KEYNOTE

Wie viel IAM braucht das Unternehmen? Viel hilft nicht immer viel.

Martin Kuppinger
Principal Analyst | KuppingerCole Analysts

kuppingercole ANALYSTS

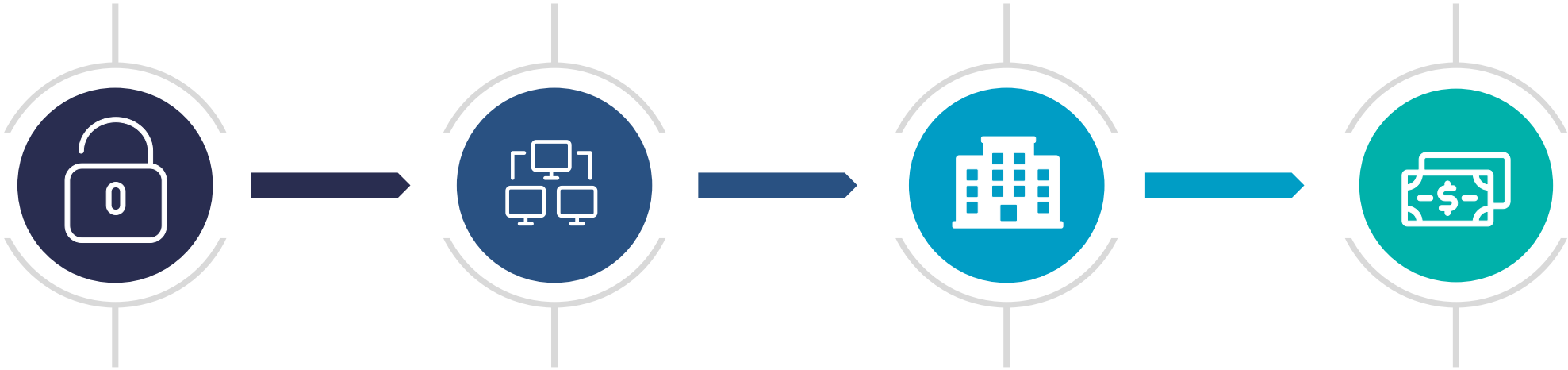
IAM (Identity & Access Management) ist eine essentielle Funktion mindestens für alle mittleren und großen Unternehmen. Da gibt es natürlich Lösungen wie Microsoft Entra ID. Es gibt komplexe Lösungen für IGA (Identity Governance & Administration), also die ganzen Prozesse rund um das Anlegen von Nutzern, die Steuerung von Berechtigungen und deren Überprüfung, also die Governance.

Viel Auswahl also und doch sind viele IAM-Projekte wohl am besten als „notleidend“ zu bezeichnen. Das liegt auch daran, dass man oft das falsche Werkzeug nutzt. Die Lösung muss immer zum Unternehmen passen. Und hier gilt eben nicht, dass viel immer viel hilft.

Es geht um effiziente Einführung, funktionierende Prozesse und die Erfüllung der konkreten Anforderungen von Business, Cybersicherheit und Regulatoren. In seinem Vortrag wird Martin Kuppinger darauf eingehen, wie der Mittelstand, von kleinen mittelständischen Unternehmen bis zum „mid market“, bei IAM vorgehen kann, um nicht an der Komplexität zu scheitern, aber ebenso wenig an fehlender Funktionalität.

Zugriffsrisiken sind Unternehmensrisiken

Das Management von Zugriffsrisiken ist essentiell für die Reduktion kritischer Unternehmensrisiken



ZUGRIFFSRISIKO

Missbräuchlicher Zugriff kann zu signifikanten finanziellen und regulatorischen Risiken ebenso wie Datenlecks führen.

IT-RISIKO

IT benötigt einen Ansatz, der alle IT-Risiken ganzheitlich betrachtet: Zugriffsrisiken, Cloud-Risiken, BCM etc.

BUSINESS-RISIKO

IT-Risiken haben einen Einfluss auf das Geschäft, z.B. Finanzen und Reputation. Sie müssen sichtbar gemacht werden.

KOSTEN

Zugriffsrisiken können den Erfolg eines Unternehmens und seinen Wert gefährden und bis hin zur Insolvenz führen.

