SSCF

Assessment Report

Timo Consulting AG

Erstellt für Timo Hofmann

24. Mai 2026

GESAMTSCORE

75%

SEAL 3 · Souverän

Inhaltsverzeichnis

Ergebnisübersicht

SSCF Index

75%

Reifegrad: Souverän

SEAL-Einstufung

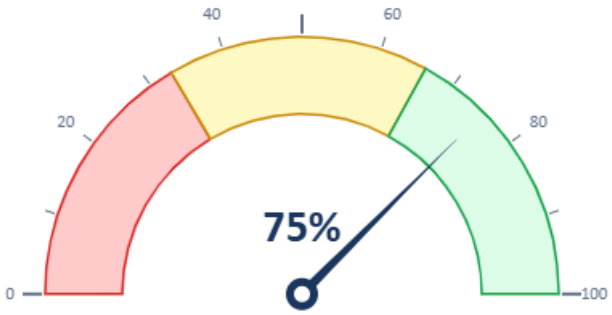
SEAL 3

Weitgehend souverän

●●●●○

Dimensionen-Übersicht

Dimension	Score	Status	Fortschritt
OK Organisatorische & Kompetenz-Souveränität	94%	Souverän	94%
TS Technologische Souveränität	78%	Souverän	78%
DS Datensouveränität	88%	Souverän	88%
SR Sicherheits- & Resilienz-Souveränität	56%	Teilweise	56%
AL Abhängigkeits- & Lieferkettensouveränität	63%	Teilweise	63%
SG Strategische & Governance-Souveränität	69%	Souverän	69%



Executive Summary

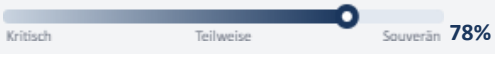
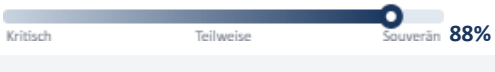
Ihr Unternehmen erreicht einen SSCF Index von 75% (SEAL 3). Die stärkste Dimension ist Organisatorische & Kompetenz-Souveränität mit 94%, während Sicherheits- & Resilienz-Souveränität mit 56% den grössten Handlungsbedarf aufweist.

Branchenvergleich: Der Durchschnitt liegt bei ca. 50%. Sie liegen über dem Branchendurchschnitt.

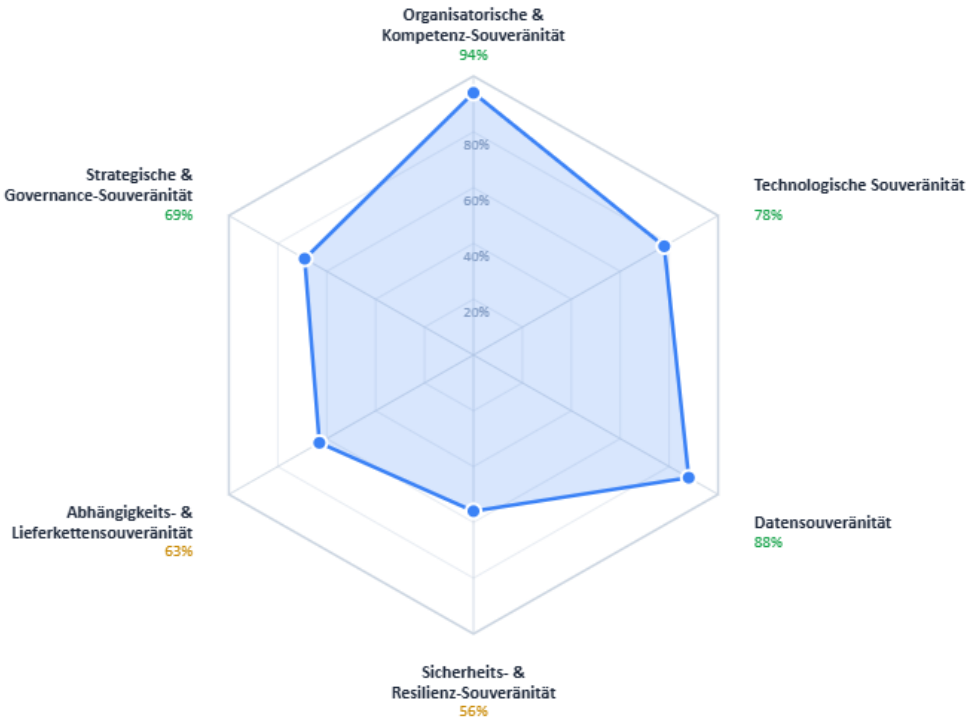
Stärken & Handlungsfelder

Top Stärken	Handlungsfelder
Organisatorische & Kompetenz-Souveränität **94%**	Sicherheits- & Resilienz-Souveränität 56%
Datensouveränität **88%**	Abhängigkeits- & Lieferkettensouveränität 63%
Technologische Souveränität **78%**	Strategische & Governance-Souveränität 69%

