KPMG

VAIT - ein Jahr versicherungsaufsichtliche Anforderungen an die IT

Herausforderungen aus Sicht eines Wirtschaftsprüfers

Vaike Metzger, Partnerin KPMG

—

42. Versicherungswissenschaftliches Fachgespräch

Berlin, 19. Juni 2019

Agenda

1 KPMG Perspektiven auf die VAIT Umsetzung

2 VAIT Benchmark im Überblick

3 IT-Governance als Basis der VAIT Erfüllung

4 Informationsrisikomanagement: Mehr als nur der Informationsverbund

5 Benutzerberechtigungsmanagement: Ein IAM als zentrales Tool zum Erfolg

6 Fazit

Agenda

1 KPMG Perspektiven auf die VAIT Umsetzung

2 VAIT Benchmark im Überblick

3 IT-Governance als Basis der VAIT Erfüllung

4 Informationsrisikomanagement: Mehr als nur der Informationsverbund

5 Benutzerberechtigungsmanagement: Ein IAM als zentrales Tool zum Erfolg

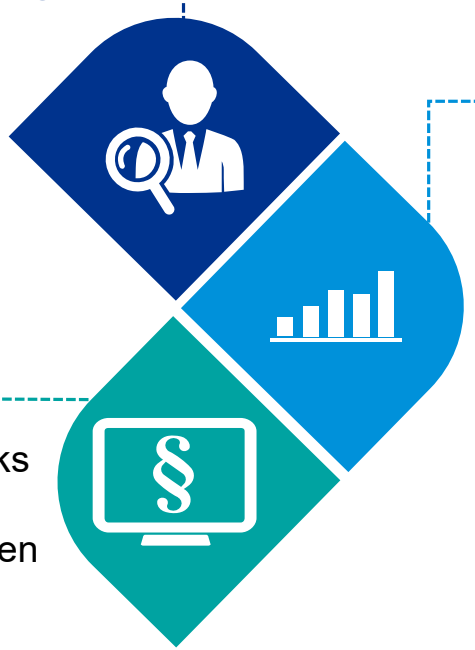
6 Fazit

Unterschiedliche Perspektiven geben KPMG einen Überblick der Umsetzungsherausforderungen der VAIT

IT Audit i.R.d. Jahresabschlussprüfung

— Schnittmenge aus IT Audit und VAIT Themenbereichen

— Stand der VAIT Umsetzung als Fokusthema



VAIT Benchmark

Vorläufiger Stand

— Durchführung eines VAIT Benchmarks 2018/19 zur Ermittlung des Umsetzungsgrades der VAIT Anforderungen

— Analyse der Antworten zur Identifikation von Umsetzungs-herausforderungen

IT-Compliance Projekte

— Durchführung von VAIT Quick-Checks und Gap-Analysen bei deutschen Versicherern unterschiedlicher Größen

— Umsetzungsprojekte zur Umsetzung von Anforderungen

— Vorbereitung auf und Begleitung von aufsichtsrechtlichen Sonderprüfungen

Agenda

1 KPMG Perspektiven auf die VAIT Umsetzung

2 VAIT Benchmark im Überblick

3 IT-Governance als Basis der VAIT Erfüllung

4 Informationsrisikomanagement: Mehr als nur der Informationsverbund

5 Benutzerberechtigungsmanagement: Ein IAM als zentrales Tool zum Erfolg

6 Fazit

Der KPMG Benchmark liefert eine Selbsteinschätzung der Branche zum Erfüllungsstand der VAIT Umsetzung

An ISO/IEC 15504 orientierte Erfüllungsgrad-skala

6-monatiger Erhebungs-zeitraum[a] (2018-2019)

Vergleichbarkeit der Aussagen durch Gliederung auf VAIT Gebiet[b]

Vorläufiger Stand

Versicherungen unterschiedlicher Größenklassen

Befragte aus verschiedenen Hierarchiestufen und Abteilungen

Erst- und Rückversicherer

Anm.: (a) Vorläufige Benchmarkergebnisse

(b) Aufnahme KRITIS als Modul der VAIT im März 2019, daher nicht Teil der diesjährigen Benchmarkstudie

