

# IAM Journey and Next Steps...

October 2023



standard  
chartered

# EXECUTIVE SUMMARY

## STATUS

- The Bank has transformed its IAM capability during the past 3 years. Central IAM capabilities and controls now sustain a **strong core performance**.
- **IAM coverage, control efficacy and performance indicators trend positively**
  - sBIA 4/5 Asset coverage is at 93% (coming from less than 50% in 2020).
  - Residual Risk will be Medium by December 2023 (coming from Very High in 2020).
- No significant incidents attributable to IAM

## IS THERE A SYSTEMIC, THEMATIC ROOT ISSUE WITH IAM?

- Due to the pervasive nature of access controls in bank wide applications (in every app), GIA typically test for access controls in over 150 audits a year.
- While volume of inspection stays high, the core IAM has shown a positive trajectory with reduction year on year with very contained, diminished criticality.
- **No single thematic root cause indicative of an access control weakness.**
- However, it is important to note that there have been recent audits where material issues have been identified (i.e. Domestic Payment Gateways, SuccessFactors). **These are attributable to gaps in business process controls, appropriateness of access and granularity of access reviews and system design and data transmission controls.**

## THE JOURNEY AHEAD

- As we fix(ed) the IAM core and central services, we must now focus to upstream and satellite processes and services sitting with Businesses and Functions.
- **ICS are taking full ownership for the totality of the IAM space**, core and periphery regardless of where issues are across the end-to-end identity lifecycle. We are owning a plan that, through 2024 and 2025 will complete the remediation.



# WHAT IS IAM



standard  
chartered

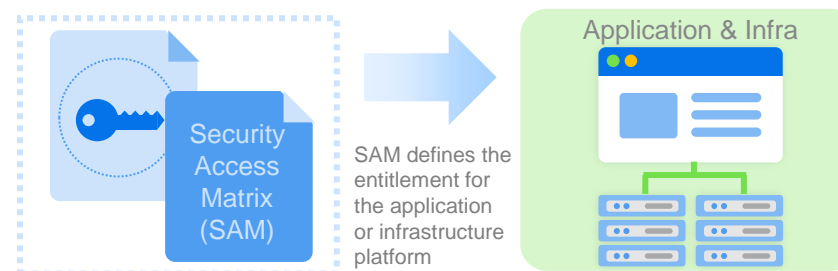
# WHAT DOES IAM DO?

## 1. Manage Identities

- Identity and Access Management (IAM) is a **centralised control framework** to manage workforce identities and entitlements to the Bank's critical applications, data and infrastructure platforms. This framework also includes key authentication mechanisms such as Single Sign On and Multifactor Authentication.
- Employees, Contractors and Robots** are managed by IAM.
- Account types:**
  - Individual Accounts, which can be Standard or Privileged
  - Generic Accounts which are used by multiple Employees.
- A Privileged Account:**
  - Administer applications and infrastructure.
  - They require additional controls
- All Account types and Entitlements are regularly **reviewed and assessed** by owners to ensure relevancy and maintain a principle of least privilege.

## 2. Enforces Entitlements

- Entitlements are **defined by the Business Owner (BSO)** within the target application and determine what action an account can perform.
- Entitlements can provide a wide range of access and are configured within each application.
- The entitlement definition for each application and infrastructure platform is captured in a **Security Access Matrix (SAM)** which is approved by the Business Owner and recertified on an annual basis.

