WHITEPAPER

Das Readiness Framework

Readiness und Digitale Souveränität werden zu den entscheidenden Fähigkeiten der digitalen Organisation

Governance · Wertströme · Plattformen & Capabilities · Informationen
Resilienz · Digitale Souveränität · AI

Martin Andenmatten
Gründer & Managing Director, Glenfis AG
Zürich · Juli 2026

GLENFIS AG

Inhalt

Geleitwort 3

1 Die grösste Herausforderung ist nicht die Technologie 5

2 Vom IT Operating Model zum Readiness Framework 7

Das Readiness Framework auf einen Blick 10

3 Governance schafft Readiness 11

4 Wertströme schaffen Readiness 14

5 Plattformen und Capabilities schaffen Readiness 17

6 Informationen schaffen Readiness 20

7 Resilienz schafft Readiness 23

8 AI schafft eine neue Dimension von Readiness 26

9 Die Organisation der Zukunft – Readiness wird zur zentralen Managementfähigkeit 29

Fazit: Die Zukunft gehört den Organisationen mit der höchsten Readiness 32

Über den Autor · Über Glenfis AG · Quellen 36

Impressum

© 2026 Glenfis AG, Zürich, Schweiz. Alle Rechte vorbehalten. Herausgeber: Glenfis AG. Autor: Martin Andenmatten, Gründer & Managing Director. Dieses Whitepaper einschliesslich aller Texte und Grafiken ist urheberrechtlich geschützt. Jede Verwertung ausserhalb der engen Grenzen des Urheberrechts ist ohne schriftliche Zustimmung der Glenfis AG unzulässig; dies gilt insbesondere für Vervielfältigung, Übersetzung und die Einspeicherung in elektronische Systeme. ITIL® ist eine eingetragene Marke von PeopleCert. COBIT® ist eine eingetragene Marke von ISACA. IT4IT™ und TOGAF® sind Marken der The Open Group.

Geleitwort

Readiness und Digitale Souveränität werden zu den entscheidenden Fähigkeiten der digitalen Organisation

Über viele Jahre standen bei der digitalen Transformation vor allem neue Technologien im Mittelpunkt. Cloud Computing, Agile, DevOps, Plattformen oder Künstliche Intelligenz versprachen mehr Geschwindigkeit, höhere Effizienz und eine bessere Zusammenarbeit zwischen Business und IT.

Diese Entwicklungen haben Unternehmen zweifellos vorangebracht. Gleichzeitig ist jedoch die Komplexität digitaler Organisationen massiv gestiegen. Heute müssen Unternehmen nicht nur innovative digitale Produkte entwickeln, sondern gleichzeitig Cyberrisiken beherrschen, regulatorische Anforderungen erfüllen, globale Plattformökosysteme steuern und zunehmend auch intelligente AI-Agenten sicher in ihre Wertschöpfung integrieren.

Die Herausforderung besteht deshalb längst nicht mehr darin, einzelne Technologien erfolgreich einzuführen.

Die eigentliche Herausforderung besteht darin, die Organisation selbst auf diese neue Realität auszurichten.

Ein modernes Operating Model muss heute weit mehr leisten als Prozesse zu definieren oder Verantwortlichkeiten zu beschreiben. Es muss sicherstellen, dass Unternehmen Veränderungen kontinuierlich, kontrolliert und nachhaltig bewältigen können. Gleichzeitig muss es gewährleisten, dass sie trotz wachsender Abhängigkeiten von Cloud-Anbietern, Plattformen und AI-Systemen ihre Entscheidungsfreiheit und Kontrolle behalten.

Genau daraus entstehen zwei zentrale Managementfähigkeiten, welche dieses Whitepaper in den Mittelpunkt stellt:

Readiness und **Digitale Souveränität**.

Readiness beschreibt die Fähigkeit einer Organisation, Veränderungen schnell, sicher, resilient und wirksam umzusetzen – unabhängig davon, ob sie durch Business, Technologie, Regulierung oder Künstliche Intelligenz ausgelöst werden.

Digitale Souveränität beschreibt die Fähigkeit einer Organisation, auch in einer hochgradig vernetzten digitalen Welt jederzeit selbstbestimmt handeln zu können. Sie bedeutet nicht, alles selbst zu betreiben. Sie bedeutet, jederzeit die Kontrolle über Daten, Identitäten, Plattformen, AI-Systeme, Entscheidungen und kritische digitale Fähigkeiten zu behalten.

Beide Begriffe ergänzen sich.

Readiness schafft die Fähigkeit zur Veränderung.

Digitale Souveränität stellt sicher, dass diese Veränderung kontrolliert und verantwortungsvoll erfolgt.

Zusammen bilden sie das Fundament eines modernen Operating Models.

Dieses Whitepaper beschreibt deshalb kein weiteres Framework neben ITIL®, COBIT®, IT4IT™, ISO/IEC 27001 oder anderen etablierten Best Practices. Vielmehr zeigt es auf, wie sich diese bewährten Ansätze zu einem integrierten Führungs- und Steuerungsmodell verbinden lassen.

Im Mittelpunkt steht das **Readiness Framework** – ein Next Generation IT Operating Model, das Governance, Wertströme, Plattformen und Capabilities, Informationsmanagement, Sicherheit, Resilienz, Digitale Souveränität und Künstliche Intelligenz zu einem ganzheitlichen Managementsystem zusammenführt.

Ziel dieses Frameworks ist nicht eine möglichst agile oder möglichst effiziente IT.

Ziel ist eine Organisation, die dauerhaft handlungsfähig bleibt.

Eine Organisation, die Innovation beschleunigen kann, ohne Stabilität zu verlieren.

Eine Organisation, die AI verantwortungsvoll nutzt, ohne die Kontrolle aufzugeben.

Eine Organisation, die regulatorische Anforderungen erfüllt, ohne ihre Innovationskraft einzuschränken.

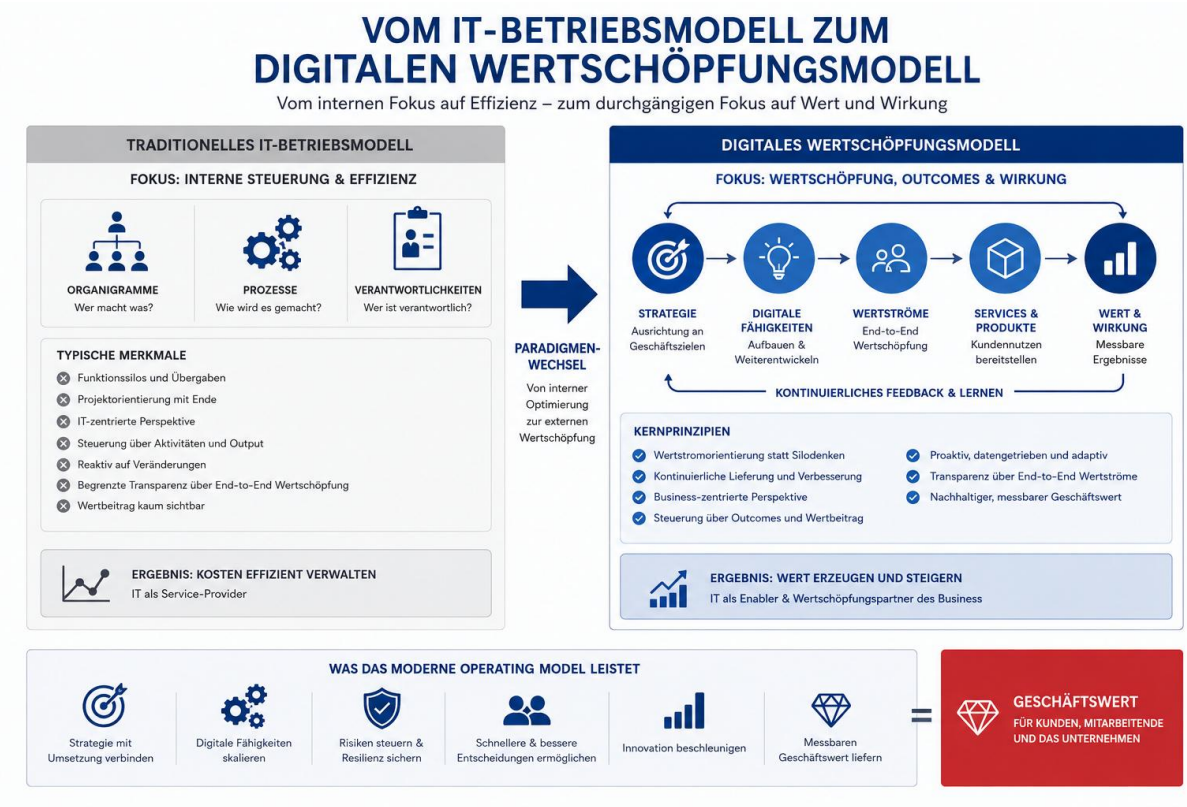
Kurz gesagt: eine Organisation mit hoher **Readiness** und hoher **Digitaler Souveränität**.

Ich bin überzeugt, dass genau diese beiden Fähigkeiten in den kommenden Jahren über den Erfolg digitaler Unternehmen entscheiden werden. Nicht die modernste Technologie wird den Unterschied machen, sondern die Fähigkeit einer Organisation, Veränderungen sicher, wirksam und selbstbestimmt zu gestalten.

Mit diesem Whitepaper möchte ich einen Beitrag dazu leisten und einen Orientierungsrahmen bieten, wie ein solches Next Generation IT Operating Model aufgebaut werden kann.

Martin Andenmatten
Gründer & Managing Director, Glenfis AG · Zürich, im Juli 2026

1 Die grösste Herausforderung ist nicht die Technologie



Der Wandel: vom klassischen IT-Betriebsmodell zum digitalen Wertschöpfungsmodell.

Unternehmen investieren heute mehr denn je in digitale Technologien. Cloud-Plattformen, Generative AI, Data Analytics, Cyber Security, Automatisierung und Plattformökosysteme versprechen höhere Effizienz, schnellere Innovation und neue Geschäftsmodelle. Gleichzeitig entstehen laufend neue regulatorische Anforderungen wie DORA, NIS2 oder der EU AI Act, welche Unternehmen zu mehr Transparenz, Resilienz und Kontrolle verpflichten.

Noch nie standen Organisationen so viele technologische Möglichkeiten zur Verfügung.

Und dennoch fällt es vielen Unternehmen schwer, den erwarteten Nutzen daraus nachhaltig zu realisieren.

Der Grund liegt erstaunlicherweise selten in der Technologie selbst.

Die meisten Unternehmen verfügen heute über leistungsfähige Cloud-Plattformen, moderne Entwicklungswerkzeuge und hochautomatisierte Infrastrukturen. Was häufig fehlt, ist die Fähigkeit der Organisation, diese Technologien dauerhaft wirksam zu nutzen, sicher zu betreiben und kontinuierlich weiterzuentwickeln.

Die eigentliche Herausforderung der digitalen Transformation liegt deshalb heute nicht mehr in der Technologie.

Sie liegt in der Organisation.

Die Komplexität wächst schneller als die Organisation

Während sich Technologien in immer kürzeren Innovationszyklen weiterentwickeln, bleiben viele Organisationsmodelle nahezu unverändert. Sie wurden für eine Zeit entwickelt, in der Projekte klar abgegrenzt waren, Anwendungen überwiegend lokal betrieben wurden und Veränderungen in grossen Releases erfolgten.

Diese Welt existiert heute kaum noch.

Digitale Produkte entwickeln sich kontinuierlich weiter. Cloud-Plattformen werden permanent erweitert. AI-Modelle verändern sich laufend. Unternehmen arbeiten mit einer Vielzahl externer Partner zusammen und digitale Services entstehen in komplexen Netzwerken aus Plattformen, Providern und spezialisierten Dienstleistern.

Dadurch verändert sich nicht nur die technologische Landschaft.

Es verändert sich die Art, wie Unternehmen geführt werden müssen.

Die Herausforderung besteht heute darin, Entscheidungen schneller zu treffen und gleichzeitig Risiken besser zu kontrollieren. Unternehmen müssen Innovation beschleunigen und gleichzeitig Informationssicherheit gewährleisten. Sie müssen regulatorische Anforderungen erfüllen, ohne ihre Lieferfähigkeit einzuschränken. Und sie müssen AI produktiv einsetzen, ohne Transparenz oder Verantwortlichkeit zu verlieren.

Diese scheinbaren Gegensätze lassen sich nicht mehr durch einzelne Projekte oder neue Technologien lösen.

Sie verlangen ein neues Organisationsmodell.

Warum Agilität allein nicht mehr genügt

Über viele Jahre galt Agilität als das wichtigste Ziel moderner IT-Organisationen. Agile Methoden, DevOps und Continuous Delivery haben Unternehmen geholfen, Software schneller bereitzustellen und näher an den Bedürfnissen ihrer Kunden zu entwickeln.

Diese Entwicklung war notwendig und erfolgreich.

Heute zeigt sich jedoch, dass Geschwindigkeit allein kein ausreichendes Ziel mehr ist.

Eine Organisation kann noch so agil arbeiten – wenn sie ihre Informationswerte nicht kennt, AI-Systeme nicht kontrollieren kann, regulatorische Anforderungen nicht erfüllt oder bei einem Cyberangriff ihre Handlungsfähigkeit verliert, entsteht kein nachhaltiger Wettbewerbsvorteil.

Die Anforderungen an moderne Unternehmen haben sich grundlegend verändert.

Nicht nur Geschwindigkeit entscheidet über den Erfolg.

Ebenso wichtig sind Transparenz, Resilienz, Sicherheit, Nachvollziehbarkeit und die Fähigkeit, Veränderungen dauerhaft zu beherrschen.

Genau deshalb reicht Agilität als Leitbild nicht mehr aus.

Readiness wird zur neuen Kernfähigkeit

Dieses Whitepaper führt deshalb einen Begriff ein, der die heutigen Anforderungen umfassender beschreibt:

Readiness.

Readiness ist die Fähigkeit einer Organisation, Veränderungen schnell, sicher, resilient und wirksam umzusetzen – unabhängig davon, ob sie durch Business, Technologie, Regulierung oder Künstliche Intelligenz ausgelöst werden.

Readiness verbindet Eigenschaften, die bislang häufig getrennt betrachtet wurden. Sie vereint Agilität mit Governance, Innovationsfähigkeit mit Sicherheit, Geschwindigkeit mit Resilienz und Autonomie mit Transparenz.

Eine Organisation mit hoher Readiness ist jederzeit in der Lage, neue Technologien einzuführen, regulatorische Veränderungen umzusetzen, Cyberrisiken zu beherrschen oder AI verantwortungsvoll einzusetzen, ohne ihre Stabilität oder ihre digitale Souveränität zu gefährden.

Readiness beschreibt damit nicht einen einmal erreichten Zielzustand.

Sie beschreibt eine dauerhafte organisatorische Fähigkeit.

