



Identity Access Governance Beratung

Profitieren Sie von unserem Beratungsangebot im Bereich Identity Access Governance (IAG). Mit unserem ganzheitlichen Ansatz begleiten wir Sie von der ersten Analyse bis hin zur Umsetzung von Framework oder Best of Breed Teillösungen für mehr IT-Sicherheit in Ihrem Unternehmen.

www.tuv.com/iam

 **TÜVRheinland**[®]
Genau. Richtig.

NEUES DIGITALES UMFELD ERFORDERT ZUKUNFTSSICHERE IAG LÖSUNGEN

Innovationsdruck, Time-to-Market oder Compliance-Treue: Unsere Umwelt ändert sich in zunehmendem Tempo. Auf die daraus resultierenden neuen Anforderungen gesellschaftlicher, technologischer und organisatorischer Art muss Ihr Unternehmen individuell, gezielt und zeitnah reagieren können.

Neben der Verknüpfung der *IT-Welt* mit dem *Internet of Things (IoT)* und der *industriellen Operational Technology (OT)* sind auch die fließenden Übergänge von On-Premise über hybride bis hin zu cloudbasierten IT-Lösungen ein wesentlicher Bestandteil unseres heutigen digitalen Umfelds. Daraus ergeben sich weitreichende neue Bedrohungslagen und damit neue Sicherheitsanforderungen. Dies drückt sich auch in neuen, strikteren regulatorischen Auflagen und Nachweispflichten aus.

All diesen Rahmenbedingungen müssen sich moderne Identity-Access-Governance-Lösungen (IAG) stellen. IAG-Lösungen ermöglichen es Identitäten, Rollen, Rechte und Prozesse Anforderungskonform zu verwalten und damit zu schützen. Sie dienen letztlich als verbindendes und steuerndes Element zwischen den regulatorischen Anforderungen und unternehmerischen Herausforderungen.

Zukunftssichere IAG-Lösungen müssen deshalb in all ihren Facetten, als **Framework-Ansätze** oder Kombination von punktuellen **Best-of-Breed-Lösungen**, die dynamischen Sicherheitsanforderungen und Bedrohungslagen flexibel adressieren können. Dies umfasst sowohl die

technologischen als auch die organisatorischen und prozessualen Aspekte.

GLOBAL RISK AND COMPLIANCE KOMBINIERT MIT INFORMATION SECURITY MANAGEMENT

Unsere Experten unterstützen und beraten Sie umfassend zu allen Fragestellungen der IT-Security. In unserem kombinatorischen Ansatz erfolgt die Betrachtung der IAG unter Einbeziehung der Themen:

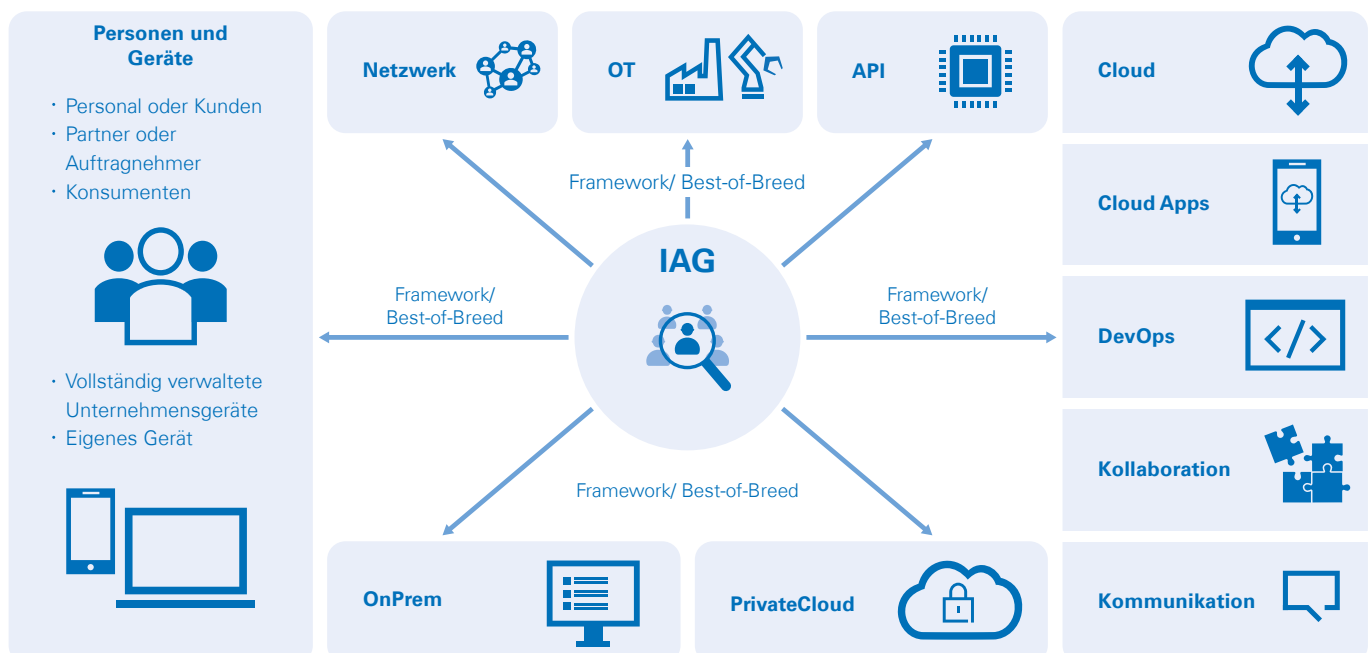
- Schutzbedarfsanalysen
- Risikoanalysen
- Global Risk and Compliance
- Information Security Management

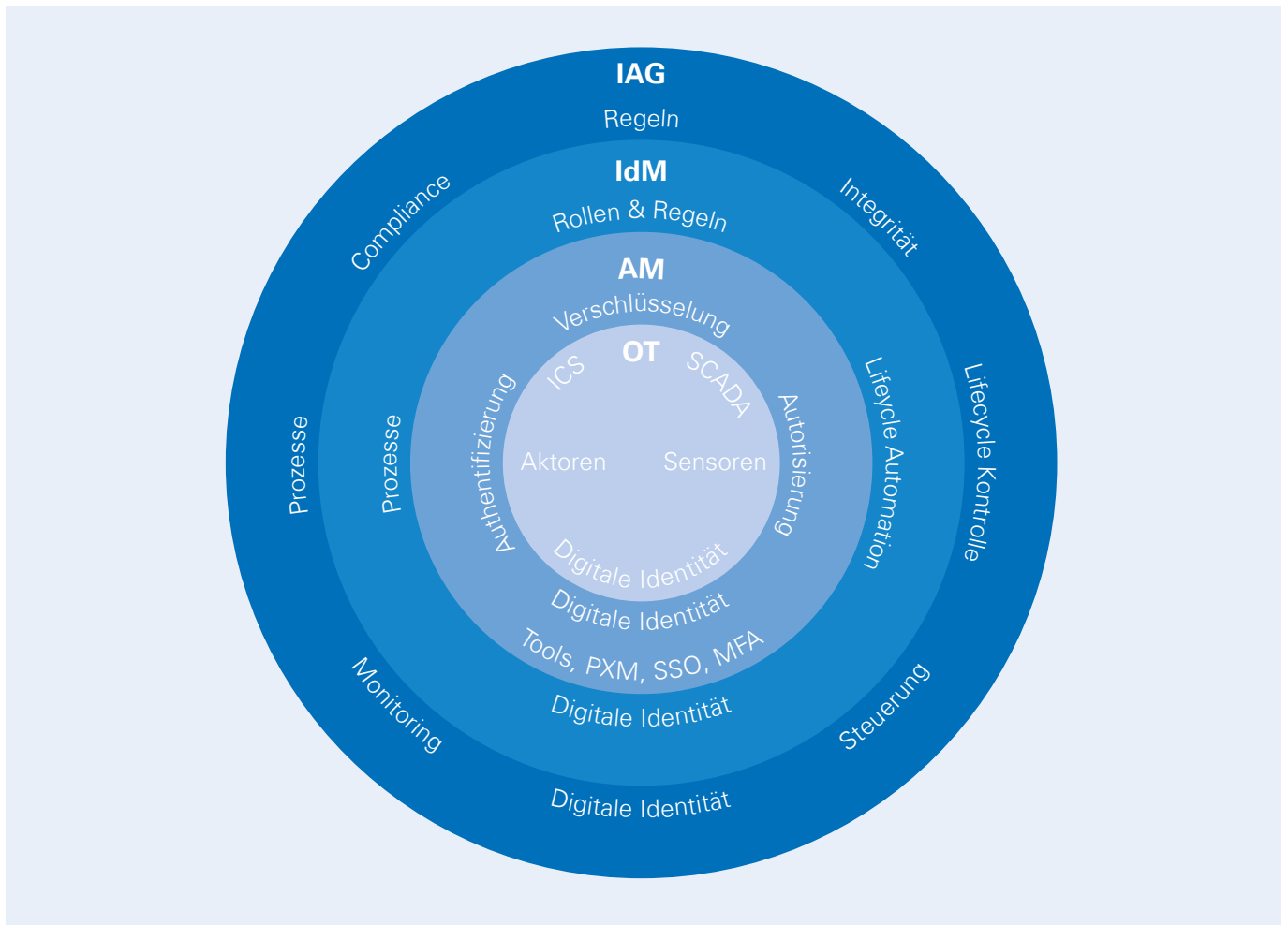
Im Kontext der Identity-Access-Governance-Beratungsmandate wird neben der Nutzung des Best-Practice-Ansatzes unser gesamtes Beratungsleistungsspektrum eingebracht: Von der Planung langfristiger **Identity-Access-Governance-Unternehmensstrategien** bis hin zur Umsetzung von **Best-of-Breed-Teillösungen** sind wir Ihr starker, vertrauensvoller Partner.