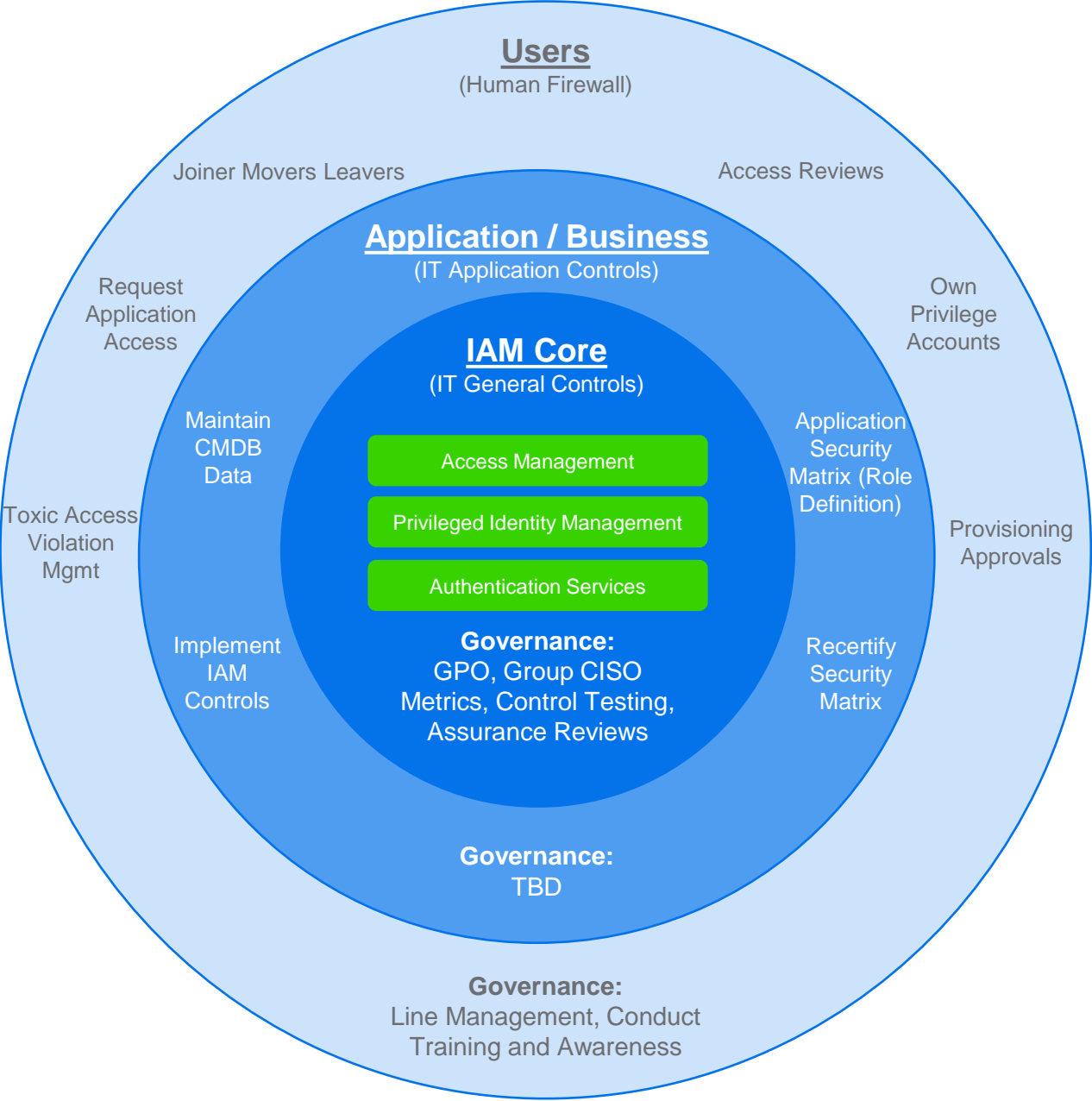


## 3. Provisions Centrally

- All Accounts types and Entitlements are managed by either manual or automated provisioning (and de-provisioning) processes between the core IAM system and downstream applications and infrastructure platforms.
- All provisioning is either automated or performed by the IAM Service Desk. Provisioning options handled by business are no longer supported and will be remediated in 2023.