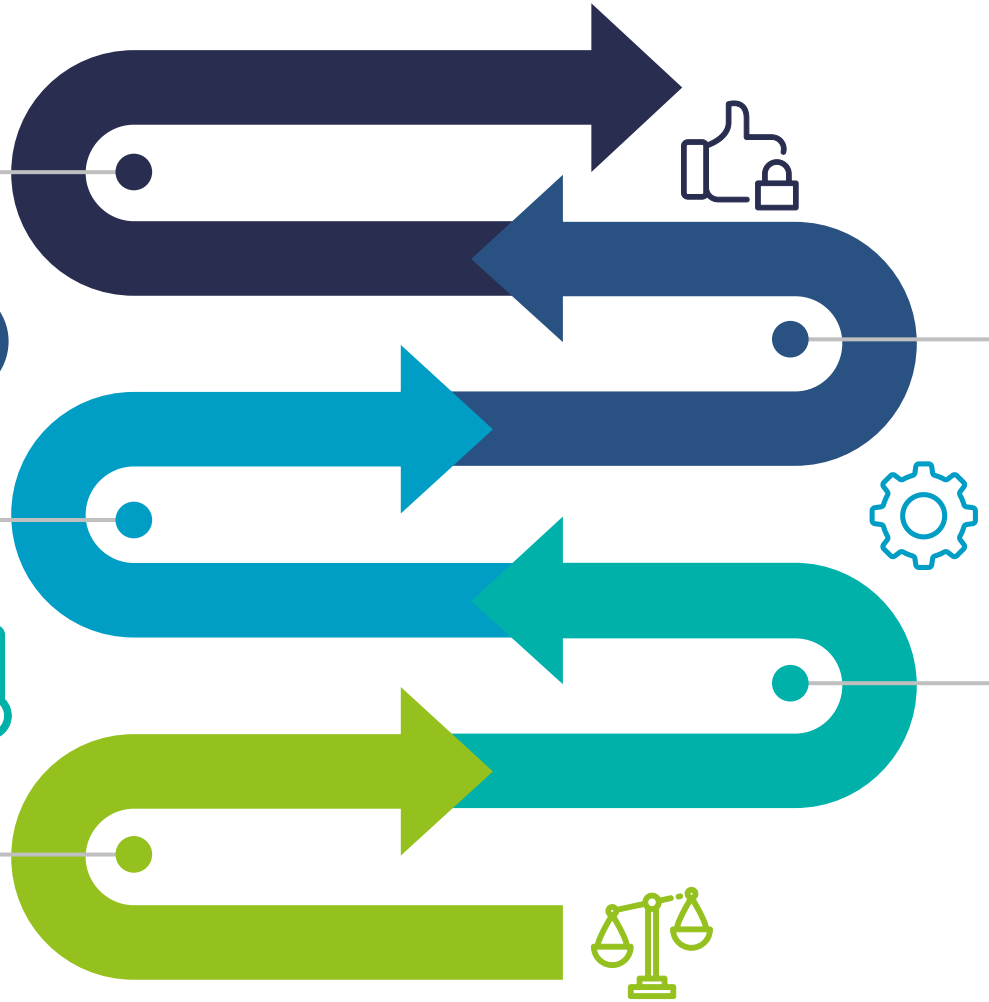
Compliance ≠ Audit ≠ Sicherheit

Es geht darum, die richtigen Maßnahmen zu ergreifen für mehr Sicherheit!

SICHERHEIT
Weder Compliance noch Audit führen zur Sicherheit – es sind die richtigen Maßnahmen.

MASSNAHMEN
Was wirklich gemacht wird, nicht was dem Auditor erzählt wird.

COMPLIANCE
Die Erfüllung von Gesetzen und Regularien.



GANZHEITLICHER ANSATZ
Compliance, Audit und Maßnahmen sind eng verbunden – sie müssen als Ganzes betrachtet werden.

AUDIT
Die Fähigkeit zu beweisen, dass man wirklich macht, was man behauptet zu tun.

EXKURS: NIS2

Die NIS2-Richtlinie ist die EU-weite Gesetzgebung zur Cybersicherheit. Sie enthält rechtliche Maßnahmen zur Steigerung des Gesamtniveaus der Cybersicherheit in der EU.

NIS2 ist am 16.01.2023 in Kraft getreten.

Die EU-Mitgliedsstaaten müssen NIS2 innerhalb von 21 Monaten in nationales Recht transferieren.

Unternehmen, die im Scope sind (KRITIS), müssen diese entsprechend ebenfalls bis Oktober 2024 umsetzen, weil es keine weiteren Übergangsfristen geben wird.

NIS2: Spezifische und generische Anforderungen

NIS2 nennt verschiedene zwingende Maßnahmen, aber auch generische Sicherheit

NIS2 nennt eine Reihe von spezifischen Anforderungen, insbesondere für das Risikomanagement und die Incident Response, aber auch für Authentifizierung und andere Maßnahmen.

Daneben wird aber auch auf gängige Best Practices, Zertifizierungen und ein generell hohes Maß und adäquates Vorgehen im Bereich der Sicherheit referenziert.

IAM ist teilweise direkt referenziert, in anderen Bereichen aber indirekt über beispielsweise die im Rahmen der Best Practices (z.B. ISO 2700x) erforderlichen Maßnahmen.

a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;

b) Bewältigung von Sicherheitsvorfällen;

c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;

d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;

e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;

f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;

g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;

h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;

i) Sicherheit des Personals, Konzepte für die **Zugriffskontrolle** und Management von Anlagen;

j) Verwendung von Lösungen zur **Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung,** gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Mittlere und große Unternehmen im Fokus

Definierte Schwellwerte, die früh erreicht werden – sehr viele Unternehmen im Scope

Durch die relativ niedrigen Schwellwerte fallen sehr viele Unternehmen unter die NIS2-Regulierung.

Das bedeutet insbesondere für mittelständische Unternehmen eine massive Verschärfung der Vorgaben.

Zudem ist die Grenze für große Unternehmen sehr niedrig gezogen.

Mittel (medium)

50-250 Beschäftigte und

10-50 Mio. Euro Umsatz und/oder

< 43 Mio. Euro Bilanz

Groß (large)

>250 Beschäftigte und

> 50 Mio. Euro Umsatz und/oder

> 43 Mio. Euro Bilanz

Wesentlich sind große Unternehmen aus den definierten Sektoren (wesentlich) sowie diverse Sonderfälle unabhängig von der Größe und ggf. weitere Unternehmen aus anderen Branchen, wenn diese als essentiell / systemisch relevant festgelegt werden.

Sehr viele Sektoren sind betroffen

Breite Definition von Sektoren, die in den Fokus von NIS2 fallen

Die breite Palette an betroffenen Sektoren macht NIS2 zu einer Regulierung, die flächendeckende Auswirkungen hat und sehr viele Unternehmen dazu zwingt, zu handeln.