INDIVIDUELLER, GANZHEITLICHER ANSATZ

Die Beratungsteilschritte sind jeweils nach Best-Practice-Vorgehen optimiert und können individuell auf Ihre Bedürfnisse abgestimmt werden. Durch einen modularen Aufbau kann das Gesamtvorhaben in **logische Ebenen** und **Einzelschritte** aufgeteilt werden. Daraus resultiert die Möglichkeit im Bedarfsfall für jede Phase eines Vorhabens eigenständige Projekte bzw. Angebote zu nutzen.

GANZHEITLICHE IDENTITY-ACCESS-GOVERNANCE-LÖSUNGEN





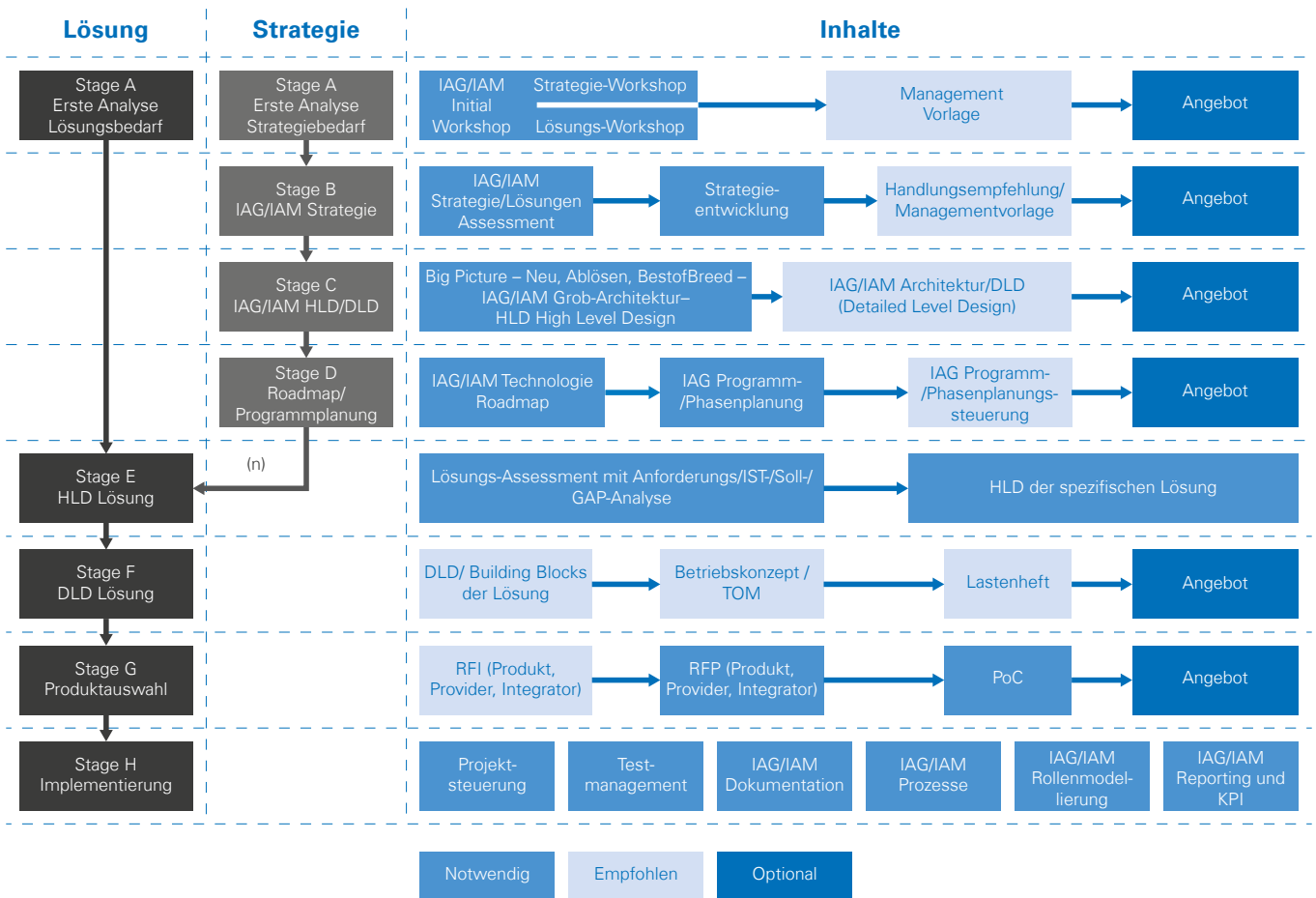
VIER DETAILLIERUNGSEBENEN IHRER IAG BERATUNG

Die IT-Security Disziplin Identity and Access Management beinhaltet in ihren verschiedenen Ebenen die unterschiedlichen Ausprägungen und Themenbereiche mit steigendem Detaillierungsgrad.

Während im Kontext *Identity Access Governance (IAG)* insbesondere die **strategische Beratung** eine Kernrolle einnimmt, wird in den Bereichen *Identity Management (IdM)* und *Access Management (AM)* der **kurzfristige Handlungscharakter** größer.

Operational Technologies (OT) und *Information Technologies (IT)* stellen währenddessen die eigentlichen Komponenten und Systeme dar, auf die zugegriffen wird. In diesem Setup können von strategischen Neuausrichtungen der IAG-Landschaft bis hin zu losgelösten Aufträgen mit dem Ziel der **punktuellen Entsprechung von Compliance-Ansprüchen** eine Vielzahl an Anforderungsmandaten erfolgreich in Anspruch genommen werden.

PHASEN DER IAG BERATUNG



IDENTITY ACCESS GOVERNANCE PHASENMODELL

Unsere Experten haben übergreifend die jeweils den Anforderungen entsprechende Beratungskompetenz inne. So kann in jeder der hier dargestellten Ebenen das Phasenmodell mit seinen spezifischen Leistungsinhalten individuell abgerufen werden.

STAGE A (LÖSUNG & STRATEGIE)

Erste Analyse Strategie- und Lösungsbedarf

In einem initialen Workshop wird mit den Stakeholdern der Bedarfsumfang erarbeitet und analysiert. Daran anknüpfend kann eine Managementvorlage erstellt werden, um die strategische Relevanz jederzeit aufzeigen zu können.

