PwC Digital Identity - Trends

Personal intro

EMEA Digital Identity Leader for PwC

I work with IAM teams, CISOs, and boards.

I'm on a mission!

PwC's global Digital Identity practice at a glance

PwC's global team of more than 1700 IAM/Digital Identity professionals are part of a larger team of 4,500+ practitioners and include **specialised consultants, architects and engineers** next to intelligence analysts, cyber-forensics investigators, attorneys and consultants, as well as industry leaders in cybersecurity and privacy. Our team has deep experience helping businesses across industries strategically assess, design, deploy, improve and run cybersecurity and IAM programs and solutions.

North America
700 professionals

South America
200 professionals

EMEA
500 professionals

Asia/Pacific
300 professionals

1700+ IAM professionals - >2.3 Billion Identities managed

- -

Experienced with technology from leading IAM vendors in the market including but not limited to:

SailPoint
Named PwC its Worldwide Partner of the Year and Admiral status of the past nine years (2023, 2022, 2021, 2020, 2019, 2018, 2017, 2016, 2014). Admiral status is only awarded to business integrators with the highest customer satisfaction.

CyberArk
Named PwC its (Global/EMEA) Systems Integrator or innovator of the Year (2023, 2022, 2021, 2020, 2018, 2017, 2016)

Saviynt
Named PwC **featured partner** (2022, 2021, 2020, 2018, 2017) And **Global GSI partner** for 2024

SAP GRC
PwC is global partner for SAP GRC, authorisations management.

OKTA
Named PwC Global and EMEA Advisory partner of 2021, 2020, 2019 Okta Elevate Partner Program Apex Partner 2023

Microsoft
PwC and Microsoft have had a strategic partnership for cybersecurity since 2018

In 2022 PwC was named Entra ID System Integrator of the Year and in 2023 Identity global finalist.

ForgeRock / Ping Identity
In Gold partnership with PwC since June 2010. PwC is a Partner Board member and partner of the year in 2022, 2020.

Market developments our clients are facing

A world where the only constant is change, more challenging than ever before

Emerging Technologies increasing risk

- Generative AI - reality with ChatGPT, DALL-E and others
- Automatic code generation in new products, software and services
- Quantum Computing
- Rapid digital transformation and increasing SaaS adoption
- Agentic AI
- BioHacking

War for cyber and privacy talent

- Ensure significant development opportunities for our talent
- Embrace new way of working
- Uptake Generative AI will impact the setup of our workforce

Increased complexity starts to drive action

- Significant Supply Chain complexity and dependency
- Increase in connected devices
- Blurring lines between IT and OT/IoT
- Multi-cloud computing

Increasing (economic) crime and cyber threats from different actors

- Criminals
- Espionage
- Nation state
- Hacktivists
- Insider Threat

New (and old) regulations continue to impact our clients

- DORA
- NIS2
- PSD3
- EUDI
- Privacy laws including GDPR, CCPA and PIPL
- ESG
- DAC7
- Regulator Scrutiny
- Responsible AI

Rising geopolitical tension is impacting (cyber) warfare and (physical) security
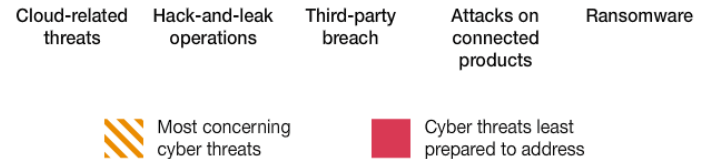
- Intellectual property
- Critical infrastructure
- Integration physical, product, production and information security
- Misinformation & political influencing
- Sanctions compliance

Cloud related (identity) threats, connected products, and third party risk is driving the convergence of Cybersecurity and Identity Management

240,000 identity-based attacks are being blocked by Microsoft every single minute of every single day.

Cyber threat concern vs preparedness
(showing % ranked 1-3)

Cloud-related threats	Hack-and-leak operations	Third-party breach	Attacks on connected products	Ransomware

Most concerning cyber threats

Cyber threats least prepared to address

The perception on compliance readiness varies between different stakeholders. IAM teams will potentially suffer the consequences

Confidence in organisation's regulation compliance

Showing % high confidence for CEO vs CISO/CSO

Artificial intelligence

Resilience

Critical Infrastructure

Data protection

Cyber disclosure

Consumer privacy

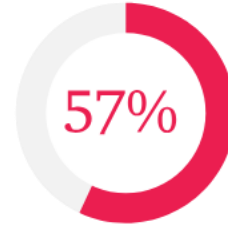Network and information security

CEO   CISO/CSO   Global is denoted by the black bars

At the same time, Digital Identity / IAM is becoming the cornerstone of successful digital transformation