Reifegrad pro Dimension

Dimension	Reifegrad
OK Organisatorische & Kompetenz-Souveränität	
TS Technologische Souveränität	
DS Datensouveränität	
SR Sicherheits- & Resilienz-Souveränität	
AL Abhängigkeits- & Lieferkettensouveränität	
SG Strategische & Governance-Souveränität	

Dimensionen-Vergleich



Radar-Diagramm: Stärken- und Schwächenprofil über alle Dimensionen

Risiko-Heatmap

Einordnung der Dimensionen nach Risikoniveau basierend auf dem Assessment-Score.

Impact ↓ / Risiko →	Gering	Mittel	Hoch
Hoch	–	–	–
Mittel	**TS, SG**	**SR, AL**	–
Gering	**OK, DS**	–	–

Dimensionen mit tiefem Score = höheres Risiko (weiter oben rechts)

Guten Tag. Als IT-Beratungsexperte von Simplicon präsentiere ich Ihnen hiermit den Assessment-Report zur digitalen Souveränität Ihrer Timo Consulting AG. Dieser Bericht basiert auf den von Ihnen bereitgestellten Informationen und unserem bewährten Modell zur digitalen Souveränität. Er dient dazu, eine klare Momentaufnahme Ihrer aktuellen Situation zu geben und konkrete Handlungsempfehlungen für Ihre strategische Weiterentwicklung aufzuzeigen.

1. Overview

Gesamt-Score: 75/100

SEAL-Level: Level 3 – Weitgehend souverän

Ampelstatus: 🟢 **Grün**. Ihr Unternehmen befindet sich auf einem soliden Weg in Richtung digitaler Souveränität. Während viele Bereiche bereits exzellent aufgestellt sind, gibt es gezielte Felder, in denen durch strategische Massnahmen eine weitere Stärkung erreicht werden kann.

Top 3 Risiken:

- **Hardware-Lieferketten-Risiko**: Die aktuelle Abhängigkeit von Hardware-Lieferanten aus potenziell nicht vertrauenswürdigen Staaten birgt ein erhebliches Sicherheits- und Versorgungsrisiko.
- **Single-Site-Architektur**: Die Konzentration der kritischen Systeme auf einen einzigen Standort erhöht die Anfälligkeit für Ausfälle und Katastrophen, was die Resilienz des Unternehmens einschränkt.
- **Fehlende Exit-Strategie für Cloud-Dienste**: Trotz minimaler Abhängigkeit existiert keine formale Exit-Strategie, was im Falle eines Anbieterwechsels unnötigen Aufwand und potenzielle Geschäftsunterbrechungen bedeuten könnte.

Top 3 Handlungsfelder:

- **Diversifizierung der Hardware-Lieferketten**: Aktive Suche und Etablierung alternativer Bezugsquellen für kritische Hardware, um geopolitische Risiken zu mindern.
- **Stärkung der IT-Resilienz**: Entwicklung und Implementierung einer Multi-Standort-Strategie für kritische Systeme, um die Verfügbarkeit und Ausfallsicherheit zu erhöhen.
- **Formalisierung von Exit-Strategien**: Erarbeitung und Dokumentation von klar definierten Exit-Strategien für alle externen Dienstleister, selbst bei geringer Abhängigkeit, um zukünftige Flexibilität zu gewährleisten.

Gesamtbewertung: Die Timo Consulting AG agiert bereits weitgehend souverän und zeigt ein ausgeprägtes Bewusstsein für digitale Souveränität, muss jedoch strategische Lücken in Bezug auf Resilienz und Lieferkettenmanagement schliessen, um ihr hohes Niveau nachhaltig abzusichern.

2. Bewertungslogik

Dieser Report basiert auf einer umfassenden Analyse Ihrer Antworten zu unserem strukturierten Fragenkatalog, der sechs kritische Dimensionen der digitalen Souveränität abdeckt. Die Bewertung nutzt eine Kombination aus systematischer Auswertung Ihrer spezifischen Angaben und unserer tiefgreifenden Praxiserfahrung aus zahlreichen IT-Beratungsprojekten. Jede Dimension wird gewichtet, um einen realistischen Gesamtscore zu ermitteln, der die Komplexität und Interdependenz der verschiedenen Aspekte der digitalen Souveränität widerspiegelt. Bitte beachten Sie, dass die Ergebnisse eine Momentaufnahme des aktuellen Zustands Ihres Unternehmens darstellen und als Ausgangsbasis für die

weitere strategische Planung dienen; sie können und sollen sich durch gezielte Massnahmen dynamisch entwickeln.