KPMG Erfahrungen und Benchmarkergebnisse zeigen Herausforderungen und Handlungsschwerpunkte der Versicherer

IT-Governance

Nachvollziehbare Ausrichtung der IT-Governance an gängigen Standards bei Versicherungsunternehmen verschiedener Größen nicht vollständig gegeben

Informationsrisikomanagement

Aufbau eines Informationsverbundes als wesentliches Handlungsfeld zum Informationsrisiko-management gesehen

Benutzerberechtigungsmanagement

Aufbau und Verwaltung eines Benutzerberechtigungsmanagements wird weiterhin als zentrale Herausforderung innerhalb der VAIT Vorgaben gesehen

1 = nicht erfüllt; 2 = teilweise erfüllt; 3 = weitgehend erfüllt; 4 = vollständig erfüllt

Agenda

1 KPMG Perspektiven auf die VAIT Umsetzung

2 VAIT Benchmark im Überblick

3 IT-Governance als Basis der VAIT Erfüllung

4 Informationsrisikomanagement: Mehr als nur der Informationsverbund

5 Benutzerberechtigungsmanagement: Ein IAM als zentrales Tool zum Erfolg

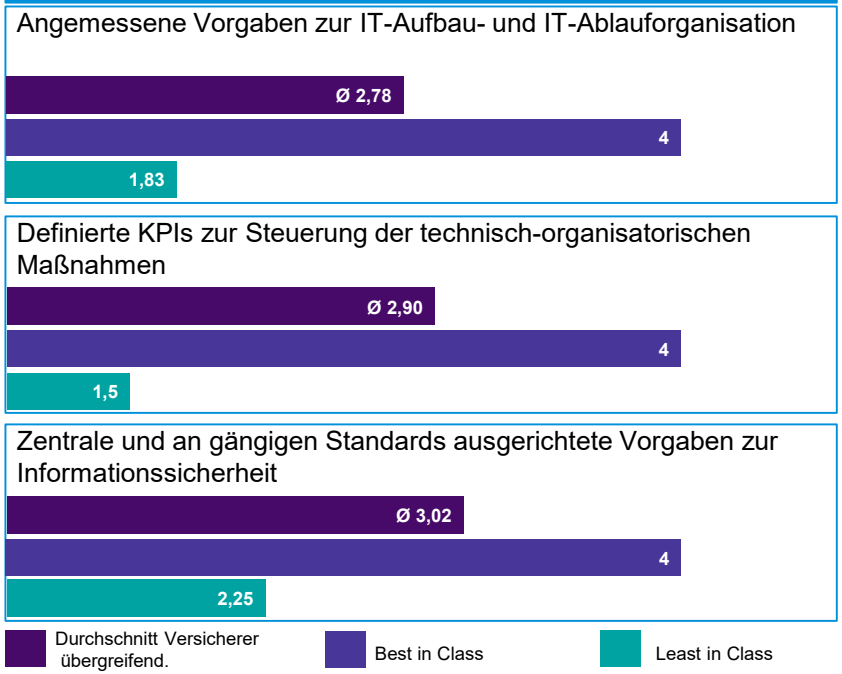
6 Fazit

IT-Governance als Basis der VAIT Erfüllung

Ausrichtung an gängigen Standards stellt Versicherer vor Herausforderungen

Benchmark Reifegrad zu IT-Governance

Benchmark Reifegrad einzelner VAIT Anforderungen



KPMG Einschätzung

Die Umsetzung der IT-Governance Vorgaben wird im Vergleich zu den weiteren VAIT Modulen mit dem höchstem Reifegrad eingeschätzt.

Vorgaben an First und Second Line of Defense Funktion hinsichtlich der Rollen und Aufgaben oft nicht trennscharf umgesetzt. Tw. noch Umsetzung getrennter Rollen für 1st und 2nd Line notwendig.