Verglichen mit der bisherigen KRITIS-Regulierung wird der Fokus massiv ausgeweitet.

Daher ist eine Prüfung der Betroffenheit und die Ergreifung von Maßnahmen zwingend.

Zudem wird sich zwangsläufig eine Auswirkung auf das, was Best Practice / State-of-the-Art ist, ergeben und damit andere Unternehmen ebenfalls betreffen.

Auch beratende Unternehmen werden über ihre Rolle als Lieferanten zu „NIS2-Unternehmen“

Hohe Kritikalität	Sonstige kritische Sektoren
Energie (Elektrizität, Fernwärme und –kälte, Erdöl, Erdgas, Wasserstoff)	Post- und Kurierdienste
Verkehr (Luftverkehr, Schienenverkehr, Schifffahrt, Straßenverkehr)	Abfallbewirtschaftung
Bankwesen	Produktion, Herstellung und Handel mit chemischen Stoffen
Finanzmarktinfrastrukturen	Produktion, Verarbeitung und Vertrieb von Lebensmitteln
Gesundheitswesen	Verarbeitendes Gewerbe / Herstellung von Waren (Medizinprodukte, IT, elektrische Ausrüstungen, Maschinenbau, Automobil und Zulieferer, sonstiger Fahrzeugbau)
Trinkwasser	Anbieter digitaler Dienste (Marktplätze, Suchmaschinen, soziale Netzwerke)
Abwasser	Forschung
Digitale Infrastruktur	
Verwaltung von ITK-Diensten	
Öffentliche Verwaltung (Zentralregierungen, regionale Regierungen)	
Weltraum	

Identity - Security

IAM schafft Sicherheit

Administrative Effizienz

Workflows, Automatisierung, Self Service

Management und Kontrolle

Einheitliche Administration aller Identitäten auf allen Systemen in der hybriden Realität der Digitalen Transformation

Sicherheit und Vertrauen

Absicherung der Identitäten, Zugänge und Berechtigungen mit starker Authentifizierung

Compliance und Governance

Wer hat auf was Zugriff, wer sollte Zugriff haben, und wie wird dieser Zugriff benutzt?

IAM muss sich weiterentwickeln: Neue Anforderungen

IAM muss liefern, von der Kostenoptimierung bis hin zur Unterstützung von Zukunftsthemen

IAM ist nicht statisch.

Anforderungen verändern sich.

Beispiele für veränderte Anforderungen:

- Work from anywhere
- Cloud
- Digitale Dienste und die Notwendigkeit, die Identitäten von Kunden und Dingen zu unterstützen

Neue Herausforderungen am Horizont:

- Web3
- Metaverse
- Dezentrale Technologien/Identitäten

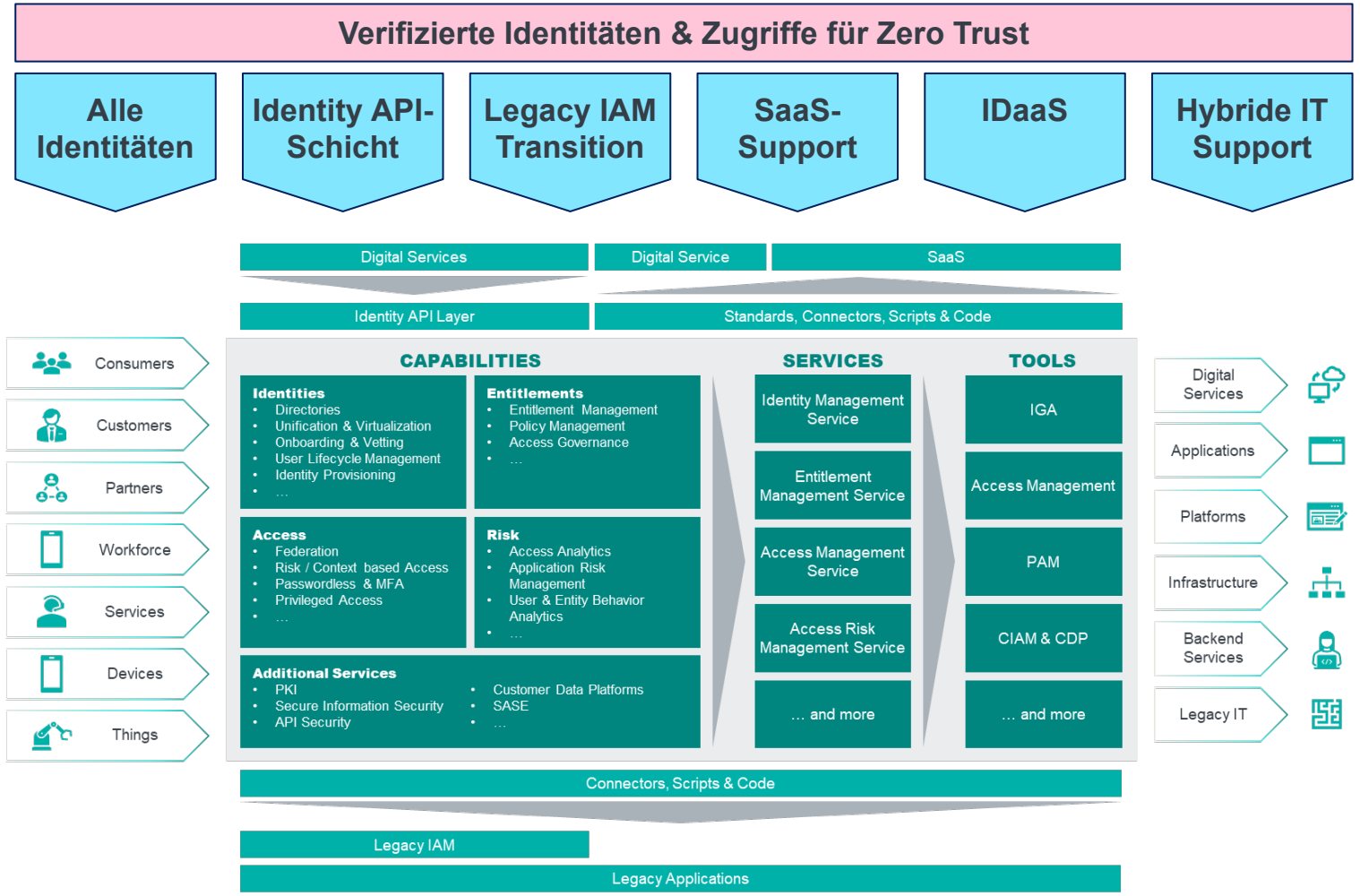
IAM weiterentwickeln, Zero Trust unterstützen, IDaaS