Ein neues Verständnis des Operating Models

Wenn Readiness das eigentliche Ziel ist, verändert sich auch die Rolle des Operating Models.

Ein Operating Model beschreibt nicht mehr lediglich Organisationsstrukturen, Prozesse oder Rollen. Es wird zum Managementsystem der digitalen Organisation. Es definiert, wie Entscheidungen getroffen werden, wie Wert entsteht, wie Risiken gesteuert werden und wie sich die Organisation kontinuierlich an neue Rahmenbedingungen anpasst.

Genau hier setzt das **Readiness Framework** an.

Es verbindet Governance, Wertströme, Plattformen und organisatorische Capabilities, Informationsmanagement, Sicherheit, Resilienz, Digitale Souveränität und Künstliche Intelligenz zu einem integrierten Führungs- und Steuerungsmodell.

Jedes dieser Elemente trägt dazu bei, die organisationale Readiness zu erhöhen.

Erst ihr Zusammenspiel ermöglicht es Unternehmen, auch unter den Bedingungen einer zunehmend digitalen, vernetzten und AI-gestützten Welt dauerhaft handlungsfähig zu bleiben.

Die folgenden Kapitel zeigen deshalb nicht nur, wie ein modernes Operating Model aufgebaut ist. Sie zeigen vor

allem, **welche organisatorischen Fähigkeiten notwendig sind, um Readiness systematisch aufzubauen und kontinuierlich weiterzuentwickeln**.

2 Vom IT Operating Model zum Readiness Framework

Das Readiness Framework: Governance, Wertströme, Plattformen, Informationen, Resilienz und Digitale Souveränität im Zusammenspiel.

Wenn heute über ein IT Operating Model gesprochen wird, denken viele zunächst an Organigramme, Prozesse oder Rollen. Tatsächlich beschreibt ein modernes Operating Model jedoch weit mehr. Es definiert, wie Entscheidungen getroffen werden, wie digitale Fähigkeiten entstehen, wie Risiken gesteuert werden und wie aus Technologie nachhaltiger Geschäftswert entsteht.

Genau deshalb genügt es heute nicht mehr, lediglich eine moderne IT-Organisation aufzubauen.

Die eigentliche Aufgabe besteht darin, eine Organisation zu schaffen, die sich kontinuierlich an neue Rahmenbedingungen anpassen kann, ohne ihre Stabilität, Sicherheit oder Steuerbarkeit zu verlieren.

Ein modernes Operating Model wird damit zum Fundament organisationaler Readiness.

Die digitale Organisation verändert sich grundlegend

Über viele Jahre stand die IT vor allem für den zuverlässigen Betrieb technischer Systeme. Anwendungen wurden entwickelt, eingeführt und anschliessend über Jahre hinweg betrieben. Projekte hatten einen klaren Anfang und ein definiertes Ende. Veränderungen erfolgten in planbaren Zyklen.

Dieses Organisationsmodell passt immer weniger zur heutigen Realität.

Digitale Produkte entwickeln sich kontinuierlich weiter. Cloud-Plattformen werden permanent erweitert. Sicherheitsbedrohungen verändern sich täglich. AI-Modelle müssen laufend überwacht und angepasst werden. Gleichzeitig entstehen neue regulatorische

Anforderungen, welche Unternehmen jederzeit nachweisen müssen.

Die digitale Organisation befindet sich damit in einem permanenten Veränderungsprozess.

Ein Operating Model kann deshalb nicht mehr als statische Organisationsbeschreibung verstanden werden.

Es muss selbst lernfähig und anpassungsfähig sein.

Ein Operating Model beschreibt nicht die Organisation – sondern ihre Fähigkeiten

Vielleicht liegt genau hier das grösste Missverständnis.

Viele Unternehmen verstehen ein Operating Model noch immer als Beschreibung ihrer Aufbauorganisation. Sie definieren Verantwortlichkeiten, zeichnen Organigramme und dokumentieren Prozesse.

All dies bleibt wichtig.

Es beantwortet jedoch nicht die entscheidende Frage:

Wie gelingt es einer Organisation, Veränderungen dauerhaft erfolgreich umzusetzen?

Ein Next Generation IT Operating Model beschreibt deshalb nicht in erster Linie Strukturen.

Es beschreibt organisatorische Fähigkeiten.

Welche Fähigkeiten benötigt eine Organisation, um neue Technologien sicher einzuführen?

Wie gelingt es, regulatorische Anforderungen effizient umzusetzen?

Wie entstehen digitale Produkte kontinuierlich weiter?

Wie werden Risiken gesteuert?

Wie bleiben Entscheidungen nachvollziehbar?

Wie kann AI verantwortungsvoll integriert werden?

Das eigentliche Ziel besteht nicht darin, Prozesse möglichst effizient zu gestalten.

Das Ziel besteht darin, die organisationale Readiness kontinuierlich zu erhöhen.

Vom Betriebsmodell zum Managementsystem

Damit verändert sich auch die Rolle des Operating Models.

Es beschreibt nicht mehr ausschliesslich den Betrieb der IT.

Es entwickelt sich zum Managementsystem der digitalen Organisation.

Es verbindet Unternehmensstrategie mit operativer Umsetzung. Es schafft gemeinsame Entscheidungsprinzipien, definiert Verantwortlichkeiten und integriert Governance, Wertströme, Plattformen, Informationsmanagement, Sicherheit und AI in ein gemeinsames Führungsmodell.

Dadurch entsteht eine Organisation, welche Veränderungen nicht nur bewältigt, sondern gezielt gestaltet.

Readiness wird damit nicht durch einzelne Projekte erreicht.

Sie entsteht durch das Zusammenspiel sämtlicher organisatorischer Fähigkeiten.

Readiness entsteht nicht zufällig

Viele Unternehmen reagieren auf neue Anforderungen mit Einzelmassnahmen.

Sie führen Cloud Governance ein.

Sie etablieren DevSecOps.

Sie investieren in Plattformen.

Sie entwickeln AI-Richtlinien.

Oder sie setzen neue regulatorische Vorgaben um.

Jede dieser Massnahmen ist sinnvoll.

Für sich allein genügt sie jedoch nicht.

Readiness entsteht nicht durch isolierte Initiativen.

Sie entsteht erst dann, wenn sämtliche organisatorischen Fähigkeiten zu einem integrierten Gesamtsystem zusammenwirken.

Governance definiert den gemeinsamen Handlungsrahmen.

Wertströme verbinden Strategie, Entwicklung und Betrieb.

Plattformen schaffen wiederverwendbare Fähigkeiten.

Informationsmanagement sorgt für Transparenz.

Resilienz gewährleistet Stabilität.

Digitale Souveränität erhält die strategische Handlungsfähigkeit.

© 2026 Glenfis AG · Next Generation IT Operating Model

AI erweitert die Organisation um intelligente digitale Akteure.

Erst das Zusammenspiel dieser Elemente macht eine Organisation dauerhaft handlungsfähig.

Genau dieses Zusammenspiel beschreibt das **Readiness Framework**.

Das Readiness Framework

Das in diesem Whitepaper vorgestellte Framework versteht ein Next Generation IT Operating Model deshalb als integriertes Managementsystem.

Im Zentrum stehen digitale Produkte und Services, welche entlang durchgängiger Wertströme entstehen und betrieben werden. Governance verbindet Unternehmensstrategie mit operativer Umsetzung. Plattformen stellen wiederverwendbare organisatorische und technische Fähigkeiten bereit. Informationsmanagement schafft Transparenz. Sicherheit und Resilienz werden zu integralen Eigenschaften jeder Capability. Digitale Souveränität sorgt dafür, dass die Organisation trotz wachsender Abhängigkeiten jederzeit selbstbestimmt handeln kann. AI erweitert das Operating Model schliesslich um intelligente digitale Akteure, welche künftig aktiv an der Wertschöpfung teilnehmen.

Jede dieser Fähigkeiten trägt zur Readiness der Organisation bei.

Gemeinsam bilden sie das Fundament des Readiness Frameworks, das nicht nur den Betrieb der IT beschreibt, sondern die kontinuierliche Veränderungsfähigkeit der gesamten digitalen Organisation sicherstellt.

Damit verändert sich auch die Perspektive auf das Operating Model selbst.

Es ist nicht länger das Ziel der Transformation.

Es ist das Instrument, mit dem Unternehmen ihre Readiness systematisch aufbauen und dauerhaft weiterentwickeln.

DREI BEGRIFFE – KLAR UNTERSCHIEDEN

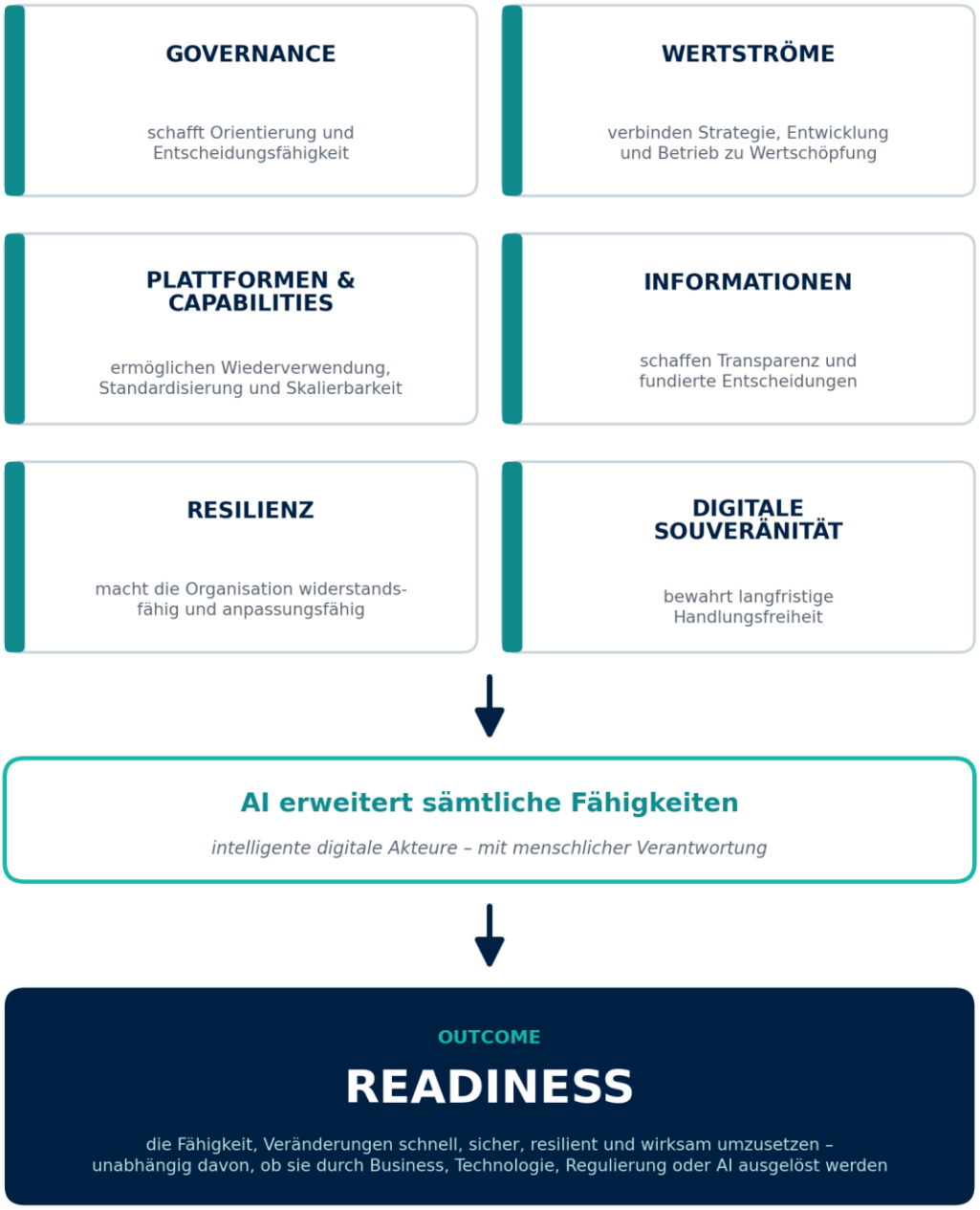
Next Generation IT Operating Model beschreibt das Zielbild der digitalen Organisation.

Readiness Framework beschreibt das Managementmodell und die Methode, mit der dieses Zielbild erreicht wird.

Readiness beschreibt die Managementfähigkeit – den Outcome, an dem sich der Erfolg misst.

DAS READINESS FRAMEWORK

Readiness entsteht aus dem Zusammenspiel von sechs organisatorischen Fähigkeiten



Next Generation IT Operating Model
das Zielbild der digitalen Organisation

Readiness Framework
das Managementmodell und die Methode

Readiness
die Managementfähigkeit – der Outcome

3 Governance schafft Readiness

Governance als Betriebssystem der digitalen Organisation.

Kaum ein Begriff wird in der IT so unterschiedlich verstanden wie Governance.

Für die einen steht Governance für Richtlinien, Freigaben und Gremien. Andere verbinden damit Kontrolle, Dokumentation oder regulatorische Compliance. Nicht selten gilt Governance sogar als Synonym für Bürokratie – als notwendiges Übel, das Innovation verlangsamt und Agilität behindert.

Dieses Verständnis stammt jedoch aus einer Zeit, in der IT weitgehend zentral gesteuert wurde und Veränderungen vergleichsweise selten waren.

Heute hat sich die Ausgangslage grundlegend verändert.

Digitale Organisationen treffen täglich tausende von Entscheidungen. Neue Cloud-Services werden integriert, AI-Anwendungen eingeführt, regulatorische Anforderungen umgesetzt und digitale Produkte kontinuierlich weiterentwickelt. Gleichzeitig steigen die Erwartungen an Informationssicherheit, Datenschutz, Resilienz und Transparenz. Keine zentrale Organisationseinheit kann diese Entscheidungen mehr vollständig kontrollieren.

Genau deshalb verändert sich die Rolle der Governance.

Ihre Aufgabe besteht heute nicht mehr darin, möglichst viele Entscheidungen selbst zu treffen.

Ihre Aufgabe besteht darin, sicherzustellen, dass überall in der Organisation die richtigen Entscheidungen getroffen werden können.

Governance wird damit zum Fundament organisationaler Readiness.

Readiness braucht Orientierung statt Kontrolle

Eine Organisation mit hoher Readiness zeichnet sich nicht dadurch aus, dass sie möglichst viele Genehmigungen einholt oder Risiken vollständig ausschliesst.

Sie zeichnet sich dadurch aus, dass Mitarbeitende, Teams und künftig auch intelligente AI-Agenten innerhalb klar definierter Leitplanken eigenständig handeln können.

Genau diese Leitplanken schafft Governance.

Sie definiert gemeinsame Ziele, Architekturprinzipien, Sicherheitsstandards, Rollen, Verantwortlichkeiten und

Entscheidungsrechte. Dadurch entsteht ein gemeinsamer Orientierungsrahmen, innerhalb dessen dezentrale Entscheidungen möglich werden.