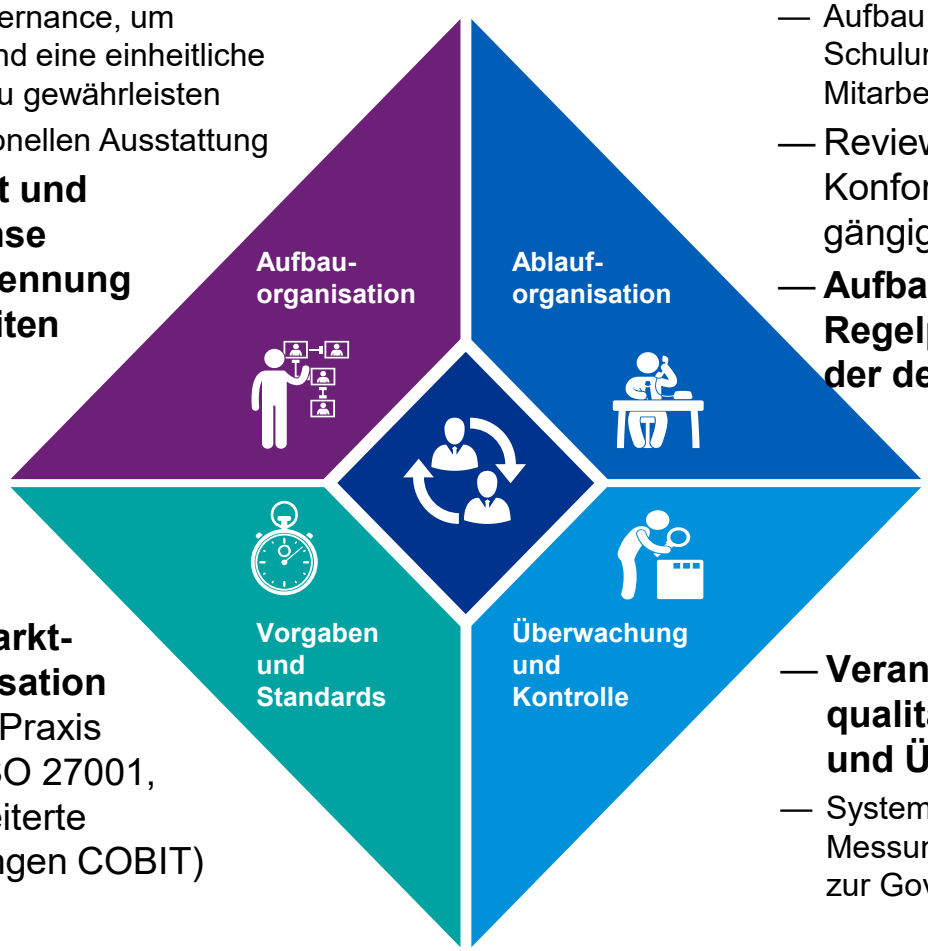
KPIs teilweise eher auf strategischer Ebene. Operationalisierung von KPIs zur Überwachung der Governance häufig noch umzusetzen.

Ausrichtung an gängigen Standards noch nicht durchgängig oder vollständig umgesetzt; einzelne Prozesse sind tw. z.B. an COBIT ausgerichtet oder Security an ISO 2700x Standards.

1 = nicht erfüllt; 2 = teilweise erfüllt; 3 = weitgehend erfüllt; 4 = vollständig erfüllt

Im Fokus der Governance Aktivitäten stehen u.a. die Ausrichtung an Standards und Abgrenzung der 1st und 2nd Line Rollen und Aufgaben

- Zentralisierung der IT-Governance, um Skaleneffekte zu nutzen und eine einheitliche Anforderungsumsetzung zu gewährleisten
- Angemessenheit der personellen Ausstattung
- **Überprüfung der First und Second Line of Defense Aufgaben mitsamt Trennung der Verantwortlichkeiten und Tätigkeiten**



- Aufbau von Regelprozessen zur Schulung und Weiterbildung von Mitarbeitern unter Einbindung von HR
- Review bestehender Prozesse auf Konformität zu den Vorgaben gängiger Markstandards
- **Aufbau (automatisierter) Regelprozesse zur Überwachung der definierten KPIs**

- **Etablierung gängiger Markt-standards in der Organisation und den Policies** (in der Praxis verbreitet sind ITIL und ISO 27001, BSI für Cloud, durch erweiterte regulatorische Anforderungen COBIT)

- **Verankerung quantitativer und qualitativer KPIs zur Steuerung und Überwachung**
- Systembasierte und automatisierte Messung von quantitativen Kennzahlen zur Governance