3. Score-Erklärung

Die Bewertung der digitalen Souveränität erfolgt auf einer Skala von 0 bis 100 Punkten, wobei 100 die höchste erreichbare Stufe der digitalen Souveränität repräsentiert. Die Ergebnisse lassen sich wie folgt interpretieren:

- **0–33 Punkte (Kritisch)**: Das Unternehmen weist erhebliche Defizite auf und ist in kritischen Bereichen stark abhängig und unkontrolliert. Dringender Handlungsbedarf besteht.
- **34–66 Punkte (Teilweise souverän)**: Es sind erste Ansätze zur Souveränität erkennbar, jedoch bestehen weiterhin signifikante Abhängigkeiten und Risiken. Strategische Massnahmen sind erforderlich.
- **67–100 Punkte (Souverän)**: Das Unternehmen hat eine hohe Kontrolle über seine digitale Infrastruktur und Daten, ist widerstandsfähig gegenüber externen Einflüssen und verfügt über eine proaktive Strategie.

Ihr **SEAL-Level (Sovereignty Effective Assurance Level)** bietet eine detailliertere Einordnung:

- **Level 0 (Keine Kontrolle)**: Starke Abhängigkeit von externen Parteien ohne umfassende Kontrolle.
- **Level 1 (Erste Massnahmen erkennbar)**: Beginnende Bestrebungen zur Reduzierung von Abhängigkeiten und zur Stärkung der Kontrolle.
- **Level 2 (Teilweise kontrolliert)**: Gute Kontrolle über wesentliche Aspekte, aber mit verbleibenden Abhängigkeiten und Optimierungspotenzial.
- **Level 3 (Weitgehend souverän)**: Hohes Mass an Kontrolle und Resilienz, mit nur geringen, strategisch akzeptierten Abhängigkeiten.
- **Level 4 (Hoch souverän)**: Maximale Kontrolle über digitale Systeme, Daten und Prozesse, mit umfassender Resilienz und Flexibilität.

Ihr aktuelles **Level 3 (Weitgehend souverän)** bedeutet, dass die Timo Consulting AG bereits eine solide Basis geschaffen hat und in vielen Bereichen ein hohes Mass an Kontrolle und Unabhängigkeit aufweist. Ein "guter" Score liegt im Bereich von 70+ Punkten und einem Level 3 oder höher. Die Timo Consulting AG ist hier bereits hervorragend positioniert, mit Potenzial zur weiteren Stärkung in spezifischen Segmenten.

4. Dimensionen

Dimension	Score	Status	Interpretation
Strategie & Governance	69%	Souverän	Die digitale Souveränität ist explizit in der Strategie verankert und wird als Marketingmittel genutzt, jedoch fehlt ein regelmässiges IT-Strategie-Review.
Technologie	78%	Souverän	Eine starke Präferenz für Open Source und private Cloud-Lösungen unterstreicht den souveränen Technologieansatz, wenngleich strategische Ziele nicht immer formalisiert sind.
Daten	88%	Souverän	Hohe Transparenz, Kontrolle über eigene Daten und die Einhaltung von Datenschutzbestimmungen sind etabliert, während Datenklassifikation fortgeschritten ist.

Sicherheit & Resilienz	56%	Teilweise	Trotz etablierter Sicherheitsmassnahmen besteht eine hohe Abhängigkeit von einer Single-Site-Architektur und es fehlen regelmässige Sicherheitsaudits.
Abhängigkeiten & Lieferkette	63%	Teilweise	Geringe Abhängigkeit von externen Anbietern, aber fehlende Roadmaps zur Reduktion und Exit-Strategien für Cloud-Dienste mindern die Souveränität.
Organisation & Kompetenz	94%	Souverän	Exzellente Kompetenzen und klares Verständnis für IT-Sicherheit und Datenschutz innerhalb der Organisation sind gegeben.