Je klarer dieser Rahmen definiert ist, desto weniger Abstimmungen werden notwendig.

Governance reduziert deshalb nicht die Geschwindigkeit einer Organisation.

Sie macht nachhaltige Geschwindigkeit überhaupt erst möglich.

Readiness entsteht genau aus diesem Zusammenspiel von Autonomie und Orientierung.

Governance beginnt bei der Unternehmensstrategie

Governance wird häufig erst mit Compliance oder operativen Kontrollen in Verbindung gebracht.

Tatsächlich beginnt sie wesentlich früher.

Bereits auf strategischer Ebene werden die Grundlagen geschaffen, welche den Handlungsspielraum der gesamten Organisation bestimmen.

Welche digitalen Fähigkeiten sollen aufgebaut werden?

Welche Plattformen sind strategisch relevant?

Welche Daten sind geschäftskritisch?

Welche regulatorischen Anforderungen gelten?

Welche Risiken ist das Unternehmen bereit einzugehen?

Welche AI-Anwendungen unterstützen die Unternehmensstrategie?

Aus diesen Entscheidungen entstehen Architekturprinzipien, Investitionsprioritäten und organisatorische Leitplanken, welche sämtliche nachgelagerten Wertströme beeinflussen.

Governance verbindet dadurch Unternehmensstrategie mit operativer Umsetzung und schafft den Rahmen, innerhalb dessen Readiness überhaupt entstehen kann.

Verantwortung ersetzt Hierarchie

Je digitaler Organisationen werden, desto weniger funktionieren sie über klassische Hierarchien.

Digitale Wertschöpfung entsteht heute in Netzwerken aus Produktteams, Plattformteams, externen Partnern und zunehmend auch intelligenten AI-Agenten. Entscheidungen müssen dort getroffen werden, wo das notwendige Wissen vorhanden ist.

Deshalb basiert das Readiness Framework nicht auf zusätzlichen Genehmigungsstufen, sondern auf klarer Verantwortung.

Service Owner verantworten den geschäftlichen Nutzen ihrer Services. Product Owner priorisieren entlang des Kundennutzens. Platform Owner entwickeln organisationsweite Fähigkeiten. Practice Owner sorgen für Standards und kontinuierliche Verbesserung. Enterprise Architecture, Informationssicherheit und Risikomanagement definieren die organisatorischen Leitplanken.

Nicht die Anzahl der Rollen entscheidet über den Erfolg.

Entscheidend ist, dass Verantwortung eindeutig zugeordnet und jederzeit nachvollziehbar ist.

Denn Readiness setzt voraus, dass Entscheidungen schnell getroffen und gleichzeitig verantwortet werden können.

Governance wird zur Plattformfähigkeit

Eine der grössten Veränderungen moderner Organisationen besteht darin, dass Governance zunehmend in digitale Plattformen integriert wird.

Früher wurden Richtlinien dokumentiert und anschliessend manuell überprüft.

Heute werden viele dieser Regeln unmittelbar Bestandteil der technischen Plattformen.

Identitätsmanagement, Infrastrukturstandards, Security Policies, Compliance-Anforderungen oder Architekturvorgaben stehen den Teams als automatisierte Guardrails zur Verfügung. Entscheidungen werden dadurch nicht langsamer, sondern konsistenter.

Governance wird nicht mehr ausschliesslich beschrieben.

Sie wird ausführbar.

Dieser Wandel erhöht die Readiness erheblich, weil organisatorisches Wissen unmittelbar in die tägliche Arbeit integriert wird.

Realtime Observability wird zur Grundlage wirksamer Governance

Governance kann ihre Wirkung jedoch nur entfalten, wenn die Organisation jederzeit weiss, was tatsächlich geschieht.

Früher reichten periodische Reports, Audits oder Management-Reviews aus. Heute entstehen Risiken und

Veränderungen in Echtzeit. Cloud-Plattformen verändern sich kontinuierlich. Neue AI-Modelle werden produktiv eingesetzt. Cyberangriffe entwickeln sich innerhalb weniger Minuten.

Governance benötigt deshalb ein permanentes Lagebild.

Observability entwickelt sich von einem Betriebswerkzeug zu einer strategischen Managementfähigkeit. Informationen über Services, Plattformen, Sicherheitskontrollen, Datenflüsse, AI-Systeme und regulatorische Anforderungen werden kontinuierlich zusammengeführt und ausgewertet.

Dadurch entsteht eine Governance, die nicht auf Vermutungen oder periodischen Kontrollen basiert, sondern auf belastbaren Informationen.

Erst diese Transparenz ermöglicht eine belastbare Compliance, eine wirksame Steuerung und fundierte Managemententscheidungen.

Governance steuert künftig auch intelligente Organisationen

Mit Generativer AI und insbesondere Agentic AI beginnt bereits heute die nächste Evolutionsstufe.

Erstmals entstehen digitale Akteure, welche innerhalb definierter Grenzen eigenständig planen, Werkzeuge nutzen, Entscheidungen vorbereiten oder Prozesse auslösen können.

Governance steuert deshalb künftig nicht mehr ausschliesslich Menschen.

Sie steuert hybride Organisationen.

AI-Agenten benötigen eigene Identitäten, Berechtigungen, Verantwortlichkeiten und Kontrollmechanismen. Gleichzeitig muss jederzeit nachvollziehbar bleiben, welche Entscheidungen von Menschen getroffen wurden, welche durch AI vorbereitet wurden und welche vollständig automatisiert erfolgt sind.

Governance erweitert sich dadurch zu einer Steuerungsschicht für Menschen, Plattformen und intelligente Agenten.

Gerade deshalb wird Governance in Zukunft wichtiger denn je.

Governance wird zum Betriebssystem der digitalen Organisation

Vielleicht lässt sich die Rolle moderner Governance am besten mit einem Betriebssystem vergleichen.

Ein Betriebssystem schreibt einem Computer nicht vor, welche Anwendungen ausgeführt werden sollen. Es verwaltet Ressourcen, schützt Informationen, steuert Zugriffe und stellt sicher, dass sämtliche Komponenten zuverlässig zusammenarbeiten.

Genau dieselbe Aufgabe übernimmt Governance innerhalb einer digitalen Organisation.

Sie verbindet Unternehmensstrategie, Wertströme, Plattformen, Informationsmanagement, Sicherheit, Resilienz und AI zu einem integrierten Führungs- und Steuerungssystem.

Sie schafft Transparenz.

Sie definiert Verantwortung.

Sie ermöglicht dezentrale Entscheidungen.

Sie erzeugt Vertrauen.

Und sie stellt sicher, dass die Organisation auch unter sich ständig verändernden Rahmenbedingungen handlungsfähig bleibt.

Governance ist deshalb nicht der Gegenpol zur Agilität.

Governance ist die Grundlage organisationaler Readiness.

Denn nur Organisationen mit klaren Leitplanken, belastbaren Informationen und eindeutigen Verantwortlichkeiten können Veränderungen schnell, sicher und souverän gestalten.

Genau darin liegt die eigentliche Aufgabe eines **Readiness Frameworks**.

Governance erhöht nicht nur die Readiness der Organisation. Sie stärkt gleichzeitig ihre Digitale Souveränität – denn nur wer Ziele, Leitplanken und Verantwortlichkeiten selbst definiert, bleibt jederzeit steuerungs- und entscheidungsfähig.

4 Wertströme schaffen Readiness

Von der funktionalen Organisation zu durchgängigen End-to-End-Wertströmen.

Über viele Jahre haben Unternehmen versucht, ihre IT durch neue Organisationsformen leistungsfähiger zu machen. Abteilungen wurden zusammengelegt, agile Teams eingeführt, Verantwortlichkeiten neu verteilt und Prozesse optimiert. Dennoch stellte sich häufig Ernüchterung ein. Obwohl sich die Organisation veränderte, blieb die eigentliche Leistungsfähigkeit weitgehend unverändert.

Der Grund dafür liegt nicht in den Menschen oder in den gewählten Organisationsformen.

Er liegt darin, dass sich zwar die Struktur verändert hat, nicht jedoch die Art und Weise, wie Wert innerhalb der Organisation entsteht.

Das Readiness Framework beginnt deshalb nicht beim Organigramm.

Es beginnt beim Fluss der Wertschöpfung.

Wert entsteht zwischen den Organisationseinheiten

Die meisten Unternehmen sind bis heute funktional organisiert. Infrastruktur, Softwareentwicklung, Architektur, Informationssicherheit, Service Management oder Betrieb verfolgen jeweils eigene Ziele und verfügen über hohe fachliche Kompetenz.

Aus Sicht der einzelnen Bereiche funktioniert dieses Modell häufig sehr gut.

Aus Sicht des Business entsteht jedoch ein anderes Bild.

Eine neue Geschäftsidee durchläuft zahlreiche organisatorische Stationen, bevor daraus ein produktiver digitaler Service entsteht. Anforderungen werden analysiert, priorisiert, entwickelt, getestet, freigegeben, implementiert und schliesslich betrieben. Jede Übergabe zwischen zwei Organisationseinheiten erzeugt Abstimmungsaufwand, Wartezeiten und Informationsverluste.

Mit jeder zusätzlichen Schnittstelle nimmt die Komplexität zu.

Die eigentliche Herausforderung liegt deshalb nicht innerhalb der einzelnen Teams.

Sie liegt zwischen ihnen.

Readiness entsteht durch den kontinuierlichen Fluss von Wert

Ein Next Generation IT Operating Model organisiert die IT deshalb nicht mehr entlang organisatorischer Zuständigkeiten.

Es organisiert sie entlang des kontinuierlichen Flusses der Wertschöpfung.

Der Ausgangspunkt ist immer ein geschäftlicher Bedarf. Daraus entstehen Investitionsentscheidungen, Architekturkonzepte, Anforderungen, digitale Produkte, Services und schliesslich betriebliche Leistungen für Kunden und Mitarbeitende. Gleichzeitig liefern Monitoring, Betrieb und Nutzerfeedback kontinuierlich neue Erkenntnisse, welche wiederum in die Weiterentwicklung einfliessen.

Damit entsteht ein geschlossener Regelkreis.

Strategie beeinflusst die Umsetzung.

Die Umsetzung erzeugt neue Erkenntnisse.

Diese Erkenntnisse verändern wiederum Strategie, Produkte und Services.

Das Readiness Framework bildet genau diesen Kreislauf ab.

Readiness entsteht dadurch nicht erst im Betrieb.

Sie entsteht entlang des gesamten Wertstroms.

Der Service Lifecycle wird zum Ordnungsprinzip

Diese Sichtweise verändert die Rolle der IT grundlegend.

Früher endete die Verantwortung häufig mit dem Abschluss eines Projekts. Danach übernahm der Betrieb. Neue Anforderungen wurden wiederum in neue Projekte überführt.

Heute existiert diese Trennung kaum noch.

Digitale Produkte entwickeln sich kontinuierlich weiter. Sicherheitsanforderungen verändern sich permanent. Cloud-Plattformen werden laufend erweitert. AI-Modelle müssen überwacht und verbessert werden. Der Betrieb liefert täglich neue Erkenntnisse für Entwicklung, Architektur und Portfolio.

Ein moderner digitaler Service besitzt deshalb keinen definierten Endpunkt.

Er befindet sich in einem permanenten Lebenszyklus.

Von der strategischen Planung.

Über Entwicklung und Bereitstellung.

Bis zum Betrieb.

Und wieder zurück zur kontinuierlichen Weiterentwicklung.

Der Service Lifecycle wird damit zum eigentlichen Ordnungsprinzip der gesamten Organisation.

IT4IT liefert den Ordnungsrahmen

Ein besonders konsequentes Referenzmodell für diese Sichtweise liefert IT4IT® der Open Group.

Im Gegensatz zu klassischen Prozessmodellen beschreibt IT4IT nicht primär organisatorische Abläufe, sondern den Fluss von Informationen, Entscheidungen und Wert innerhalb einer digitalen Organisation.

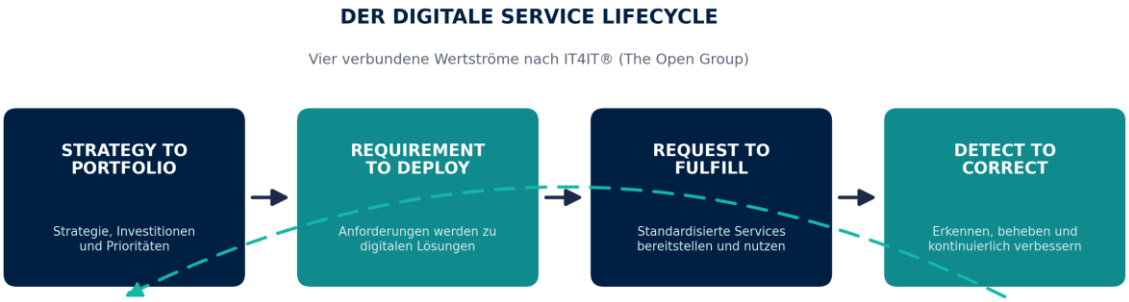
Im Mittelpunkt stehen vier miteinander verbundene Wertströme.

Der erste verbindet Unternehmensstrategie mit Portfolioentscheidungen und schafft die Grundlage für Investitionen und Prioritäten. Darauf aufbauend werden Anforderungen in digitale Lösungen umgesetzt. Anschliessend werden diese Lösungen als standardisierte Services bereitgestellt und betrieben. Der vierte Wertstrom sorgt schliesslich dafür, dass Ereignisse, Störungen und neue Erkenntnisse kontinuierlich in Verbesserungen einfliessen.

Diese vier Wertströme ersetzen keine Prozesse.

Sie verbinden Prozesse, Rollen, Informationen, Plattformen und Technologien zu einem durchgängigen Steuerungsmodell.

Genau diese Logik bildet auch das Readiness Framework ab.



Die vier Wertströme des digitalen Service Lifecycles nach IT4IT® (The Open Group).

Wertströme schaffen Transparenz

Mit zunehmender Digitalisierung steigt die Zahl der Abhängigkeiten innerhalb einer Organisation erheblich.

Geschäftsprozesse, Cloud-Plattformen, AI-Services, Datenplattformen, externe Provider und regulatorische Anforderungen greifen permanent ineinander.

Dadurch wird Transparenz zur eigentlichen Grundlage organisationaler Steuerung.

Welche Geschäftsanforderung hat zu einer bestimmten Funktion geführt?

Welche Architekturentscheidung beeinflusst einen kritischen Service?

Welche AI-Komponente verarbeitet welche Informationen?

Welche regulatorischen Anforderungen gelten entlang des gesamten Lebenszyklus?

Welche Auswirkungen hat eine Änderung auf andere Services?

Ein wertstromorientiertes Operating Model beantwortet diese Fragen nicht über Dokumente oder Organigramme.

Es beantwortet sie über eine durchgängige Informationsarchitektur.

