# IAM CAPABILITY BLUEPRINT

**Shawn Wells**
**Managing Director**
**shawn.wells@accenturefederal.com**
**443-534-0130**

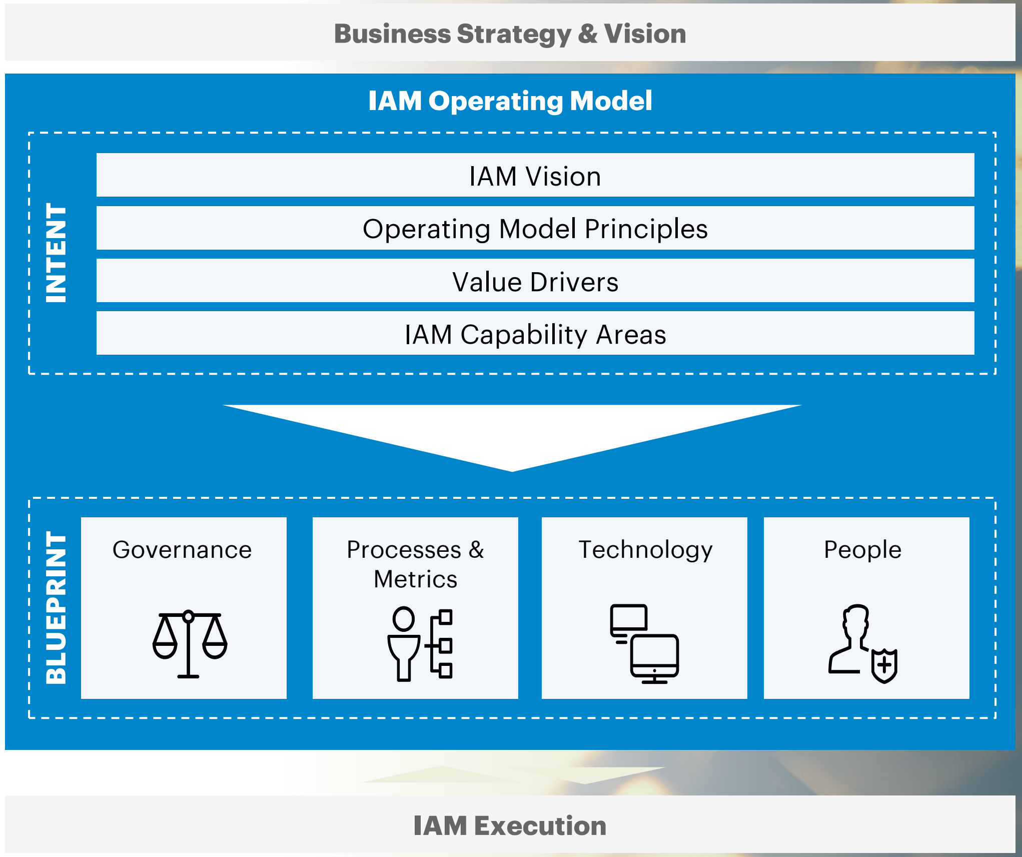
accenture

# CONTENTS

## IAM CAPABILITY MODEL

### Contents

1. IAM Vison
2. Operating Model Principles
3. Value drivers
4. IAM Capability Areas
5. Metrics
6. Governance & Processes
7. Technology & Vendors
8. People (Roles and sourcing)



accenture

# FOR READABILITY OF THIS DOCUMENT A TRACKER HAS BEEN ADDED

## READERS' GUIDE

*Vision*

*Principles*

*Value drivers*

*IAM capability areas*

*Metrics*

*Governance & Processes*

*Technology*

*People (Roles and sourcing)*

# WHAT WOULD WE LIKE TO ACHIEVE WITH THE IAM OPERATING MODEL?

## VISION STATEMENT

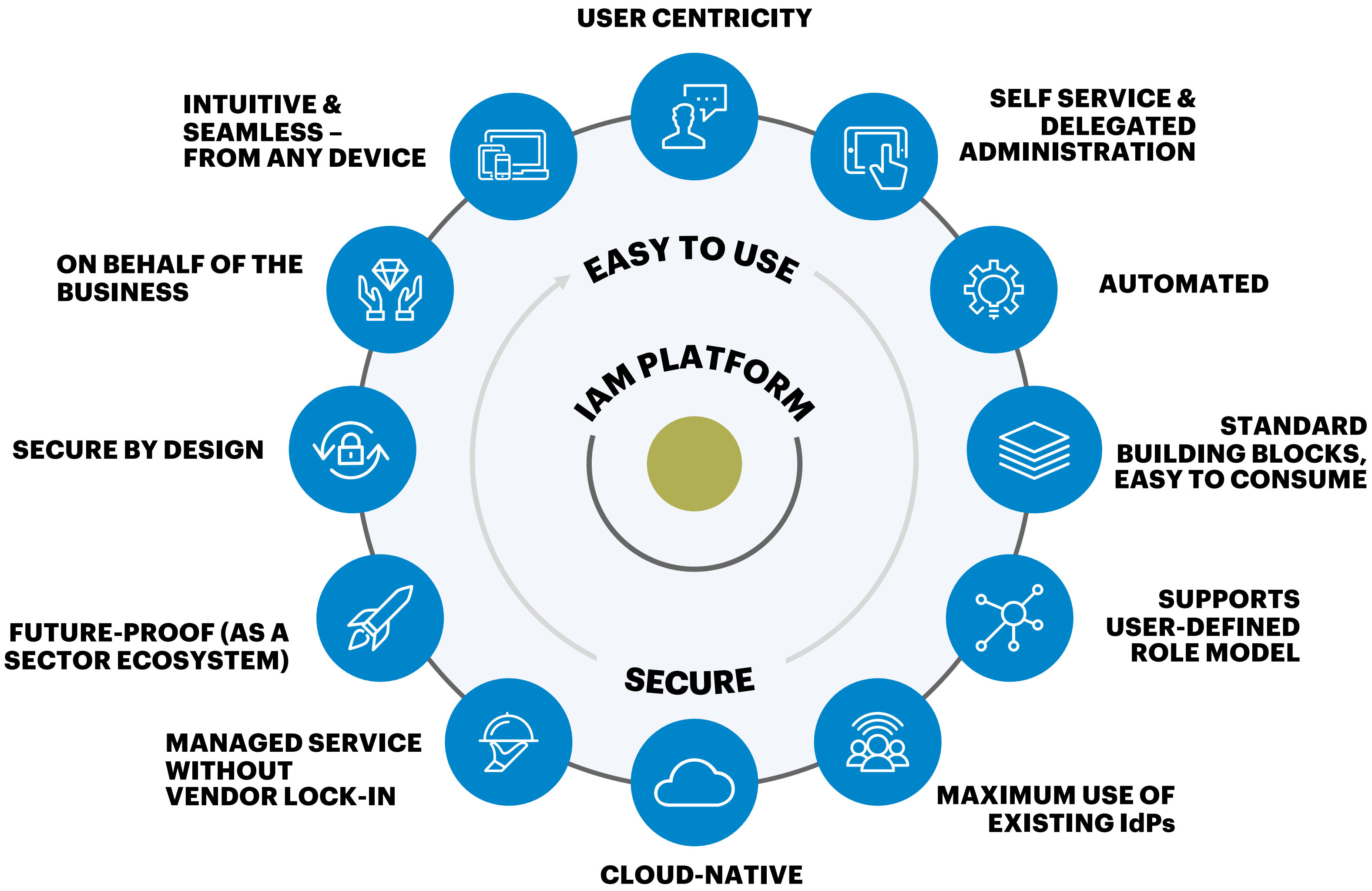
**Vision**

A future-proof and self-sufficient IAM platform that enables (and secures) <CLIENT NAME> business objectives

accenture

# PRINCIPLES ARE THE BASIS FOR ALL (FUTURE) CHOICES CONCERNING THE IAM OPERATING MODEL

## DESIGN PRINCIPLES (DEFINITIONS IN APPENDIX)


USER CENTRICITY
SELF SERVICE & DELEGATED ADMINISTRATION
AUTOMATED
STANDARD BUILDING BLOCKS, EASY TO CONSUME
SUPPORTS USER-DEFINED ROLE MODEL
MAXIMUM USE OF EXISTING IdPs
CLOUD-NATIVE
MANAGED SERVICE WITHOUT VENDOR LOCK-IN
FUTURE-PROOF (AS A SECTOR ECOSYSTEM)
SECURE BY DESIGN
ON BEHALF OF THE BUSINESS
INTUITIVE & SEAMLESS – FROM ANY DEVICE
EASY TO USE
IAM PLATFORM
SECURE

# IDENTIFYING THE RIGHT VALUE DRIVERS SO IAM CREATES VALUE FOR THE BUSINESS

## VALUE DRIVERS

| VALUE DRIVERS | OPERATIONAL EFFICIENCY | END-USER SATISFACTION | RISK & COMPLIANCE | ECOSYSTEM ENABLEMENT |
|---|---|---|---|---|
| TARGET | ✓ **Reduce costs** through self-service, automation and effective license management<br>✓ **Increasing employee productivity** | ✓ Providing **seamless access to applications**<br>✓ Focus on "core business" by making **standard functionalities** available to development teams | ✓ **Securing digital assets** by strengthening and future-proofing the security perimeter<br>✓ Ensuring **effective control mechanisms**<br>✓ Ensuring and **facilitating audit/legal compliance**<br>✓ **Central separation of roles,** capacities and responsibilities | ✓ Enhance **ecosystem connectivity**<br>✓ **Shortening time-to-market** for new applications<br>✓ Enable **analytics & insights** |

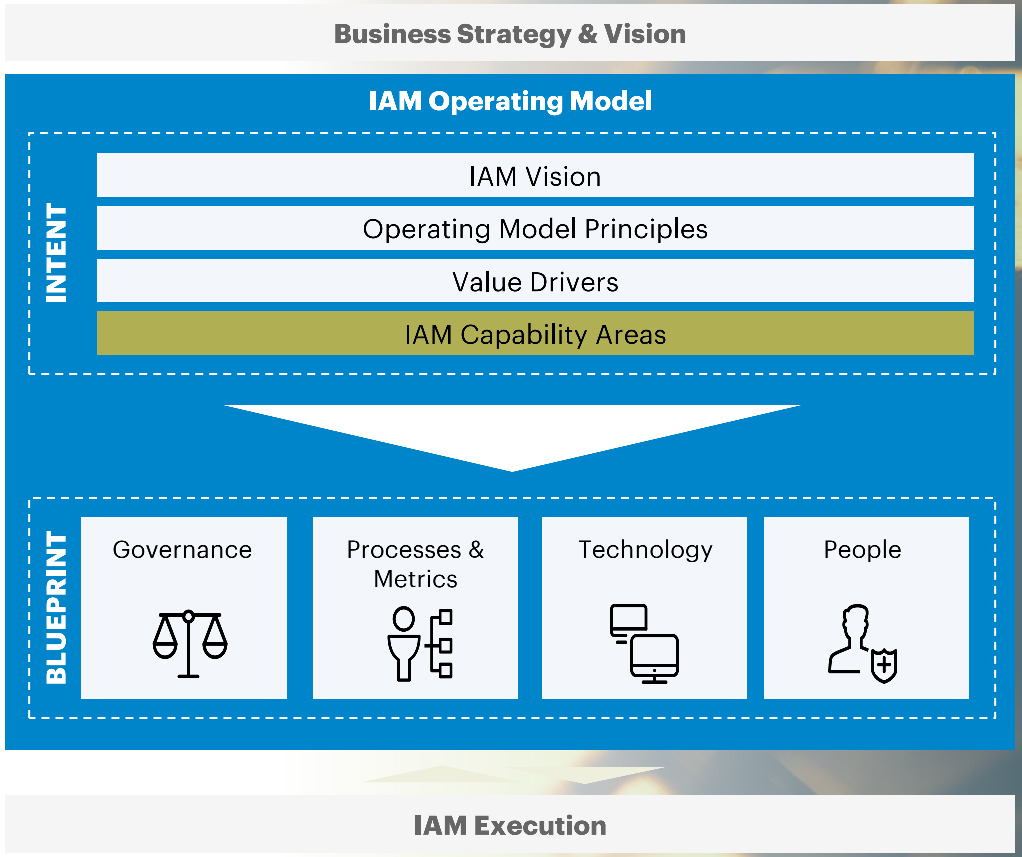
accenture

# CONTENTS

## IAM CAPABILITY MODEL

**Contents**

1. IAM Vison
2. Operating Model Principles
3. Value drivers
4. **IAM Capability Areas**
5. Metrics
6. Governance & Processes
7. Technology & Vendors
8. People (Roles and sourcing)