Agenda

1 KPMG Perspektiven auf die VAIT Umsetzung

2 VAIT Benchmark im Überblick

3 IT-Governance als Basis der VAIT Erfüllung

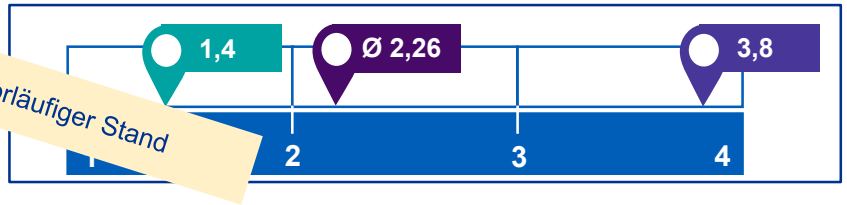
4 Informationsrisikomanagement: Mehr als nur der Informationsverbund

5 Benutzerberechtigungsmanagement: Ein IAM als zentrales Tool zum Erfolg

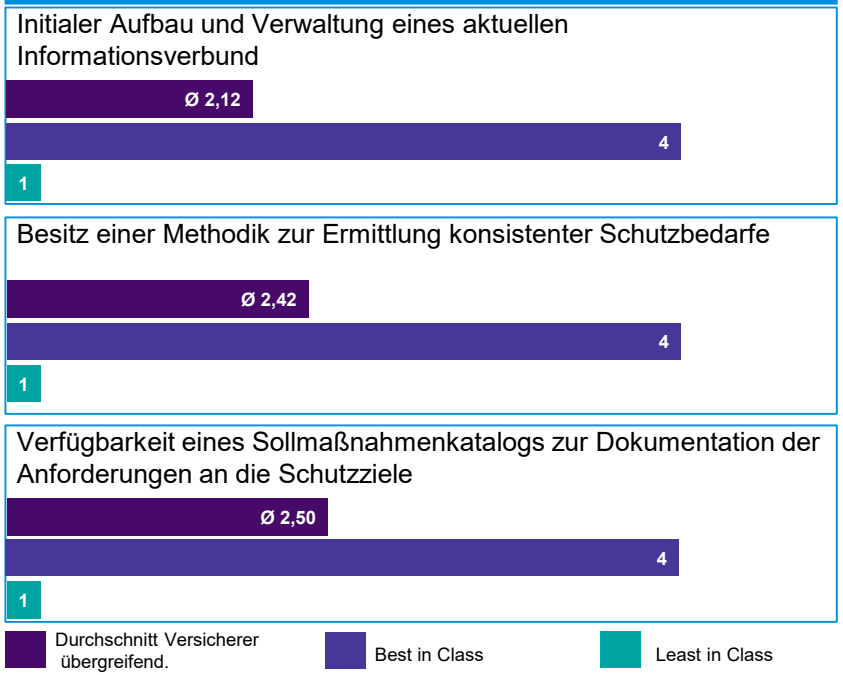
6 Fazit

Status zum Informationsverbund und Sollmaßnahmenkatalog entscheidend für den Erfüllungsgrad

Benchmark Reifegrad zu Informationsrisikomanagement



Benchmark Reifegrad einzelner VAIT Anforderungen



KPMG Einschätzung

Dokumentation eines übergreifenden Informationsverbundes als wesentliche Herausforderung gesehen aufgrund der hohen Komplexität der IT-Landschaften.

Tools und Prozesse zur Dokumentation des Informationsverbunds häufig noch in Umsetzung. Erfassung von IDVn und Einbezug von Schnittstellen an Dienstleister als zentrale Herausforderung.

Kataloge mit IT-Risiken bisher nicht umfassend an Standards wie BSI ausgerichtet. Eher überschaubarer Umfang an Risiken für die IT als Grundlage für Ermittlung von Schutzbedarfskategorien definiert.

In den meisten Fällen sind Sollmaßnahmen für die identifizierten Risiken festgelegt. Allerdings sind Sollmaßnahmenkataloge um die noch nicht abgedeckten Risiken zu ergänzen.