IAM ist nicht statisch, sondern entwächst dem traditionellen Mitarbeiterfokus: Identity Fabrics

Identity Fabrics sind ein grundlegendes Paradigma: Eine integrierte Sicht über alle Bereiche von IAM, mit denen reibungsloser, aber dennoch sicherer Zugriff von allen Identitäten auf alle Ressourcen und Dienste bereitgestellt wird. Modular, flexibel, adaptiv.

- Unterstützung aller Identitäten: Menschen, Dinge, Geräte.
- Unterstützung für die Verwaltung von Diensten und die Bereitstellung von Diensten: Identity API-Schicht.
- Einbindung und Erweiterung des Legacy-IAM für eine reibungslose Transition.
- Unterstützung von modernen SaaS- (und IaaS/PaaS-) Infrastrukturen.
- Bereitstellung als SaaS-Dienst.
- Gebaut für die hybride Realität der heutigen IT-Infrastrukturen.

Kernbaustein von Zero Trust: Verifizierte Identitäten.



KuppingerCole Identity Fabrics Model

IAM ist evolutionär. Nicht revolutionär.

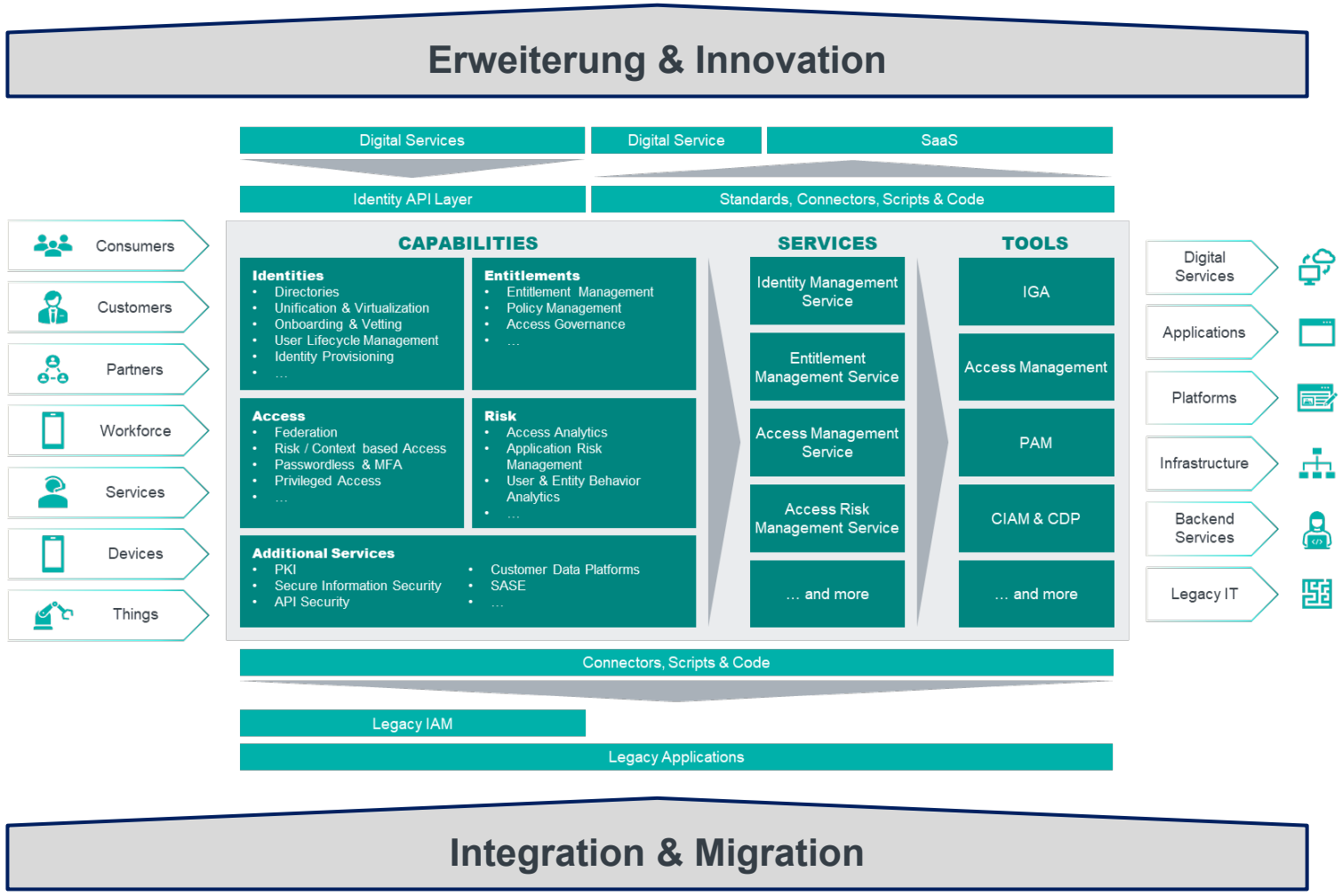
Es geht nicht um radikales Ersetzen, sondern um Integration, Migration, Erweiterung, Innovation.