Dadurch entsteht eine End-to-End-Traceability, welche für Governance, Informationssicherheit, Compliance und operative Resilienz unverzichtbar wird.

Readiness benötigt genau diese Transparenz.

Denn nur wer den gesamten Wertstrom versteht, kann Veränderungen kontrolliert steuern.

Wertströme verbinden Menschen, Plattformen und AI

Mit Generativer AI und insbesondere Agentic AI verändert sich die digitale Wertschöpfung erneut grundlegend.

AI unterstützt heute bereits die Analyse von Anforderungen, Architekturentwürfe, Softwareentwicklung, Testautomatisierung, Dokumentation oder den Service Desk. Zukünftig werden intelligente Agenten ganze Abschnitte eines Wertstroms eigenständig koordinieren. Sie priorisieren Anforderungen, erzeugen Testfälle, überwachen Services, analysieren Sicherheitsereignisse oder schlagen Optimierungen vor.

Dadurch entstehen völlig neue Informationsflüsse.

Das Readiness Framework muss künftig nicht nur menschliche Zusammenarbeit organisieren.

Es muss die Zusammenarbeit zwischen Menschen, Plattformen und intelligenten Agenten steuern.

Wertströme werden dadurch zur gemeinsamen Sprache einer hybriden Organisation.

Wertströme schaffen organisationale Readiness

Vielleicht liegt genau hier der grösste Unterschied zwischen klassischen und modernen Operating Models.

Früher optimierten Unternehmen einzelne Prozesse oder Organisationseinheiten.

Heute optimieren sie den kontinuierlichen Fluss der Wertschöpfung.

Denn Veränderungen entstehen niemals innerhalb eines einzelnen Teams.

Sie durchlaufen immer den gesamten Lebenszyklus eines digitalen Services.

Ein wertstromorientiertes Operating Model sorgt deshalb dafür, dass Strategie, Governance, Architektur, Entwicklung, Betrieb, Informationssicherheit und AI nicht nebeneinander arbeiten, sondern gemeinsam Wert erzeugen.

Genau dadurch entsteht organisationale Readiness.

Veränderungen werden schneller umgesetzt.

Risiken früher erkannt.

Abhängigkeiten transparenter.

Entscheidungen nachvollziehbarer.

Und Innovationen können kontinuierlich erfolgen, ohne Stabilität oder Sicherheit zu gefährden.

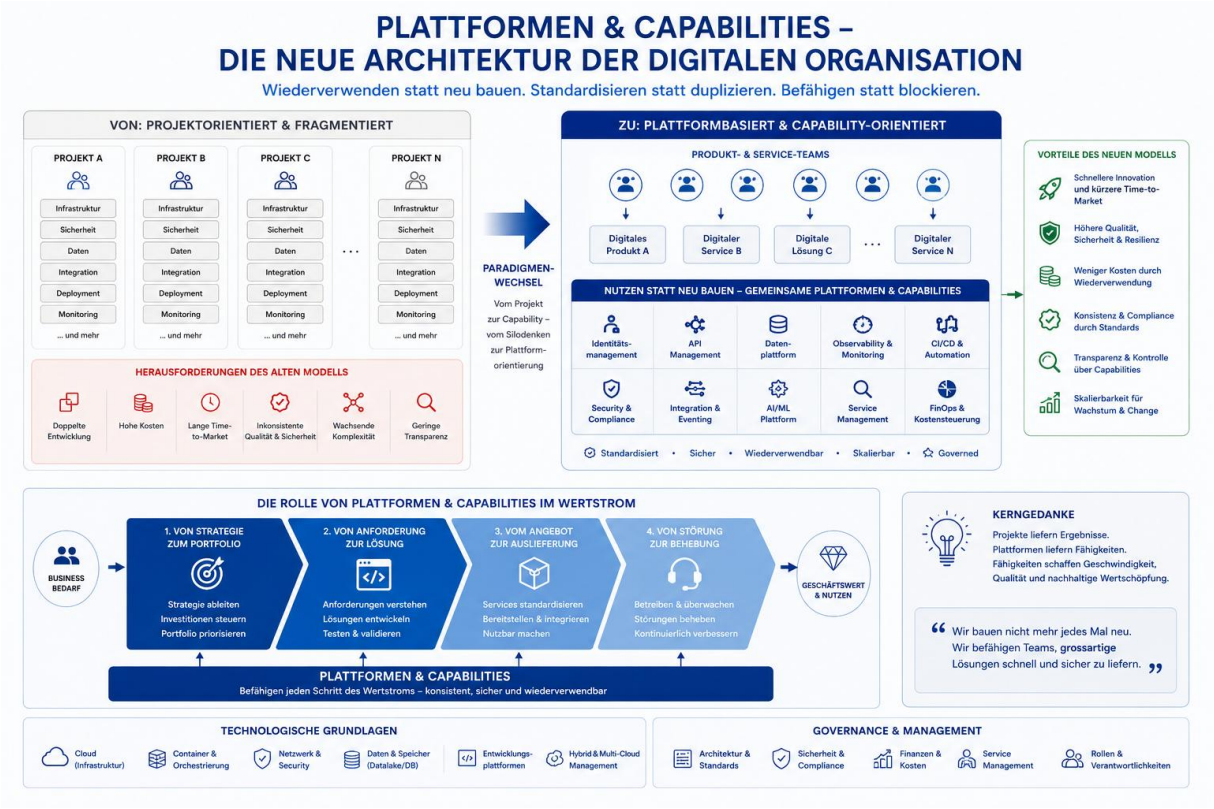
Wertströme organisieren deshalb nicht nur digitale Arbeit.

Sie schaffen die Fähigkeit einer Organisation, Veränderungen dauerhaft, sicher und wirksam zu bewältigen.

Sie schaffen Readiness.

> **Wertströme erhöhen nicht nur die Readiness der Organisation. Sie stärken gleichzeitig ihre Digitale Souveränität – denn nur wer seine Wertschöpfung Ende-zu-Ende versteht, behält die Kontrolle über Abhängigkeiten, Daten und Entscheidungen.**

5 Plattformen und Capabilities schaffen Readiness



Der Paradigmenwechsel: von Projekten zu Plattformen und organisatorischen Capabilities.

Nachdem Wertströme beschreiben, **wie** digitale Wertschöpfung entsteht, stellt sich unmittelbar die nächste Frage:

Wodurch wird diese Wertschöpfung eigentlich ermöglicht?

Die Antwort darauf verändert moderne Organisationen derzeit grundlegend.

Über viele Jahre wurden digitale Lösungen überwiegend projektorientiert entwickelt. Jedes Projekt brachte seine eigene Infrastruktur mit, implementierte individuelle Sicherheitsmechanismen, entwickelte eigene Schnittstellen und löste ähnliche Probleme immer wieder neu. Mit jedem erfolgreichen Projekt wuchs gleichzeitig die Komplexität der IT-Landschaft. Neue Technologien entstanden, bestehende Lösungen wurden erweitert und organisatorisches Wissen verteilte sich zunehmend auf einzelne Teams.

Dieses Modell funktionierte, solange Veränderungen vergleichsweise selten waren.

Für eine Organisation, die sich kontinuierlich weiterentwickeln muss, ist es jedoch nicht mehr ausreichend.

Das Readiness Framework verfolgt deshalb einen grundlegend anderen Ansatz.

Es organisiert nicht mehr Projekte.

Es organisiert organisatorische Fähigkeiten.

Plattformen sind organisatorische Fähigkeiten

Der Begriff Plattform wird häufig auf Cloud-Infrastrukturen oder technische Laufzeitumgebungen reduziert. Tatsächlich beschreibt eine Plattform jedoch wesentlich mehr.

Eine Plattform stellt einer Organisation Fähigkeiten zur Verfügung, welche von vielen Teams gemeinsam genutzt werden können. Sie übernimmt Aufgaben, die nicht jedes Produktteam selbst lösen sollte, und schafft dadurch die Voraussetzungen für Geschwindigkeit, Konsistenz und Skalierbarkeit.

Dazu gehören technische Fähigkeiten wie Identitätsmanagement, API-Management, CI/CD, Datenplattformen oder Observability ebenso wie organisatorische Fähigkeiten, beispielsweise Service Management, Architekturstandards, Governance oder Informationssicherheit.

Plattformen standardisieren deshalb nicht einzelne Technologien.

Sie standardisieren die Art und Weise, wie digitale Wertschöpfung entsteht.

Genau dadurch reduzieren sie Komplexität und erhöhen gleichzeitig die Fähigkeit einer Organisation, Veränderungen schnell und sicher umzusetzen.

Der eigentliche Wandel betrifft die organisatorischen Capabilities

Vielleicht liegt hier einer der grössten Paradigmenwechsel moderner Operating Models.

Über Jahrzehnte standen Projekte im Mittelpunkt der Organisation. Projekte erhielten Budgets, wurden umgesetzt und nach ihrer Einführung wieder aufgelöst.

Heute entwickeln sich digitale Produkte kontinuierlich weiter. Gleichzeitig entstehen Fähigkeiten, die unabhängig von einzelnen Produkten dauerhaft benötigt werden.

Ein leistungsfähiges Identitätsmanagement wird von nahezu allen digitalen Services genutzt.

Dasselbe gilt für Observability, Logging, API-Management, Datenplattformen, Deployment, AI-Plattformen oder Governance Services.

Diese Fähigkeiten entwickeln sich kontinuierlich weiter und stehen der gesamten Organisation zur Verfügung.

Sie besitzen einen eigenen Lebenszyklus.

Sie verfügen über Verantwortliche.

Sie werden gemessen.

Und sie werden permanent verbessert.

Ein Next Generation IT Operating Model betrachtet diese Fähigkeiten deshalb nicht mehr als technische Komponenten.

Es versteht sie als organisatorische Capabilities.

Capabilities schaffen Readiness

Readiness entsteht nicht dadurch, dass jede Organisationseinheit sämtliche Fähigkeiten selbst entwickelt.

Readiness entsteht durch Wiederverwendung.

Je mehr organisatorische Fähigkeiten als standardisierte Capabilities zur Verfügung stehen, desto schneller kann die Organisation auf neue Anforderungen reagieren.

Neue regulatorische Vorgaben müssen nicht für jedes Projekt neu interpretiert werden.

Neue Sicherheitsmechanismen werden einmal entwickelt und organisationsweit genutzt.

Neue AI-Funktionen stehen sämtlichen Produktteams gleichzeitig zur Verfügung.

Neue Plattformdienste können unmittelbar in bestehende Wertströme integriert werden.

Dadurch sinkt nicht nur die Komplexität.

Auch die Qualität steigt.

Veränderungen werden schneller.

Risiken werden geringer.

Innovationen lassen sich wesentlich einfacher skalieren.

Plattformen schaffen dadurch nicht nur Effizienz.

Sie erhöhen die organisationale Readiness.

Plattformen verbinden Governance mit Delivery

Besonders interessant wird diese Entwicklung dort, wo Governance unmittelbar Bestandteil der Plattformen wird.

Architekturstandards, Sicherheitsrichtlinien, Compliance-Anforderungen oder Identitätsmanagement werden nicht mehr ausschliesslich dokumentiert oder manuell überprüft.

Sie werden direkt in die Plattform integriert.

Governance wird dadurch ausführbar.

Produktteams arbeiten innerhalb definierter Guardrails und können dennoch eigenständig entscheiden. Sicherheitsmechanismen, Infrastrukturstandards oder regulatorische Vorgaben begleiten jede Bereitstellung automatisch.

Governance wird dadurch nicht zum Hindernis für Innovation.

Sie wird zum Enabler einer sicheren und schnellen Delivery.

Genau diese Verbindung von Plattformen und Governance macht den eigentlichen Unterschied zwischen klassischen Betriebsmodellen und einem Readiness Framework aus.

Plattformen entwickeln sich zu intelligenten Ökosystemen

Mit Generativer AI und insbesondere Agentic AI beginnt bereits die nächste Evolutionsstufe.

Plattformen stellen künftig nicht mehr nur technische Services bereit.

Sie entwickeln sich zu intelligenten Organisationsplattformen.

AI-Agenten unterstützen Produktteams bei Architekturentscheidungen, generieren Software, überwachen Plattformen, analysieren Sicherheitsereignisse oder koordinieren komplexe Workflows. Gleichzeitig übernehmen Plattformen selbst zunehmend Steuerungsaufgaben. Sie erkennen Risiken, optimieren Ressourcen oder schlagen Verbesserungen vor.

Dadurch entsteht eine neue Form organisatorischer Zusammenarbeit.

Menschen, Plattformen und intelligente Agenten entwickeln gemeinsam digitale Fähigkeiten weiter.

Das Readiness Framework muss deshalb nicht nur technische Plattformen beschreiben.

Es muss diese intelligente Zusammenarbeit organisatorisch steuern.

Plattformen schaffen digitale Souveränität

Mit der zunehmenden Nutzung von Cloud-Plattformen wächst gleichzeitig die Abhängigkeit von externen Anbietern.

Digitale Souveränität bedeutet deshalb nicht, auf Plattformen zu verzichten.

Sie bedeutet, Plattformen bewusst zu gestalten.

Unternehmen müssen jederzeit wissen, welche organisatorischen Fähigkeiten sie selbst beherrschen müssen, welche Leistungen von Partnern bezogen werden können und welche kritischen Capabilities niemals ausser Kontrolle geraten dürfen.

Gerade Identitätsmanagement, Informationsmanagement, Sicherheitsmechanismen, AI Governance oder Datenplattformen entwickeln sich deshalb zu strategischen Fähigkeiten einer Organisation.

Nicht weil sie technisch besonders anspruchsvoll sind.

Sondern weil sie die Grundlage organisationaler Souveränität bilden.

Plattformen bilden das Fundament des Readiness Frameworks

Vielleicht liegt genau hier der entscheidende Unterschied zu klassischen IT-Architekturen.

Früher wurden Plattformen aufgebaut, um Infrastruktur effizienter bereitzustellen.

Heute werden Plattformen aufgebaut, um organisatorische Fähigkeiten bereitzustellen.

Sie verbinden Governance mit Delivery.

Sie standardisieren Wertschöpfung.

Sie reduzieren Komplexität.

Sie integrieren Sicherheit und Compliance.

Sie ermöglichen den sicheren Einsatz von AI.

Und sie schaffen jene Wiederverwendbarkeit, welche kontinuierliche Veränderung überhaupt erst wirtschaftlich macht.

Plattformen sind deshalb weit mehr als Technologie.

Sie sind die organisatorischen Fähigkeiten, auf denen die Readiness einer digitalen Organisation aufbaut.

> **Plattformen und Capabilities erhöhen nicht nur die Readiness der Organisation. Sie stärken gleichzeitig ihre Digitale Souveränität – denn wer seine kritischen Fähigkeiten bewusst gestaltet, entscheidet selbst, was er beherrschen muss und was er beziehen kann.**

6 Informationen schaffen Readiness

Kaum ein Begriff wird im Zusammenhang mit der digitalen Transformation so häufig verwendet wie Daten. Unternehmen investieren in Data Lakes, Analytics-Plattformen, Data Governance oder Künstliche Intelligenz. Gleichzeitig entstehen riesige Mengen digitaler Informationen, welche in unterschiedlichsten Anwendungen, Cloud-Plattformen und Geschäftsprozessen gespeichert werden.