Business Strategy & Vision

IAM Operating Model

INTENT

IAM Vision

Operating Model Principles

Value Drivers

IAM Capability Areas

BLUEPRINT

Governance

Processes & Metrics

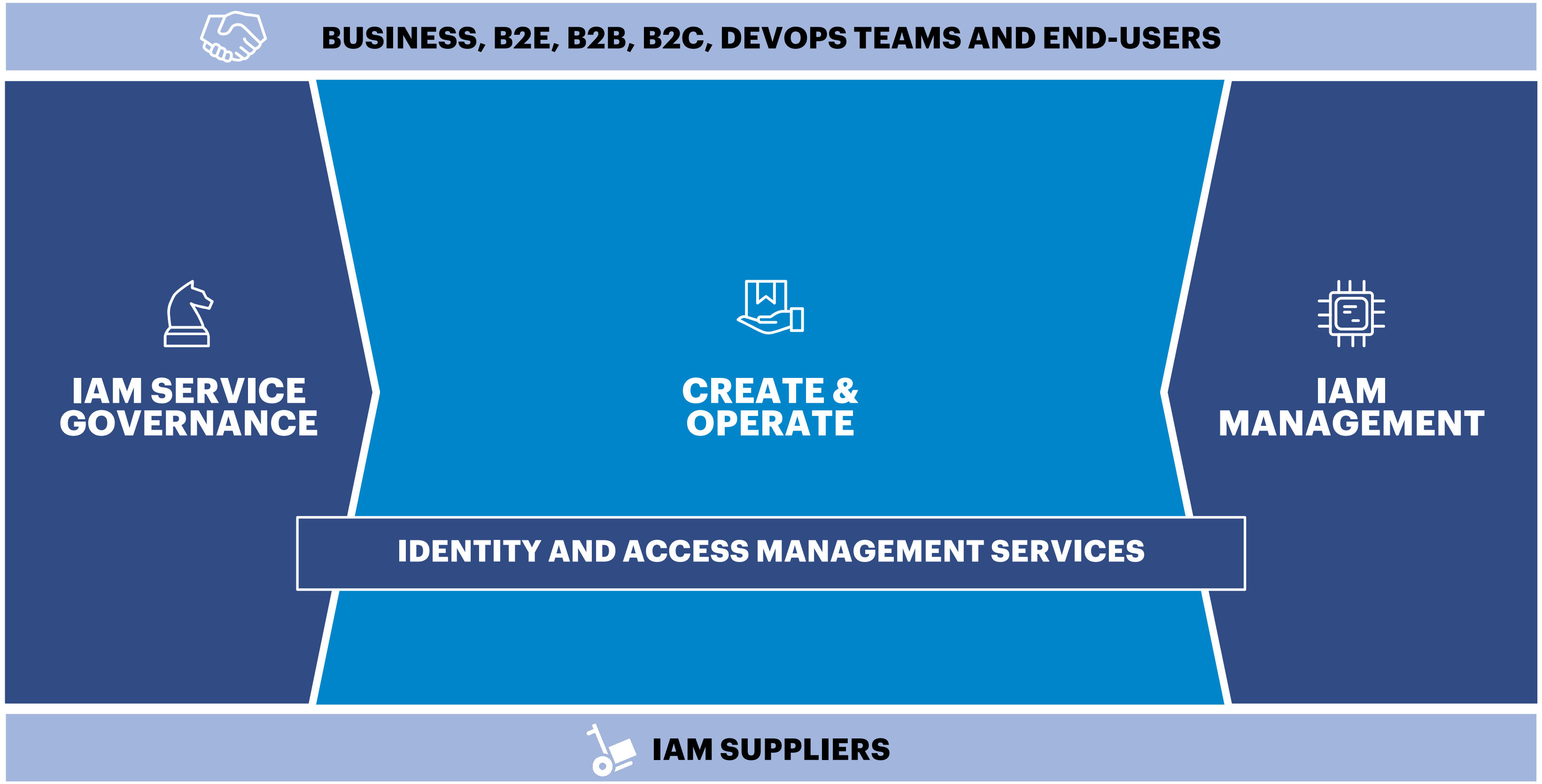
Technology

People

IAM Execution

# IAM SERVICE CAPABILITY MODEL– LEVEL 0

## LEVEL 0



BUSINESS, B2E, B2B, B2C, DEVOPS TEAMS AND END-USERS

IAM SERVICE GOVERNANCE

CREATE & OPERATE

IAM MANAGEMENT

IDENTITY AND ACCESS MANAGEMENT SERVICES

IAM SUPPLIERS

accenture

# IAM SERVICE OPERATING FRAMEWORK – LEVEL 1

## LEVEL 1

BUSINESS, B2E, B2B, B2C, DEVOPS TEAMS AND END-USERS

### IAM SERVICE GOVERNANCE

Understanding the priorities of the business and from there developing and aligning IAM policies.

### IAM SERVICE STRATEGY

Ensure a clear service definition and architecture. Developing a roadmap with a clear roadmap in line with overall strategic priorities. Alignment with users.

### IAM OPERATIONS

To provide reliable, sustainable and efficient IAM services, which are in line with the overall standards and policies of <CLIENT>.

### IAM ASSET MANAGEMENT

Managing the assets (target applications) within the <CLIENT> IAM Capability including on/off boarding of new assets, integration for SIEM/SOC and platform consultancy.

### IAM PLATFORM MANAGEMENT

Daily management of the IAM platform and processing and application of changes within the platform

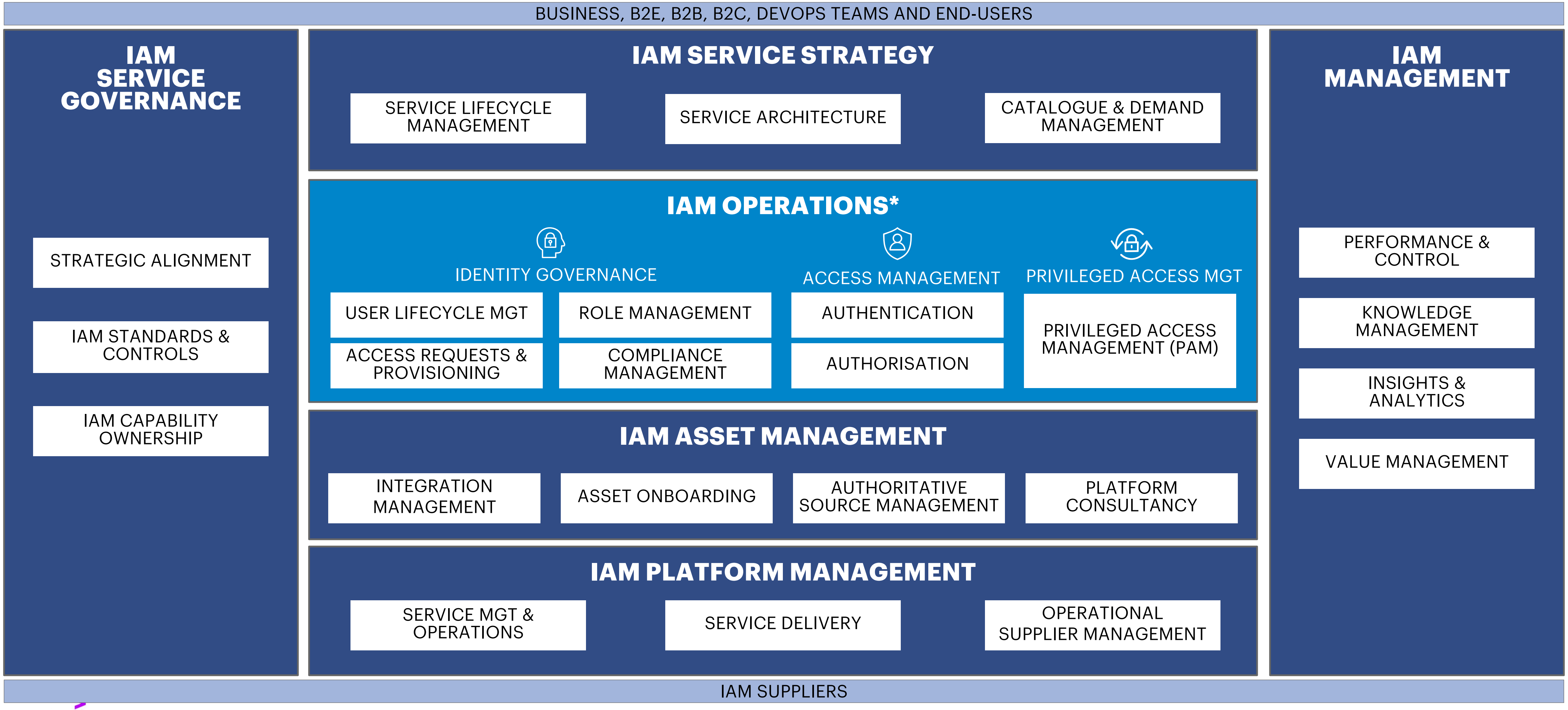
### IAM MANAGEMENT

Checking the quality and value of the IAM services provided, adherence to controls, as well as knowledge assurance and insights.

IAM SUPPLIERS

# IAM SERVICE CAPABILITY MODEL– LEVEL 1 & 2

## LEVEL 1 & 2



BUSINESS, B2E, B2B, B2C, DEVOPS TEAMS AND END-USERS

### IAM SERVICE GOVERNANCE

- STRATEGIC ALIGNMENT
- IAM STANDARDS & CONTROLS
- IAM CAPABILITY OWNERSHIP

### IAM SERVICE STRATEGY

- SERVICE LIFECYCLE MANAGEMENT
- SERVICE ARCHITECTURE
- CATALOGUE & DEMAND MANAGEMENT

### IAM OPERATIONS*

IDENTITY GOVERNANCE

- USER LIFECYCLE MGT
- ROLE MANAGEMENT
- ACCESS REQUESTS & PROVISIONING
- COMPLIANCE MANAGEMENT

ACCESS MANAGEMENT

- AUTHENTICATION
- AUTHORISATION

PRIVILEGED ACCESS MGT

- PRIVILEGED ACCESS MANAGEMENT (PAM)

### IAM ASSET MANAGEMENT

- INTEGRATION MANAGEMENT
- ASSET ONBOARDING
- AUTHORITATIVE SOURCE MANAGEMENT
- PLATFORM CONSULTANCY

### IAM PLATFORM MANAGEMENT

- SERVICE MGT & OPERATIONS
- SERVICE DELIVERY
- OPERATIONAL SUPPLIER MANAGEMENT

### IAM MANAGEMENT

- PERFORMANCE & CONTROL
- KNOWLEDGE MANAGEMENT
- INSIGHTS & ANALYTICS
- VALUE MANAGEMENT

IAM SUPPLIERS

# IAM SERVICE GOVERNANCE, IAM SERVICE STRATEGY AND IAM ASSET MANAGEMENT

## LEVEL 2 CAPABILITY DEFINITIONS (1/3)

| L1 Capability | L2 Capability | Definition |
|---|---|---|
| **IAM SERVICE STRATEGY** | **STRATEGIC ALIGNMENT** | Aligning frameworks and prioritization around IAM in line with the broader <CLIENT> business strategy and objectives. |
| | **IAM STANDARDS & CONTROLS** | Prescribing IAM policies, control frameworks and standards to which the IAM service must adhere to. |
| | **IAM CAPABILITY OWNERSHIP** | Managing this capability model and related definitions. |
| **IAM MANAGEMENT** | **PERFORMANCE & CONTROL** | Continuously improving the IAM service by monitoring the established KPIs and validating whether IAM operates within the set frameworks. |
| | **KNOWLEDGE MANAGEMENT** | Ensure that relevant information for users and developers, such as policies and training materials, is documented and available in a central location within <CLIENT>. |
| | **INSIGHTS & ANALYTICS** | Develop and maintain dashboards and reports around the IAM service for, for example, compliance. |
| | **VALUE MANAGEMENT** | Continuously monitoring and validating how the IAM services contribute to the defined value drivers. |
| **IAM SERVICE STRATEGY** | **SERVICE LIFECYCLE MANAGEMENT** | Managing and safeguarding the lifecycle and roadmap of all IAM services. |
| | **SERVICE ARCHITECTURE** | Setting the standards around the IAM service architecture in line with the overall enterprise architecture of <CLIENT>. Architecture means a detailed (technical) overview of IAM, as well as the relationships between the components and the environment in which they reside. Additional standards and guidelines that guide the design and development of IAM are also included in the architecture. |
| | **CATALOGUE & DEMAND MANAGEMENT** | Providing and managing a service catalogue at a central location (e.g. a separate IAM portal or integrated in ITSM) that indicates which IAM services are delivered (whether or not in standard building blocks) to the business and IT teams. The available services should be coordinated with the customers, who are also offered the opportunity to give feedback on the IAM service. |

