Integrations-Checkliste: Passkey-Einführung in bestehende Infrastruktur

Checkpunkt	Beschreibung	Status (✔/✖/⚠)	Bemerkungen
1. IAM-System vorhanden	Zentral verwaltetes Identitäts- und Zugriffsmanagement mit FIDO2/WebAuthn-Unterstützung		z. B. Azure AD, Okta, ForgeRock
2. Authentifizierungsserver eingerichtet	Backend zur Registrierung, Verwaltung und Validierung von Passkeys		Eigenständig oder integriert in IAM
3. Webanwendungen kompatibel	Anwendungen unterstützen OIDC, SAML oder lassen sich an IdP anbinden		Frontend/Backend ggf. anpassen
4. Schnittstellen-Standards verfügbar	OpenID Connect, OAuth2, SAML oder AD FS implementiert		Für Integration in Drittsysteme notwendig
5. Geräte- und Authentikatorstrategie definiert	Auswahl zwischen Plattform- und Roaming-Authentifikatoren je nach Nutzergruppe		Siehe Leitfaden (Punkt 3)
6. Recovery-/Fallback-Strategien geplant	Verlust oder Wechsel von Geräten abgedeckt (z. B. Cloud-Sync, Backup-Key)		Wichtig für User Support
7. Pilotumgebung eingerichtet	Getesteter Anwendungsbereich mit klar abgegrenzter Nutzergruppe		z. B. internes Portal oder Testsystem
8. Schulung & Dokumentation vorbereitet	Nutzeraufklärung, Helpdesk-Briefing, Self-Service-FAQ verfügbar		Erfolgsfaktor für Akzeptanz
9. MDM-Integration für Geräteverwaltung	Verwaltung von Sicherheitsrichtlinien, Gerätezulassungen und Zertifikaten		Optional bei BYOD relevant
10. Compliance & Datenschutz geprüft	Verarbeitung von biometrischen Daten, Cloud-Speicherung, Logging bewertet		DSGVO-/BDSG-konform umsetzen