Der Startpunkt: Eine ganzheitliche Vision und ein Plan für das zukünftige IAM.

Was ist da, was fehlt?

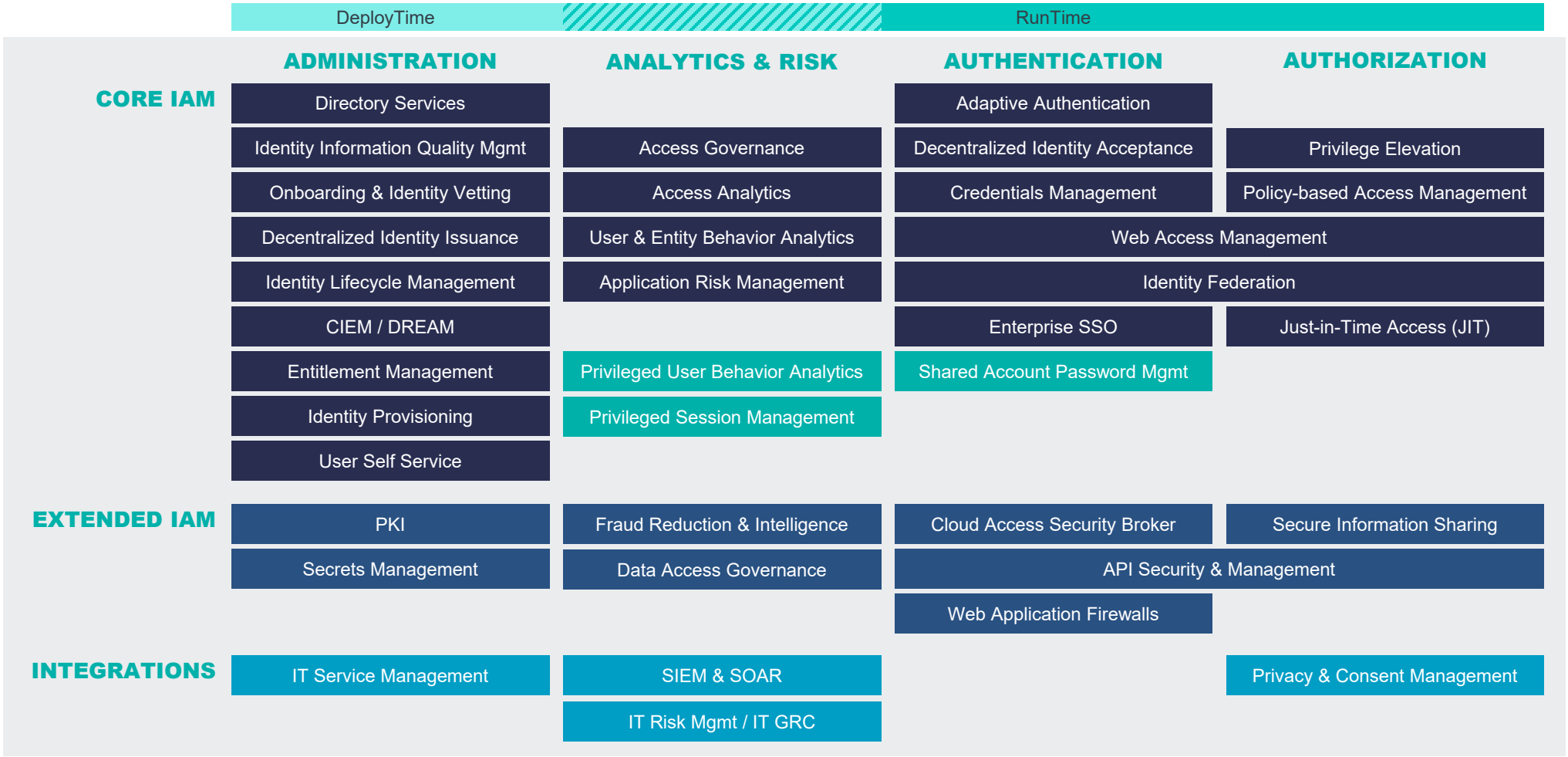
Was kann in eine Identity Fabric integriert werden, was muss neu dazukommen?

Erweiterung in Richtung neuer Dienste.