Trotzdem fällt es vielen Organisationen zunehmend schwer, aus diesen Informationen verlässliche Entscheidungen abzuleiten.

Der Grund liegt nicht im Mangel an Daten.

Es fehlt häufig an einer gemeinsamen Informationsbasis.

Denn Informationen entfalten ihren Wert nicht allein dadurch, dass sie vorhanden sind. Sie müssen vollständig, aktuell, vertrauenswürdig und für die richtigen Personen zum richtigen Zeitpunkt verfügbar sein.

Genau hier beginnt organisationale Readiness.

Informationen sind der eigentliche Rohstoff der digitalen Organisation

Über Jahrzehnte wurden Informationen vor allem als Ergebnis von Geschäftsprozessen verstanden. Anwendungen erzeugten Daten, Berichte fassten sie zusammen und Managemententscheidungen wurden auf Basis periodischer Auswertungen getroffen.

Dieses Verständnis verändert sich grundlegend.

In einer digitalen Organisation werden Informationen selbst zum strategischen Vermögenswert. Sie bilden die Grundlage für Entscheidungen, Automatisierung, Künstliche Intelligenz und kontinuierliche Verbesserung. Ohne belastbare Informationen verliert eine Organisation ihre Fähigkeit, Veränderungen wirksam zu steuern.

Informationen werden damit zu einer organisatorischen Capability.

Nicht weil sie gespeichert werden.

Sondern weil sie Entscheidungen ermöglichen.

Readiness beginnt mit Transparenz

Jede Veränderung beginnt mit einer einfachen Frage:

Was wissen wir über unsere Organisation?

Welche Services unterstützen welche Geschäftsprozesse?

Welche Anwendungen verarbeiten kritische Informationen?

Welche Plattformen sind voneinander abhängig?

Welche AI-Modelle greifen auf welche Daten zu?

Welche regulatorischen Anforderungen gelten?

Welche Risiken entstehen durch eine geplante Veränderung?

Erstaunlicherweise können viele Organisationen diese Fragen nur teilweise beantworten.

Nicht weil die Informationen fehlen.

Sondern weil sie über zahlreiche Systeme verteilt sind, unterschiedlich gepflegt werden oder nicht miteinander in Beziehung stehen.

Das Readiness Framework betrachtet Informationen deshalb nicht isoliert.

Es verbindet sie.

Erst dadurch entsteht Transparenz.

Und Transparenz ist die Voraussetzung jeder wirksamen Governance.

Information verbindet sämtliche Wertströme

Informationen begleiten den gesamten Lebenszyklus digitaler Produkte und Services.

Sie entstehen bereits bei der strategischen Planung. Sie beschreiben Geschäftsanforderungen, Architekturentscheidungen, Risiken, Sicherheitsanforderungen, Serviceangebote, Betriebsdaten, Ereignisse und kontinuierliche Verbesserungen.

Jeder Wertstrom erzeugt neue Informationen.

Gleichzeitig nutzt jeder Wertstrom die Informationen aller anderen.

Dadurch entsteht ein kontinuierlicher Informationsfluss, der sämtliche organisatorischen Fähigkeiten miteinander verbindet.

Ein modernes Operating Model betrachtet Informationen deshalb nicht als Nebenprodukt der Wertschöpfung.

Informationen sind selbst Bestandteil der Wertschöpfung.

Traceability wird zur Voraussetzung organisationaler Steuerung

Mit zunehmender Digitalisierung steigen auch die Anforderungen an Nachvollziehbarkeit.

Unternehmen müssen heute wesentlich mehr beantworten können als die Frage, ob ein Service funktioniert.

Sie müssen nachvollziehen können,

welche Geschäftsanforderung zu einer bestimmten Funktion geführt hat,

welche Architekturentscheidung dahintersteht,

welche Daten verarbeitet werden,

welche AI-Komponenten beteiligt sind,

welche regulatorischen Anforderungen gelten,

welche Risiken akzeptiert wurden

und welche Auswirkungen eine Änderung auf andere Services besitzt.

Diese durchgängige Nachvollziehbarkeit wird als **End-to-End Traceability** zu einer der wichtigsten Fähigkeiten moderner Organisationen.

Sie schafft Transparenz.

Sie reduziert Risiken.

Und sie ermöglicht fundierte Entscheidungen.

Readiness entsteht genau durch diese Transparenz.

Datenqualität wird zur Managementaufgabe

Mit Generativer AI verändert sich die Bedeutung hochwertiger Informationen nochmals grundlegend.

Während klassische Anwendungen überwiegend deterministisch arbeiten, basiert AI auf Wahrscheinlichkeiten. Die Qualität ihrer Ergebnisse hängt unmittelbar von der Qualität der zugrunde liegenden Informationen ab.

Unvollständige Stammdaten, widersprüchliche Dokumentationen oder unklare Verantwortlichkeiten führen zwangsläufig zu fehlerhaften Empfehlungen oder automatisierten Fehlentscheidungen.

Data Governance wird dadurch zu weit mehr als einer technischen Disziplin.

Sie entwickelt sich zu einer Managementaufgabe.

Wer AI erfolgreich einsetzen möchte, muss seine Informationswerte genauso professionell steuern wie seine Finanzen oder seine kritischen Geschäftsprozesse.

Knowledge wird zum Wettbewerbsvorteil

Neben strukturierten Daten gewinnt ein weiterer Informationswert zunehmend an Bedeutung.

Das Wissen der Organisation.

Über Jahrzehnte befand sich dieses Wissen vor allem in den Köpfen einzelner Mitarbeitender. Erfahrungen wurden persönlich weitergegeben, Dokumentationen waren häufig unvollständig und viele Entscheidungen blieben implizit.

Mit AI verändert sich auch dieses Bild.

Dokumentiertes Wissen wird plötzlich unmittelbar nutzbar. AI-Systeme können Betriebsdokumentationen analysieren, Architekturentscheidungen nachvollziehen,

Supportanfragen beantworten oder regulatorische Anforderungen interpretieren.

Damit wird Wissensmanagement zu einer strategischen Fähigkeit.

Nicht weil mehr Dokumente entstehen.

Sondern weil organisatorisches Wissen erstmals systematisch verfügbar wird.

Observability schafft Vertrauen

Je komplexer digitale Organisationen werden, desto wichtiger wird die Fähigkeit, den aktuellen Zustand der Organisation jederzeit nachvollziehen zu können.

Observability wird deshalb häufig mit Monitoring gleichgesetzt.

Tatsächlich geht sie weit darüber hinaus.

Observability beschreibt die Fähigkeit einer Organisation, aus ihren verfügbaren Informationen jederzeit den tatsächlichen Zustand ihrer digitalen Wertschöpfung ableiten zu können.

Sie verbindet technische Telemetriedaten mit Geschäftsinformationen, Sicherheitsereignissen, AI-Aktivitäten und Governance-Daten zu einem gemeinsamen Lagebild.

Dadurch entsteht eine Organisation, die Veränderungen nicht nur erkennt.

Sie versteht ihre Auswirkungen.

Gerade für AI, Cyber Security und regulatorische Compliance wird diese kontinuierliche Transparenz zu einer zentralen Voraussetzung belastbarer Entscheidungen.

Informationen schaffen digitale Souveränität

Informationen bilden gleichzeitig die Grundlage digitaler Souveränität.

Nur wer weiss,

welche Informationen vorhanden sind,

wo sie gespeichert werden,

wer darauf zugreifen darf,

welche AI-Systeme sie verwenden

und welche regulatorischen Anforderungen gelten,

behält dauerhaft die Kontrolle über seine digitale Wertschöpfung.

Informationsmanagement entwickelt sich dadurch von einer administrativen Disziplin zu einer strategischen Führungsaufgabe.

Es entscheidet darüber, ob eine Organisation ihre Handlungsfähigkeit langfristig bewahren kann.

Informationen schaffen Readiness

Vielleicht verändert sich kein Bereich moderner Organisationen derzeit stärker als der Umgang mit Informationen.

Früher unterstützten Informationen Entscheidungen.

Heute ermöglichen sie Entscheidungen.

Sie verbinden Governance, Wertströme, Plattformen, Resilienz, Digitale Souveränität und AI zu einem gemeinsamen Informationssystem. Sie schaffen Transparenz über die gesamte Organisation und bilden die Grundlage für Automatisierung, intelligente Assistenzsysteme und kontinuierliche Verbesserung.

Readiness entsteht deshalb nicht allein durch gute Prozesse oder moderne Technologien.

Sie entsteht dort, wo aus Informationen belastbares Wissen wird und aus Wissen fundierte Entscheidungen entstehen.

Informationen sind damit nicht nur ein Vermögenswert der digitalen Organisation.

Sie sind die Grundlage ihrer Readiness.

> **Informationen erhöhen nicht nur die Readiness der Organisation. Sie stärken gleichzeitig ihre Digitale Souveränität – denn nur wer seine Informationswerte kennt, klassifiziert und kontrolliert, behält die Hoheit über seine digitale Wertschöpfung.**

7 Resilienz schafft Readiness

Resilienz als Eigenschaft des gesamten Betriebsmodells – nicht als nachgelagerte Funktion.

Über viele Jahre bestand die zentrale Aufgabe der IT darin, Systeme möglichst stabil und zuverlässig zu betreiben. Hohe Verfügbarkeit, geringe Ausfallzeiten und eine sichere Infrastruktur galten als wichtigste Qualitätsmerkmale eines professionellen IT-Betriebs.

Diese Anforderungen bleiben unverändert wichtig.

Sie reichen jedoch nicht mehr aus.

Digitale Organisationen stehen heute unter permanentem Veränderungsdruck. Cyberangriffe nehmen zu, regulatorische Anforderungen verändern sich kontinuierlich, Cloud-Plattformen entwickeln sich laufend weiter und intelligente AI-Systeme übernehmen zunehmend eigenständige Aufgaben innerhalb der Wertschöpfung. Gleichzeitig erwarten Kunden und Mitarbeitende, dass digitale Services jederzeit verfügbar bleiben.

Stabilität bedeutet deshalb heute nicht mehr, Veränderungen zu vermeiden.

Stabilität bedeutet, Veränderungen sicher beherrschen zu können.

Genau diese Fähigkeit beschreibt organisationale Resilienz.

Resilienz beginnt lange vor einer Krise

Resilienz wird häufig mit Business Continuity, Disaster Recovery oder Notfallplanung gleichgesetzt. Diese Fähigkeiten bleiben unverzichtbar.

Sie beschreiben jedoch lediglich den Umgang mit aussergewöhnlichen Ereignissen.

Das Readiness Framework versteht Resilienz wesentlich umfassender.

Resilienz beginnt bereits bei der Gestaltung der Organisation. Sie entsteht dort, wo Governance klare Verantwortlichkeiten schafft, Wertströme transparent werden, Plattformen wiederverwendbare Fähigkeiten bereitstellen und Informationen jederzeit verfügbar sind.

Eine Organisation, welche ihre kritischen Services, Abhängigkeiten und Risiken kennt, kann auf Veränderungen wesentlich schneller reagieren als eine Organisation, deren Wissen auf zahlreiche Systeme, Teams oder externe Partner verteilt ist.

Resilienz ist deshalb keine zusätzliche Funktion.

Sie ist eine Eigenschaft des gesamten Operating Models.

Informationssicherheit wird Teil jeder Capability

Auch die Rolle der Informationssicherheit verändert sich grundlegend.

Früher wurde Sicherheit häufig als eigenständige Disziplin verstanden. Anwendungen wurden entwickelt, anschliessend geprüft und danach produktiv gesetzt. Sicherheitskontrollen begleiteten den Betrieb, standen jedoch oftmals ausserhalb der eigentlichen Wertschöpfung.

Dieses Vorgehen passt immer weniger zur heutigen Realität.

Digitale Produkte entwickeln sich kontinuierlich weiter. Plattformen verändern sich laufend. Neue AI-Modelle werden produktiv eingesetzt. Sicherheitsbedrohungen entstehen täglich.

Informationssicherheit muss deshalb unmittelbar Bestandteil jeder organisatorischen Capability werden.

Identity & Access Management, Verschlüsselung, Observability, Schwachstellenmanagement, Datenschutz, Sicherheitsarchitektur oder Supply Chain Security begleiten einen digitalen Service vom ersten Architekturentwurf bis zum laufenden Betrieb. Sie werden nicht nachträglich ergänzt, sondern von Beginn an in Wertströme, Plattformen und Capabilities integriert.

Security entwickelt sich dadurch von einer kontrollierenden Funktion zu einer integrierten organisatorischen Fähigkeit.

Operative Resilienz wird zur Managementaufgabe

Mit der zunehmenden Digitalisierung verändern sich auch die Erwartungen der Gesetzgeber.

Regulatorische Anforderungen wie DORA, NIS2 oder der EU AI Act verlangen heute weit mehr als klassische Sicherheitsmassnahmen. Unternehmen müssen ihre kritischen digitalen Leistungen kennen, Risiken systematisch bewerten, Sicherheitsvorfälle beherrschen und ihre operative Widerstandsfähigkeit kontinuierlich nachweisen.

Operative Resilienz wird dadurch zu einer Führungsaufgabe.

Sie umfasst nicht nur den Schutz einzelner Systeme, sondern die Fähigkeit des gesamten Unternehmens, auch unter schwierigen Bedingungen handlungsfähig zu bleiben. Dazu gehören ein professionelles Risiko-Management ebenso wie Incident Management, Problem Management, Business Continuity Management, Disaster Recovery, Krisenmanagement und kontinuierliche Verbesserungsprozesse.

Resilienz beschreibt damit keinen Ausnahmezustand.

Sie beschreibt den Normalbetrieb einer modernen digitalen Organisation.

Resilienz endet nicht an der Unternehmensgrenze

Kaum ein Unternehmen betreibt seine digitalen Services heute noch vollständig selbst.

Cloud Provider, Software-as-a-Service-Anbieter, Managed Service Provider und spezialisierte Plattformbetreiber sind längst Teil der eigenen Wertschöpfung.

Damit verändert sich auch das Risikobild.

Die Stabilität eines Unternehmens hängt zunehmend von Partnern ab, auf deren operative Prozesse nur begrenzter Einfluss besteht.

Ein modernes Operating Model muss deshalb weit über die eigene Organisation hinausreichen. Lieferantensteuerung, gemeinsame Sicherheitsstandards, Exit-Strategien, kontinuierliche Leistungsüberwachung und transparente Verantwortlichkeiten werden zu festen Bestandteilen der Governance.

Partner sind heute nicht mehr lediglich Dienstleister.

Sie sind Teil der eigenen digitalen Wertschöpfung.