# IAM OPERATIONS

## LEVEL 2 CAPABILITY DEFINITIONS (2/3)

| L1 Capability | L1.5 Capability | L2 Capability | Definition |
|---|---|---|---|
| **IAM OPERATIONS** | **IDENTITY GOVERNANCE** | **User Lifecycle Management** | Services to manage and/or integrate the identities, their life cycle and granted consent (for consent platform). |
| | | **Access Requests & Provisioning** | Services around access requests as well as their execution and management in the target applications. |
| | | **Role Management** | Services to define, identify and maintain roles. |
| | | **Compliance Management** | Services to integrate legal and regulatory requirements into the IAM service, as well as performing operational IAM compliance services such as certification. |
| | **ACCESS MANAGEMENT** | **Authentication** | Services to ensure that identities presented are verified for authenticity (are you who you say you are?). |
| | | **Authorisation** | Services to validate that internal and external identities have the correct rights to access applications and systems. |
| | | **Directory Management** | Managing and synchronizing the databases where most essential information concerning identity profiles and access rights is stored and organized. |
| | **PRIVILEGED ACCESS MANAGEMENT** | **Privileged Access Management** | Services for managing (and rotating passwords of) non-personal and privileged accounts, which have elevated privileges in/around managing systems and/or infrastructure. |

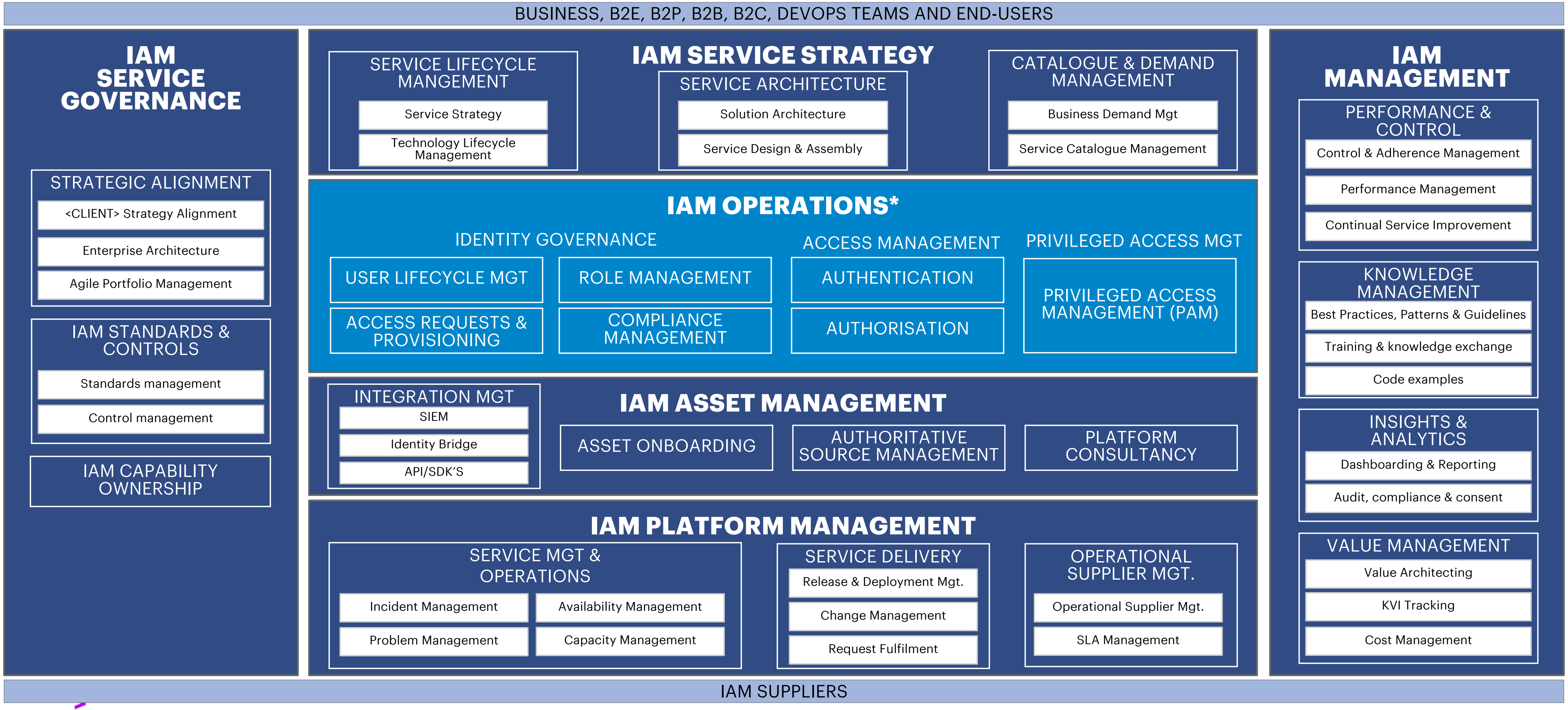
# IAM PLATFORM MANAGEMENT AND IAM ASSET MANAGEMENT

## LEVEL 2 CAPABILITY DEFINITIONS (3/3)

| L1 Capability | L2 Capability | Definition |
|---|---|---|
| **IAM PLATFORM MANAGEMENT** | **SERVICE MGT & OPERATIONS** | Implementation and management of high quality IAM services that meet the needs of <CLIENT> around availability & capacity, among others. This also includes setting up and monitoring operational service management processes (such as incident & problem management). |
| | **SERVICE DELIVERY** | Ensuring that (code) changes to the IAM platform are performed in a controlled, secure and consistent manner with minimal disruption to platform availability. |
| | **OPERATIONAL SUPPLIER MGT.** | Operationally managing and monitoring the relationships with suppliers on aspects such as: monitoring the performance delivered, compliance with agreements (SLAs) and identifying any points for improvement (e.g. in operational costs). |
| **IAM ASSET MANAGEMENT** | **ASSET ONBOARDING** | The onboarding of new assets to the IAM platform. This includes the technical integration, as well as linking (technical) user and management accounts. |
| | **AUTHORITATIVE SOURCE MANAGEMENT** | Maintaining the (linking of) the (technical) source of information that serves as a basis for relevant identity attributes, e.g. from an HR system. |
| | **PLATFORM CONSULTANCY** | Advising development teams and administrators on functionalities of / integration with the IAM platform. |
| | **INTEGRATION MANAGEMENT** | Managing integrations with / through e.g. SIEM, API/CSK and identity bridges. |

# IAM CAPABILITY MODEL– LEVEL 1, 2 & 3

## LEVEL 1, 2 & 3



BUSINESS, B2E, B2P, B2B, B2C, DEVOPS TEAMS AND END-USERS

### IAM SERVICE GOVERNANCE

STRATEGIC ALIGNMENT
- <CLIENT> Strategy Alignment
- Enterprise Architecture
- Agile Portfolio Management

IAM STANDARDS & CONTROLS
- Standards management
- Control management

IAM CAPABILITY OWNERSHIP

### IAM SERVICE STRATEGY

SERVICE LIFECYCLE MANGEMENT
- Service Strategy
- Technology Lifecycle Management

SERVICE ARCHITECTURE
- Solution Architecture
- Service Design & Assembly

CATALOGUE & DEMAND MANAGEMENT
- Business Demand Mgt
- Service Catalogue Management

### IAM OPERATIONS*

IDENTITY GOVERNANCE
- USER LIFECYCLE MGT
- ROLE MANAGEMENT
- ACCESS REQUESTS & PROVISIONING
- COMPLIANCE MANAGEMENT

ACCESS MANAGEMENT
- AUTHENTICATION
- AUTHORISATION

PRIVILEGED ACCESS MGT
- PRIVILEGED ACCESS MANAGEMENT (PAM)

### IAM ASSET MANAGEMENT

INTEGRATION MGT
- SIEM
- Identity Bridge
- API/SDK'S

ASSET ONBOARDING

AUTHORITATIVE SOURCE MANAGEMENT

PLATFORM CONSULTANCY

### IAM PLATFORM MANAGEMENT

SERVICE MGT & OPERATIONS
- Incident Management
- Availability Management
- Problem Management
- Capacity Management

SERVICE DELIVERY
- Release & Deployment Mgt.
- Change Management
- Request Fulfilment

OPERATIONAL SUPPLIER MGT.
- Operational Supplier Mgt.
- SLA Management

### IAM MANAGEMENT

PERFORMANCE & CONTROL
- Control & Adherence Management
- Performance Management
- Continual Service Improvement

KNOWLEDGE MANAGEMENT
- Best Practices, Patterns & Guidelines
- Training & knowledge exchange
- Code examples

INSIGHTS & ANALYTICS
- Dashboarding & Reporting
- Audit, compliance & consent

VALUE MANAGEMENT
- Value Architecting
- KVI Tracking
- Cost Management

IAM SUPPLIERS

* For the overview of the IAM Operations L3 processes, see the next slide

# IAM OPERATIONS

## LEVEL 1, 2 & 3 – OVERVIEW IAM CAPABILITIES

## IAM OPERATIONS

### IDENTITY GOVERNANCE

**USER LIFECYCLE MANAGEMENT**

- Identity Journey Management
- Delegated Administration
- Privacy & User Consent
- Self-Service
- Identity Integration
- Progressive Profiling

**ACCESS REQUESTS & PROVISIONING**

- Provisioning / Deprovisioning
- Workflow Management
- Reconciliation
- Account Management
- Entitlement Management
- Just-In-Time Provisioning

**ROLE MANAGEMENT**

- Role Management
- Role Mining
- Policy Management

**COMPLIANCE MANAGEMENT**

- Subject Rights Management
- Certification
- Segregation of Duties

### ACCESS MANAGEMENT

**AUTHENTICATION**

- Basic Authentication
- Strong Authentication
- Session Management
- Single Sign-On (SSO)
- Federation
- Adaptive Authentication
- API Gateway
- Token Management

**AUTHORISATION**

- Role-Based Access control
- Policy-Based Access control

**DIRECTORY MANAGEMENT**

- Directory Management
- Directory Synchronization

### PRIVILEGED ACCESS MGT

**PRIVILEGED ACCESS MANAGEMENT (PAM)**

- Privileged Account LCM
- Hard-Coded Password Mgt.
- Privileged Session Management
- Remote Maintenance Access
- Firefighter Access
- DevOps Pipeline Management
- Credential Rotation

# IAM MANAGEMENT

## LEVEL 3 PROCESS DEFINITIONS (2/4)

| L1 Capability | L2 Capability | L3 Process | Definition |
|---|---|---|---|
| **IAM MANAGEMENT** | **PERFORMANCE & CONTROL** | Control & Adherence Management | Validating that IAM operates within the framework set and adjusting and/or escalating where necessary. |
| | | Performance Management | Drawing up (technical) KPIs for the IAM platforms, for example concerning availability and throughput time, monitoring these in a central location and adjusting and/or escalating where necessary. |
| | | Continual Service Improvement | Continuously identify improvements to enhance IAM services in coordination with users. |
| | **INSIGHTS & ANALYTICS** | Dashboarding & Reporting | The provision of standard and/or specific dashboards and reports concerning the IAM service, for the benefit of (senior) management, for example, to support decision-making. |
| | | Audit, Compliance & Consent | Generating insights for audit, compliance and consent purposes in order to comply with internal and external regulations (e.g. AVG). |
| | **VALUE MANAGEMENT** | Value Architecting | Identifying the value drivers and key value indicators (KVIs) to express what value IAM delivers. |
| | | KVI Tracking | Monitoring and providing insight into the KVIs drawn up. |
| | | Cost Management | Understanding and controlling the costs of IAM services. |
| | **KNOWLEDGE MANAGEMENT** | Best Practices, Patterns & Guidelines | Develop and collect IAM best practices, patterns and guidelines from both internal (e.g., staff, publications) and external sources (e.g., web, other companies, conferences). |
| | | Training & Knowledge Exchange | Gathering and making available IAM-related knowledge through training and establishing a central point for knowledge sharing. |
| | | Code Examples | Provision of sample codes, allowing uniform application of previously developed codes within <CLIENT> (and thus faster development). |

# IAM SERVICE GOVERNANCE & IAM ASSET MANAGEMENT

## LEVEL 3 PROCESS DEFINITIONS (3/4)

| L1 Capability | L2 Capability | L3 Process | Definition |
|---|---|---|---|
| **IAM SERVICE STRATEGY** | **SERVICE LIFECYCLE MANAGEMENT** | Service Strategy | Drawing up and managing a clear IAM vision and roadmap, within the established frameworks from Enterprise Architecture. |
| | | Technology Lifecycle Management | Managing a future-proof roadmap and lifecycle of IAM-related technologies in line with the latest developments and innovations. This includes the timely announcement of any phasing out and coordination with stakeholders. |
| | **SERVICE ARCHITECTURE** | Solution Architecture | Drawing up a detailed architecture for IAM solutions, including an overview of how all components work together, within the established frameworks from Enterprise Architecture. |
| | | Service Design & Assembly | Designing and setting up (technically configuring) the IAM service(s). In addition, controlling and monitoring the introduction of and changes to IAM services. |
| | **CATALOGUE & DEMAND MANAGEMENT** | Business Demand Mgt | Matching the demand for available IAM services with the users, who are also given the opportunity to give feedback on the IAM service. |
| | | Service Catalogue Management | Providing and managing a service catalogue at a central location (e.g. a separate IAM portal or integrated into ITSM) that indicates which IAM services are delivered (whether or not in standard building blocks) to the business and IT teams. |
| **IAM ASSET MANAGEMENT** | **INTEGRATION MANAGEMENT** | SIEM (Security Information and Event Management) | Providing IAM related (log and/or user) data and insights for the benefit of the SIEM tooling and SOC services. |
| | | Identity Bridge | Linking of directories from on-premises to cloud and other directories through an API to give users easier access to applications. |
| | | API/SDK's | Linking to API-related software development kits for browser-related IT development for certain cloud services. |

# IAM PLATFORM MANAGEMENT

## LEVEL 3 PROCESS DEFINITIONS (4/4)

| L1 Capability | L2 Capability | L3 Process | Definition |
|---|---|---|---|
| **IAM PLATFORM MANAGEMENT** | **SERVICE MGT & OPERATIONS** | Incident Management | Managing all incidents - to ensure that IAM services are up and running again as soon as possible and to minimize the impact on operations. |
| | | Problem Management | Determine what is needed as a solution to (recurring) problems so that they do not recur, for example by applying a Root-Cause Analysis (RCA). |
| | | Availability Management | The process responsible for ensuring that IAM services meet the current and future availability needs of <CLIENT>. |
| | | Capacity Management | The process responsible for ensuring that the capacity of IAM services and IAM infrastructure meets agreed capacity and performance requirements. |
| | **SERVICE DELIVERY** | Release & Deployment Mgt. | Scheduling of controlled releases to the test and production environments of the IAM platform, for example through automated deployments in a CI/CD pipeline. |
| | | Change Management | Assessing and managing changes in the IAM platforms to implement them with minimal disruption to the IAM operation. |
| | | Request Fulfilment | Executing applications and standard requests (whether or not after applying a pre-established approval and review process). |
| | **OPERATIONAL SUPPLIER MGT.** | Operational Supplier Mgt. | Operational management of supplier services (weekly reconciliation, reports, service improvement). |
| | | SLA Management | Assessing suppliers against agreed Service Level Agreements (SLAs) and Operational Level Agreements (OLAs)s and escalating where necessary. |

accenture

# IAM OPERATIONS - IDENTITY GOVERNANCE

## LEVEL 3 PROCESS DEFINITIONS (1/4)

| L1.5 Capability | L2 Capability | L3 Process | Description |
|---|---|---|---|
| **IDENTITY GOVERNANCE** | **USER LIFECYCLE MANAGEMENT** | Identity Journey Management | Processes related to the creation, management and definition of the identity and related attributes from the moment it is known to the source (e.g. HR) until the moment the account is deactivated and deleted. |
| | | Delegated Administration | Delegated administration processes that allow local administrators or supervisors to perform changes on a limited part of the IAM platform, for example for the benefit of market participants. This includes scenarios where a user is authorised to perform actions on behalf of another user. |
| | | Self-Service | Processes that allow users to manage their own identity data and passwords within the set frameworks. |
| | | Identity Integration | Processes for integrating (attributes related to) an internal or external identity between applications and environments, for example using APIs. |
| | | Privacy & User Consent | Processes to allow use of data after consent from the owner of this (personal) data. |
| | | Progressive Profiling | Progressive profiling is a technique that allows to gradually collect more data on leads at strategically timed intervals throughout the identity journey. |
| | **ACCESS REQUESTS & PROVISIONING** | Workflow Management | Processes for managing the workflow for validation and approval for granting access. The workflow provides a distribution of the tasks to be performed in this process, for example, for approval by the user's manager. |
| | | Provisioning/Deprovisioning | Processes for creating, modifying and deleting user accounts and access rights in IAM-managed target applications and systems (after following defined workflows). |
| | | Account Management | Processes to manage user accounts by creating, modifying, updating and deleting user records in target applications and systems managed by IAM. |
| | | Reconciliation | Processes for reconciling roles and rights in the IAM solution with the target application(s) if differences are identified. |

# IAM OPERATIONS - IDENTITY GOVERNANCE

## LEVEL 3 PROCESS DEFINITIONS (2/4)

| L1.5 Capability | L2 Capability | L3 process | Description |
|---|---|---|---|
| **IDENTITY GOVERNANCE** | **ACCESS REQUESTS & PROVISIONING** | Just-In-Time Provisioning | The creation of accounts in (web) applications at the first login attempt of a user. |
| | | Entitlement Management | The ability to centrally manage access rights from target applications. |
| | **ROLE MANAGEMENT** | Role Management | Processes to define and maintain roles and rights. |
| | | Policy Management | Management and maintenance of policies in a Policy Administration Point (**PAP**), looking at: 1) the attributes of a user (e.g. in-service status, job title), 2) the resource the user is trying to access, 3) the action the user is trying to do (read, write) and 4) the environment context (e.g. location, time zone or device type). These policies are stored in the Policy Information Point (**PIP**). |
| | | Role Mining | Ability to automatically discover the role structure by analysing the rights assigned to users with similar identity attributes. |
| | **COMPLIANCE MANAGEMENT** | Data Subjects Rights Management | Identifying where IAM plays a role in relation to the rights of a data subject, arising from the AVG, as well as setting up and enforcing compliance. |
| | | Segregation of Duties (SoD) | Enable segregation of duties and powers to prevent one person being responsible for critical actions in a business process or having access to data outside their capacity (e.g. supplier). |
| | | Certification | Periodic process of validating proper access and issuing "certificates" after validation, as well as revoking non-valid access. |

# IAM OPERATIONS - ACCESS MANAGEMENT

## LEVEL 3 PROCESS DEFINITIONS (3/4)

| L1.5 Capability | L2 Capability | L3 Process | Description |
|---|---|---|---|
| **ACCESS MANAGEMENT** | **AUTHENTICATION** | Basic Authentication | Validate, using a username and password, whether the identity presented by the user is correct. |
| | | Strong Authentication | Combination of username, password and an additional factor such as tokens, biometric data, smart cards or certificates. Multi-factor authentication is when something the user knows (password) is supplemented by something the user has (token, smart card) or something the user is (fingerprint, biometric data). |
| | | API Gateway | Providing and managing central authentication components for both internal and external APIs within <CLIENT>. |
| | | Session Management | Method that, during a user session (after authentication), allows the user to seamlessly access applications as long as the authentication ticket or token is valid. This process also includes enforcement of session duration controls, idle session timeouts, protection against session hijacking, etc. |
| | | Adaptive Authentication | Based on the risk profile and behaviour of the user, different authentication factors can be requested from the user. This is a form of multi-factor authentication. |
| | | Federation | Collaboration based on a trust relationship between different identity providers, for example from partners as well as from external identity providers such as IDIN or eRecognition. After entering into the trust relationship, users can use the same credentials to access multiple environments. |
| | | Single Sign-On (SSO) | Method whereby the user can access multiple applications with a single login. |
| | | Token Management | Management of access tokens, which are used for token-based authentication such as APIs. |
| | **DIRECTORY MANAGEMENT** | Directory Management | Managing the directories where identity profiles and access rights are stored and organized. |
| | | Directory Synchronization | Synchronizing between directories where access rights and identity profiles are stored and organized so that they are up-to-date in the various systems. For example, between Cloud and on-premises directories. |

# IAM OPERATIONS - ACCESS MANAGEMENT AND PRIVILEGED ACCESS MANAGEMENT

## LEVEL 3 PROCESS DEFINITIONS (4/4)

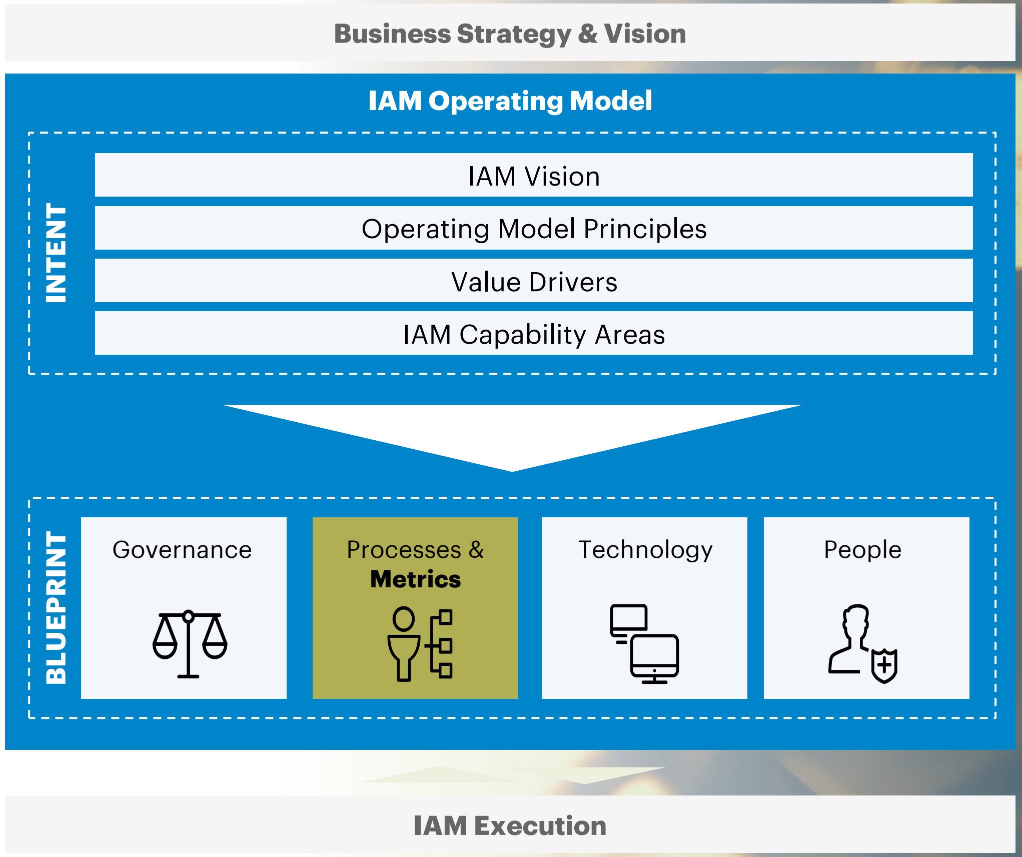
| L1.5/L2 Capability | | L3 Process | Description |
|---|---|---|---|
| **ACCESS MANAGEMENT** | **AUTHORISATION** | Role-Based Access Control | A form of course-grained authorization, in which a user has one or more roles assigned based on function and/or position within the organization. This form of authorization is dependent on a pre-defined role. |
| | | Policy-Based Access Control | A form of fine-grained authorization, where one or more attributes of the user are used to determine access rights based on predefined policies. Authorization decisions are enforced by a Policy Enforcement Point (**PEP**) and evaluated by a Policy Decision Point (**PDP**). |
| **PRIVILEGED ACCESS MANAGEMENT** | | Privileged Account LCM | The lifecycle management of privileged accounts largely follows the regular Identity Journey Process. However, for privileged accounts, onboarding and decommissioning are especially relevant because of the risk of the increased rights these accounts have. |
| | | Firefighter Access | The possibility of using a highly privileged account for exceptional situations. |
| | | Hard-Coded Password Management | Process of externalizing passwords, allowing hard-coded credentials to be removed from application code and replaced with more secure configurations. |
| | | Remote Maintenance Access | Providing the possibility to grant third parties access to perform remote (maintenance) work. |
| | | Privileged Session Management | This process is similar to the regular session management process, only specifically for setting up sessions for privileged accounts that are centrally logged and reviewed. |
| | | DevOps Pipeline Management | The ability to automatically manage the passwords of the accounts used in the DevOps pipeline through the other privileged account management processes. |
| | | Credential Rotation | Changing and resetting passwords in order to shorten their lifespan and increase security. |

# CONTENTS

## IAM VISION

### Contents

1. IAM Vison
2. Operating Model Principles
3. Value drivers
4. IAM Capability Areas
5. **Metrics**
6. Governance & Processes
7. Technology & Vendors
8. People (Roles and sourcing)



Business Strategy & Vision

IAM Operating Model

INTENT

IAM Vision

Operating Model Principles

Value Drivers

IAM Capability Areas

BLUEPRINT

Governance

Processes & **Metrics**

Technology

People

IAM Execution

accenture

# DEPENDING ON THE GUARDRAILS AND SOLUTIONING THE DEFINITIVE KPI'S NEED TO BE DEVELOPED IN COOPERATION WITH THE BUSINESS

## ILLUSTRATIVE KPI'S AND METRICS

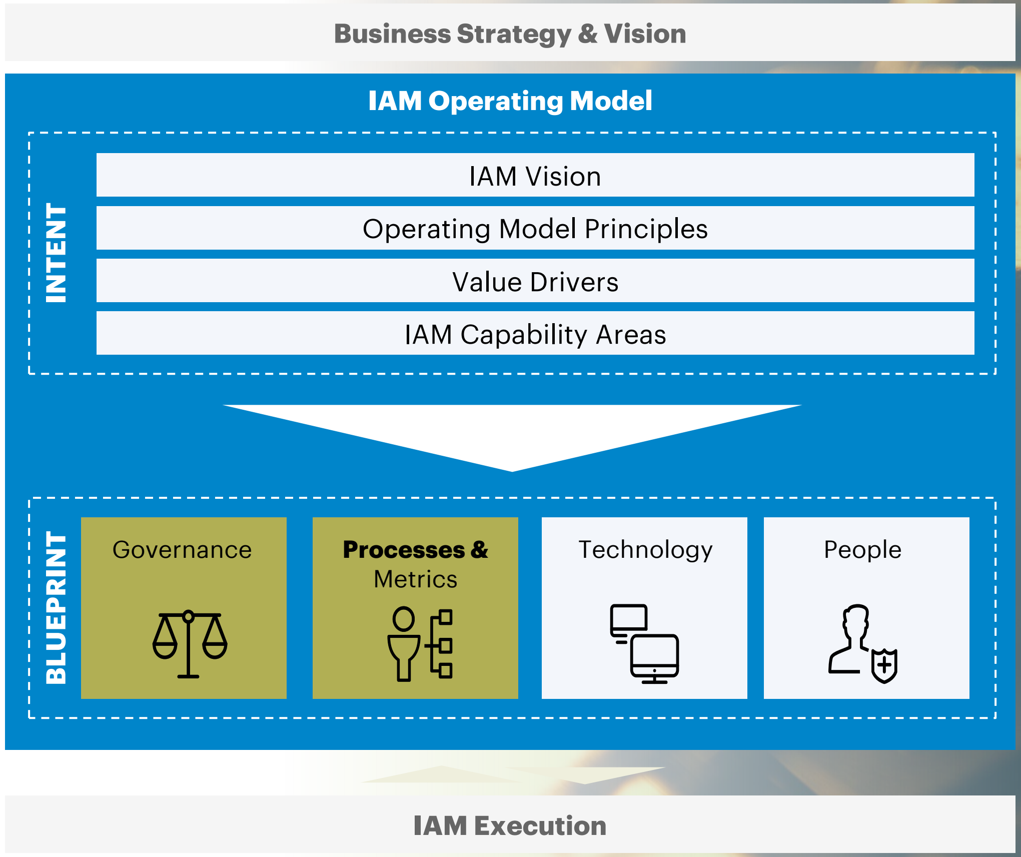
| | | OPERATIONAL EFFICIENCY | END-USER SATISFACTION | RISK & COMPLIANCE | ECOSYSTEM ENABLEMENT |
|---|---|---|---|---|---|
| **Coverage** | Metrics concerning the reach of IAM, such as:<br>• The % applications which is onboarded to IAM of SSO<br>• The % users is being managed by IAM | ☑ | ☑ | ☑ | ☑ |
| **Performance** | Metrics concerning the (technical) performance of IAM, such as:<br>• Average time to gain access<br>• Average % availability (up-time) compared to set goals | ☑ | ☑ | | |
| **Effectivity** | Metrics concerning the effectivity of IAM, measured from the implementation, such as:<br>• Average time to get the right access<br>• % of automatically generated audit reports (against the total number) | ☑ | ☑ | | |
| **Compliance & Hygiene** | Metrics on how IAM operates within the set guardrails, such as:<br>• # SoD violations and their duration<br>• % accounts without an identity (orphaned accounts) | | | ☑ | |

# CONTENTS

## IAM CAPABILITY MODEL

**Contents**

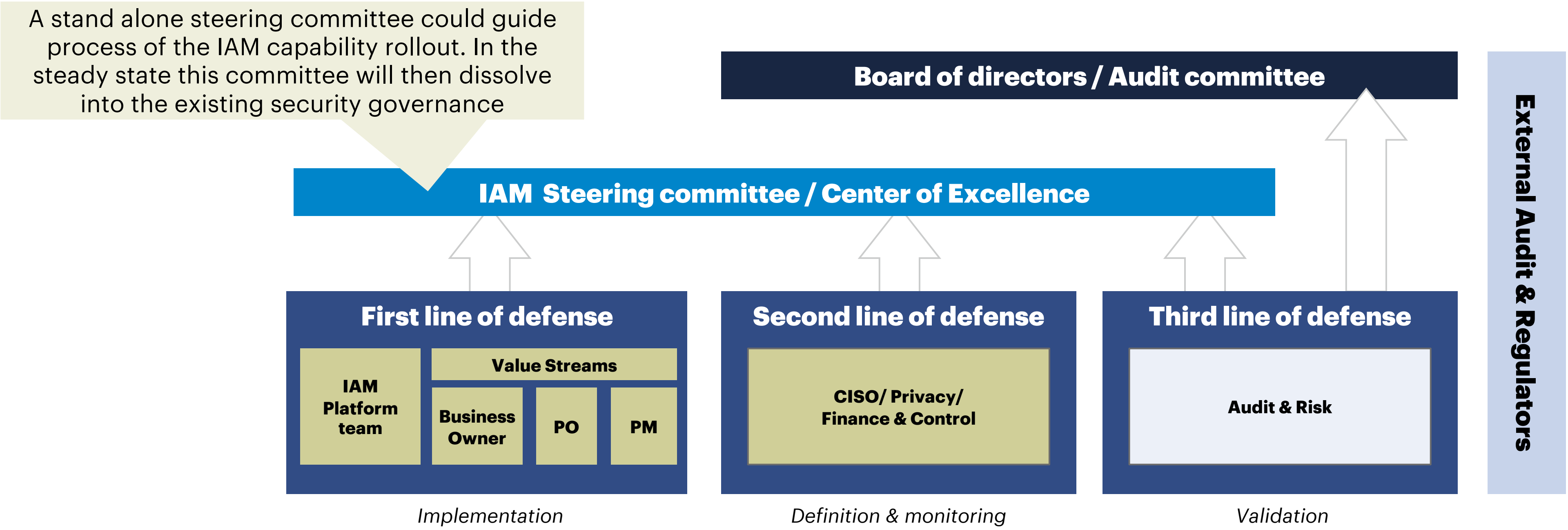
1. IAM Vison
2. Operating Model Principles
3. Value drivers
4. IAM Capability Areas
5. Metrics
6. **Governance & Processes**
7. Technology & Vendors
8. People (Roles and sourcing)



accenture

# THE IAM FUNCTION SHOULD FOLLOW THE THREE LINES OF DEFENSE RETORICS

## IAM AS CONTROL FUNCTION


A stand alone steering committee could guide process of the IAM capability rollout. In the steady state this committee will then dissolve into the existing security governance
Board of directors / Audit committee
IAM Steering committee / Center of Excellence
First line of defense
IAM Platform team
Value Streams
Business Owner
PO
PM
Second line of defense
CISO/ Privacy/ Finance & Control
Third line of defense
Audit & Risk
External Audit & Regulators
Implementation
Definition & monitoring
Validation

**Applicable Controls/ standards (non-exhaustive list)**

- *Privacy policy*
- *Internal control frameworks*
- *IAM policy*
- *Business risk profile*

**Other relevant IAM entities**

- Enterprise Architecture (guardrails)
- B2B/Partner registration (user lifecycle mgt & onboarding)
- Employees

# CLOSE COLLABORATION BETWEEN DIFFERENT FUNCTIONS IS REQUIRED TO ENABLE THE IAM PLATFORMS

## GOVERNANCE

**Either a set multidisciplinairy program team is setup, or execution is done within Agile (SAFE) ceremonies**

| IAM Guardrails | | | IAM Platforms | | | | Identities | Applications & access (implementation) | |
|---|---|---|---|---|---|---|---|---|---|
| **Enterprise Architecture** | **Privacy & Security** | **Finance & Control** | **IAM Product team** | | | | **HR / B2B** | **Business Application Owners** | |
| Architecture principles | IAM Standards & Controls | | **IAM Service Strategy** | **IAM Operations** | **IAM Platform Mgt.** | **IAM Management** | **Identity Governance** (source) | Access Requests & Provisioning | Asset Onboarding |
| | | | Service Lifecycle Management | Authentication | Operational supplier Mgt. | Performance & Control | User Lifecycle Management | Role Management | Integration Management |
| | | | Service Architecture | Authorisation | Service Delivery | Knowledge Management | Authoritative Source Mgt. | Compliance Management | |
| | | | Catalogue & Demand Mgt. | Privileged Access Management | Service Mgt & Operations | Insights & Analytics | Enabled by technical IAM platform capabilities | | |
| | | | | | Platform Consultancy | Value Management | | | |

accenture

🟩 = Responsible

# ROLES AND RESPONSIBILITIES CONCERNING IAM ARE AFFECTING THE WHOLE ORGANIZATION

## IMPORTANT STAKEHOLDERS

### Guardrails

**CISO / Privacy Finance & Control**
Act as the second line of defense, defining the controls

**Enterprise Architects**
Defining technical & architectural guardrails

### Responsible for implementation and compliancy of controls

**Value Stream/ Application Owner**
Application owner, responsible for onboarding of applications and complying with control guidelines

**Responsible Supervisor/Manager**
Manager of the employee, responsible for the validation of access and role/policy administration

**Employee**
User of the systems

### Platform Ownership

**IAM Platform**
Owner of the IAM capability, platform(s) and processes. Including strategy, vision and management

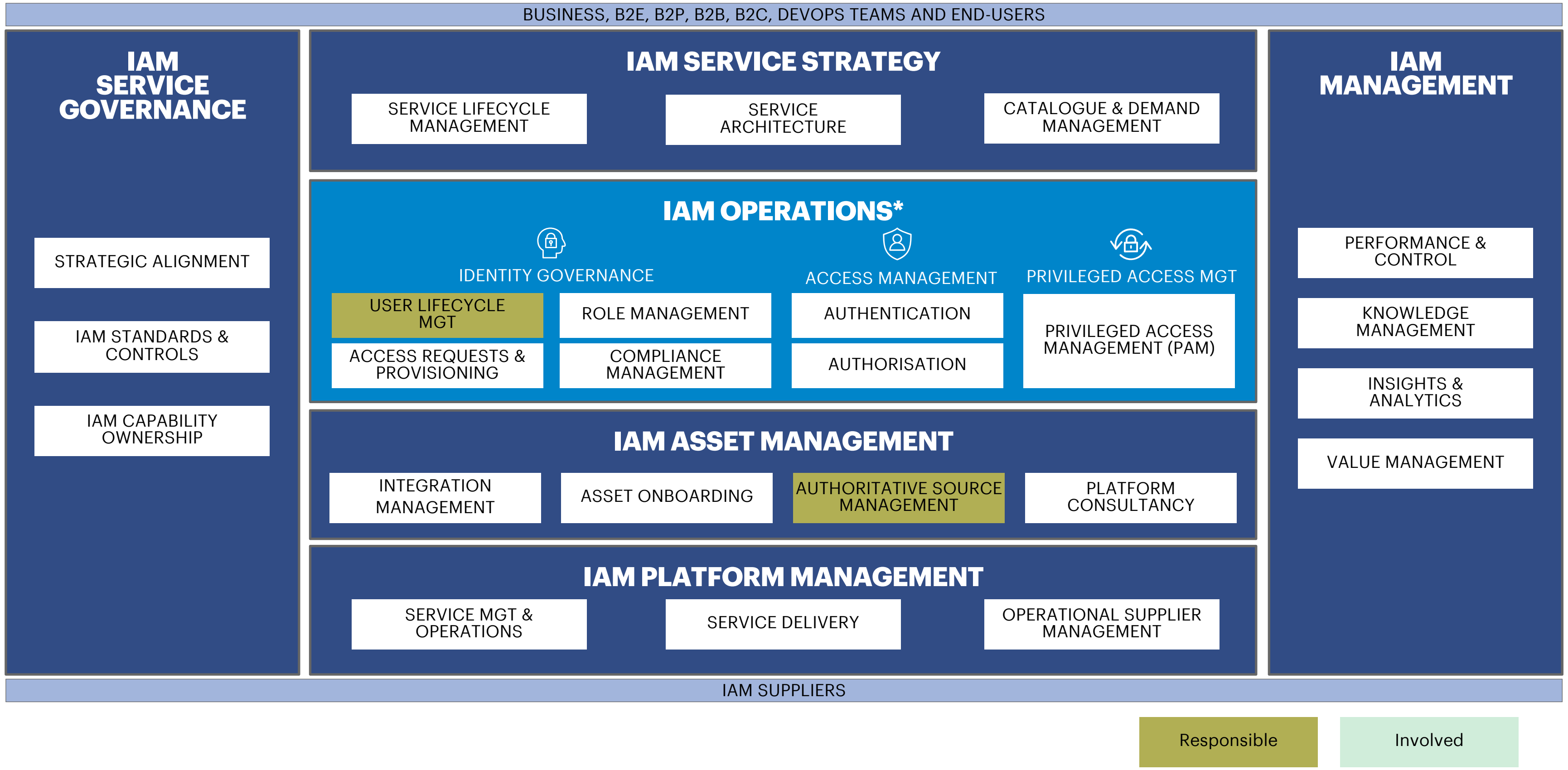
### Management of Identities

**HR**
Owner of the organizational and employee data

**B2B/Partner registration**
Owner of the B2B/partner registration process

# A DAY IN THE LIFE OF .... HR EMPLOYEE

## ROLES & RESPONSIBILITIES



BUSINESS, B2E, B2P, B2B, B2C, DEVOPS TEAMS AND END-USERS

**IAM SERVICE GOVERNANCE**

- STRATEGIC ALIGNMENT
- IAM STANDARDS & CONTROLS
- IAM CAPABILITY OWNERSHIP

**IAM SERVICE STRATEGY**

- SERVICE LIFECYCLE MANAGEMENT
- SERVICE ARCHITECTURE
- CATALOGUE & DEMAND MANAGEMENT

**IAM OPERATIONS***

IDENTITY GOVERNANCE

- USER LIFECYCLE MGT (Responsible)
- ROLE MANAGEMENT
- ACCESS REQUESTS & PROVISIONING
- COMPLIANCE MANAGEMENT

ACCESS MANAGEMENT

- AUTHENTICATION
- AUTHORISATION

PRIVILEGED ACCESS MGT

- PRIVILEGED ACCESS MANAGEMENT (PAM)

**IAM ASSET MANAGEMENT**

- INTEGRATION MANAGEMENT
- ASSET ONBOARDING
- AUTHORITATIVE SOURCE MANAGEMENT (Responsible)
- PLATFORM CONSULTANCY

**IAM PLATFORM MANAGEMENT**

- SERVICE MGT & OPERATIONS
- SERVICE DELIVERY
- OPERATIONAL SUPPLIER MANAGEMENT

**IAM MANAGEMENT**

- PERFORMANCE & CONTROL
- KNOWLEDGE MANAGEMENT
- INSIGHTS & ANALYTICS
- VALUE MANAGEMENT

IAM SUPPLIERS

Responsible | Involved

## Management of Identities

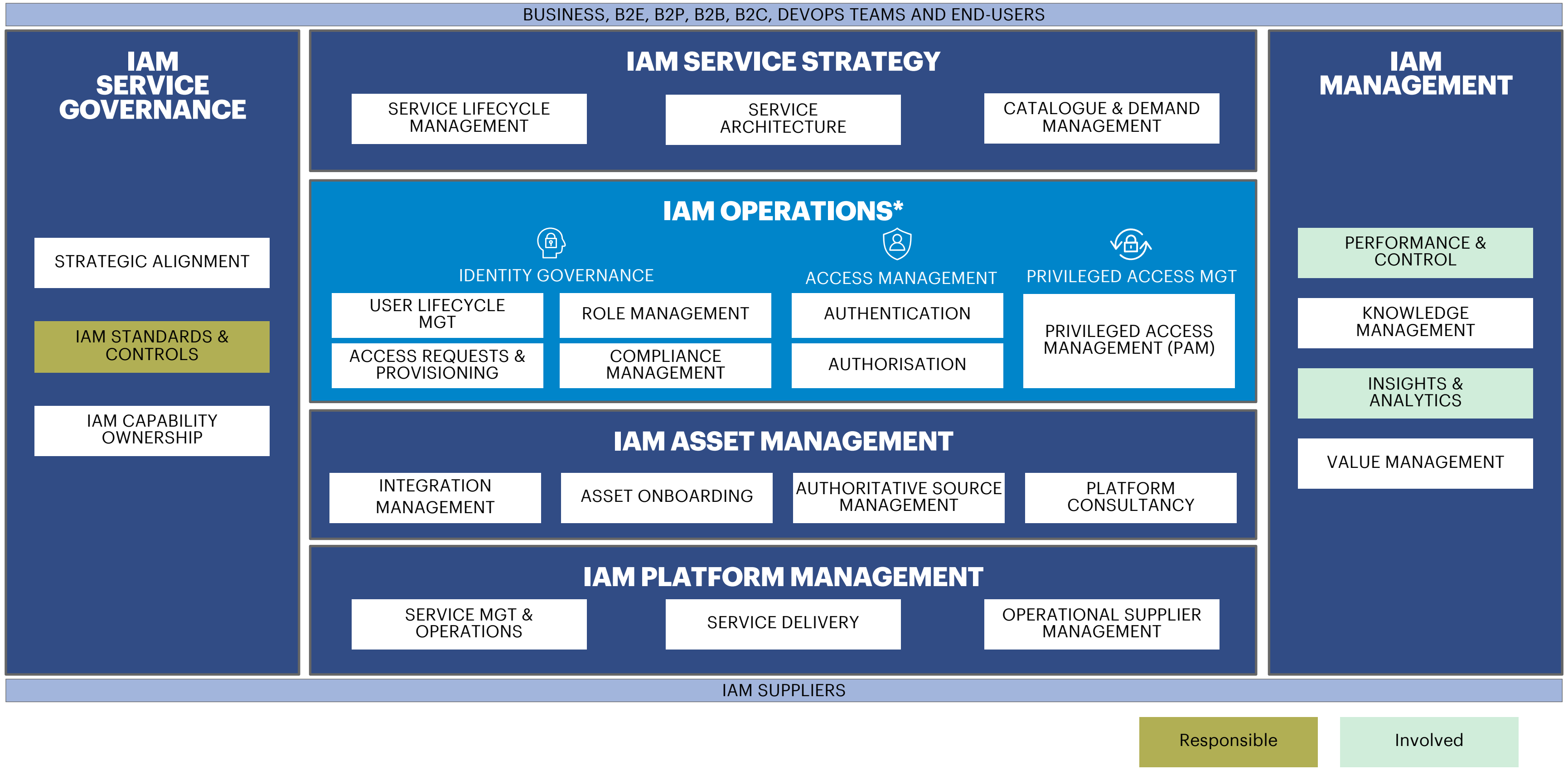
### HR

Owner of the organizational and employee data

- **Responsible for the joiner leaver, mover process for employees**
- **Owner of the identity data of employees and organizational structure**
- **Ensures that this data is communicated correctly for IAM purposes**

# A DAY IN THE LIFE OF…. CISO/ PRIVACY/AUDIT & CONTROL OFFICER

## ROLES & RESPONSIBILITIES



BUSINESS, B2E, B2P, B2B, B2C, DEVOPS TEAMS AND END-USERS

### IAM SERVICE GOVERNANCE

- STRATEGIC ALIGNMENT
- IAM STANDARDS & CONTROLS
- IAM CAPABILITY OWNERSHIP

### IAM SERVICE STRATEGY

- SERVICE LIFECYCLE MANAGEMENT
- SERVICE ARCHITECTURE
- CATALOGUE & DEMAND MANAGEMENT

### IAM OPERATIONS*

IDENTITY GOVERNANCE

- USER LIFECYCLE MGT
- ROLE MANAGEMENT
- ACCESS REQUESTS & PROVISIONING
- COMPLIANCE MANAGEMENT

ACCESS MANAGEMENT

- AUTHENTICATION
- AUTHORISATION

PRIVILEGED ACCESS MGT

- PRIVILEGED ACCESS MANAGEMENT (PAM)

### IAM ASSET MANAGEMENT

- INTEGRATION MANAGEMENT
- ASSET ONBOARDING
- AUTHORITATIVE SOURCE MANAGEMENT
- PLATFORM CONSULTANCY

### IAM PLATFORM MANAGEMENT

- SERVICE MGT & OPERATIONS
- SERVICE DELIVERY
- OPERATIONAL SUPPLIER MANAGEMENT

### IAM MANAGEMENT

- PERFORMANCE & CONTROL
- KNOWLEDGE MANAGEMENT
- INSIGHTS & ANALYTICS
- VALUE MANAGEMENT

IAM SUPPLIERS

Responsible

Involved

## Guardrails

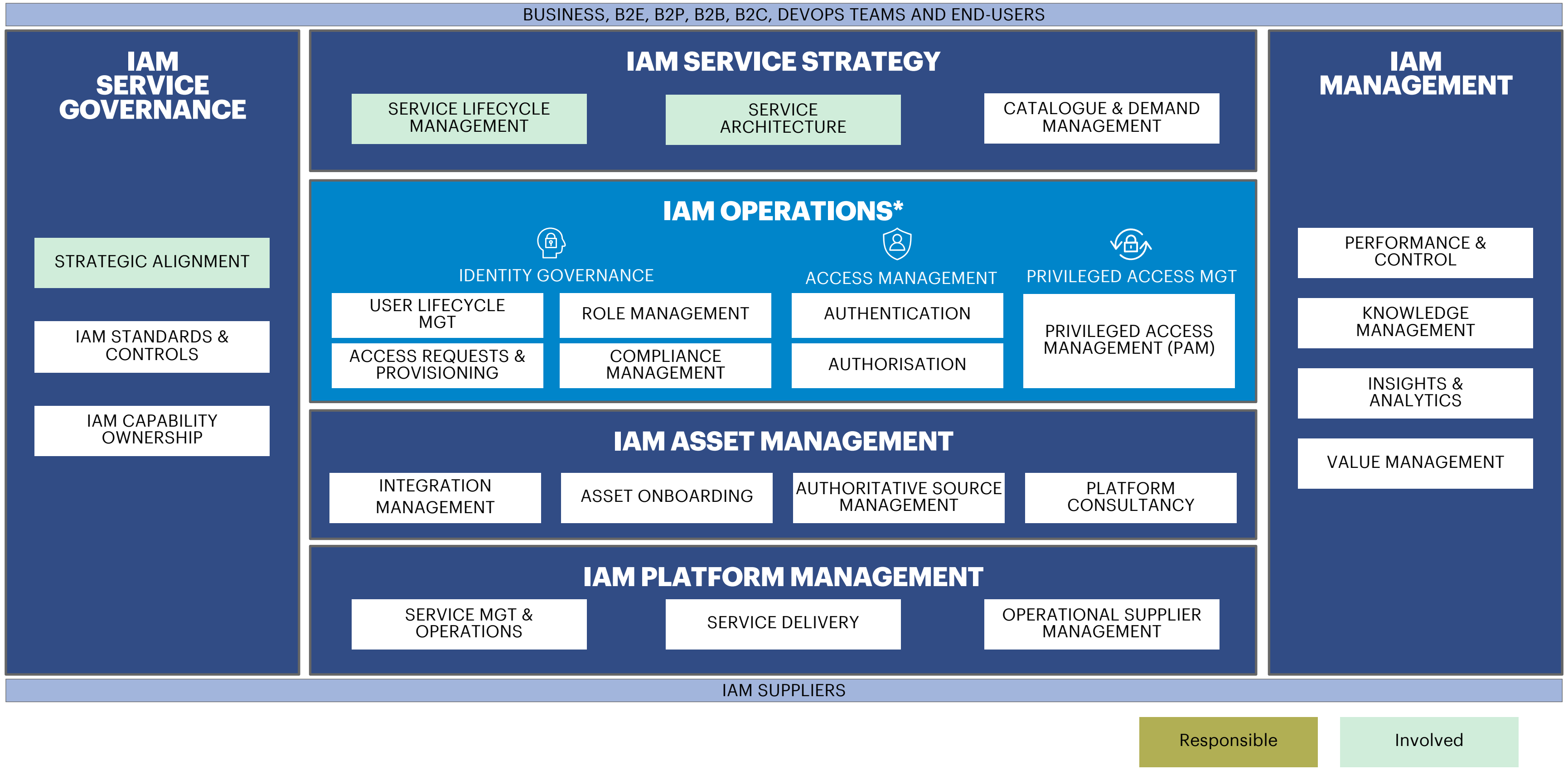
### CISO/ Privacy/Audit & Control

Act as second line of defense

- **Defining standards and control frameworks in line with legal guidelines**
- **Validation and reporting of compliance of the IAM policy**

# A DAY IN THE LIFE OF …. ENTERPRISE ARCHITECT

## ROLES & RESPONSIBILITIES



BUSINESS, B2E, B2P, B2B, B2C, DEVOPS TEAMS AND END-USERS

**IAM SERVICE GOVERNANCE**

- STRATEGIC ALIGNMENT
- IAM STANDARDS & CONTROLS
- IAM CAPABILITY OWNERSHIP

**IAM SERVICE STRATEGY**

- SERVICE LIFECYCLE MANAGEMENT
- SERVICE ARCHITECTURE
- CATALOGUE & DEMAND MANAGEMENT

**IAM OPERATIONS***

IDENTITY GOVERNANCE

- USER LIFECYCLE MGT
- ROLE MANAGEMENT
- ACCESS REQUESTS & PROVISIONING
- COMPLIANCE MANAGEMENT

ACCESS MANAGEMENT

- AUTHENTICATION
- AUTHORISATION

PRIVILEGED ACCESS MGT

- PRIVILEGED ACCESS MANAGEMENT (PAM)