1 = nicht erfüllt; 2 = teilweise erfüllt; 3 = weitgehend erfüllt; 4 = vollständig erfüllt

Handlungsmaßnahmen in Bezug auf das Informationsrisikomanagement

1. Identifikation von Assets

Identifikation aller Information Assets inkl. Art, Owner und Übertrag in ein Assetregister (Informationsverbund).
Regelmäßige Überprüfung des Registers.

2. Klassifizierung von Assets

Bewertung der Methoden und Erneuerung der Schutzbedarfsanalyse zur Evaluation der Auswirkung bei einem Verlust von Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität.

3. Identifizierung des Risikos

Update der Risikoanalyse auf Basis komplettierter Informationsrisiken insbesondere unter Einbezug gängiger Standards.

4. Aufbau von Zielschutzvorgaben

Festlegung von Zielschutzvorgaben/ Minimum Standards für vordefinierte Schutzgruppen basierend auf deren Kritikalitätsniveau. Nutzung von gängigen Risikokategorien gemäß Standards.

5. Durchführung Risikobewertung

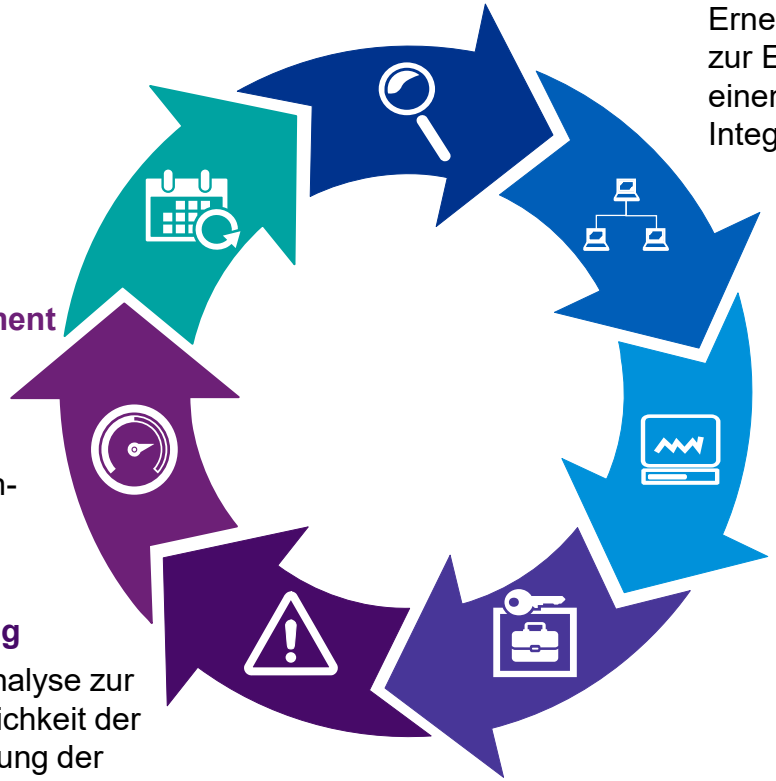
Durchführen einer initialen Risikoanalyse zur Bewertung der Eintrittswahrscheinlichkeit der identifizierten Risiken unter Beachtung der implementierten Zielschutzvorgaben.

6. Durchführung Risikomanagement

Zuordnung von Sollmaßnahmen in einem Sollmaßnahmenkatalog pro identifizierten IT-Risiko. Pflege und Aktualisierung des Sollmaßnahmen-katalogs.