Positioning cybersecurity as a competitive advantage

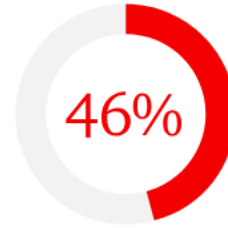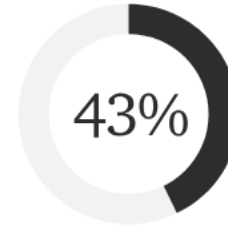(showing % selected 'To a large extent')
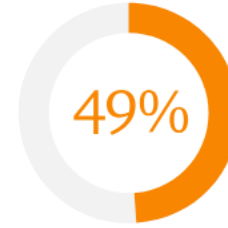
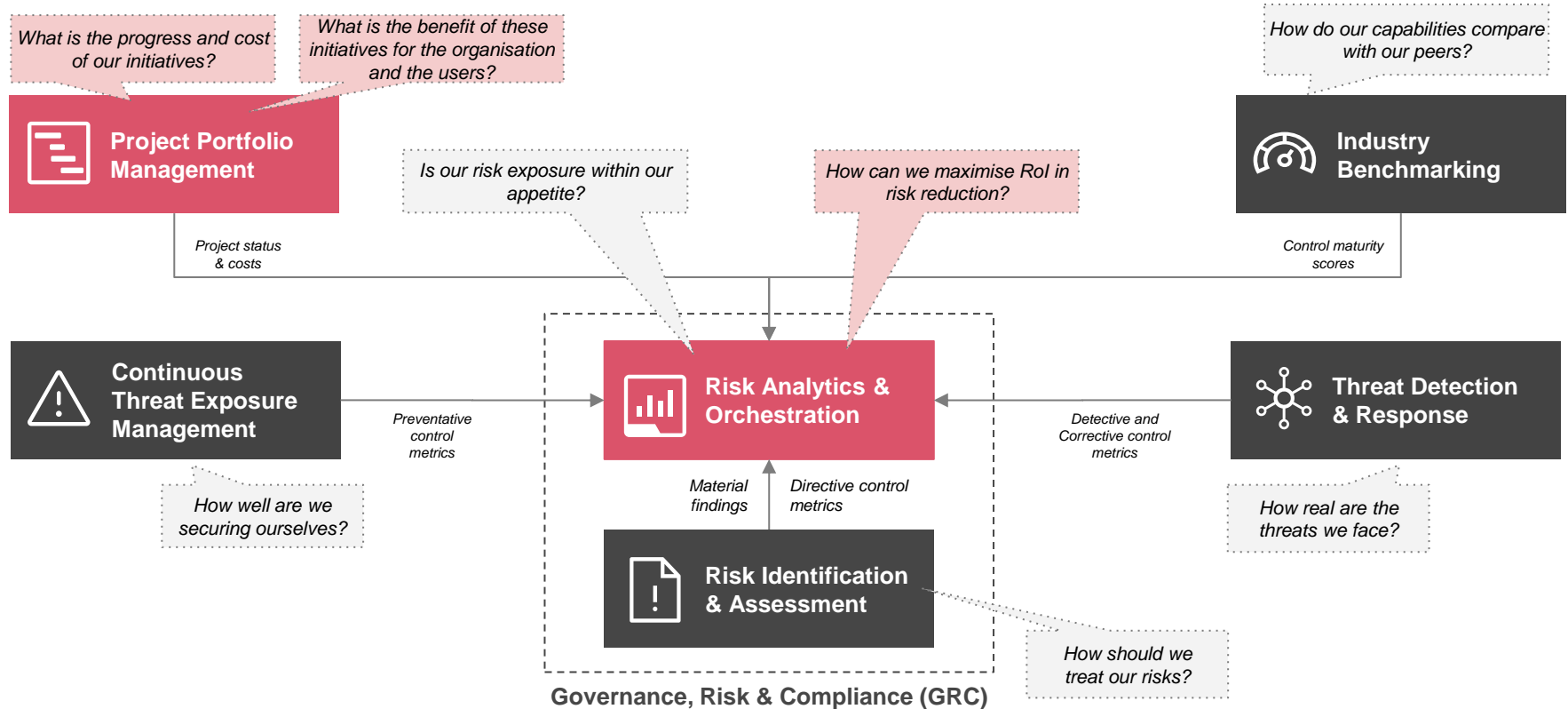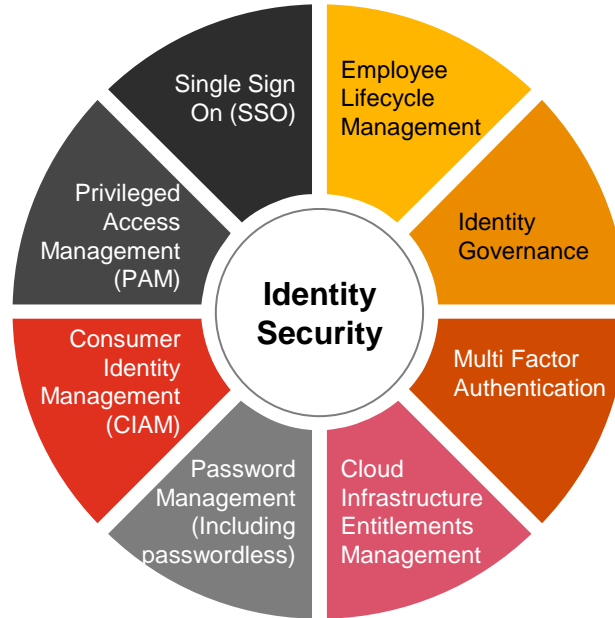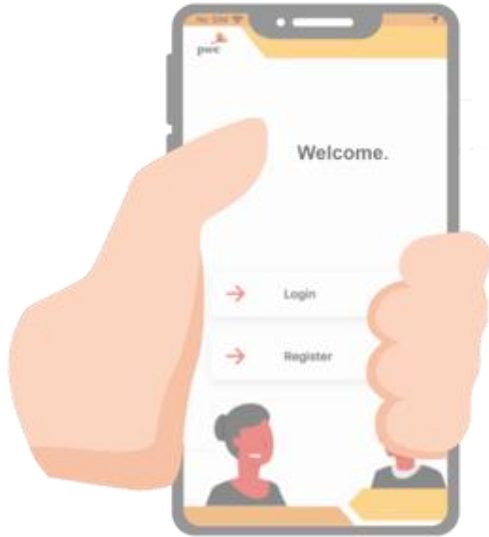|		
57%	**49%**	**46%**
Customer trust	Brand integrity and loyalty	Business growth opportunities
46%	**43%**	**41%**
Staying ahead of business disruption	Leadership in the market	Public relations
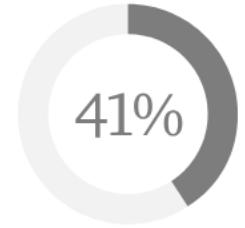
Q19. To what extent does your organisation position cybersecurity as a competitive advantage in these areas?
Base: All respondents= 4042
Source: PwC 2025 Global Digital Trust Insights