Identity & Access Management ist mehr als nur IGA

KuppingerCole IAM Reference Architecture: Kernbausteine für IAM



Von vielen Bausteinen zu konkreten Prioritäten

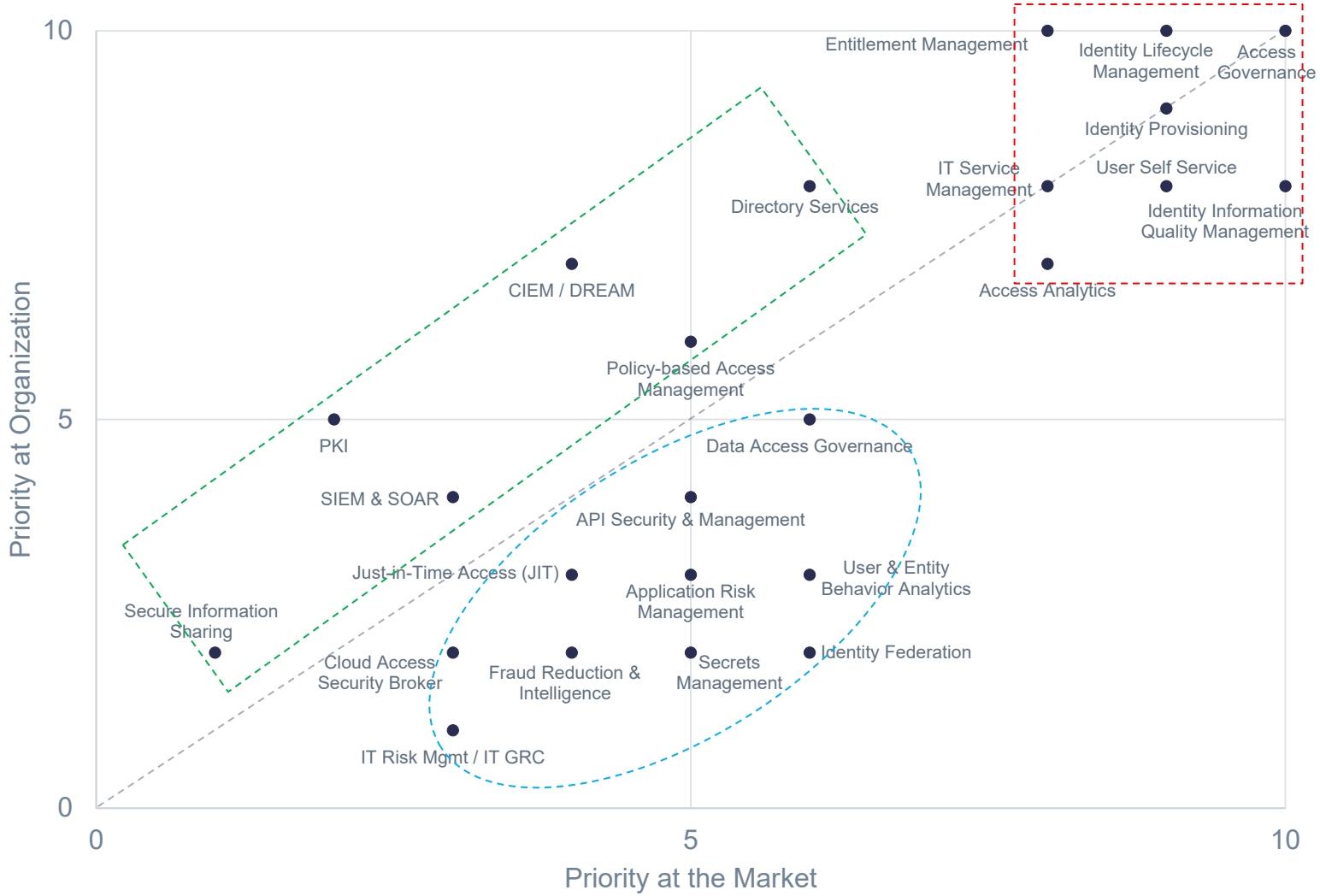
Scattergram: Priorisierung von Funktionen für Kundenszenarien

Erläuterung des Scattergrams
- Höhere Priorität weiter oben/rechts
- Gestrichelte Linie zeigt ausgeglichene Priorität zwischen Organisation und Markt an
- Alles über/links der Linie ist für die Organisation wichtiger als für den Markt
- Alles rechts/unter der Linie ist für den Markt wichtiger als für die Organisation
- Lässt sich alternativ auch mit “Gap” auf der x-Achse machen

Bereich hoher Priorität
- Diese Themen sind sowohl für den Markt als auch die Organisation besonders wichtig
- Die meisten gehören zu IGA oder Access Management (nicht im Beispiel enthalten) und sind etabliert