STAGE B (STRATEGIE)

IAG/IAM Strategie

In Stage B geht es, neben dem Verständnis für die die IAG/IAM umgebende Landschaft, auch um die konkrete Entwicklung der IAG/IAM-Strategie.

Sie entwickeln konkrete Handlungsempfehlungen und eventuell notwendige Managementvorlagen, um den strategischen Lösungscharakter zu stärken.

STAGE C (STRATEGIE)

IAG/IAM HLD/DLD

In dieser Phase entwickeln Sie neue Lösungen, überarbeiten bestehende Lösungen oder entwickeln mithilfe des Best-of-Breed-Ansatzes eine Grob-Architektur, die im High-Level-Design (HLD) verankert wird. Es empfiehlt sich daran anknüpfend die Erstellung des Detailed-Level-Designs (DLD) zur IT-Architektur.

STAGE D (STRATEGIE)

Roadmap/Programmplanung

Aus den Stages A bis C abgeleitet, wird in dieser Phase die IAG/IAM-Technologie-Roadmap entwickelt und festgehalten.

Wir empfehlen die daraus resultierende IAG-Programm- und Phasenplanungssteuerung ebenfalls zu entwickeln. Damit ist die reibungslose Abfolge und der kontrollierte Fortschritt im Projektvorhaben sichergestellt wird.

Sind die in Stage A definierten/analysierten Lösungsbedarfe bereits identifiziert und das Vorhaben entsprechend spezifisch bewertet, kann auf die Stages B bis D verzichtet werden. Es wird nach Stage A unmittelbar an Stage E angeknüpft.

STAGE E (LÖSUNG & STRATEGIE)

HLD Lösung

In dieser Phase erfolgt die Betrachtung der für die Gesamtarchitektur notwendigen einzelnen Lösungsbausteine. Dazu wird ein Lösungsassessment je benötigtem Lösungsbaustein durchgeführt. Der spezifische Lösungsumfang wird in das vorhandene HLD eingebracht.

STAGE F (LÖSUNG & STRATEGIE)

DLD Lösung

Die hier verankerten Inhalte sind allesamt empfohlene Handlungsparameter. So wird hier das DLD durch die entsprechenden Building Blocks strukturiert, Betriebskonzepte und technisch, organisatorische Maßnahmen (TOMs) bestimmt und ein Lastenheft erstellt.

STAGE G (LÖSUNG & STRATEGIE)

Produktauswahl

Im Bedarfsfall kann hier die Request-for-Information (RFI) die Produktauswahl entsprechend einleiten und eine erste Spezifizierung der Shortlist bieten.

In Abhängigkeit des abgestimmten Umfangs wird der Request-for-Proposal (RFP) prozessiert. Produkte, Provider oder Integratoren werden dem Gesamtvorhaben ausgewählt und in einem anknüpfenden Proof-of-Concept (PoC) verprobt und pilotiert.

STAGE H (LÖSUNG & STRATEGIE)

Implementierung

Je nach gewähltem Lösungsprodukt kann die Implementierung durch uns oder einen dementsprechend zu dirigierenden Implementierungspartner vorgenommen werden. Darüber hinaus wird das Testmanagement der zu implementierenden Lösung vorangetrieben, die IAG/IAM relevanten Prozesse entworfen und dokumentiert sowie entsprechende Rollen modelliert. Abschließend werden IAM/IAG relevante KPIs und Reporting-Methoden entworfen, um Relevanz, Fortschritt und Erfolg des Vorhabens zu manifestieren.

GERNE UNTERSTÜTZEN WIR SIE RUND UM DAS THEMA ZUKUNFTSORIENTIERTE IDENTITY ACCESS GOVERNANCE LÖSUNGEN MIT UNSEREM MODULARISIERTEN BERATUNGSANGEBOT. FRAGEN SIE UNS!

[ONLINE KONTAKT](#)

TÜV Rheinland Industrie Service &
Cybersecurity
Am Grauen Stein
51105 Köln
Tel. +49 221 806-0
cybersecurity@tuv.com

www.tuv.com/iam

 **TÜVRheinland®**
Genau. Richtig.