Prioritizing the right digital identity initiatives

What is the progress and cost of our initiatives?

What is the benefit of these initiatives for the organisation and the users?

How do our capabilities compare with our peers?

Project Portfolio Management

Industry Benchmarking

Is our risk exposure within our appetite?

How can we maximise RoI in risk reduction?

Project status & costs

Control maturity scores

Continuous Threat Exposure Management

Risk Analytics & Orchestration

Threat Detection & Response

Preventative control metrics

Detective and Corrective control metrics

How well are we securing ourselves?

Material findings

Directive control metrics

How real are the threats we face?

Risk Identification & Assessment

How should we treat our risks?

Governance, Risk & Compliance (GRC)

Digital Identity capabilities to consider

Identity Security capabilities:

- Single Sign On (SSO)
- Employee Lifecycle Management
- Identity Governance
- Multi Factor Authentication
- Cloud Infrastructure Entitlements Management
- Password Management (Including passwordless)
- Consumer Identity Management (CIAM)
- Privileged Access Management (PAM)

88% of C-suite executives who participated in our Global Trust Insights survey state that *quantification of cyber risks can help prioritise their investments*

2025 PwC Global Digital Trust Insights survey, pwc.com/dti
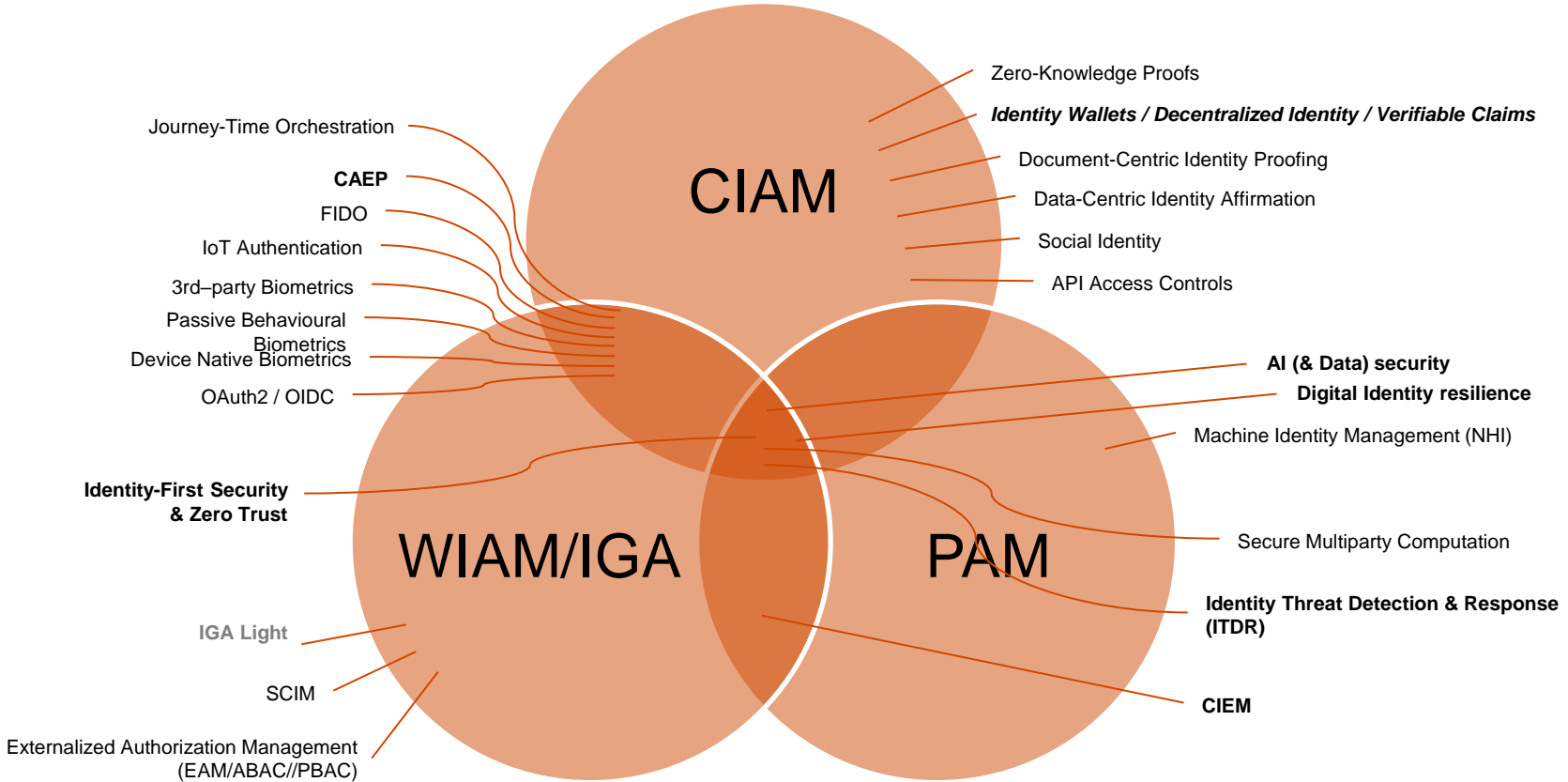
Improved end user experience

Regulatory compliance and enhanced security of users and their data

Efficiency gains through automation of repetitive processes