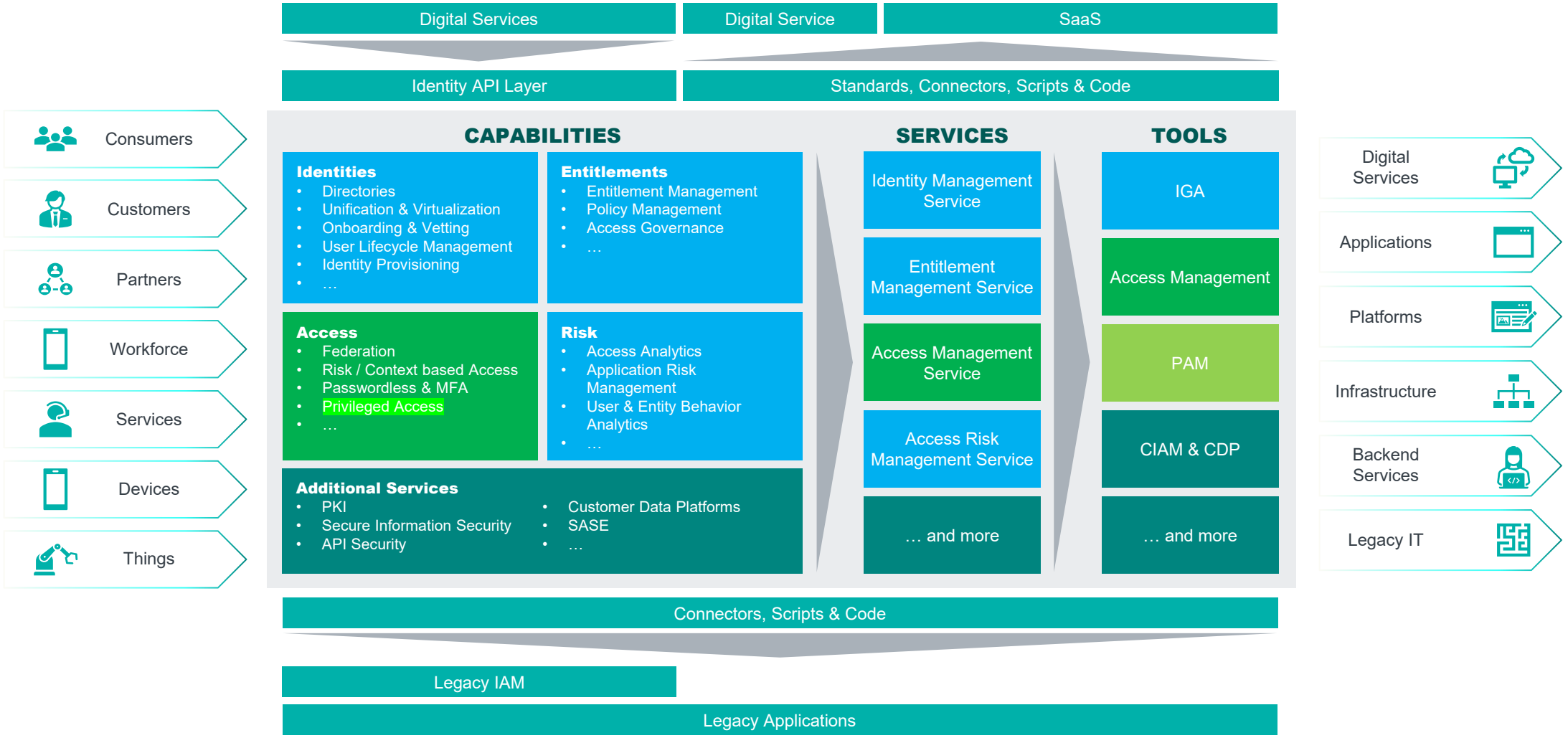
Zukunftsthemen
- Der Markt sieht diese als zunehmend relevant an
- Die Organisation sollte diese Themen beobachten und ggf. später aufgreifen

Kundenspezifische Herausforderungen
- Diese Themen sind für die Organisation besonders relevant



Identity Fabrics: Keine Ein-Hersteller-Lösung

Identity Fabrics bestehen selten nur aus einer Komponente. Z.B. IGA vs. Access Management.



KuppingerCole Identity Fabrics Model

Funktionale Anforderungen: 20 Kernfunktionen an IGA

Eine Auswahlliste als Startpunkt für die konkrete Anforderungsanalyse

Funktionale Breite	Authentifizierungs-funktionen	Benutzer-provisionierung	Identity Lifecycle Management (ILM)	Repository/Directory	Directory-Synchronisation
Zentrale administrative UI	Benutzer-Self-Service	Granulare Autorisierung	Access Governance	Berechtigungs-anforderung	Access Analytics
AI-/ML-basierte Analysten	Review/ Rezertifizierung	Unterstützung hybrider Zielsysteme	API-Unterstützung	Standardprotokoll-unterstützung	Reports
		Dashboards	Unterstützung der Kern-Business-Anwendungen		

Richtig vorbereitet in das IAM-Projekt

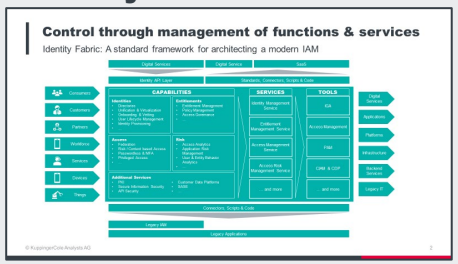
Produktauswahl: Drei Säulen als Grundlage

Vision vs. Produktauswahl: Es muss passen!

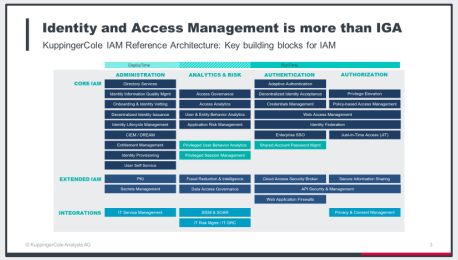
Strategie: IAM Scoping

Was soll konkret erreicht werden?
Was wird spezifisch dafür benötigt?

KC Identity Fabrics als Grundmodell



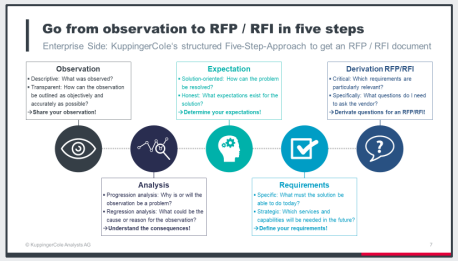
KC IAM Reference Architecture
verbindet strategisches & operationales Level



Unternehmen

Probleme und Anforderungen müssen bekannt sein: Was wird gebraucht / gesucht?

KC's Five-Step-Approach



1. **Beobachtung**: Warum das Ganze?
2. **Analyse**: Was sind die Konsequenzen?
3. **Erwartung**: Was soll erreicht werden?
4. **Anforderungen**: Klare Definition!
5. **Ableitung RFP/RFI**: Welche Fragen müssen im RFP/RFI gestellt werden?