# IAM: THE CORE, THE BUSINESS, THE USER



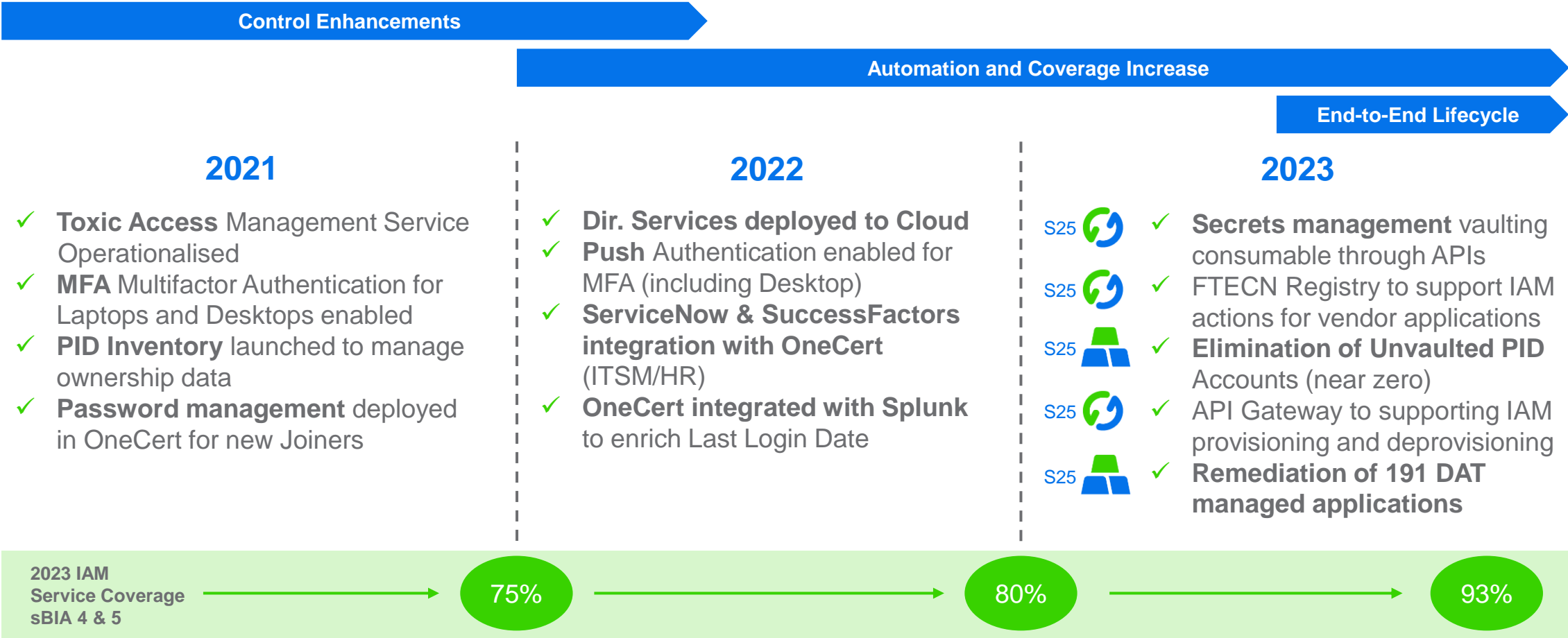
# THE JOURNEY



standard  
chartered

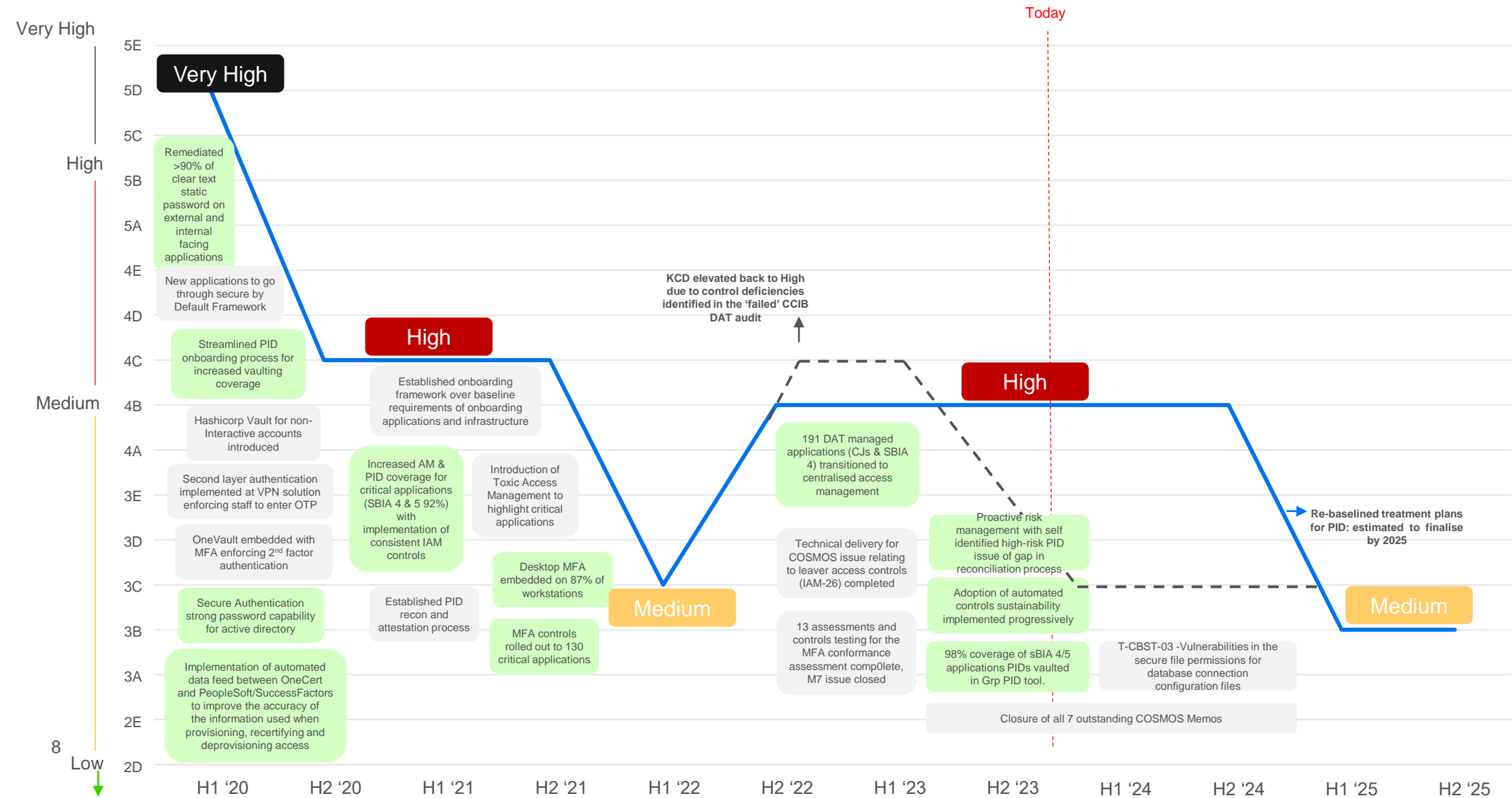
# IAM CAPABILITY JOURNEY

IAM coverage continues to increase, controls are stabilised, however, issues related to connected applications continue to dominate in 2023.



# IAM Risk Journey

In 2020, IAM residual risk was **VERY HIGH** and is on track in 2023 to reduce to **MEDIUM**



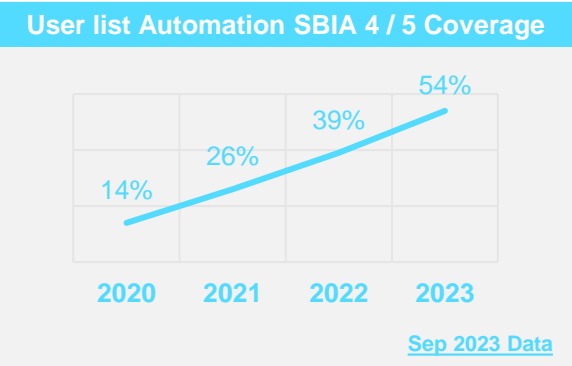
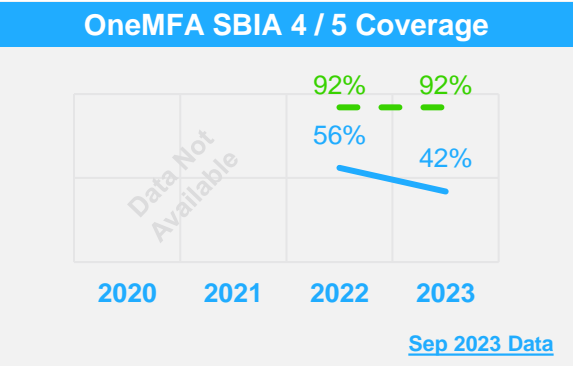
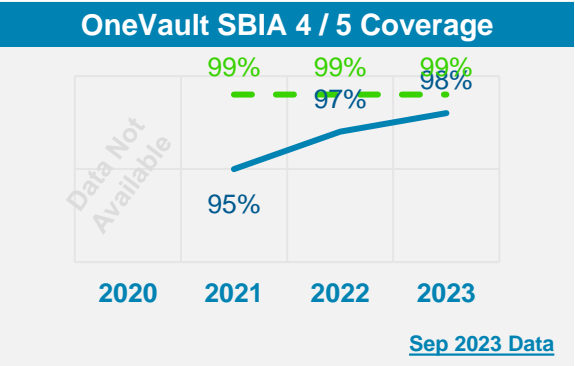
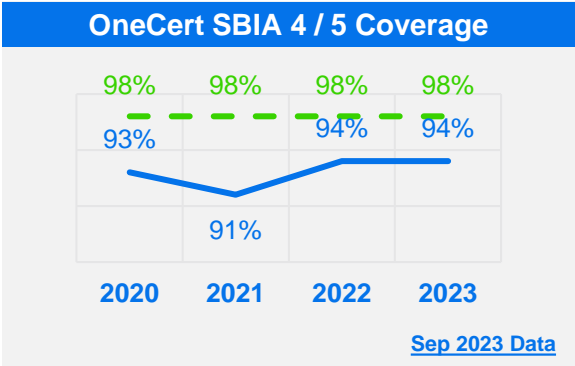
In collaboration with  
business and Enterprise  
Technology  
IAM Team



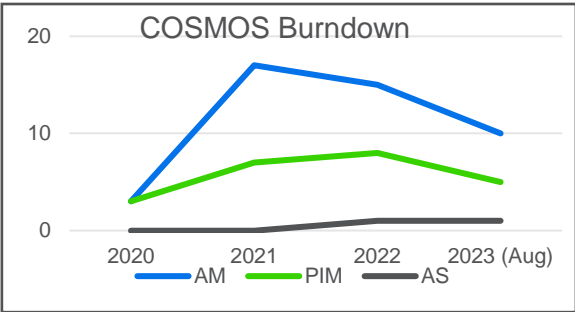


# IAM METRIC AND COVERAGE PERFORMANCE

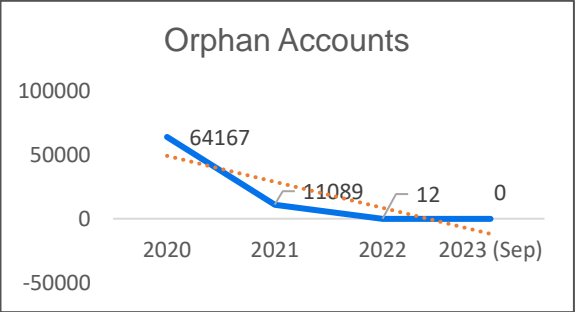
## IAM Service Coverage



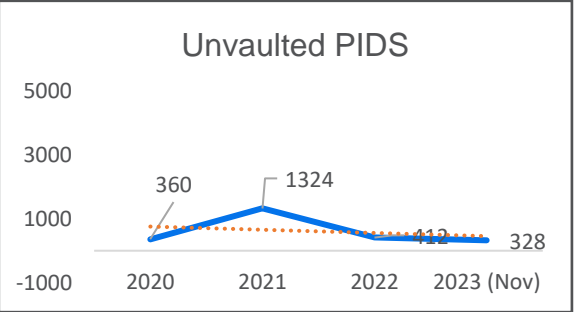
## IAM Risk Management



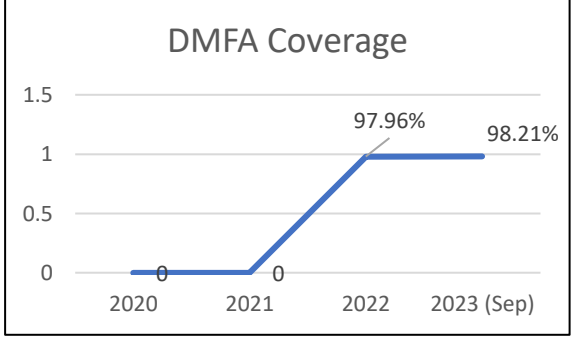
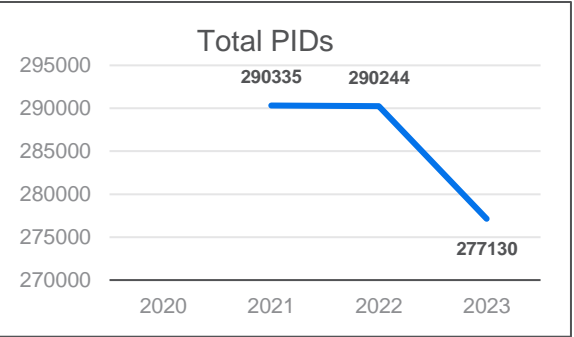
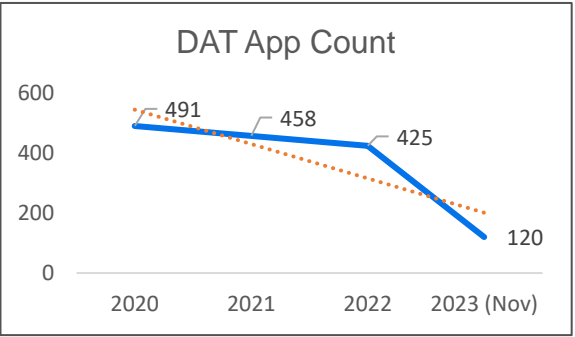
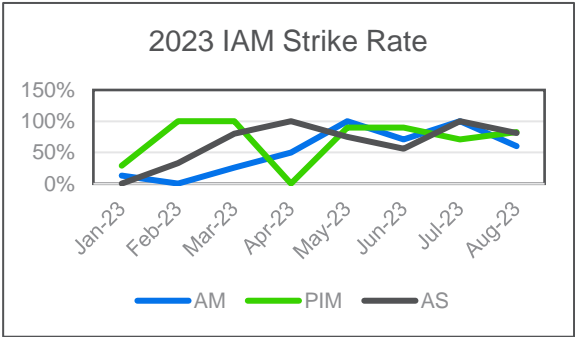
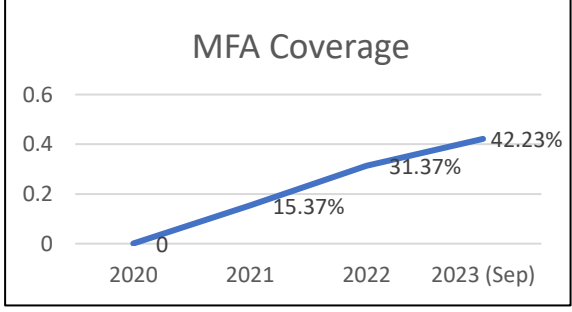
## Access Management



## Privileged Identity Management



## Authentication Services



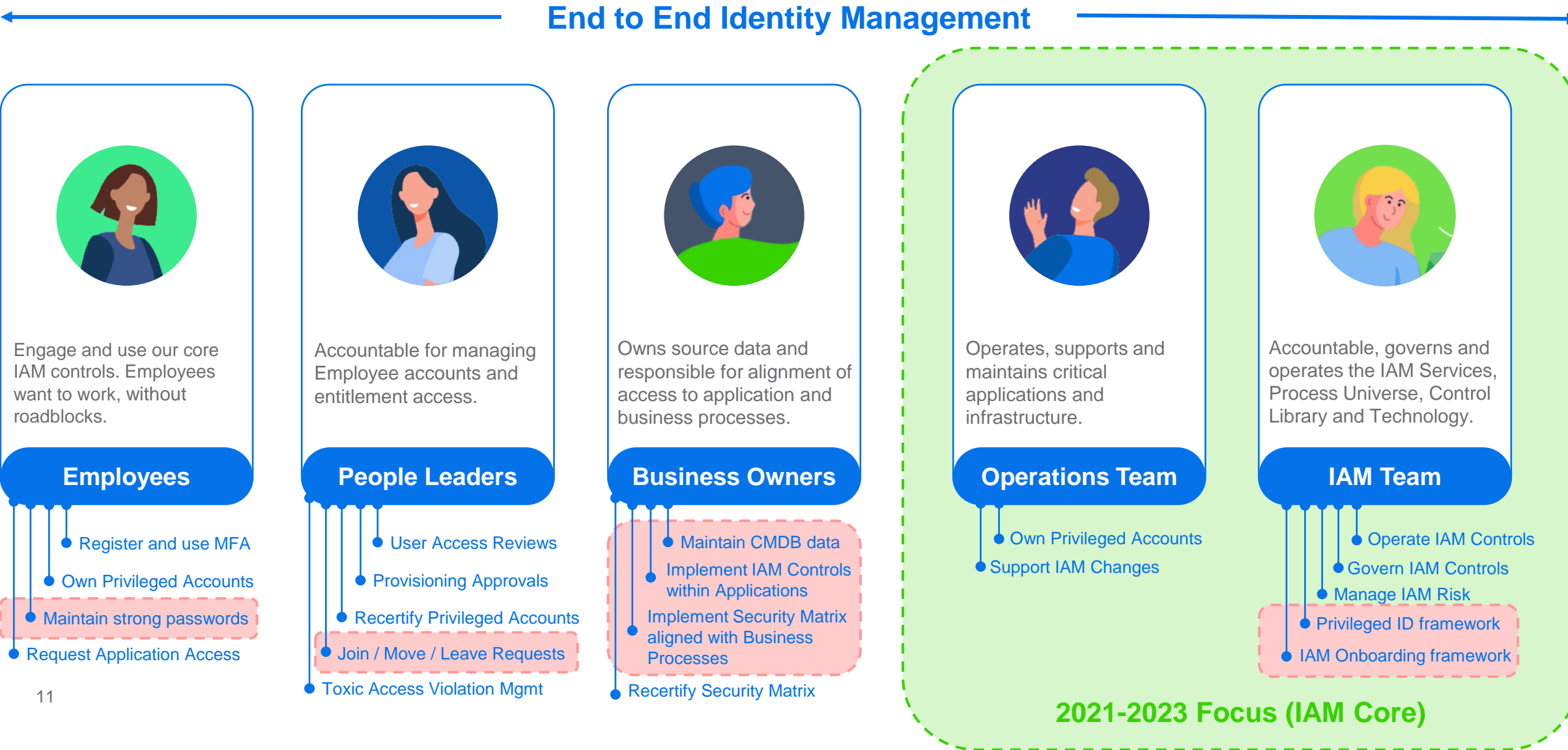
# SO, WHAT IS LEFT ?



standard  
chartered

# END TO END MANAGEMENT


IAM manages an interconnected landscape which depends on source and target data to execute controls