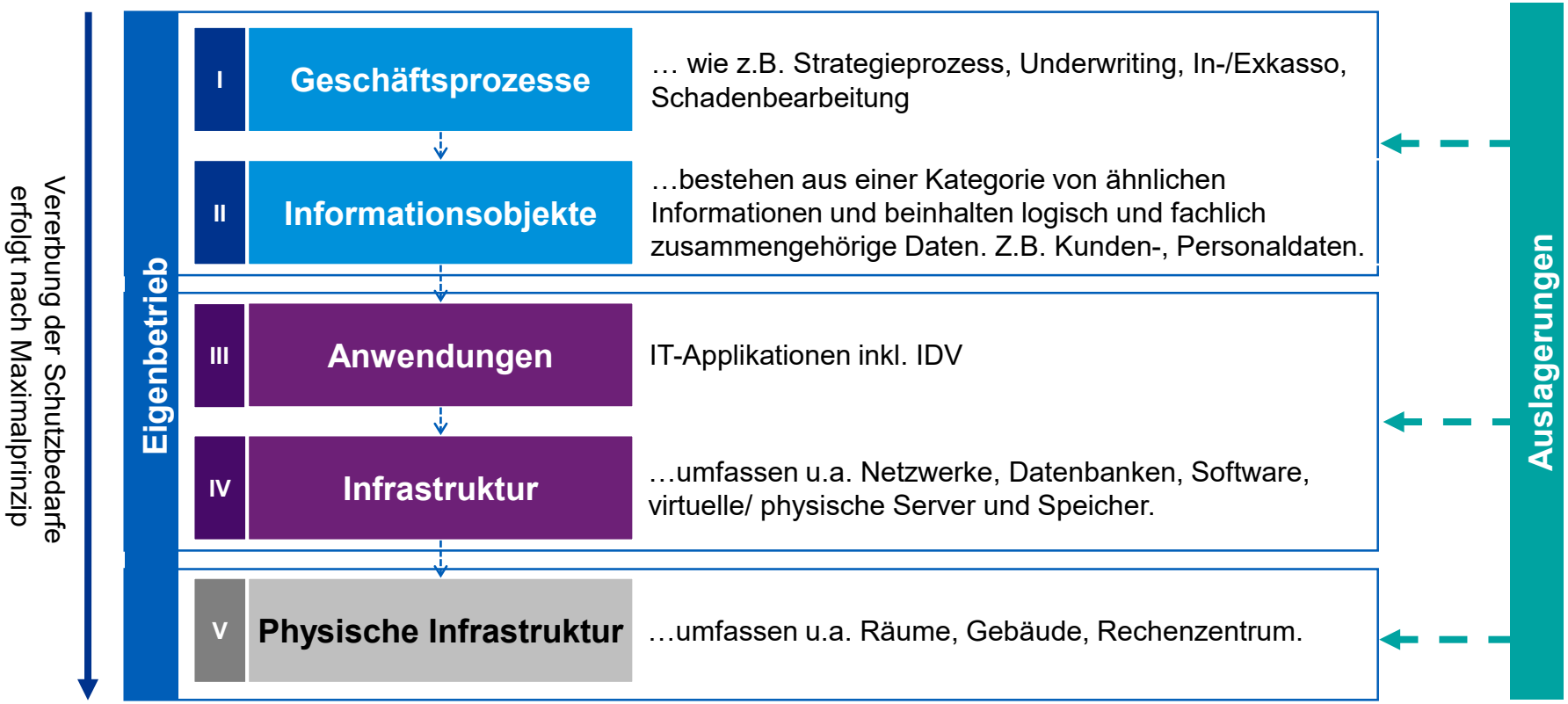
7. Durchführung Risikoüberwachung

Aufbau von Dashboards und Scorecard-Systemen zur Risikobeurteilung (automatisiertes Mapping von Schwachstellen auf betroffene Informationen und somit Wertschöpfung) unter zeitgleichen Etablierung eines regelmäßigen Berichterstattungsprozesses.



Komponenten und Logik des Informationsverbunds

Der Informationsverbund enthält IT und non-IT Komponenten und verbindet Fachbereichs- mit IT-Sichten.