Resilienz entsteht deshalb immer im gesamten digitalen Ökosystem.

Observability wird zur Grundlage resilienter Organisationen

Je dynamischer digitale Organisationen werden, desto wichtiger wird die Fähigkeit, Veränderungen frühzeitig zu erkennen.

Observability entwickelt sich deshalb zu einer zentralen Managementfähigkeit.

Sie verbindet technische Telemetriedaten mit Informationen über Services, Plattformen, Geschäftsprozesse, Sicherheitsereignisse und AI-Systeme. Dadurch entsteht ein kontinuierliches Lagebild der gesamten Organisation.

Resilienz bedeutet damit nicht nur, auf Störungen reagieren zu können.

Resilienz bedeutet, Veränderungen rechtzeitig zu erkennen, ihre Auswirkungen zu verstehen und fundierte Entscheidungen treffen zu können.

Erst diese Transparenz ermöglicht belastbare Governance, wirksame Compliance und eine schnelle Reaktion auf neue Risiken.

AI erweitert das Verständnis von Resilienz

Mit Generativer AI und insbesondere Agentic AI entsteht eine weitere Dimension organisatorischer Resilienz.

Bisher standen vor allem Systeme, Netzwerke und Daten im Mittelpunkt der Sicherheitsarchitektur.

Künftig müssen auch intelligente Agenten sicher betrieben werden.

Sie greifen auf Unternehmensinformationen zu, nutzen Werkzeuge, koordinieren Prozesse und führen eigenständig Aktionen aus. Dadurch entstehen neue Anforderungen an Identitäten, Berechtigungen, Protokollierung und kontinuierliche Überwachung.

Resilienz bedeutet künftig deshalb auch, AI-Systeme jederzeit kontrollieren, nachvollziehen und bei Bedarf begrenzen zu können.

Informationssicherheit schützt nicht mehr ausschliesslich Informationen und Systeme.

Sie schafft Vertrauen in die Zusammenarbeit zwischen Menschen und intelligenten digitalen Akteuren.

Resilienz schafft digitale Souveränität

Resilienz und Digitale Souveränität sind eng miteinander verbunden.

Nur eine Organisation, welche ihre kritischen Abhängigkeiten kennt, Risiken kontinuierlich bewertet und ihre digitalen Fähigkeiten bewusst steuert, kann ihre Handlungsfreiheit langfristig erhalten.

Resilienz bedeutet deshalb nicht, jede Störung verhindern zu können.

Resilienz bedeutet, auch unter veränderten Bedingungen selbstbestimmt handeln zu können.

Damit wird sie zu einer wesentlichen Voraussetzung Digitaler Souveränität.

Resilienz schafft Readiness

Vielleicht liegt genau hier der grösste Unterschied zwischen klassischen und modernen Operating Models.

Früher bestand die Aufgabe der IT darin, Systeme möglichst stabil zu betreiben.

Heute besteht ihre Aufgabe darin, eine Organisation aufzubauen, die sich kontinuierlich verändern kann, ohne ihre Stabilität, Sicherheit oder Handlungsfähigkeit zu verlieren.

Ein Next Generation IT Operating Model versteht Resilienz deshalb nicht als eigenständige Disziplin.

Sie ist eine Grundeigenschaft jeder organisatorischen Capability, jedes Wertstroms und jeder Plattform.

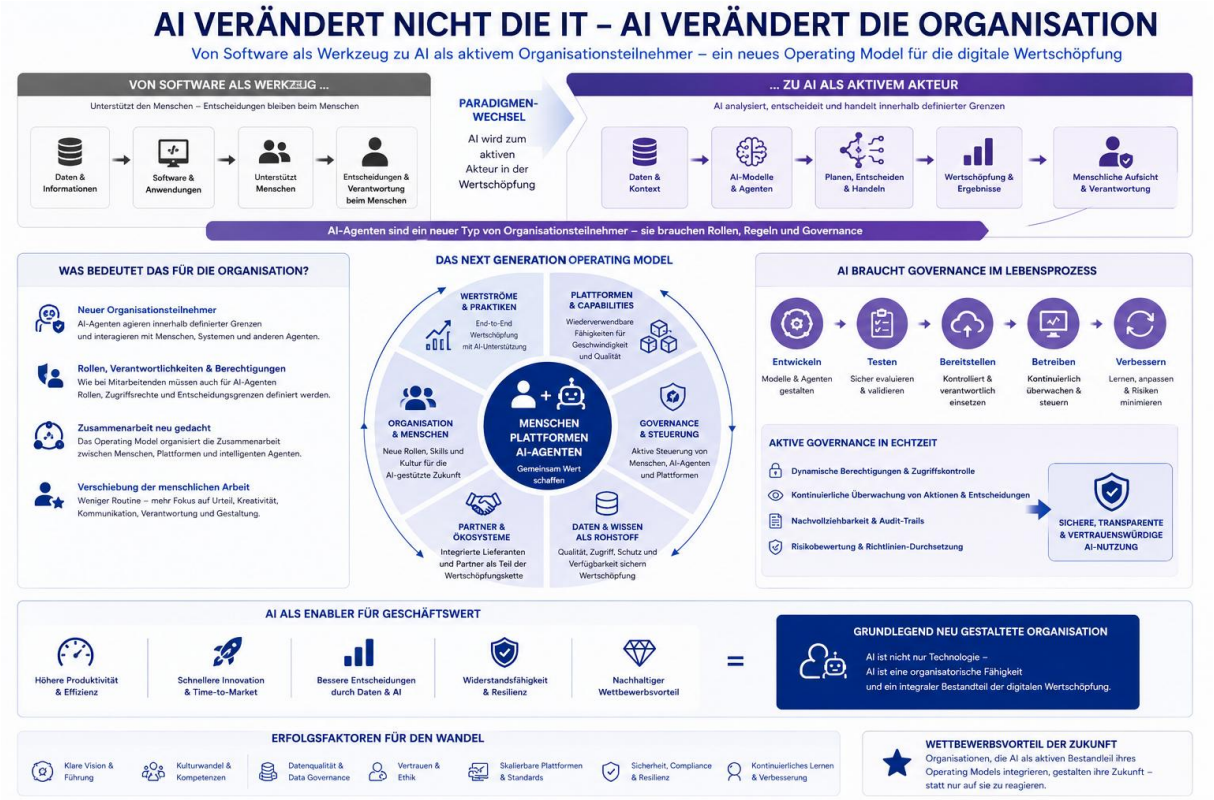
Readiness entsteht dort, wo Veränderungen nicht als Ausnahme betrachtet werden, sondern als Normalzustand einer lernenden Organisation.

Resilienz macht diese Organisation dauerhaft handlungsfähig.

Sie schafft Readiness.

> **Resilienz erhöht nicht nur die Readiness der Organisation. Sie stärkt gleichzeitig ihre Digitale Souveränität – denn nur wer auch unter veränderten Bedingungen handlungsfähig bleibt, kann jederzeit selbstbestimmt entscheiden.**

8 AI schafft eine neue Dimension von Readiness



AI wird zum Organisationsteilnehmer – eine neue Dimension von Readiness.

Kaum eine technologische Entwicklung verändert Unternehmen derzeit so tiefgreifend wie Künstliche Intelligenz.

Nahezu täglich entstehen neue Sprachmodelle, AI-Plattformen oder intelligente Assistenten. Unternehmen investieren in Pilotprojekte, automatisieren Geschäftsprozesse und suchen nach Möglichkeiten, die Produktivität ihrer Mitarbeitenden zu steigern.

Die Diskussion konzentriert sich dabei häufig auf technologische Fragen.

Welches Modell liefert die besten Ergebnisse?

Welche Plattform soll eingesetzt werden?

Welche Prozesse lassen sich automatisieren?

Diese Fragen sind wichtig.

Sie greifen jedoch zu kurz.

Die eigentliche Veränderung liegt nicht in der Technologie selbst.

Sie liegt darin, dass AI zunehmend Teil der Organisation wird.

Erstmals entstehen digitale Akteure, die nicht nur Informationen analysieren oder Inhalte erzeugen, sondern innerhalb definierter Grenzen eigenständig handeln können. Sie planen Aufgaben, koordinieren Abläufe, treffen Entscheidungen und interagieren mit anderen Systemen.

Damit verändert sich nicht nur die Art, wie gearbeitet wird.

Es verändert sich das Operating Model selbst.

AI wird Teil der Organisation

Über Jahrzehnte war Software in erster Linie ein Werkzeug.

Anwendungen unterstützten Menschen bei ihrer Arbeit, während Verantwortung und Entscheidungen grundsätzlich beim Menschen blieben.

Mit Generativer AI beginnt sich dieses Verhältnis grundlegend zu verändern.

Modelle erstellen heute Konzepte, entwickeln Software, analysieren Dokumente, generieren Architekturvorschläge oder unterstützen den Service Desk bei der Bearbeitung von Anfragen.

Agentic AI geht einen entscheidenden Schritt weiter.

Intelligente Agenten beschränken sich nicht mehr darauf, Empfehlungen zu geben. Sie nutzen Werkzeuge, koordinieren Abläufe, initiieren Prozesse und führen innerhalb definierter Grenzen eigenständig Aktionen aus.

Aus unterstützender Software werden damit aktive Teilnehmer der digitalen Wertschöpfung.

Vielleicht ist genau dies der grösste Paradigmenwechsel der kommenden Jahre.

Unternehmen integrieren künftig nicht einfach eine weitere Technologie.

Sie integrieren einen neuen Typ von Organisationsteilnehmer.

Das Operating Model muss Menschen und AI gemeinsam organisieren

Jeder Mitarbeitende erhält heute eine Rolle, Verantwortlichkeiten, Berechtigungen und einen klar definierten Handlungsspielraum.

Genau dieselben Fragen müssen künftig auch für intelligente Agenten beantwortet werden.

Welche Informationen dürfen sie verwenden?

Auf welche Systeme dürfen sie zugreifen?

Welche Entscheidungen dürfen sie selbstständig treffen?

Wann ist eine menschliche Freigabe erforderlich?

Wer trägt letztlich die Verantwortung für die Auswirkungen einer automatisierten Entscheidung?

Diese Fragen lassen sich nicht allein durch Technologie beantworten.

Sie betreffen Governance, Informationssicherheit, Architektur, Service Management und Risikomanagement gleichermassen.

Das Operating Model muss deshalb künftig nicht mehr nur Menschen organisieren.

Es organisiert die Zusammenarbeit zwischen Menschen, Plattformen und intelligenten Agenten.

AI verändert Verantwortung

Mit der Einführung intelligenter Agenten verändert sich gleichzeitig die Rolle des Menschen.

Je mehr Routinearbeiten automatisiert werden, desto stärker verschiebt sich der Schwerpunkt menschlicher Arbeit.

Mitarbeitende verbringen künftig weniger Zeit mit der Bearbeitung standardisierter Aufgaben oder der Suche nach Informationen.

Dafür gewinnen Tätigkeiten an Bedeutung, die Urteilsvermögen, Kreativität, Kommunikation, ethische Verantwortung und unternehmerisches Denken erfordern.

Menschen definieren Ziele.

Sie bewerten Risiken.

Sie treffen strategische Entscheidungen.

Sie gestalten die Rahmenbedingungen, innerhalb derer AI ihre Stärken entfalten kann.

Das Readiness Framework entwickelt sich dadurch von einer Arbeitsorganisation zu einem Führungsmodell für hybride Teams aus Menschen und intelligenten Agenten.

AI Governance wird zur Runtime Governance

Diese Entwicklung verändert auch das Verständnis von Governance.

Bisher wurden Anwendungen entwickelt, getestet und anschliessend produktiv gesetzt. Danach arbeiteten sie innerhalb weitgehend stabiler Rahmenbedingungen.

Agentic AI funktioniert grundlegend anders.

Intelligente Agenten reagieren kontinuierlich auf neue Informationen, treffen laufend Entscheidungen und passen ihr Verhalten an den jeweiligen Kontext an.

Governance kann deshalb nicht mehr ausschliesslich vor der Produktivsetzung stattfinden.

Sie muss den laufenden Betrieb begleiten.

Identitäten müssen verwaltet werden.

Berechtigungen müssen dynamisch überprüft werden.

Aktionen müssen kontinuierlich überwacht werden.

Entscheidungen müssen nachvollziehbar protokolliert werden.

Governance entwickelt sich dadurch von einer statischen Regelwelt zu einer aktiven Steuerungsschicht innerhalb der Organisation.

Daten werden zur strategischen Infrastruktur

Mit AI verändert sich gleichzeitig der Stellenwert von Informationen.

Über viele Jahre wurden Daten vor allem als Ergebnis digitaler Prozesse betrachtet.

Für AI werden sie zum eigentlichen Rohstoff der Wertschöpfung.

Die Qualität einer AI-Anwendung hängt unmittelbar von der Qualität der zugrunde liegenden Informationen ab.

Fehlerhafte Stammdaten.

Unvollständige Dokumentationen.

Inkonsistente Wissensquellen.

Unklare Verantwortlichkeiten.

All dies führt zwangsläufig zu fehlerhaften Entscheidungen.

Data Governance entwickelt sich dadurch zu einer strategischen Kernfähigkeit des Operating Models.

Wer AI erfolgreich einsetzen möchte, muss seine Informationen ebenso professionell steuern wie seine Plattformen oder seine kritischen Geschäftsprozesse.

Observability schafft Vertrauen

Mit zunehmender Autonomie intelligenter Agenten genügt es nicht mehr, lediglich den technischen Zustand eines Systems zu überwachen.

Unternehmen müssen verstehen,

welche Informationen verwendet wurden,

welches Modell eine Entscheidung beeinflusst hat,

warum ein Agent eine bestimmte Aktion ausgelöst hat,

welche Auswirkungen daraus entstanden sind

und ob regulatorische Anforderungen jederzeit eingehalten wurden.

Observability entwickelt sich dadurch von einem Betriebswerkzeug zu einer strategischen Managementfähigkeit.

Sie schafft Transparenz.

Sie schafft Vertrauen.

Und sie bildet die Grundlage für Governance in einer AI-gestützten Organisation.

AI erweitert die organisationale Readiness

Vielleicht liegt genau hier die eigentliche Bedeutung von AI.

Nicht die Automatisierung einzelner Tätigkeiten verändert Unternehmen grundlegend.

Sondern die Fähigkeit, intelligente Systeme sicher, verantwortungsvoll und wirksam in die Organisation zu integrieren.

Organisationen mit hoher Readiness werden AI nicht einfach schneller einsetzen.

Sie werden AI besser steuern.

Sie werden Governance, Informationsmanagement, Sicherheit, Plattformen und Wertströme so miteinander verbinden, dass Menschen und intelligente Agenten gemeinsam Wert schaffen können.

Damit wird AI nicht zu einer zusätzlichen organisatorischen Fähigkeit.

Sie verbindet sämtliche organisatorischen Fähigkeiten auf einer neuen Ebene.

