Deloitte.

Digital Identity by Deloitte

Digital identity is a crucial element of a successful digital transformation. However, it is a challenge to find the scarce skilled talent, implement and integrate the right technologies, and establish leading security processes for digital identity, while keeping up with the ever-changing demands and threats of a globally connected world. A great digital identity system can ward off future challenges and protect your company's success and reputation.

Reality of today's cyber world

The growing number and complexity of identities have led to a corresponding increase in identity-related breaches. As identities multiply in both type and quantity, the challenge of protecting them also escalates.

Ransomware
200%
Increase in human-operated ransomware attacks since September 2022.[1]

Cyber Incidents
90%
of businesses experienced at least one identity-related incident in the past year.[2]

Credentials
49%
of all data breaches involved credentials.[3]

Secure Identities
98%
of businesses see securing identities as a top 10 priority.[4]

Privilege Abuse
80%
of breaches involve compromised or abused privileged credentials.[5]

[1]Source: 2023 Digital Defense Report (MSFT)
[2]Source: 2024 Trends in Securing Digital Identities (IDSA Report)
[3]Source: 2023 Data Breach Investigations Report (Verizon)
[4]Source: 2024 Trends in Securing Digital Identities (IDSA Report)
[5]Source: Forrester's Research

Planning — Confirm scope and coverage of IAM goals and vision

Current State Analysis — Gain an understanding of the current state, including business challenges, business processes, and existing infrastructure

Future State Analysis — Identify required IAM services for the short, medium, and long term. Discuss business process and technology options for these IAM needs

Gap Analysis — Perform gap analysis of the IAM environment from current state to target state. Define maturity model for IAM. Identify technology tool options

Strategy and Roadmap — Create an IAM strategy that outlines IAM initiatives with timelines, priority, and costs considered. Prepare IAM program business case

Cost Analysis — Determine budget requirements and cost analysis for the IAM program

Planning — Establish project management and governance

Requirements — Collect and validate IAM requirements and document desired end result

Design — Hold workshops and document the solution architecture and design, including functional and nonfunctional components

Build — Develop code and perform configuration according to design specifications

Test — Perform system integration testing to verify functional correctness, performance testing to verify non-functional expectations and support client user acceptance testing

Deploy — Assess production readiness, deploy solution to production and validate

Transition — Conduct knowledge transfer sessions to support them

Planning — Confirm scope, discovery, and high-level transition plan

Service Enablement — Gain an understanding of the client's IAM processes in terms of platforms, business processes, and key stakeholders through knowledge transfer and shadowing

Service Delivery — Deliver the development, support, and platform administration services by leveraging the processes established during the service enablement phase

Transition — Conduct knowledge transfer sessions and oversee managed transition
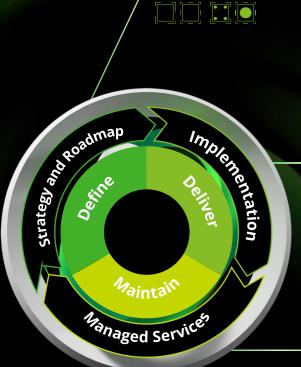
Deloitte in action.

The Challenge
One of the largest banks in SEA was undergoing a digital transformation for their workforce and customer identity management.

The Solution
Deloitte's Digital Identity team served the bank in various digital identity projects including the design and implementation of multi-factor authentication, transaction authorization, risk-based authentication, integration with hardware security modules, identity lifecycle management, CIAM, single sign-on and identity governance.

The Deliverables
The deliverables include the provision of implementation services to strategize, design, build and operate the digital identity platforms as turn-key projects. We also provided support and maintenance services, including integration with supporting systems such as CI/CD, SIEM, CRM, BI, monitoring and altering tools.

Strategy and Roadmap · Implementation · Define · Deliver · Maintain · Managed Services

Deloitte.

Digital Identity by Deloitte

Unified Identity Security Services

Access Management

Identity lifecycle-driven SSO with Multi-factor Authentication (MFA) and password-less options to ensure the workforce has simple yet highly secure access.

- SSO, Multi-factor Authentication (MFA) and Password-less
- Accelerated Connectivity to On-Premises Targets
- Federated Identity
- Adaptive Authentication
- Customer Identity & Access Management

Identity Governance & Administration

Manage the complete lifecycle of identities, by orchestrating Hire to Retire events to ensure the right access for the right people at the right time.

- Centralized User Admin and Identity Analytics
- Identity Lifecycle Management (Joiner/Mover/Leaver)
- Access Request & Workflow
- Accelerated Connectivity to Cloud and On-Premises Target Systems
- Delegated Administration
- ML/AI Driven Role Mining via Peer-Group Analysis
- Segregation of Duties

Privileged Access Management

Protect critical assets by enforcing Least Privilege and providing vaulted credential storage, management, and secure access to endpoints with session monitoring, reporting, and auditing.

- Vaulted Credentials (Least Privilege)
- Credential Management
- Privileged Session Monitoring and Forensics
- Credential Cycling
- Privileged Account Discovery
- Privileged Account Lifecycle Management

Digital Identity by Deloitte Services

Your identity needs in one place.

- Identity Governance and Administration
- Access Management
- Privileged Access Management
- Unified Identity Security Services

Digital Identity by Deloitte Advantage

Accelerating Business Outcomes
Faster time to value with cloud and automation

Metrics-based, KPI-driven
Leverages data to optimize performance and outcomes

Centralized Governance
Operational and cost efficiencies with centralized governance

Centralized and local approach
The scale of standardized SEA Delivery Center combined with

Seamless User Experience
Integrating solutions that function across your businesses and systems to create seamless user experiences and brand affinity

Contacts

Thio Tse Gan
SEA Cyber Leader
+65 6216 3158
tgthio@deloitte.com

Jefferson Costa
Executive Director,
Digital Privacy & Trust
+65 6531 5216
jeffersoncosta@deloitte.com

Eric Lee
Executive Director,
Digital Privacy & Trust
+65 6800 2100
ewklee@deloitte.com

Irence Wee
Executive Director
+65 6530 5555
iwee@deloitte.com