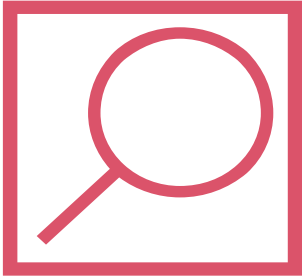
Technology Mapping - Trends we are tracking

Journey-Time Orchestration

CAEP

FIDO

IoT Authentication

3rd–party Biometrics

Passive Behavioural Biometrics

Device Native Biometrics

OAuth2 / OIDC

Identity-First Security & Zero Trust

IGA Light

SCIM

Externalized Authorization Management (EAM/ABAC//PBAC)

CIAM

WIAM/IGA

PAM

Zero-Knowledge Proofs

Identity Wallets / Decentralized Identity / Verifiable Claims

Document-Centric Identity Proofing

Data-Centric Identity Affirmation

Social Identity

API Access Controls

AI (& Data) security

Digital Identity resilience

Machine Identity Management (NHI)

Secure Multiparty Computation

Identity Threat Detection & Response (ITDR)
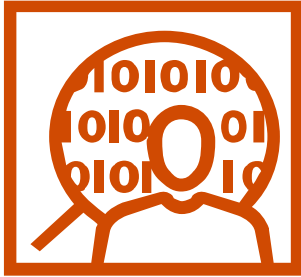
CIEM

Technology Trends - Priorities

Cloud Security & resilience

Gen & Agentic AI

Zero trust & ITDR

Wallets, SSI, Verifiable credentials

The biggest legacy tech challenges for risk – sound familiar?

41%

Poor data integration and management limits a holistic view of risks

39%

High maintenance costs

37%

Increased risk of operational failure

36%

Increased security vulnerabilities

Q. In what ways, if any, have legacy technologies impacted your organisation's ability to manage and respond to risk?
Base: All respondents=3910 Source: PwC's Global Risk Survey 2023

Considerations for next steps

Centralize IAM capability (under CISO)

Revisit your roadmap and engagement models

Address technical debt and operational work through Cloud & DevOps modernization

Thank you

pwc.co.uk