5. Findings

Titel	Beschreibung	Kategorie	Dimension	Impact
Etablierte Datenkontrolle	Die Timo Consulting AG hat vollständige Kontrolle über ihre eigenen Geschäftsdaten und weiss, wo diese physisch gespeichert und verarbeitet werden. Dies gewährleistet eine hohe Datensouveränität.	Stärke	Daten	Hoch
Hohes IT-Sicherheitsbewusstsein	Die Kompetenz und das Bewusstsein der Mitarbeitenden im Umgang mit digitalen Tools, IT-Sicherheit und Datenschutz sind exzellent. Dies fördert eigenverantwortliches Handeln.	Stärke	Organisation & Kompetenz	Hoch
Open Source als bevorzugte Strategie	Eine "OSS first"-Strategie ist etabliert und wird in vielen kritischen Bereichen wie Betriebssystemen, Datenbanken und Kollaborationstools umgesetzt. Dies reduziert Abhängigkeiten und erhöht die Flexibilität.	Stärke	Technologie	Hoch
Starke strategische Verankerung der digitalen Souveränität	Digitale Souveränität ist explizit in der Geschäftsstrategie verankert und wird als wichtiges Marketinginstrument genutzt ("Eat your own dogfood").	Stärke	Strategie & Governance	Mittel
Single-Site-Architektur als Risiko	Kritische Systeme sind auf einen einzelnen Standort konzentriert, was ein hohes Risiko bei einem Ausfall oder einer Katastrophe darstellt und die Resilienz stark einschränkt.	Risiko	Sicherheit & Resilienz	Hoch
Abhängigkeit von Hardware-Lieferanten aus unsicheren Staaten	Es besteht eine Abhängigkeit von Hardware-Lieferanten aus potenziell nicht vertrauenswürdigen Staaten, was Fragen der geopolitischen Kontrolle und der Lieferkettensicherheit aufwirft.	Risiko	Abhängigkeiten & Lieferkette	Hoch
Fehlende formale Exit-Strategien	Trotz minimaler Abhängigkeit von Cloud-Diensten gibt es keine	Schwäche	Abhängigkeiten & Lieferkette	Mittel

	dokumentierten Exit-Strategien für den Fall eines Anbieterwechsels. Dies schafft unnötige administrative Risiken und potenziellen Mehraufwand.			
Ad-hoc IT-Strategie-Review	Die IT-Strategie wird nicht regelmässig überprüft und angepasst, sondern meist ad-hoc basierend auf aktuellen Ereignissen. Dies könnte zu verpassten strategischen Chancen führen.	Schwäche	Strategie & Governance	Mittel
Unregelmässige IT-Sicherheitsaudits	Es werden keine regelmässigen IT-Sicherheitsaudits durchgeführt, was die proaktive Identifizierung von Schwachstellen und die Überprüfung der Sicherheitslage erschwert.	Schwäche	Sicherheit & Resilienz	Hoch
Ungenutzte Automatisierungspotenziale in der IT-Strategie	Die Automatisierung der IT-Infrastruktur erfolgt zwar über manuelle Skripte bis Infrastructure as Code, jedoch ist das Potenzial der Automatisierung als strategisches Ziel zur Stärkung der Souveränität nur gering eingestuft.	Schwäche	Technologie	Mittel
Mangelnde strukturierte Bewertung von Standardisierung/Flexibilität	Es erfolgt keine systematische Bewertung der Auswirkungen von Standardisierung und Flexibilität auf die Lieferkette und resultierende Abhängigkeiten und Risiken.	Schwäche	Abhängigkeiten & Lieferkette	Mittel
Kritikalität proprietärer Software auf Windows	Es besteht eine kontrollierte Abhängigkeit von proprietärer Software, die auf Windows-Betriebssystemen läuft, insbesondere aufgrund von Kundenanforderungen. Dies kann zukünftige Flexibilität einschränken.	Schwäche	Abhängigkeiten & Lieferkette	Tief

6. Abhängigkeiten

Bereich	Anbieter / System	Risiko-Level	Kritikalität	SPOF
Hardware	Lieferanten (aus nicht vertrauenswürdigen Staaten)	Hoch	Kritisch	Ja
Infrastruktur	Single-Site Architektur	Hoch	Kritisch	Ja
Betriebssysteme	Microsoft Windows	Mittel	Wichtig	Nein
IT-Sicherheit	Interne Ressourcen (Audit)	Mittel	Wichtig	Ja

Cloud Services	Buchhaltungs-Cloud-Anbieter	Tief	Normal	Nein
Prozesse	Fehlende Exit-Strategien	Mittel	Wichtig	Nein
Software	Proprietäre Software auf Windows	Mittel	Wichtig	Nein
IT-Strategie	Ad-hoc Review-Prozess	Mittel	Normal	Nein

