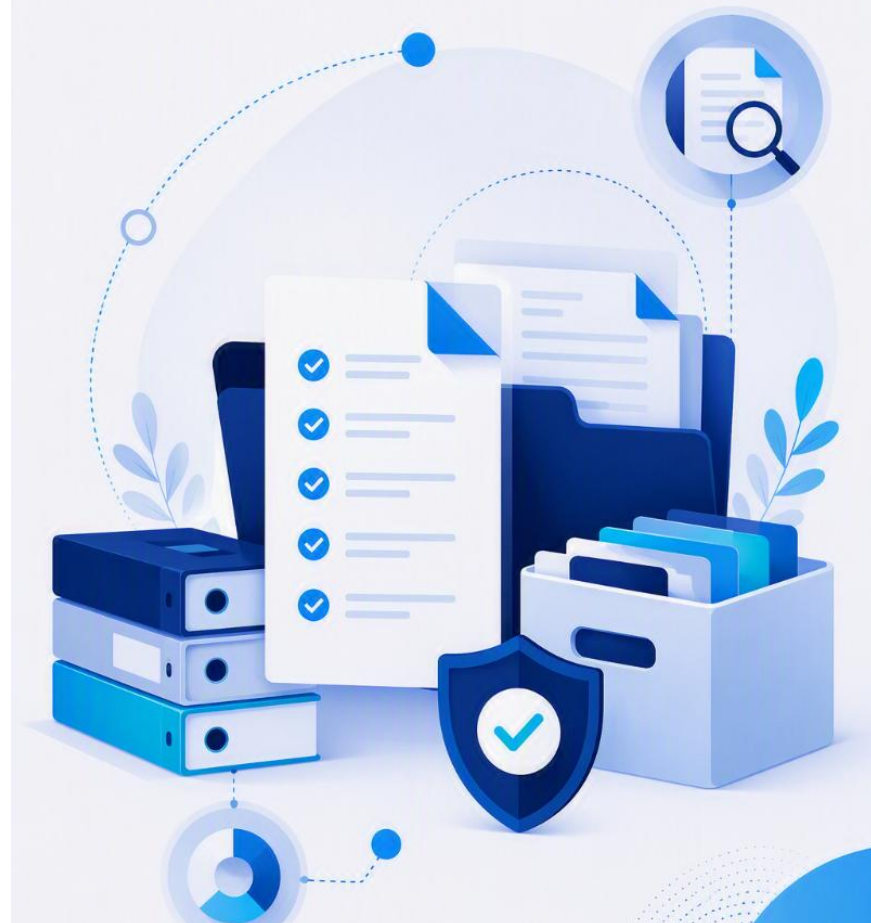
- Sicherheitsarchitektur



Nachweise

Nachweise können nicht gezeigt werden, da sie nicht dokumentiert wurden, oder nicht auffindbar sind (stark abhängig vom Wissen einzelner Personen).

- Freigabe und Review von Richtlinien
- Berechtigungsüberprüfung (nicht durchgeführt/nachweisbar)
- Freigaben, z.B. Risiken, Risikobehandlungspläne
- Wirksamkeitsprüfung von Maßnahmen zur Schließung von Nichtkonformitäten



- Ergebnis der Risikoanalyse ist nicht nachvollziehbar
- wesentliche Entscheidungskriterien sind nicht dokumentiert
- Abweichungen von Vorgaben, die auskunftsmäßig vereinbart wurden sind nicht nachvollziehbar, fehlende Risikoanalyse u. Freigabe
- kein ausreichendes Management von Lieferanten und deren Risiken





- fehlende Härtungsvorgaben und regelm. Überprüfung dieser
- Einsatz von Werkzeugen um Sicherheitskonfiguration regelm. zu prüfen fehlt
- Kryptographie-Vorgaben werden nicht umgesetzt
- Schwachstellenmanagement entspricht nicht den Vorgaben