

Reifegradanalyse – Digitale Souveränität

Reifegrad-Check Ihrer digitalen Souveränität

Situation

Digitale Souveränität entscheidet sich nicht in der Technik, sondern in der Steuerungsfähigkeit der Führung.

Regulatorik (u. a. NIS-2, DORA, KRITIS-Vorgaben), geopolitische Verschiebungen und die zunehmende Abhängigkeit von wenigen globalen Cloud- und Technologieanbietern zwingen Geschäftsleitungen, ihre Selbstbestimmung über Daten, Technologien und Anbieterbeziehungen bewusst zu gestalten. Digitale Souveränität dominiert damit zunehmend die strategische Agenda – nicht mehr nur die IT-Agenda.

In vielen Organisationen wird das Thema jedoch weiterhin primär operativ und punktuell behandelt, etwa als einzelne Migrations- oder Exit-Frage im IT-Betrieb. Auf strategischer Ebene fehlt häufig ein gemeinsames Zielbild: Was digitale Souveränität konkret bedeuten soll, welches Ambitionsniveau angestrebt wird und wer im Führungskreis dafür die Steuerungsverantwortung trägt, ist selten explizit geklärt.

Herausforderung

Zielbild schärfen, Reife sichtbar machen, Kurs halten und konsequent steuern.

Die zentrale Herausforderung ist nicht ein Mangel an technischen Einzelmaßnahmen, sondern das Fehlen einer belastbaren strategischen Steuerungsfähigkeit für digitale Souveränität. Aus unserer Erfahrung liegt es meist an zu geringer Sichtbarkeit über den tatsächlichen Reifegrad der Organisation (strategisch, organisatorisch und in der Governance), einer fehlenden Formulierung des angestrebten Zielbilds und Ambitionsniveaus, fehlenden Entscheidungsprinzipien für Zielkonflikte sowie einem unklaren Mandat für die Steuerung.

- Kein explizites Zielbild und kein bewusst festgelegtes Ambitionsniveau – von „vollständiger Unabhängigkeit“ über „kontrollierte Diversifizierung“ bis zur „bewussten Akzeptanz von Abhängigkeiten“.
- Fehlende Entscheidungsprinzipien für Zielkonflikte (z. B. Souveränität vs. Innovationsgeschwindigkeit, Souveränität vs. Kosten- und Skaleneffekte).
- Keine klar verankerte Governance: Zuständigkeit, Mandat und Steuerungsbefugnis für Souveränitätsfragen sind nicht eindeutig zugeordnet.

- Divergierende Einschätzungen zwischen Geschäftsleitung, CIO/CDO und IT-Leitung, die unerkannt bleiben und zu widersprüchlichen Entscheidungen führen.
- Eine geäußerte Ambition, die nicht durch die tatsächliche organisatorische Reife gedeckt ist – mit dem Risiko von Fehlinvestitionen.

Implikation

Das Reifegrad-Assessment Digitale Souveränität ist ein moderiertes Führungs-Assessment, das den strategischen Reifegrad entlang von fünf Dimensionen mit insgesamt 26 Leitfragen erhebt und bewertet:

- A – Strategische Bedeutung & Zielbild: Stellenwert der Souveränität und angestrebtes Ambitionsniveau.
- B – Entscheidungsprinzipien & Zielkonflikte: Prinzipien für den bewussten Umgang mit Abwägungen.
- C – Governance & Steuerungsfähigkeit: Mandat, Zuständigkeit und Steuerungsbefugnis.
- D – Organisatorische & strategische Fähigkeiten: Kompetenzen, Plattform- und Technologievielfalt.
- E – Priorisierung & Roadmap-Fähigkeit: Fähigkeit, Souveränität in eine priorisierte Roadmap zu überführen.

Grundlage bildet ein „Reifegradmodell“ mit fünf Stufen (1 unreflektiert bis 5 Gestaltend), ein Vorab-Fragebogen und ein moderierter Assessment-Workshop mit dem Führungskreis. Jede Frage wird nicht auf einer feingranularen Punkteskala, sondern durch Zuordnung zu einer Reifegradstufe beantwortet – der Wert liegt im gemeinsamen Führungsgespräch. Divergenzen zwischen den Teilnehmenden werden bewusst nicht weggemittelt, sondern als eigenständiger Befund ausgewiesen.