7. Risiken

Risiko	Beschreibung	Impact	Wahrscheinlichkeit	Priorität
Ausfall kritischer Systeme durch Single-Site-Architektur	Die Konzentration aller kritischen IT-Systeme auf einen einzigen physischen Standort birgt ein erhebliches Risiko. Im Falle eines lokalen Ereignisses (z.B. Brand, Hochwasser, längerer Stromausfall) können alle geschäftsrelevanten Anwendungen und Daten betroffen sein, was zu einem vollständigen Stillstand der Geschäftstätigkeit führen würde. Die Ergänzung "Sollte das Unternehmen ausreichend wachsen, werden wir die Datenhaltung entsprechend auch auf mehrere Geolokationen verteilen" deutet auf ein bewusstes, aber noch nicht adressiertes Risiko hin.	Kritisch	Mittel	Kritisch
Geopolitische Risiken in der Hardware-Lieferkette	Die Abhängigkeit von Hardware-Lieferanten aus "nicht vertrauenswürdigen Staaten" setzt das Unternehmen potenziellen geopolitischen Einflüssen, Exportbeschränkungen oder sogar der Gefahr von Hardware-Manipulation aus. Dies kann die Beschaffung kritischer Komponenten erschweren, zu Lieferengpässen führen oder die Integrität der Infrastruktur gefährden. Die Bemerkung "Hardware-Lifecycle, Abhängigkeit zu Lieferanten aus nicht vertrauenswürdigen Staaten" unterstreicht die Relevanz dieses Risikos.	Hoch	Mittel	Hoch
Fehlende Identifikation von Schwachstellen durch unregelmässige Audits	Das Unternehmen führt keine regelmässigen IT-Sicherheitsaudits durch. Dies kann dazu führen, dass Schwachstellen, Fehlkonfigurationen oder Compliance-Verstösse unentdeckt bleiben und erst im Rahmen eines Sicherheitsvorfalls oder eines externen Angriffs zu Tage treten, wodurch der Reaktionszeitpunkt stark eingeschränkt wird.	Hoch	Mittel	Hoch
Operative Ineffizienz und Sicherheitslücken durch fehlende Exit-Strategien	Das Fehlen formaler Exit-Strategien für externe Anbieter, einschliesslich Cloud-Dienste, führt im Falle eines notwendigen Anbieterwechsels zu einem unerwartet hohen Aufwand, potenziellen Datenverlusten und längeren Migrationszeiten. Auch wenn die Abhängigkeit aktuell als minimal bewertet wird ("bisher ist das Risiko bzw. der Nutzen einer Exitstrategie gering"), kann sich dies schnell ändern und dann zu einer erheblichen Belastung werden.	Hoch	Tief	Mittel

Verpasste strategische Chancen durch ad-hoc IT-Strategie-Review	Die IT-Strategie wird nicht regelmässig überprüft, sondern ad-hoc an aktuelle Ereignisse angepasst. Dieser reaktive Ansatz kann dazu führen, dass strategische Weiterentwicklungen, Anpassungen an neue Technologien oder Marktveränderungen verspätet oder gar nicht erkannt werden, was die langfristige Wettbewerbsfähigkeit beeinträchtigen könnte.	Mittel	Mittel	Mittel
Eingeschränkte Flexibilität durch proprietäre Windows-Software	Die partielle Abhängigkeit von proprietärer Software, die ausschliesslich auf Windows-Betriebssystemen läuft, schränkt die technologische Flexibilität ein. Obwohl die Risiken bekannt sind ("Die Risiken sind bekannt und werden adressiert"), kann dies Migrationskosten erhöhen und die Nutzung alternativer, möglicherweise souveränerer Betriebssysteme oder Software erschweren. Dies kann auch die Anpassung an spezielle Kundenumgebungen bei Problemen beeinträchtigen.	Mittel	Tief	Tief

8. Empfehlungen

Massnahme	Beschreibung	Kategorie	Dimension	Nutzen
Einführung regelmässiger IT-Sicherheitsaudits	Etablierung eines halbjährlichen oder jährlichen Zyklus für externe IT-Sicherheitsaudits, um systematisch Schwachstellen zu identifizieren, Best Practices zu überprüfen und die Compliance sicherzustellen. Dies erhöht die proaktive Verteidigungsfähigkeit und das Vertrauen.	Quick Win	Sicherheit & Resilienz	Erhöhte Widerstandsfähigkeit gegen Cyberangriffe, frühzeitige Erkennung von Schwachstellen.
Entwicklung einer Roadmap zur Hardware-Lieferantendiversifizierung	Erarbeitung einer Strategie zur Identifizierung und Qualifizierung von alternativen Hardware-Lieferanten, insbesondere aus vertrauenswürdigeren geografischen Regionen. Dies reduziert die Abhängigkeit von einzelnen Lieferanten mit potenziellen geopolitischen Risiken.	Quick Win	Abhängigkeiten & Lieferkette	Reduktion geopolitischer Risiken, Erhöhung der Versorgungssicherheit, Stärkung der Lieferkettenresilienz.
Formalisierung von Exit-Strategien für Schlüsseldienste	Erstellung von dokumentierten Exit-Strategien für die kritischeren externen Dienste, auch wenn die Abhängigkeit gering ist (z.B. Buchhaltungs-Cloud). Dies umfasst Datenexportformate, Prozessbeschreibungen und	Mid-term	Abhängigkeiten & Lieferkette	Reduzierung von Umstiegsrisiken, Erhöhung der Verhandlungsposition gegenüber Anbietern, Sicherstellung der Betriebskontinuität.