Agenda

1 KPMG Perspektiven auf die VAIT Umsetzung

2 VAIT Benchmark im Überblick

3 IT-Governance als Basis der VAIT Erfüllung

4 Informationsrisikomanagement: Mehr als nur der Informationsverbund

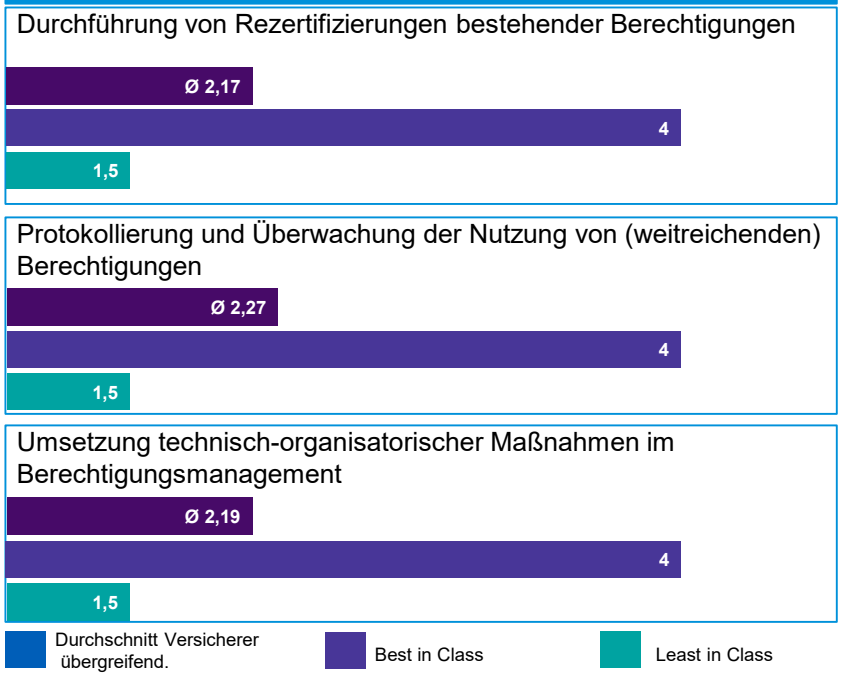
5 **Benutzerberechtigungsmanagement: Ein IAM als zentrales Tool zum Erfolg**

6 Fazit

Verwenden eines IAM-Systems als Rückgrat zur Erfüllung der VAIT Anforderungen zum Berechtigungsmanagement

Benchmark Reifegrad Benutzerberechtigungsmanagement

Benchmark Reifegrad einzelner VAIT Anforderungen



KPMG Einschätzung

Bei der Auswahl, Einführung und Integration von IAM-Systemen stellen die Legacy-Systeme eine wesentliche Herausforderung dar.

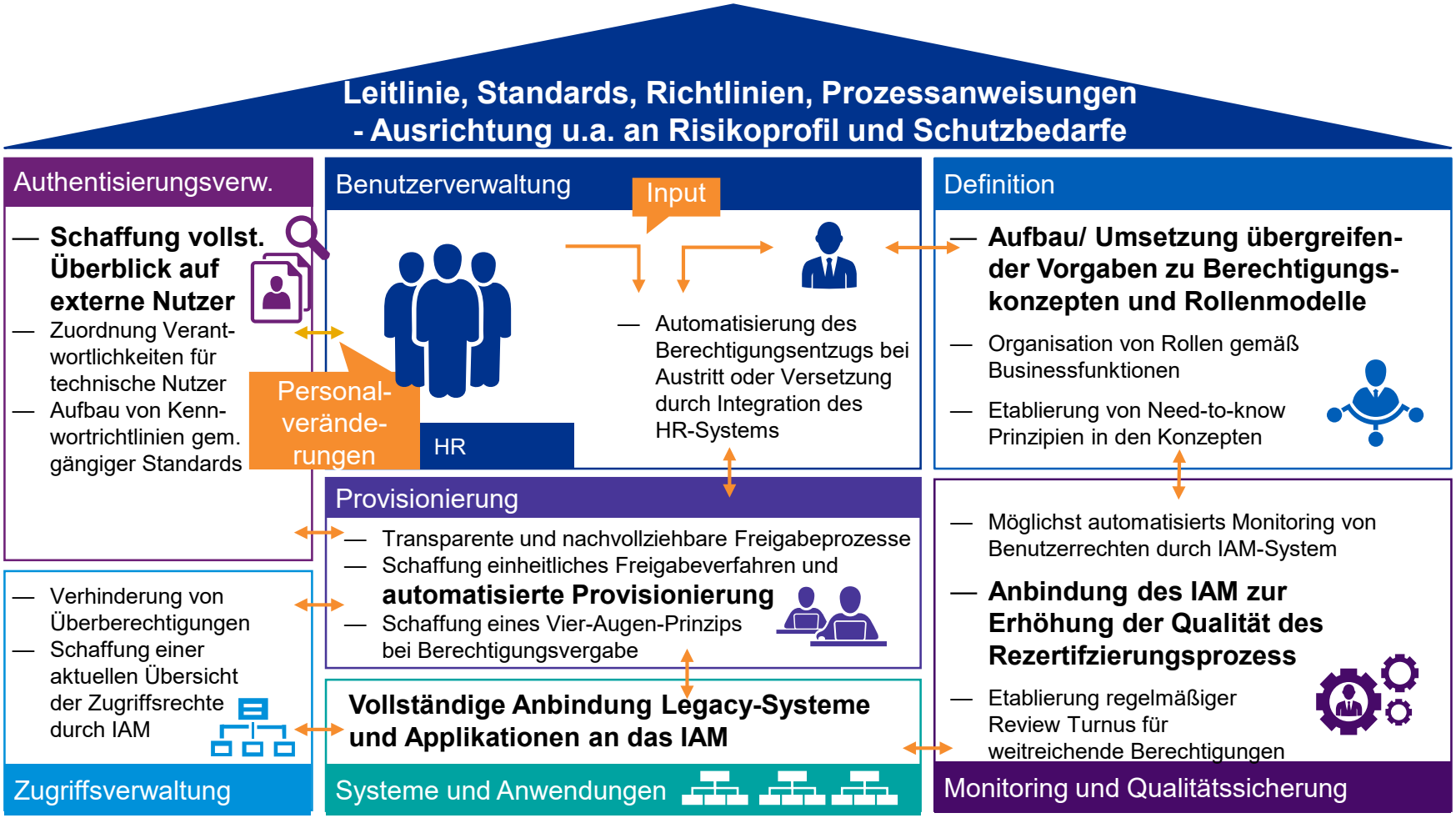
Rezertifizierungen werden häufig noch mit manuellen und nicht ausreichend dokumentierten Prozessen durchgeführt. Frequenz für Review von Nutzern mit weitreichenden Berechtigungen oft in Überarbeitung.