Zentrale

Controlware GmbH
Waldstraße 92
63128 Dietzenbach
Tel. +49 6074 858-00
Fax +49 6074 858-108

info@controlware.de
www.controlware.de
blog.controlware.de

Besuchen Sie uns auf:





Die Reife wird je Dimension als Mindeststufe plus Tendenz bestimmt und gegen das in Dimension A erhobene Ambitionsniveau gespiegelt. So wird die Ambitions-Reife-Lücke sichtbar – der wichtigste Einzelbefund, wenn eine hohe Ambition auf geringe Governance- oder Fähigkeitsreife trifft.

Nutzen

Egal ob digitale Souveränität als Compliance-Anforderung, als strategisches Ziel oder als Antwort auf konkrete Anbieterabhängigkeiten adressiert wird – es ist ein zuverlässiges Steuerungsinstrument nötig, um souveränitätsbezogene Initiativen im Unternehmen zu überprüfen und zu steuern. Dazu bedarf es einer Bestandsaufnahme der strategischen Reife. Erst danach entsteht ein kontinuierlicher Entwicklungsprozess, der die Rahmenbedingungen für eine souveräne, selbstbestimmte IT schafft.

Warum sollten Sie das Reifegrad-Assessment durchführen?

Nach dem Assessment haben Sie den nötigen Einblick, um Souveränitätsentscheidungen auf die strategischen Ziele Ihres Unternehmens abzustimmen. Darüber hinaus erhalten Sie:

- eine belastbare Einstufung Ihres aktuellen Reifegrads über alle fünf Dimensionen, inkl. Blockaden, Einschränkungen und Entwicklungsmöglichkeiten,
- ein gemeinsames Zielbild und aufgedeckte Divergenzen im Führungskreis, bevor sie zu widersprüchlichen Entscheidungen führen,
- eine klare Benennung strategischer Zielkonflikte – unaufgelöste oder nur implizite Konflikte erhalten höhere Priorität als bereits bewusst gehandhabte,
- eine High-Level-Roadmap mit priorisierten Entwicklungsfeldern, geordnet nach Hebelwirkung.

Ziel

Neben der Klarheit über den eigenen strategischen Reifegrad und den Ist-Zustand der Souveränitätssteuerung werden sowohl die Potenziale als auch die Schwachstellen erkannt und konkrete, priorisierte Maßnahmen auf Basis der Analyse geplant. Das Ergebnis ist Handlungsfähigkeit statt diffuser Betroffenheit – mit einem geteilten Zielbild und einer belastbaren Roadmap als Grundlage für die weitere Steuerung. Bei Bedarf bereitet das Assessment den Einstieg in ein tiefergehendes Risikoprofil Digitale Souveränität vor.

Warum Controlware

Controlware ist ein unabhängiger Systemintegrator und Managed Service Provider mit Sitz in Deutschland, gegründet 1980. IT-Security ist seit den 1990er Jahren fester Bestandteil des Portfolios; der Customer-Service-Betrieb ist nach ISO/IEC 27001 zertifiziert. Mit einem herstellerunabhängigen Beratungsansatz begleiten wir Sie von der Standortbestimmung bis zur technischen Umsetzung. GRC-Beratung, Cyber Defense Services und Managed SOC kommen dabei aus einer Hand, sodass erkannte Folgeaktivitäten ohne Bruch in die Umsetzung überführt werden können.

Unsere Spezialistinnen und Spezialisten verfügen über umfangreiche Expertise in verschiedenen Branchen, mit vielfältigen Technologien und in Organisationen unterschiedlicher Größe.

Weitere Informationen und Details entnehmen Sie bitte der zugehörigen Leistungsbeschreibung.

Zentrale

Controlware GmbH
Waldstraße 92
63128 Dietzenbach
Tel. +49 6074 858-00
Fax +49 6074 858-108

info@controlware.de
www.controlware.de
blog.controlware.de

Besuchen Sie uns auf:

