Vertiefte digitale Souveränitätsanalyse

Fiktiver Fall: Kommunaler digitaler Arbeitsplatz

Version 1.0 · 04. November 2026 · Beispiel ohne realen Auftraggeber

Untersuchungsgegenstand	Aussagegrenze
Kollaborations- und Identitätsdienste einer fiktiven Verwaltung	Illustrative Annahmen; keine tatsächlich überprüften IT-Systeme.
Methodik	OpenDirection ODSA: 35 Kriterien, sieben Dimensionen, getrennte Betrachtung von Reife, Risiko und Nachweissicherheit.

HINWEIS: Sämtliche Befunde, Werte und Empfehlungen in diesem Musterbericht sind frei konstruiert. Sie dürfen nicht als reale Prüfung oder Aussage über konkrete Anbieter verstanden werden.

1 Management Summary

Die fiktive Organisation verfügt über teilweise dokumentierte Steuerungsprozesse und geordnete Verantwortlichkeiten. Die praktische Übertragbarkeit der Identitäts- und Kollaborationslandschaft ist jedoch nicht hinreichend belegt. Die größte Steuerungslücke ergibt sich nicht aus einer bestimmten Produktwahl, sondern aus dem fehlenden Nachweis, dass kritische Dienste unabhängig weitergeführt werden können.

Priorität	Illustrativer Kernbefund	Managemententscheidung
Hoch	Kein repräsentativer Ende-zu-Ende-Exit-Test	Testmigration für Identitäten und Kalender priorisieren
Hoch	Abhängigkeiten von einem zentralen Integrationsdienst unvollständig dokumentiert	Abhängigkeitsinventar und Eigentümerschaft klären
Mittel	Support- und Wiederherstellungsoptionen nur vertraglich beschrieben	Unabhängigen Restore-Test beauftragen

Die Analyse empfiehlt nicht automatisch eine Migration. Zunächst muss überprüft werden, welche strategischen Freiheitsgrade real bestehen und welche Verbesserungen mit vertretbarem Aufwand erreichbar sind.

2 Bewertungsumfang und Grenzen

Einbezogen wurden beispielhaft E-Mail, Kalender, Dateien, zentrale Identitäten und ein Kollaborationsdienst. Netzwerkinfrastruktur, Fachverfahren, Endgeräte und physische Sicherheit sind nicht Bestandteil dieses fiktiven Prüfumfangs.

Eine echte Analyse beginnt mit einer schriftlichen Scope-Festlegung und dem Abgleich der verfügbaren Nachweise. Ein nicht geprüfter Sachverhalt wird nicht als fehlende Fähigkeit oder als Nullwert interpretiert.

3 Methodik

Bewertungsdimension	Definition
Reifegrad (0–4)	0 nicht vorhanden · 1 ansatzweise · 2 dokumentiert · 3 umgesetzt · 4 praktisch validiert
Risiko	Gesonderte fachliche Einordnung Niedrig / Mittel / Hoch / Kritisch; kein mathematischer Ausgleich über Durchschnittswerte
Nachweissicherheit	Nicht bewertet / Selbstauskunft / Dokumentiert / Technisch validiert
Abdeckung	Anteil der bewertbaren Kriterien mit ausreichender Grundlage

Die sieben Bereiche sind Strategie & Governance, Technologie, Daten & KI, Betrieb, Recht, Lieferkette und Kompetenzen. Kritische Einzelbefunde bleiben unabhängig von allen Durchschnittswerten sichtbar.

4 Illustratives Souveränitätsprofil

Dimension	Ø Reife	Abdeckung	Risiko-Schwerpunkt
Strategie & Governance	2,8 / 4	100 %	Mittel
Technologie	1,8 / 4	80 %	Hoch
Daten & KI	2,2 / 4	80 %	Hoch
Betrieb	1,4 / 4	100 %	Hoch
Recht	2,6 / 4	80 %	Mittel
Lieferkette	1,2 / 4	60 %	Hoch
Kompetenzen	2,4 / 4	100 %	Mittel

Die Werte sind illustrative Annahmen und keine algorithmisch erzeugten Ergebnisse einer wirklichen Kriterienbewertung. Eine hohe Dimensionenreife belegt keine ausreichende Exit-Fähigkeit; hierfür sind konkrete Nachweise erforderlich.

5 Nachweislage

Nachweisart	Beispielhafte Verfügbarkeit
Selbstauskunft	Interviews der IT-Verantwortlichen
Dokumentiert	Architekturunterlagen und Vertragsauszüge in Teilbereichen
Technisch validiert	Wiederherstellung eines Testpostfachs – nicht des Gesamtsystems
Offen	Identitätsmigration, Export von Kalenderberechtigungen, Wechsel des Betriebsdienstleisters

6 Kritische Abhängigkeiten und Risiken

ID	Abhängigkeit	Einordnung
A-01	Zentraler Identitätsprovider	Ein Wechsel könnte Rollen und Dienstzugriffe betreffen; Test fehlt.
A-02	Spezifische Kalenderintegration	Metadaten und Freigabeberechtigungen sind noch nicht migrationsgetestet.
A-03	Einziger qualifizierter Betriebsdienstleister	Übergabe- und Vertretungsfähigkeit wurde nicht praktisch erprobt.

7 Priorisierte Maßnahmen

Priorität	Maßnahme	Akzeptanzkriterium
P1	Exit-Probe für Identitäten und Kalender	Dokumentiertes Migrationsprotokoll mit Daten- und Rechteabgleich
P1	Lieferanten- und Komponentenregister konsolidieren	Alle kritischen Komponenten besitzen Verantwortliche und Ausweichoption
P2	Wiederherstellung ohne bisherigen Betreiber prüfen	Erfolgreicher Restore-Test mit extern übergebener Dokumentation
P2	Souveränitätsanforderungen in Beschaffung aufnehmen	Verbindliche Prüfkriterien für Exit, Schnittstellen und Datenexport

8 Nächste Schritte und Entscheidungen

Vorgeschlagen wird eine fachliche Validierung der drei identifizierten Hauptrisiken, gefolgt von einem Maßnahmen-Workshop. Die Reihenfolge einzelner Maßnahmen richtet sich nach Kritikalität, Kosten, technischen Abhängigkeiten und Vergabebedingungen.

Schritt	Ergebnis	Verantwortung
1. Scope bestätigen	Freigegebener Untersuchungsgegenstand	Auftraggeber / IT-Leitung
2. Nachweise zusammentragen	Nachweisregister mit Fundstellen	System- und Vertragsverantwortliche
3. Kritische Tests durchführen	Protokollierte Feststellungen	Technische Prüfteams
4. Management-Entscheid	Priorisierte Maßnahmen mit Budgetrahmen	Steuerungsgremium

9 Grenzen der Aussage

Dieses Dokument ist eine fiktive Demonstration der Methodik. Eine reale vertiefte Souveränitätsanalyse ist eine Beratungsleistung innerhalb des vereinbarten Umfangs. Sie ersetzt kein unabhängiges Audit, keine Zertifizierung, keine Rechtsberatung und keinen Penetrationstest.

OpenDirection · opendirection.de · Beispielbericht, Stand 04.11.2026