Protokollierung von Nutzern mit weitreichenden Berechtigungen für Datenbanken ist oft nicht ausr. definiert oder nicht vorhanden. Wahrnehmung hat in den vergangenen Jahren aber stetig zugenommen.

IAM-Systeme selten schon umfänglich implementiert, die Vorgaben von Leitlinien etc. vollständig abbilden. Manuelle Prozesse fehleranfällig bzgl. Berechtigungsvergaben und Rezertifizierungen.

1 = nicht erfüllt; 2 = teilweise erfüllt; 3 = weitgehend erfüllt; 4 = vollständig erfüllt

Handlungsmaßnahmen in Bezug auf das Benutzerberechtigungs-management



Agenda

1 KPMG Perspektiven auf die VAIT Umsetzung

2 VAIT Benchmark im Überblick

3 IT-Governance als Basis der VAIT Erfüllung

4 Informationsrisikomanagement: Mehr als nur der Informationsverbund

5 Benutzerberechtigungsmanagement: Ein IAM als zentrales Tool zum Erfolg

6 Fazit

Fazit

Handlungsfelder sind oft bekannt, teilweise herrscht jedoch Unsicherheit zur Umsetzungstiefe oder der Umsetzungsaufwand wird unterschätzt

Die VAIT beschleunigen den Druck auf die Umsetzung und Ausweitung von Compliance Projekten.

Weitere Transparenz über die erwartete Umsetzungstiefe wird aus laufenden und kommenden aufsichtlichen Prüfungen erwartet.

Das strukturierte Zusammenspiel zwischen Fachbereich und IT wird zunehmend als Voraussetzung für effektive Lösungen gesehen.

Gängige Standards helfen beim Aufbau notwendiger Strukturen und Prozesse.

Die Einführung von Tools (z.B. IAM, SIEM) soll nicht nur die Umsetzung der VAIT Anforderungen und das Schließen von Audit Feststellungen unterstützen.

Es wird auch das Heben von Prozesseffizienzen erwartet.

Vaike Metzger

Partnerin, Financial Services,
Leiterin Business Technology

T +49 89 9282-4816

M+49 172 2895793

vmetzger@kpmg.com

www.kpmg.de/socialmedia

www.kpmg.de