	technische Anforderungen für einen Anbieterwechsel.			
Entwicklung einer Multi-Standort-Resilienzstrategie	Ausarbeitung eines Konzepts zur Verteilung kritischer Systemkomponenten und Datenhaltung auf mindestens zwei geografisch getrennte Standorte. Dies kann durch Replikation, geografische Lastverteilung oder Disaster Recovery as a Service (DRaaS) erfolgen.	Strategisch	Sicherheit & Resilienz	Signifikante Erhöhung der Ausfallsicherheit und der geografischen Resilienz bei lokalen Katastrophen.
Implementierung eines regelmässigen IT-Strategie-Review-Prozesses	Einführung eines quartalsweisen oder halbjährlichen Meetings zur Überprüfung und Anpassung der IT-Strategie, einschliesslich der Rolle der digitalen Souveränität. Dies stellt sicher, dass die Strategie stets aktuell ist und auf neue Herausforderungen reagieren kann.	Quick Win	Strategie & Governance	Proaktive Steuerung der IT-Entwicklung, bessere Reaktion auf Marktveränderungen, Sicherung langfristiger Wettbewerbsvorteile.
Aufbau einer Wissensdatenbank für souveräne Alternativen	Erstellung und Pflege einer internen Wissensdatenbank zu Open-Source-Alternativen und souveränen Softwarelösungen für proprietäre Systeme, mit Fokus auf Migration und Integrationsfähigkeit.	Mid-term	Technologie	Stärkung der Position gegenüber proprietärer Software, langfristige Reduktion von Abhängigkeiten, Beschleunigung von Anbieterwechseln.
Systematische Bewertung von Standardisierung und Flexibilität	Einführung eines strukturierten Prozesses zur Bewertung der Auswirkungen von IT-Standardisierung und Flexibilität auf die Lieferkette. Dies beinhaltet die Analyse von Interoperabilität, Schnittstellen und möglichenvendor Lock-in-Effekten bei der Beschaffung neuer Systeme.	Mid-term	Abhängigkeiten & Lieferkette	Verbesserte Entscheidungsfindung bei IT-Investitionen, proaktive Vermeidung neuer Abhängigkeiten, optimierte Lieferkettensteuerung.
Definition von Metriken für digitale Souveränität	Festlegung von messbaren Kennzahlen (KPIs) für die digitale Souveränität in den Bereichen Abhängigkeiten, IT-Sicherheit und Datenkontrolle. Diese KPIs dienen als Grundlage für das Monitoring und die Kommunikation des Fortschritts.	Strategisch	Strategie & Governance	Transparente Erfolgsmessung, datenbasierte Entscheidungsfindung, verstärkte Sensibilisierung im Unternehmen.
Erkundung von Open-Source-Alternativen für Windows-Software	Proaktive Recherche und Evaluierung von Open-Source-Alternativen für kritische, Windows-basierte proprietäre Software. Dies schafft eine Option für zukünftige Migrationen und reduziert die Abhängigkeit vom Microsoft-Ökosystem.	Mid-term	Technologie	Erhöhung der Plattformunabhängigkeit, potenzielle Kosteneinsparungen, langfristige Flexibilität.

Sensibilisierung für die Hardware-Lieferkette	Regelmässige Informationen und Schulungen für Stakeholder und Entscheidungsträger über die Risiken in der Hardware-Lieferkette und die Bedeutung der Diversifizierung. Dies fördert ein unternehmensweites Bewusstsein.	Quick Win	Abhängigkeiten & Lieferkette	Stärkung des Bewusstseins, Unterstützung bei strategischen Beschaffungsentscheidungen.