**IAM ASSET MANAGEMENT**

- INTEGRATION MANAGEMENT
- ASSET ONBOARDING
- AUTHORITATIVE SOURCE MANAGEMENT
- PLATFORM CONSULTANCY

**IAM PLATFORM MANAGEMENT**

- SERVICE MGT & OPERATIONS
- SERVICE DELIVERY
- OPERATIONAL SUPPLIER MANAGEMENT

**IAM MANAGEMENT**

- PERFORMANCE & CONTROL
- KNOWLEDGE MANAGEMENT
- INSIGHTS & ANALYTICS
- VALUE MANAGEMENT

IAM SUPPLIERS

Responsible

Involved

### Guardrails

**Enterprise Architects**

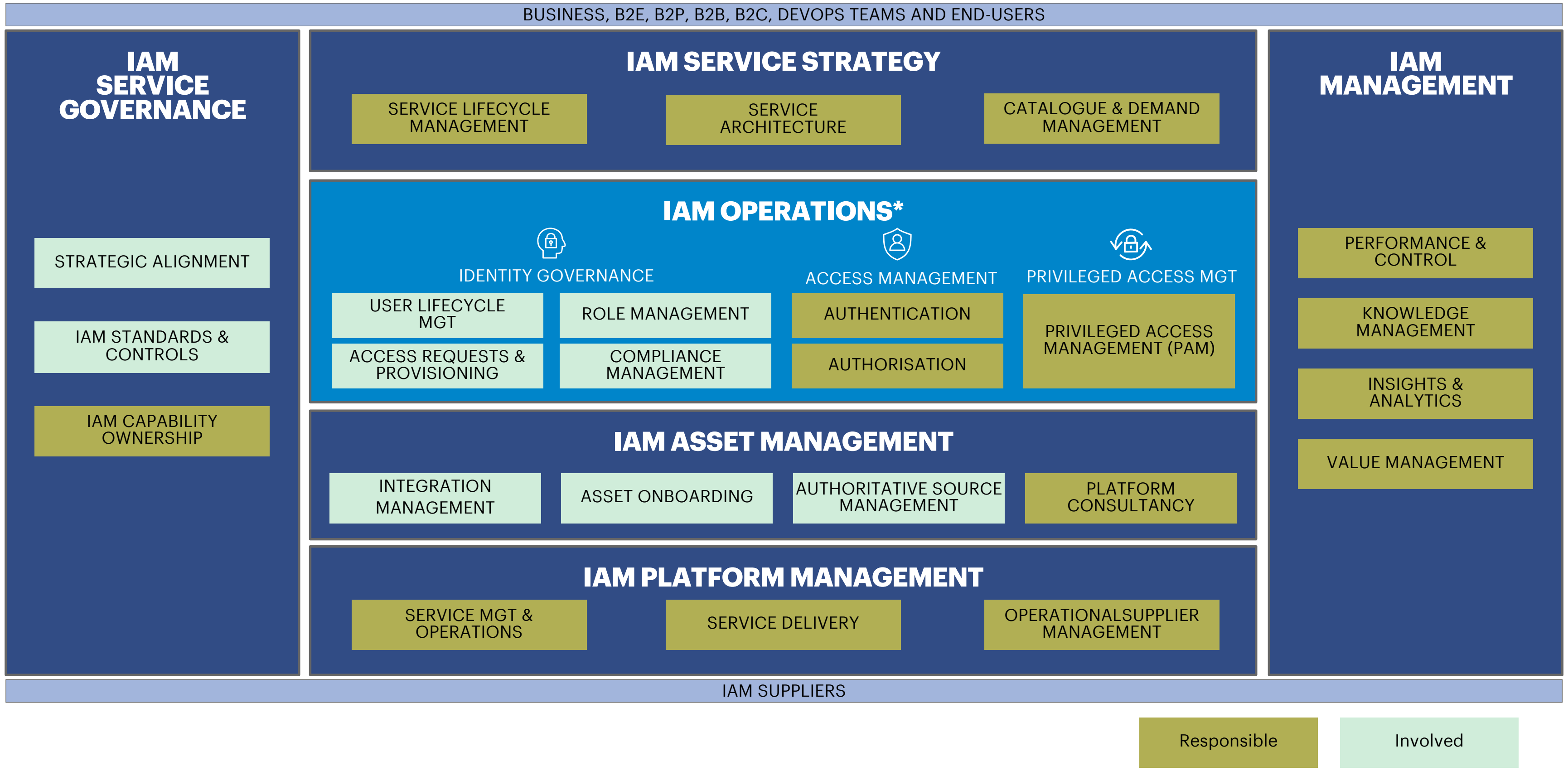
Defining technical guardrails

- **Set up architectural guardrails in line with strategic goals and ambition of the client**
- **Provide consultancy for technology related decisions concerning IAM platforms**
- **Assist IAM platform in definition of service architecture**

accenture

# A DAY IN THE LIFE OF .... IAM PLATFORM EMPLOYEE

## ROLES & RESPONSIBILITIES



## Platform Ownership

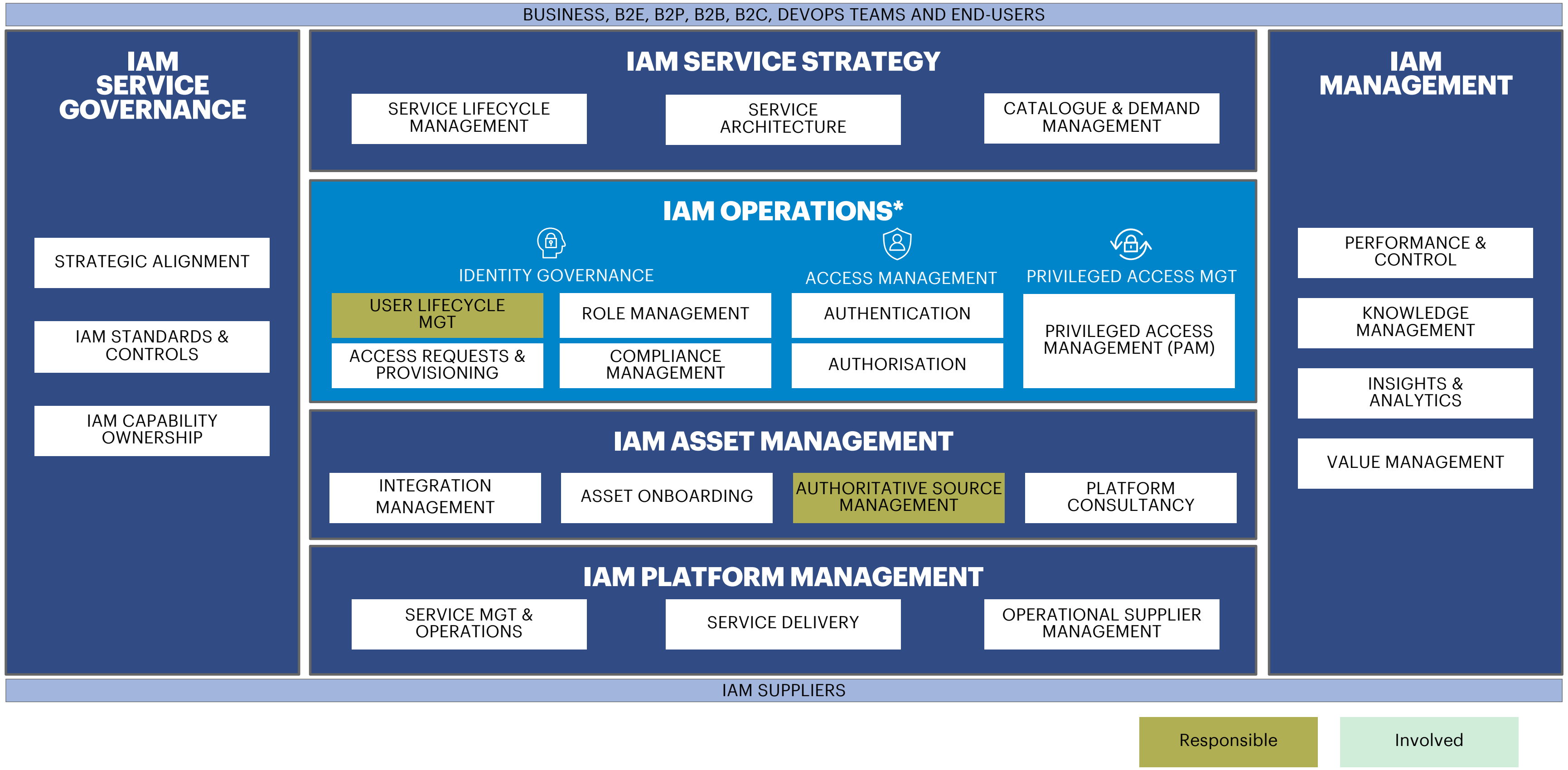
### IAM Platform

Owner of the IAM capability, platform(s) and processes. Including strategy, vision and management

- **Designs and delivers IAM platform**
- **Decide together with EA on technology options with regards to IAM**
- **Takes care of operational IAM activities by providing technical solutions for IGA and PAM**
- **Consults on IAM topics for value streams and DevOps teams where necessary**
- **IAM platform management can be handed over to a system integrator, but will remain a responsibility of the IAM platform team**

# A DAY IN THE LIFE OF .... B2B/PARTNER REGISTRATION EMPLOYEE

## ROLES & RESPONSIBILITIES



## Management of Identities

### B2B/Partner registration

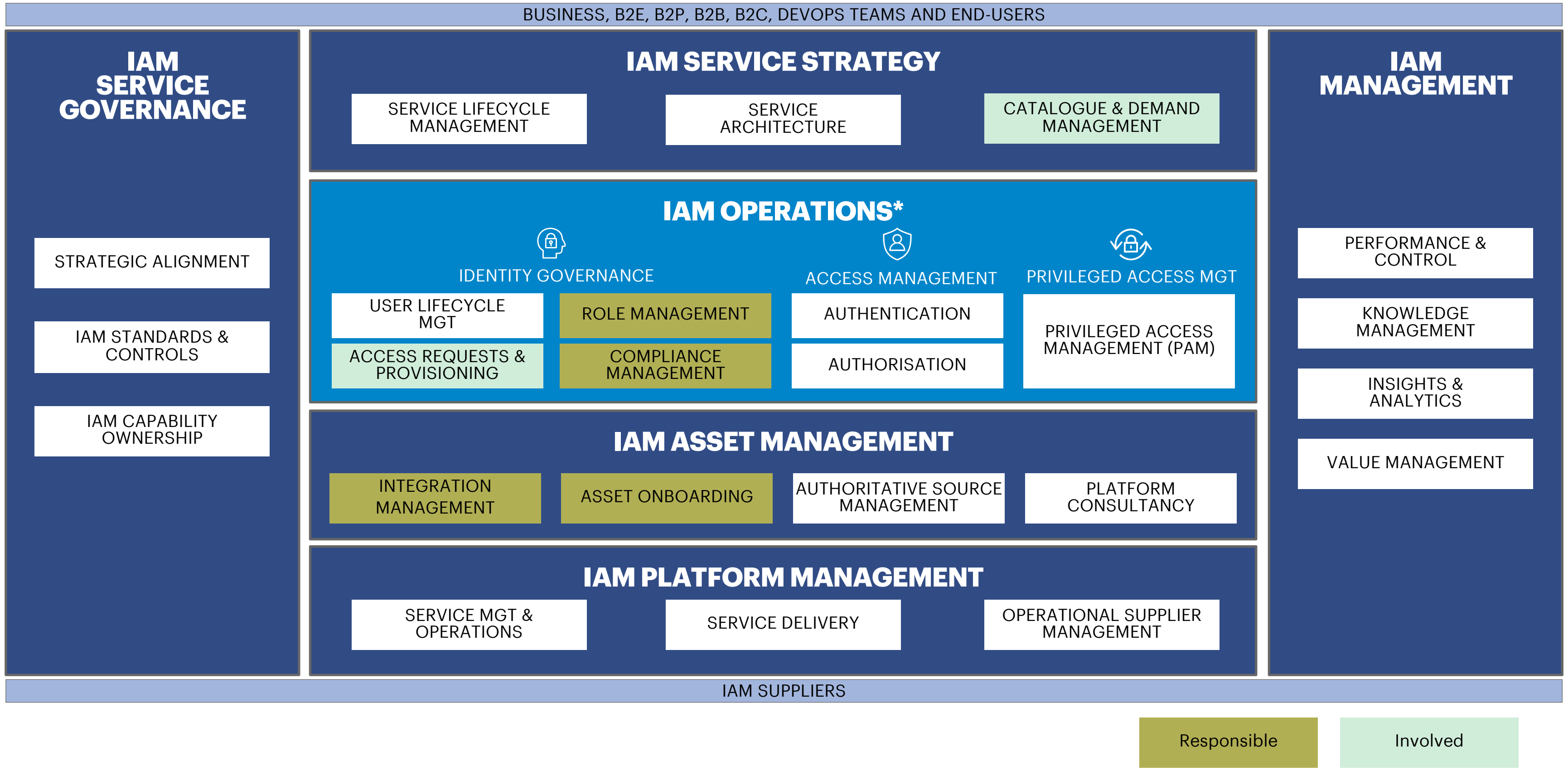
Owner of the B2B/partner registration process