# KEY OPPORTUNITIES

Our key initiatives for 2024 and beyond

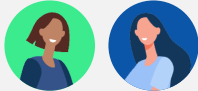
1



TOO MANY PASSWORDS

TTO  
Strat 25


2



REINFORCING IAM RESPONSIBILITIES

TTO  
Strat 25


3



APPLICATION PROCESS DESIGN AND AUTHORISATION MODELS REQUIRE STRENGTHENING

TTO  
Strat 25


4



TOO MANY PRIVILEGED ACCOUNTS

TTO  
Strat 25


5



SIMPLIFY AND AUTOMATE

TTO  
Strat 25

6







ACCELERATE IAM ONBOARDING

TTO  
Strat 25



# THE PLAN

Move past the core

	<u>E2E Stakeholders</u>	<u>Initiative</u>	<u>Outcome</u>	<u>Strategy 25</u>	<u>Funding</u>	<u>Date</u>
  <b>Employees and People Leaders</b> <i>Maintain strong passwords</i>	<b>1</b>	<b>Too many Passwords</b>	<p>We continue to see a high number of support calls, ~17K per month for password resets.</p> <p>In 2023, we introduce our first phase of Passwordless. A frictionless customer experience, reducing frustration and risk of passwords being written down and improving operational efficiency by reducing call volume to the service desk.</p> <p><b>Line Mangers and Information System Owners submitting late or incorrect data for processing.</b></p>	Establish Strong Digital Foundations Drive Process Excellence Accelerate Transformation	\$5.2M (to be funded by Tech Simplification)	2025
		<b>2</b>	<b>Reinforcing IAM responsibilities</b>	Line Managers who do not process Leaver records on time, create unnecessary risk. Similar for ISO’s who submit incomplete or undeclared roles privileges for their applications. In 2024, we plan on driving a culture and knowledge campaign, based on personas to ensure that responsibilities and consequences are understood.	Drive Process Excellence	BAU
 <b>Business Owners</b> <i>Implement Security Matrix aligned with Business Processes</i>	<b>3</b>	<b>Application process design and authorisation models require strengthening</b>	<p><b>Our critical Applications and Data have inherently basic and over privileged access models, usually delivered out of the box.</b></p> <p>In 2024, we propose to start Risk Modelling the security matrices and authorisation models for applications. This capability will enable visibility and continuous monitoring of critical Bank applications to track and analyse activity in accordance with the Least Privilege Model.</p>	Establish Strong Digital Foundations Drive Process Excellence Accelerate Transformation	\$1.2M – ICS	2024
 <b>IAM and Operations Teams</b> <i>Privileged ID Framework Simplifying Authentication IAM Onboarding Framework</i>	<b>4</b>	<b>Too many Privileged Accounts</b>	<p><b>PIDs are seen as permanent support tools to manage operations.</b></p> <p>The more privileged accounts we manage, the more overheads we need to staff and support with recertifying, remediating and attesting. In 2023, we introduce a Just In Time privileged model, providing session managed Privileged Accounts only when needed during Incidents or Changes, and removing after use.</p>	Establish Strong Digital Foundations Drive Process Excellence Accelerate Transformation	\$12.65M – ICS	2024
	<b>5</b>	<b>Simplify and Automate</b>	<p><b>Parts of the IAM estate need to be updated and automated</b></p> <p>In 2024, we plan to automate the key services for account reconciliation and further enhance the access provisioning process with ServiceNow and Public Cloud Providers.</p>	Accelerate Transformation	4.53M – ICS	2024
	<b>6</b>	<b>Accelerate IAM Onboarding</b>	<p><b>There are 16 minimum mandatory controls for IAM boarding, it can take from 14-90 days to onboard.</b></p> <p>To maintain our high levels of coverage and reduce the friction for customers to onboard, we will continue to invest in automated onboarding. With the recent success of MFA and HashiCorp Secrets automation we will build broader APIs with Microservices and embedment with ADO / eSDLC</p>	Accelerate Transformation	\$3.85M – ICS	2025

# Thank you!



standard  
chartered

# APPENDIX

(Some really useful stuff  
here)