Markt

Vorbereitet sein: Welche Anbieter, Produte und Partner gibt es am Markt?

IAM-Anbieter und -Produkte
Es gibt zahlreiche Hersteller mit unterschiedlichen Produkten, Funktionalitäten, Partner-Netzwerken und Spezialisierungen.

Herkunft und Spezialisierung
Jeder Anbieter hat seine eigene Historie und entsprechende Stärken und Schwächen und eine Spezialisierung. Das muss passen.

Branchenfokus
IAM ist überall relevant. Dennoch gibt es Branchenschwerpunkte und spezifische Anforderungen z.B. in den Prozessen und bei der Zielsystemanbindung.Der Branchenexperte ist meist besser geeignet als der Generalist.

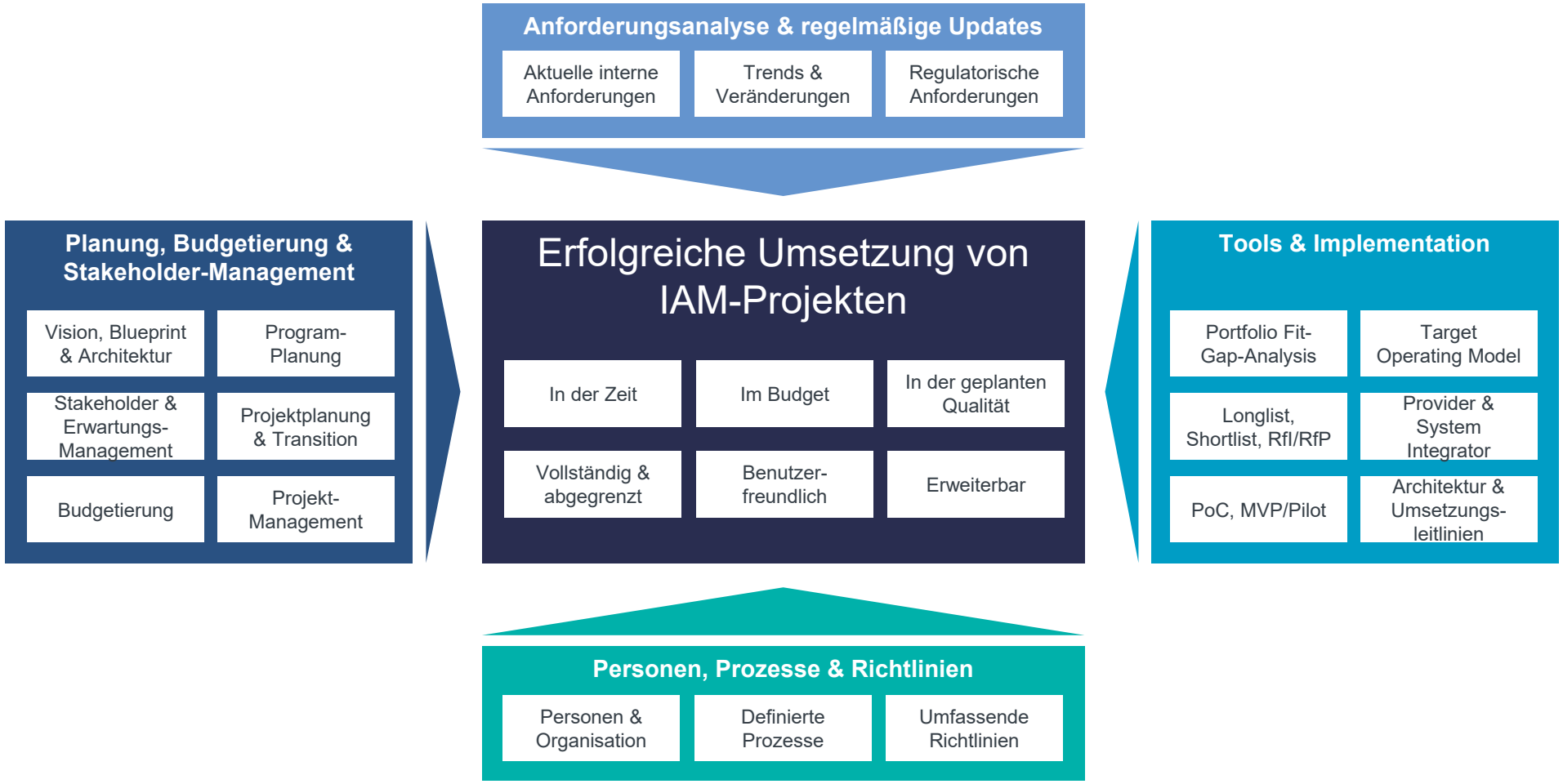
Strategische Ausrichtung
IAM entwickelt sich schnell weiter. Deshalb sollte auf Hersteller fokussiert warden, die eine klare Strategie haben und gezeigt haben, dass sie sich an geänderte Anforderungen anpassen können.

10 häufige Stolpersteine in IAM-Projekten

Die Bereiche, auf die man achten sollte, um ein IAM-Projekt erfolgreich umzusetzen

Schlüsselfaktoren für den Erfolg von IAM-Projekten

Viele Faktoren bestimmen den Erfolg von IAM-Projekten



DANKE!

Fragen?

Bei Fragen können Sie sich gerne direkt an mich wenden (mk@kuppingercole.com)

KuppingerCole Analysts AG
Wilhelmstr. 20 - 22
65185 Wiesbaden | GERMANY

P: +49 | 211 - 23 70 77 - 0
F: +49 | 211 - 23 70 77 – 11

E: info@kuppingercole.com
www.kuppingercole.com