AI schafft die nächste Generation organisationaler Readiness

Vielleicht wird in einigen Jahren nicht mehr zwischen digitaler Transformation und AI-Transformation unterschieden.

Beides wird selbstverständlich zusammengehören.

Die eigentliche Frage wird dann nicht mehr lauten, **ob** Unternehmen AI einsetzen.

Sondern **wie gut ihre Organisation darauf vorbereitet ist.**

Ein Next Generation IT Operating Model integriert AI deshalb nicht als zusätzliche Technologie oder als weiteres Innovationsprojekt.

Es versteht AI als aktiven Bestandteil der Organisation.

Als neue organisatorische Fähigkeit.

Und als Partner des Menschen innerhalb der digitalen Wertschöpfung.

Readiness bedeutet deshalb künftig nicht mehr nur, Veränderungen beherrschen zu können.

Readiness bedeutet, Menschen und intelligente Agenten gemeinsam sicher, souverän und wirksam handeln zu lassen.

Genau darin liegt die nächste Evolutionsstufe der digitalen Organisation.

> **AI erhöht die Readiness einer Organisation nur dann, wenn Governance, Informationen, Plattformen, Resilienz und Digitale Souveränität**

bereits vorhanden sind. Erst dieses Fundament macht aus Künstlicher Intelligenz eine sichere, souveräne und wirksame organisatorische Fähigkeit.

9 Die Organisation der Zukunft – Readiness wird zur zentralen Managementfähigkeit

Über viele Jahre wurde die Entwicklung moderner IT-Organisationen vor allem durch neue Technologien geprägt. Cloud Computing, DevOps, Plattformen, Agile, Künstliche Intelligenz oder Cyber Security standen im Mittelpunkt nahezu jeder Transformationsinitiative.

Dabei entstand häufig der Eindruck, die Zukunft werde in erster Linie durch technologische Innovation bestimmt.

Tatsächlich verhält es sich genau umgekehrt.

Nicht die Technologie entscheidet über den Erfolg einer Organisation.

Entscheidend ist ihre Fähigkeit, neue Technologien wirksam in ihre Wertschöpfung zu integrieren.

Genau deshalb verändert ein Next Generation IT Operating Model nicht in erster Linie die IT.

Es verändert die gesamte Organisation.

Die Grenzen zwischen Business und IT verschwinden

Lange Zeit wurden Business und IT als zwei unterschiedliche Welten betrachtet.

Das Business formulierte Anforderungen.

Die IT entwickelte Lösungen.

Anschliessend übernahm der Betrieb.

Dieses Modell funktionierte, solange digitale Lösungen einzelne Geschäftsprozesse unterstützten.

Heute bildet Software selbst den Kern vieler Geschäftsmodelle.

Digitale Produkte entwickeln sich kontinuierlich weiter. Daten bestimmen unternehmerische Entscheidungen. AI unterstützt Mitarbeitende bei ihrer täglichen Arbeit. Plattformen verbinden ganze Ökosysteme miteinander.

Dadurch verschwindet die klassische Trennung zwischen Business und IT zunehmend.

Digitale Wertschöpfung entsteht nicht mehr innerhalb einer einzelnen Organisationseinheit.

Sie entsteht durch das Zusammenspiel aller organisatorischen Fähigkeiten.

Ein modernes Operating Model organisiert deshalb keine IT-Abteilung mehr.

Es organisiert die digitale Organisation.

Menschen bleiben der entscheidende Erfolgsfaktor

Gerade weil AI immer leistungsfähiger wird, gewinnt der Mensch an Bedeutung.

Routinearbeiten werden zunehmend automatisiert. Informationen lassen sich schneller analysieren. Standardisierte Entscheidungen können durch intelligente Systeme vorbereitet oder teilweise übernommen werden.

Dadurch verschiebt sich die Rolle der Mitarbeitenden grundlegend.

Menschen schaffen künftig ihren grössten Mehrwert dort, wo Kreativität, Erfahrung, Verantwortungsbewusstsein, Kommunikation und unternehmerisches Denken gefragt sind.

Sie definieren Ziele.

Sie gestalten Strategien.

Sie bewerten Risiken.

Sie übernehmen Verantwortung.

Und sie entscheiden dort, wo ethische, wirtschaftliche oder gesellschaftliche Fragestellungen berücksichtigt werden müssen.

AI ersetzt diese Fähigkeiten nicht.

Sie verstärkt sie.

Die Zukunft gehört deshalb nicht einer Organisation ohne Menschen.

Sie gehört Organisationen, in denen Menschen durch intelligente Systeme besser werden.

Führung verändert sich grundlegend

Mit dieser Entwicklung verändert sich auch Leadership.

Führung bedeutet künftig weniger operative Steuerung einzelner Aufgaben.

Sie bedeutet vielmehr, Rahmenbedingungen zu schaffen, innerhalb derer Menschen, Plattformen und intelligente Agenten gemeinsam erfolgreich arbeiten können.

Führungskräfte definieren Orientierung statt Detailvorgaben.

Sie schaffen Vertrauen statt Kontrolle.

Sie fördern Zusammenarbeit statt Silodenken.

Sie entwickeln Fähigkeiten statt Strukturen.

Und sie gestalten eine Kultur, welche Lernen, Verantwortung und kontinuierliche Verbesserung selbstverständlich macht.

Leadership wird damit zu einer der wichtigsten Voraussetzungen organisationaler Readiness.

Kultur wird zur Infrastruktur der Veränderung

Jedes Operating Model beschreibt Strukturen, Rollen, Prozesse und Verantwortlichkeiten.

Ob diese in der Praxis funktionieren, entscheidet jedoch die Kultur einer Organisation.

Eine Kultur der Schuldzuweisung verhindert Innovation.

Eine Kultur der Intransparenz erschwert Governance.

Eine Kultur des Silodenkens verhindert Wertströme.

Und eine Kultur der Angst verhindert den verantwortungsvollen Einsatz von AI.

Die Organisation der Zukunft benötigt deshalb eine andere Form der Zusammenarbeit.

Sie basiert auf Vertrauen.

Auf Transparenz.

Auf kontinuierlichem Lernen.

Auf gemeinsamer Verantwortung.

Und auf der Bereitschaft, Veränderungen als normalen Bestandteil des täglichen Arbeitens zu verstehen.

Kultur ist damit kein weicher Faktor.

Sie ist die Infrastruktur, auf der Readiness überhaupt erst entstehen kann.

Organisationen lernen kontinuierlich

Früher wurden Veränderungen häufig als Projekte organisiert.

Nach erfolgreicher Einführung kehrte die Organisation wieder in einen stabilen Betriebszustand zurück.

Dieses Bild existiert heute kaum noch.

Digitale Organisationen entwickeln sich kontinuierlich weiter.

Neue regulatorische Anforderungen entstehen laufend.

Neue Technologien verändern bestehende Geschäftsmodelle.

Neue AI-Fähigkeiten erweitern die Möglichkeiten der Zusammenarbeit.

Organisationen befinden sich deshalb in einem permanenten Lernprozess.

Das Readiness Framework schafft die Voraussetzungen dafür, dass dieses Lernen systematisch erfolgt.

Governance liefert Orientierung.

Wertströme erzeugen Feedback.

Plattformen ermöglichen Wiederverwendung.

Informationen schaffen Transparenz.

Resilienz sichert Stabilität.

Digitale Souveränität erhält die Handlungsfreiheit.

AI erweitert die organisatorischen Fähigkeiten.

Gemeinsam entsteht daraus eine Organisation, die Veränderungen nicht als Ausnahme betrachtet, sondern als Normalzustand.

Readiness wird zur neuen Managementdisziplin

Vielleicht liegt genau hier der eigentliche Paradigmenwechsel.

In den vergangenen Jahrzehnten wurde Management vor allem über Planung, Kontrolle und Effizienz definiert.

Die digitale Organisation der Zukunft benötigt eine zusätzliche Fähigkeit.

Sie muss jederzeit bereit sein.

Bereit für neue Technologien.

Bereit für neue regulatorische Anforderungen.

Bereit für neue Geschäftsmodelle.

Bereit für Krisen.

Bereit für intelligente Agenten.

Bereit für Veränderungen, die heute noch gar nicht bekannt sind.

Diese Bereitschaft lässt sich nicht durch einzelne Projekte erreichen.

Sie entsteht durch das bewusste Zusammenspiel von Governance, Wertströmen, Plattformen, Informationen, Resilienz, Digitaler Souveränität und AI.

Genau dieses Zusammenspiel beschreibt das Readiness Framework.

Die Organisation der Zukunft ist bereit

Vielleicht wird genau dies die wichtigste Erkenntnis der kommenden Jahre sein.

Die erfolgreichsten Unternehmen werden nicht diejenigen sein, die über die modernsten Technologien verfügen.

Auch nicht diejenigen, die am schnellsten neue Trends übernehmen.

Erfolgreich werden jene Organisationen sein, die Veränderungen schneller verstehen, souveräner steuern und wirksamer umsetzen können als andere.

Sie verbinden Innovation mit Stabilität.

Sie verbinden Autonomie mit Governance.

Sie verbinden AI mit menschlicher Verantwortung.

Sie verbinden Geschwindigkeit mit Vertrauen.

Und sie bewahren dabei ihre Fähigkeit, jederzeit selbstbestimmt zu handeln.

Readiness wird damit zur zentralen Managementfähigkeit der digitalen Organisation.

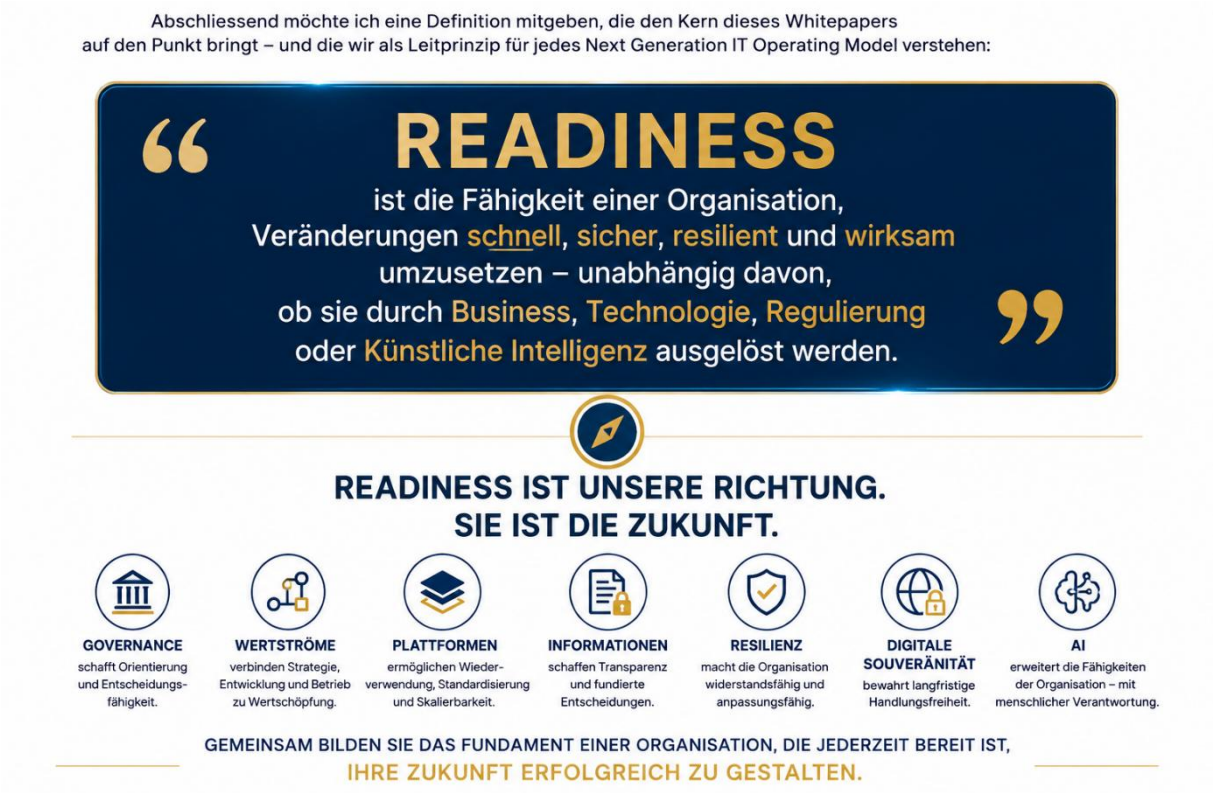
Nicht als Methode.

Nicht als Framework.

Nicht als Projekt.

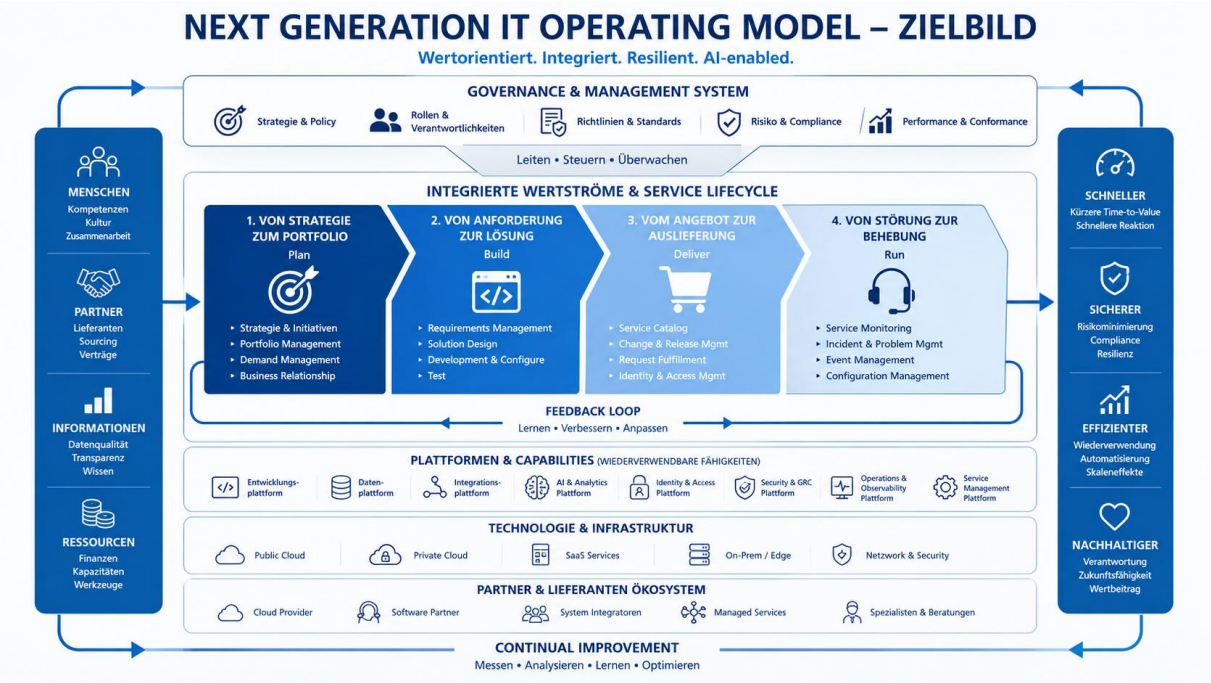
Sondern als grundlegende Eigenschaft einer Organisation, die gelernt hat, mit kontinuierlichem Wandel erfolgreich umzugehen.