9. Roadmap

Phase 1: Quick Wins (Monat 1–3)

- **Zeitraum**: Monat 1–3
  Massnahmen:
- **Initiierung regelmässiger IT-Sicherheitsaudits**: Definition des Umfangs und Beauftragung eines externen Dienstleisters für das erste Audit, um eine initiale Standortbestimmung und Schwachstellenanalyse zu erhalten.
- **Erste Schritte zur Roadmap Hardware-Lieferantendiversifizierung**: Identifizierung kritischer Hardware-Komponenten und erste Recherche potenzieller alternativer Lieferanten, insbesondere aus geografisch weniger risikobehafteten Regionen.
- **Implementierung eines regelmässigen IT-Strategie-Review-Prozesses**: Festlegung eines festen Termins (z.B. quartalsweise) für einen strukturierten Review der IT-Strategie und der Fortschritte bezüglich digitaler Souveränität.
- **Sensibilisierung für die Hardware-Lieferkette**: Kurze Informationsveranstaltung oder internes Memo an relevante Stakeholder zur Schaffung eines Bewusstseins für die Risiken in der Hardware-Lieferkette.
- **Ziel**: Schaffung einer proaktiven Sicherheitskultur durch Audits, Beginn der Minderung von Hardware-Risiken und Etablierung eines dynamischen Strategie-Managements.

Phase 2: Optimierung (Monat 4–6)

- **Zeitraum**: Monat 4–6
  Massnahmen:
- **Formalisierung von Exit-Strategien für kritische externe Dienste**: Erstellung detaillierter Exit-Pläne, beginnend mit der Buchhaltungs-Cloud und weiteren relevanten Diensten, die mindestens einen Datenexportpfad und einen Plan für den Dienstleisterwechsel umfassen.
- **Aufbau einer Wissensdatenbank für souveräne Alternativen**: Start der Erfassung und Dokumentation von Open-Source-Alternativen zu proprietärer Software, mit Fokus auf Windows-basierte Anwendungen, die aktuell genutzt werden.
- **Systematische Bewertung von Standardisierung und Flexibilität**: Entwicklung einer Checkliste oder eines Rahmens zur systematischen Bewertung von Abhängigkeiten und Risiken bei der Einführung neuer IT-Lösungen im Kontext der Lieferkette.
- **Erkundung von Open-Source-Alternativen für Windows-Software**: Pilotprojekt zur Evaluierung einer vielversprechenden Open-Source-Alternative zu einer kleineren, aber kritischen Windows-Anwendung.

- **Ziel**: Reduzierung operativer Risiken durch klare Ausstiegsstrategien, Stärkung der technologischen Unabhängigkeit durch Alternativevaluation und verbesserte Entscheidungsfindung bei IT-Investitionen.

Phase 3: Transformation (Monat 7–12)

- **Zeitraum**: Monat 7–12
  Massnahmen:
- **Entwicklung einer Multi-Standort-Resilienzstrategie**: Aufnahme der Ergebnisse der Risikoanalyse der Single-Site-Architektur und Erarbeitung eines konkreten Konzepts für die geografische Aufteilung oder Replikation kritischer Systeme. Dies beinhaltet eine Kostenschätzung und einen Umsetzungsplan.
- **Definition von Metriken für digitale Souveränität**: Festlegung von Key Performance Indicators (KPIs) zur Messung des Fortschritts in den Bereichen Abhängigkeitsreduktion, IT-Sicherheit und Datenkontrolle, sowie die Integration dieser Metriken in das regelmässige IT-Strategie-Review.
- **Fortlaufende Diversifizierung der Hardware-Lieferkette**: Implementierung der ersten identifizierten alternativen Beschaffungswege und vertragliche Absicherung mit neuen Lieferanten, um geopolitische Risiken weiter zu minimieren.
- **Pilotimplementierung der Multi-Standort-Resilienzstrategie**: Start der Umsetzung eines ersten Teilbereichs der Multi-Standort-Strategie, z.B. Replikation von kritischen Daten oder einer nicht-produktionskritischen Anwendung.
- **Ziel**: Signifikante Erhöhung der Resilienz des Unternehmens durch geografische Diversifizierung, Etablierung eines datengestützten Management-Frameworks für digitale Souveränität und nachhaltige Reduktion strategischer Abhängigkeiten.

10. Zielbild

Today (Ist-Zustand)

Die Timo Consulting AG zeigt bereits heute ein beeindruckendes Mass an digitaler Souveränität, insbesondere in Bezug auf die Datenkontrolle, organisatorische Kompetenz und den strategischen Einsatz von Open-Source-Lösungen. Die interne Organisation und das Bewusstsein für IT-Sicherheit sind exzellent, was eine starke Basis für Autonomie bildet. Gleichwohl bestehen Lücken im Bereich der Resilienz, da eine Single-Site-Architektur dominiert und die Hardware-Lieferketten Abhängigkeiten von geopolitisch unsicheren Regionen aufweisen. Das Fehlen formaler Exit-Strategien und unregelmässige Strategie-Reviews weisen auf ein Optimierungspotenzial in der Proaktivität und Risikominimierung hin.

Future (Soll-Zustand)

Im souveränen Zielzustand ist die Timo Consulting AG ein Vorbild für umfassende digitale Souveränität. Die IT-Infrastruktur ist durch eine robuste Multi-Standort-Architektur extrem widerstandsfähig gegen Ausfälle jeglicher Art. Die Lieferketten für Hardware sind diversifiziert und abgesichert, wodurch geopolitische Risiken minimiert werden. Alle externen Dienstleistungen sind durch klar definierte Exit-Strategien abgesichert, was maximale Flexibilität und Handlungsfreiheit garantiert. Die IT-Strategie wird proaktiv und regelmässig überprüft, gesteuert durch präzise Kennzahlen, die den Fortschritt der digitalen Souveränität messbar machen. Dies ermöglicht eine agile Anpassung an zukünftige technologische Entwicklungen bei voller Kontrolle über Daten und Systeme.

Prinzipien

- **Unabhängigkeit**: Die Timo Consulting AG agiert weitgehend unabhängig von einzelnen Anbietern oder Technologien. Dies wird durch eine strikte Open-Source-Strategie, diversifizierte Lieferketten und die Fähigkeit zum schnellen Wechsel von Dienstleistern erreicht, wodurch die Entscheidungsfreiheit und Wettbewerbsfähigkeit dauerhaft gesichert sind.
- **Kontrolle**: Das Unternehmen hat zu jeder Zeit vollständige Transparenz und Kontrolle über seine Daten, Systeme und Prozesse. Dies beinhaltet nicht nur die physische Datenhoheit, sondern auch die Fähigkeit zur Auditierung, zur aktiven Steuerung von Datenflüssen und zur Durchsetzung eigener Sicherheitsstandards gegenüber Dritten.
- **Resilienz**: Die gesamte IT-Infrastruktur und die zugehörigen Prozesse sind so ausgelegt, dass sie maximal widerstandsfähig gegen Störungen, Angriffe und Ausfälle sind. Eine verteilte Architektur, regelmässige Notfallübungen und eine proaktive Absicherung der Lieferketten gewährleisten die kontinuierliche Geschäftsfähigkeit unter allen Umständen.

11. Nächste Schritte

Um die in diesem Report identifizierten Potenziale vollständig auszuschöpfen und die digitale Souveränität Ihrer Timo Consulting AG weiter zu stärken, bieten wir Ihnen folgende konkrete Follow-up-Angebote an:

💬 Austausch & Sparring

Gerne bieten wir Ihnen ein **30–60 Minuten persönliches Gespräch** an, in dem wir die detaillierten Ergebnisse des Reports gemeinsam besprechen. Wir werden Ihre individuellen Prioritäten für die vorgeschlagenen Massnahmen erörtern, alle offenen Fragen beantworten und Ihnen eine erste Einschätzung geben, welche Schritte für Ihr Unternehmen am dringlichsten sind. Dieser Austausch dient dazu, die Erkenntnisse des Assessments fundiert zu interpretieren und erste Weichenstellungen vorzunehmen.

🎯 Workshop

Für eine tiefere Analyse und die gemeinsame Erarbeitung einer massgeschneiderten Strategie empfehlen wir einen **halb- oder ganztägigen Workshop** mit relevanten Stakeholdern aus Ihrem Unternehmen. In diesem interaktiven Format werden wir die kritischsten Dimensionen detailliert durchleuchten, Ursachen für identifizierte Schwachstellen erarbeiten und gemeinsam konkrete Lösungsansätze definieren. Ziel ist es, eine detaillierte Strategie und einen Aktionsplan zu entwickeln, einschliesslich der Zuweisung von Verantwortlichkeiten und der Festlegung erster Meilensteine.

🚀 Umsetzungsbegleitung

Sollten Sie Unterstützung bei der Implementierung der empfohlenen Massnahmen wünschen, stehen wir Ihnen gerne als erfahrener Partner zur Seite. Unsere **Umsetzungsbegleitung** reicht von der detaillierten Planung einzelner Projekte bis hin zur langfristigen strategischen Beratung. Wir unterstützen Sie bei der Auswahl und Einführung neuer Technologien, der Optimierung von Prozessen und der Sicherstellung der Compliance. Durch regelmässige Reviews und Fortschrittsmessungen begleiten wir Sie auf dem Weg zu einer vollständig souveränen IT-Landschaft und schlagen nach 6–12 Monaten eine Wiederholung des Assessments vor, um den erzielten Fortschritt transparent zu machen.

Ihr Ansprechpartner

Name	Emanuele Rizzo
E-Mail	emanuele.rizzo@simplicon.ch
Telefon	+41 79 962 41 09
Spezialisierung	Consulting

Wir freuen uns, Sie auf Ihrem Weg zur SSCF-Konformität zu begleiten.

Report generiert am 25.5.2026, 07:36:23