# IAM User Management Lifecycle

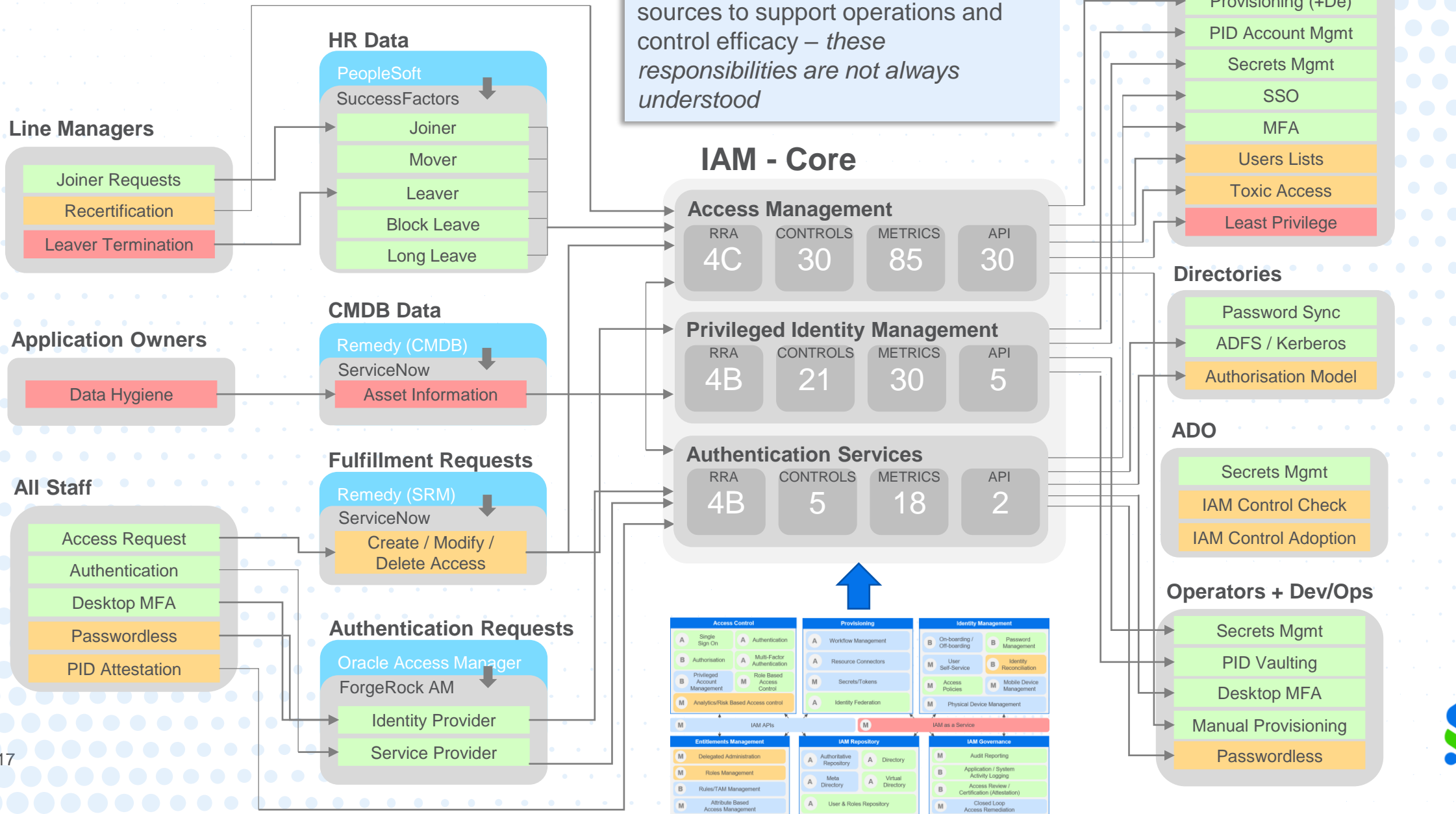
	Create / Provision / Onboard	Manage	Delete / De-Provision / Offboard	Governance Controls Operated By	Areas of Concern
IT General Controls	<ul style="list-style-type: none"> <li>Application onboarding into OneCert, OneVault / HashiCorp Vault, and OneMFA</li> <li>Infrastructure onboarding into OneCert and OneVault / HashiCorp</li> <li>Access creation</li> <li>Vault PIDs in OneVault</li> <li>DMFA enablement for eligible users</li> <li>SIA validation for new application onboarding</li> </ul>	<ul style="list-style-type: none"> <li>Manage annual security matrix recertification</li> <li>Manage annual toxic access rules certification</li> <li>Manage bi-annual access and privileged ID certification</li> <li>Manage annual not required recertification for OneCert onboarding and Authentication Controls</li> <li>Access, entitlement and privileged ID reconciliation</li> <li>Dormant accounts</li> <li>Orphan accounts</li> <li>Token access</li> <li>Manage annual attestation for non-standard MFA solution</li> <li>Manage / monitor SSH keys usage for privileged IDs</li> <li>Manage / monitor privileged IDs utilization</li> <li>Manage static password release via secured sessions</li> <li>Manage password rotation for manual managed privileged IDs</li> </ul>	<ul style="list-style-type: none"> <li>Application offboarding from OneCert, OneVault / HashiCorp Vault, and OneMFA</li> <li>Infrastructure offboarding from OneCert and OneVault / HashiCorp</li> <li>Access deletion / disablement</li> <li>Remove PIDs from OneVault</li> </ul>	<ul style="list-style-type: none"> <li>Central IAM Team</li> </ul>	<ul style="list-style-type: none"> <li>IAM Onboarding is too manual and slow</li> <li>Operationalising Build and Maintain WOW</li> </ul>
Application Controls	<ul style="list-style-type: none"> <li>Define security matrix</li> <li>Define toxic Access rules</li> <li>Eform and workflow creation</li> <li>User list creation</li> <li>Identity ownership for all accounts</li> <li>Implement 25-character password requirement</li> <li>Implement MFA and Central Authentication</li> <li>SIA initiation and execution</li> </ul>	<ul style="list-style-type: none"> <li>Perform annual security matrix recertification</li> <li>Ad hoc security matrix changes</li> <li>Perform annual toxic access rules certification</li> <li>Perform annual not required recertification for OneCert onboarding and authentication controls</li> <li>Reassignment of account owners (movers / leavers)</li> <li>Session recording review</li> <li>Perform annual attestation for non-standard MFA solution</li> <li>Maintain privileged ID criteria and annual certification</li> </ul>	<ul style="list-style-type: none"> <li>Decommission application / infrastructure</li> <li>Remove application / infrastructure from CMDB</li> </ul>	<ul style="list-style-type: none"> <li>No Central Governance Structure in place</li> <li><b>Recommendation:</b> Build the governance capability within IAM or TTO</li> </ul>	<ul style="list-style-type: none"> <li>Too many Privileged Identities...</li> <li>Too many Passwords...</li> <li>Poor application process design and authorisation models</li> <li>Source of Truth Asset information is unreliable</li> </ul>
Employee Controls	<ul style="list-style-type: none"> <li>Joiner request</li> <li>Token request for authentication</li> </ul>	<ul style="list-style-type: none"> <li>Perform bi-annual access certification for direct reports</li> <li>Mover request</li> <li>Leaver request</li> </ul>	<ul style="list-style-type: none"> <li>Deletion / disablement request</li> </ul>	<ul style="list-style-type: none"> <li>Line Managers</li> <li>Conduct Teams</li> </ul>	<ul style="list-style-type: none"> <li>Employees do not understand their responsibilities</li> </ul>





# The connectivity of IAM

IAM has key dependencies on upstream and downstream data sources to support operations and control efficacy – *these responsibilities are not always understood*



# IAM Capability Journey

Transforming the IAM capability model and control library to establish and optimise our central core IAM services.