Genau dafür steht das Readiness Framework.



Readiness als Leitprinzip: die Definition und die Säulen des Next Generation IT Operating Models.

Fazit: Die Zukunft gehört den Organisationen mit der höchsten Readiness



Das Next Generation IT Operating Model: wertorientiert, integriert, resilient, AI-enabled.

Über viele Jahre galt Agilität als das wichtigste Ziel moderner Organisationen. Unternehmen sollten schneller werden, flexibler handeln und Veränderungen rascher umsetzen. Methoden wie Scrum, DevOps oder SAFe haben diese Entwicklung massgeblich geprägt und einen wichtigen Beitrag dazu geleistet, IT und Business enger miteinander zu verbinden.

Diese Entwicklung war richtig.

Sie ist heute jedoch nicht mehr ausreichend.

Die digitale Welt ist komplexer geworden. Unternehmen müssen heute nicht nur Innovationen schneller umsetzen. Sie müssen gleichzeitig Cyberangriffe abwehren, regulatorische Anforderungen erfüllen, globale Plattformökosysteme steuern, ihre Digitale Souveränität bewahren und Künstliche Intelligenz verantwortungsvoll in ihre Organisation integrieren.

Geschwindigkeit allein genügt dafür nicht mehr.

Eine Organisation kann sehr agil sein und dennoch scheitern, wenn ihr Governance, Transparenz, Resilienz oder die Kontrolle über ihre digitalen Fähigkeiten fehlen.

Deshalb braucht es einen neuen Blick auf organisatorische Leistungsfähigkeit.

Readiness geht weiter als Agilität

Agilität beantwortet eine wichtige Frage:

Wie schnell können wir auf Veränderungen reagieren?

Readiness beantwortet die entscheidendere Frage:

Sind wir jederzeit in der Lage, Veränderungen erfolgreich, sicher und souverän zu bewältigen?

Diese Unterscheidung ist von grundlegender Bedeutung.

Eine agile Organisation kann schnell handeln.

Eine Organisation mit hoher Readiness kann schnell handeln, ohne ihre Stabilität, Sicherheit oder Handlungsfähigkeit zu verlieren.

Sie verbindet scheinbare Gegensätze.

Sie beschleunigt Innovation und behält gleichzeitig die Kontrolle.

Sie fördert Eigenverantwortung und schafft dennoch einheitliche Governance.

Sie nutzt AI produktiv und gewährleistet gleichzeitig Transparenz und Nachvollziehbarkeit.

Sie setzt auf Cloud-Plattformen und bewahrt dennoch ihre Digitale Souveränität.

Genau diese Balance entscheidet künftig über den nachhaltigen Erfolg digitaler Organisationen.

Readiness entsteht nicht zufällig

Readiness lässt sich nicht durch einzelne Projekte erreichen.

Sie entsteht auch nicht allein durch neue Technologien.

Und sie ist weit mehr als eine weitere Managementmethode.

Readiness ist das Ergebnis eines bewusst gestalteten Operating Models.

Governance schafft Orientierung und Entscheidungsfähigkeit.

Wertströme verbinden Strategie, Entwicklung und Betrieb zu einem kontinuierlichen Fluss der Wertschöpfung.

Plattformen und organisatorische Capabilities ermöglichen Wiederverwendung, Standardisierung und Skalierbarkeit.

Informationen schaffen Transparenz und fundierte Entscheidungen.

Resilienz macht die Organisation widerstandsfähig gegenüber Veränderungen und Krisen.

Digitale Souveränität bewahrt ihre langfristige Handlungsfreiheit.

Und Künstliche Intelligenz erweitert die Fähigkeiten der Organisation, ohne die Verantwortung des Menschen zu ersetzen.

Erst das Zusammenspiel dieser Elemente schafft eine Organisation, die dauerhaft bereit ist, sich erfolgreich weiterzuentwickeln.

Readiness wird zur neuen Managementfähigkeit

Ich bin überzeugt, dass sich der Fokus der Unternehmensführung in den kommenden Jahren grundlegend verändern wird.

Die entscheidende Frage wird künftig nicht mehr lauten:

„Wie agil ist unsere Organisation?"

Sondern:

„Wie hoch ist unsere Readiness?"

Denn Technologien werden sich weiterentwickeln.

Regulatorische Anforderungen werden zunehmen.

Cyberbedrohungen werden komplexer.

Geschäftsmodelle werden sich schneller verändern.

Und AI wird zunehmend zu einem aktiven Bestandteil unserer Organisationen.

Der eigentliche Wettbewerbsvorteil wird deshalb nicht darin liegen, wer die modernste Technologie besitzt.

Er wird darin liegen, wer seine Organisation am besten darauf vorbereitet hat, mit Veränderungen souverän umzugehen.

Readiness wird zum Leitprinzip der digitalen Organisation

Dieses Whitepaper beschreibt deshalb kein weiteres Framework neben den bestehenden Methoden und Standards.

Es versteht sich vielmehr als übergreifendes Managementmodell, das bewährte Ansätze wie Governance, Enterprise Architecture, IT Service Management, Informationssicherheit, Plattformorganisation und AI Governance in einer gemeinsamen Zielsetzung verbindet.

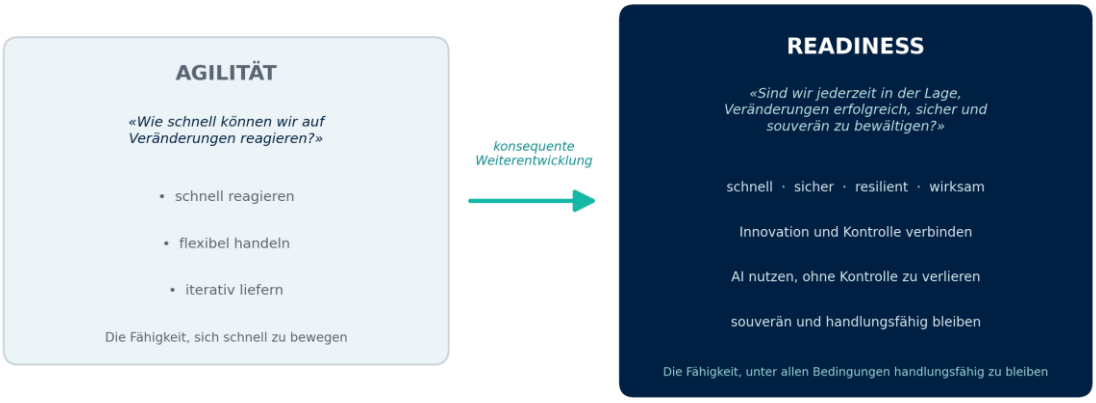
Diese Zielsetzung lautet:

Readiness.

Readiness ist die Fähigkeit einer Organisation, Veränderungen schnell, sicher, resilient und wirksam umzusetzen – unabhängig davon, ob sie durch Business, Technologie, Regulierung oder Künstliche Intelligenz ausgelöst werden.

> **Readiness ist damit nicht nur das Ziel eines Next Generation IT Operating Models – sie wird zum Massstab, an dem sich die Zukunftsfähigkeit digitaler Organisationen messen lässt.**

Vielleicht wird genau dieser Begriff die Managementdiskussion der kommenden Jahre prägen.



Von der Agilität zur Readiness: Geschwindigkeit wird zur dauerhaften Handlungsfähigkeit weiterentwickelt.

Nicht weil Agilität an Bedeutung verliert.

Sondern weil Agilität allein nicht mehr ausreicht.

Die digitale Organisation der Zukunft muss schneller sein als früher.

Vor allem aber muss sie jederzeit bereit sein.

Bereit für neue Technologien.

Bereit für intelligente AI-Agenten.

Bereit für neue Geschäftsmodelle.

Bereit für Krisen.

Bereit für Chancen.

Readiness wird damit zur zentralen Managementfähigkeit der digitalen Organisation.

Nicht als Ersatz für Agilität.

Sondern als deren konsequente Weiterentwicklung.

Denn Agilität beschreibt die Fähigkeit, sich schnell zu bewegen.

Readiness beschreibt die Fähigkeit, unter allen Bedingungen handlungsfähig zu bleiben.

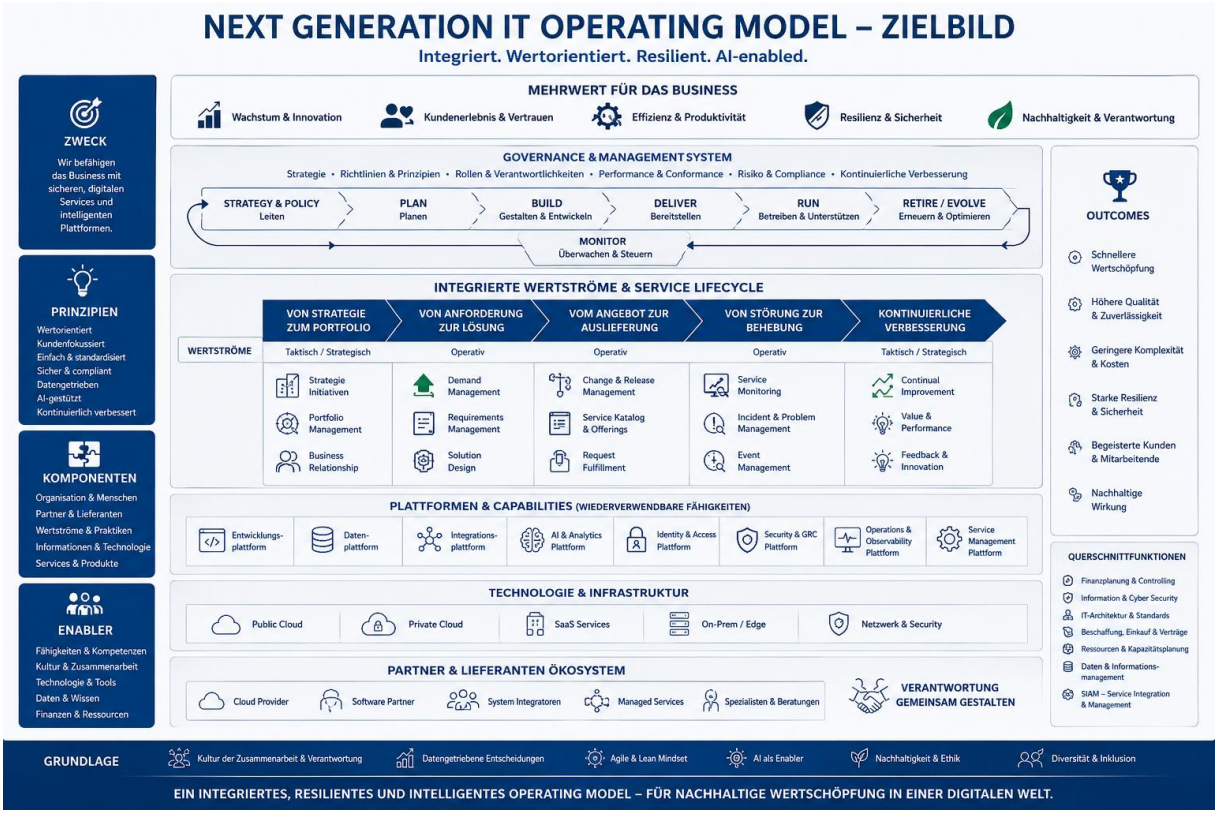
Und genau das ist die Aufgabe eines **Next Generation IT Operating Models**.

Es schafft nicht einfach eine moderne IT.

Es schafft eine Organisation, die bereit ist für alles, was als Nächstes kommt.

Das Zielbild

Next Generation IT Operating Model



Das Zielbild des Next Generation IT Operating Models.

Über den Autor

Martin Andenmatten ist Gründer und Managing Director der Glenfis AG. Als ausgewiesener Experte für IT Governance, Service Management und digitale Betriebsmodelle begleitet er seit über zwei Jahrzehnten Unternehmen und öffentliche Institutionen bei der Gestaltung ihrer IT-Organisationen. Seine Schwerpunkte umfassen IT4IT, ITIL®, COBIT, ISO/IEC-Normen, Cloud- und Sourcing-Governance sowie den Aufbau zukunftsfähiger Target Operating Models. Er ist Autor zahlreicher Fachpublikationen und schreibt regelmässig im Blog «Disruptive agile Service Management» (blog.itil.org) über Governance, digitale Souveränität, AI und die Zukunft des Service Managements.

Über Glenfis AG

Die Glenfis AG ist ein Schweizer Beratungs- und Ausbildungsunternehmen mit Sitz in Zürich. Glenfis unterstützt Organisationen bei der Transformation ihrer IT – von der Standortbestimmung über die Gestaltung von Operating Models bis zur Umsetzung von Governance-, Service-Management- und Sourcing-Strukturen. Die Glenfis Academy bietet ein umfassendes Trainingsportfolio zu ITIL®, COBIT, IT4IT, TOGAF, Cloud Computing, Cyber Security, DevOps und agilen Methoden. Vom Kennen zum Können zum Tun.

Quellen und weiterführende Beiträge

Dieses Whitepaper basiert auf den folgenden Beiträgen von Martin Andenmatten im Blog «Disruptive agile Service Management» (blog.itil.org) sowie den zugehörigen LinkedIn-Artikeln: Next Generation IT Operating Model (Juli 2026) · Asset Management kennt alles. Ausser das Wertvollste. (Juni 2026) · Von der AI-Wildnis zum AI Operating Model (Juni 2026; englisch: The AI Wilderness Is Growing Faster Than Governance) · Digitale Souveränität steuern statt darüber diskutieren – Ein Governance-Ansatz auf Basis von COBIT (Mai 2026) · Digitale Souveränität als verhandelbare Service Levels (Februar 2026) · Das Spannungsfeld zwischen Governance und Innovation (Februar 2026) · Steuerung in Zeiten radikaler Umbrüche: Governance als Schlüssel zur digitalen Resilienz (November 2025; englisch: Why GRC Has Become the Foundation of Digital Resilience and Business Trust).

Referenzierte Rahmenwerke und Standards: IT4IT™ Reference Architecture (The Open Group), ITIL® 4 (PeopleCert), COBIT® (ISACA), ISO/IEC 27001, ISO/IEC 42001, EU AI Act, DORA, NIS2, DSGVO/DSG, Cyber Resilience Act.

© 2026 Glenfis AG, Zürich. Alle Rechte vorbehalten. ITIL® ist eine eingetragene Marke von PeopleCert. COBIT® ist eine eingetragene Marke von ISACA. IT4IT™ ist eine Marke der The Open Group.