- **Facilitates the on and offboarding process for new B2B/Partner companies, including creation of the super user**
- **Transfers the responsibility of onboarding and registering B2B/partners' employees to their respective superuser**
- **Responsible for correct usage of B2B/Partner data related to IAM**

accenture

# A DAY IN THE LIFE OF …. APPLICATION OWNER

## ROLES & RESPONSIBILITIES



BUSINESS, B2E, B2P, B2B, B2C, DEVOPS TEAMS AND END-USERS

**IAM SERVICE GOVERNANCE**
- STRATEGIC ALIGNMENT
- IAM STANDARDS & CONTROLS
- IAM CAPABILITY OWNERSHIP

**IAM SERVICE STRATEGY**
- SERVICE LIFECYCLE MANAGEMENT
- SERVICE ARCHITECTURE
- CATALOGUE & DEMAND MANAGEMENT

**IAM OPERATIONS***
- IDENTITY GOVERNANCE: USER LIFECYCLE MGT; ROLE MANAGEMENT; ACCESS REQUESTS & PROVISIONING; COMPLIANCE MANAGEMENT
- ACCESS MANAGEMENT: AUTHENTICATION; AUTHORISATION
- PRIVILEGED ACCESS MGT: PRIVILEGED ACCESS MANAGEMENT (PAM)

**IAM ASSET MANAGEMENT**
- INTEGRATION MANAGEMENT
- ASSET ONBOARDING
- AUTHORITATIVE SOURCE MANAGEMENT
- PLATFORM CONSULTANCY

**IAM PLATFORM MANAGEMENT**
- SERVICE MGT & OPERATIONS
- SERVICE DELIVERY
- OPERATIONAL SUPPLIER MANAGEMENT

**IAM MANAGEMENT**
- PERFORMANCE & CONTROL
- KNOWLEDGE MANAGEMENT
- INSIGHTS & ANALYTICS
- VALUE MANAGEMENT

IAM SUPPLIERS

Responsible

Involved

### Implementation Controls

### Value Stream/ Application Owner

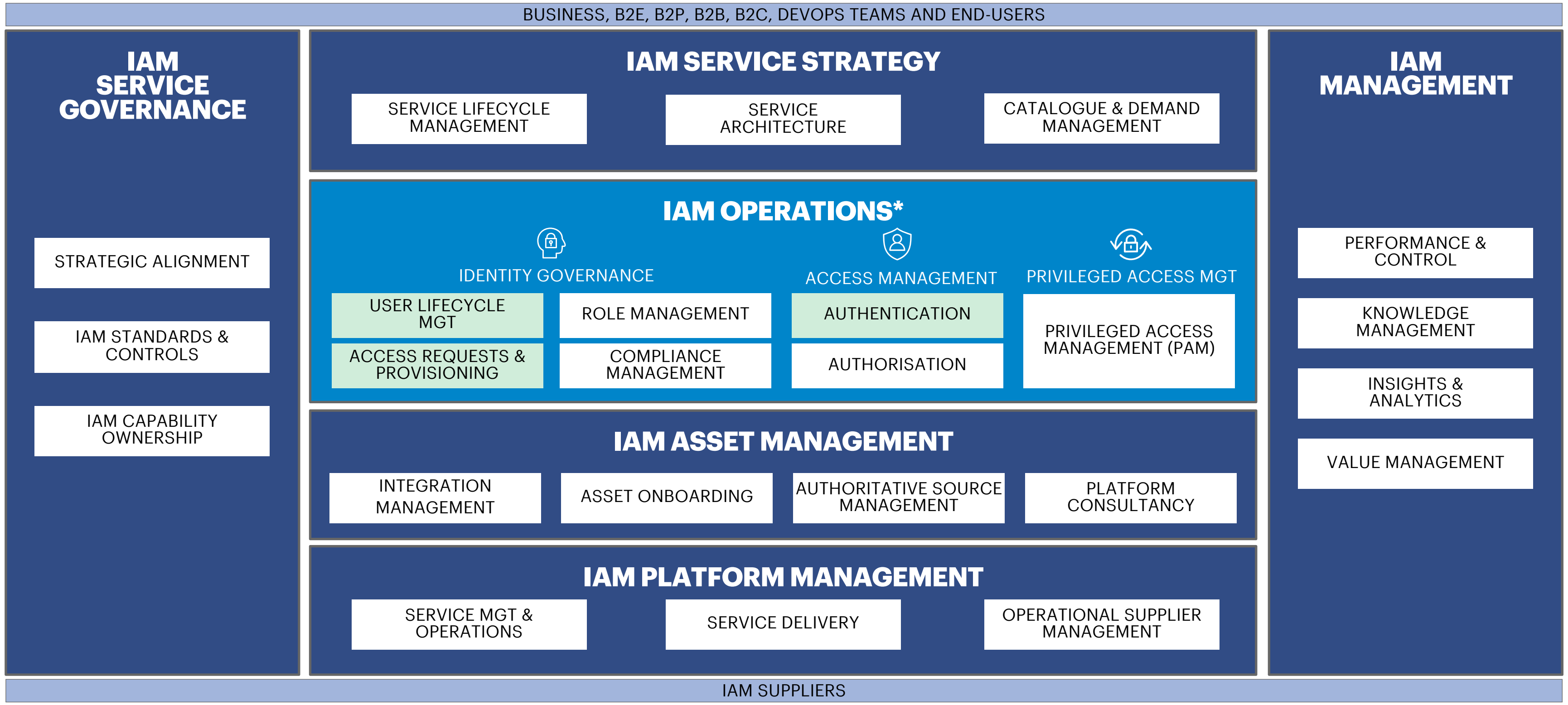
Onboarding of applications and complying with control guidelines

- **Defining and maintaining the roles and policies regarding access to the platform**
- **Defining and maintaining the possible authorisations to the platform**
- **Validation of (additional) access to the platform and take part in the audit cycles (certification)**
- **Responsible for the onboarding and integration of applications with the IAM platform(s)**
- **Request standard building blocks and align with IAM platform team using the service catalogue / portal**

accenture

# A DAY IN THE LIFE OF .... USER

## ROLES & RESPONSIBILITIES



BUSINESS, B2E, B2P, B2B, B2C, DEVOPS TEAMS AND END-USERS

**IAM SERVICE GOVERNANCE**

- STRATEGIC ALIGNMENT
- IAM STANDARDS & CONTROLS
- IAM CAPABILITY OWNERSHIP

**IAM SERVICE STRATEGY**

- SERVICE LIFECYCLE MANAGEMENT
- SERVICE ARCHITECTURE
- CATALOGUE & DEMAND MANAGEMENT

**IAM OPERATIONS***

IDENTITY GOVERNANCE

- USER LIFECYCLE MGT 🟩
- ACCESS REQUESTS & PROVISIONING 🟩
- ROLE MANAGEMENT
- COMPLIANCE MANAGEMENT

ACCESS MANAGEMENT

- AUTHENTICATION 🟩
- AUTHORISATION

PRIVILEGED ACCESS MGT

- PRIVILEGED ACCESS MANAGEMENT (PAM)

**IAM ASSET MANAGEMENT**

- INTEGRATION MANAGEMENT
- ASSET ONBOARDING
- AUTHORITATIVE SOURCE MANAGEMENT
- PLATFORM CONSULTANCY

**IAM PLATFORM MANAGEMENT**

- SERVICE MGT & OPERATIONS
- SERVICE DELIVERY
- OPERATIONAL SUPPLIER MANAGEMENT

**IAM MANAGEMENT**

- PERFORMANCE & CONTROL
- KNOWLEDGE MANAGEMENT
- INSIGHTS & ANALYTICS
- VALUE MANAGEMENT

IAM SUPPLIERS

| | |
|---|---|
| 🟨 | Responsible |
| 🟩 | Involved |

### Implementation Controls

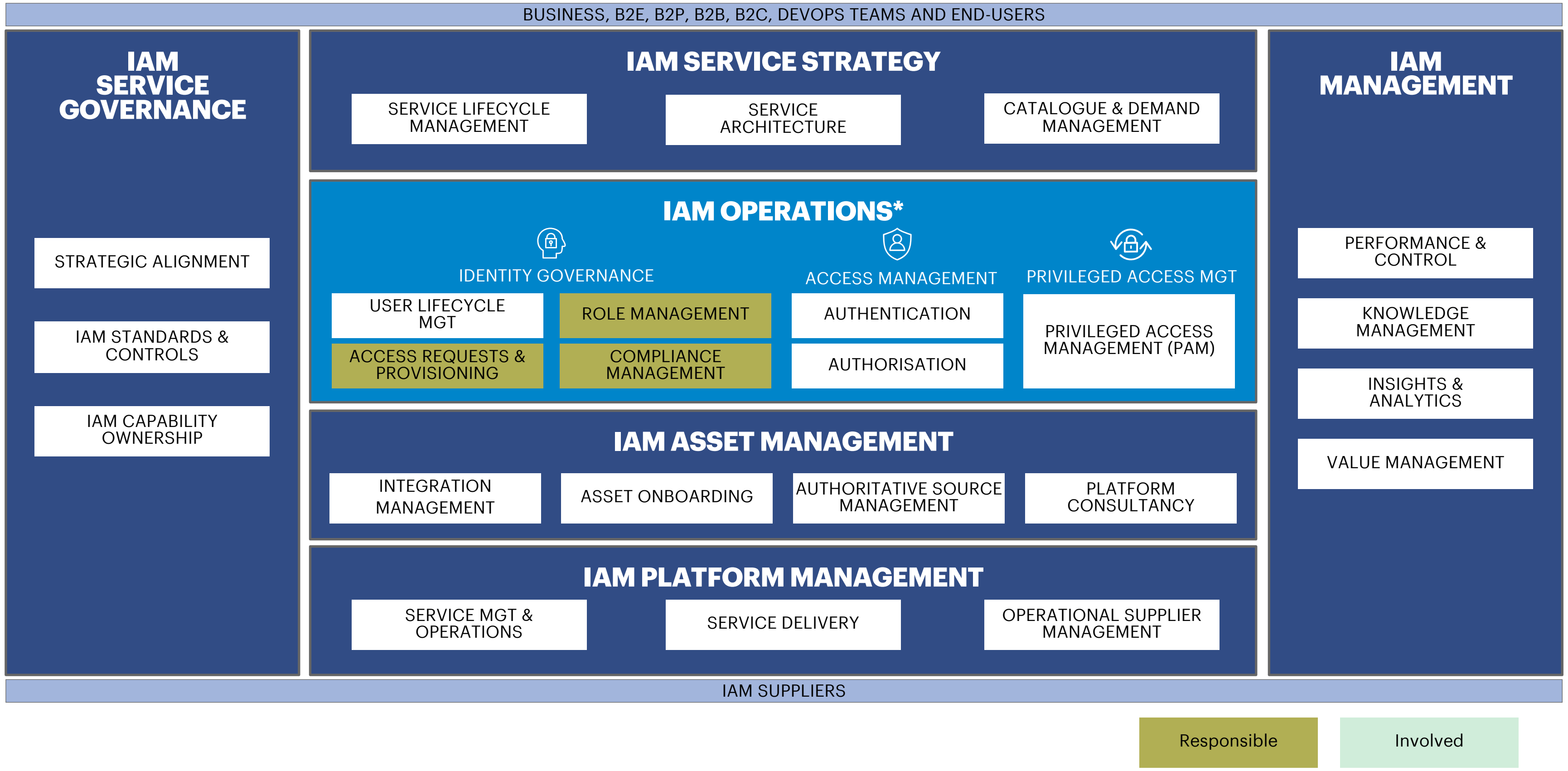
**Employee**

User of systems

- **Make use of self service for i.e. requesting access and password-resets**

# A DAY IN THE LIFE OF …. RESPONSIBLE SUPERVISOR/MANAGER

## ROLES & RESPONSIBILITIES



BUSINESS, B2E, B2P, B2B, B2C, DEVOPS TEAMS AND END-USERS

**IAM SERVICE GOVERNANCE**

STRATEGIC ALIGNMENT

IAM STANDARDS & CONTROLS

IAM CAPABILITY OWNERSHIP

**IAM SERVICE STRATEGY**

SERVICE LIFECYCLE MANAGEMENT

SERVICE ARCHITECTURE

CATALOGUE & DEMAND MANAGEMENT

**IAM OPERATIONS***

IDENTITY GOVERNANCE

USER LIFECYCLE MGT

ROLE MANAGEMENT

ACCESS REQUESTS & PROVISIONING

COMPLIANCE MANAGEMENT

ACCESS MANAGEMENT

AUTHENTICATION

AUTHORISATION

PRIVILEGED ACCESS MGT

PRIVILEGED ACCESS MANAGEMENT (PAM)

**IAM ASSET MANAGEMENT**

INTEGRATION MANAGEMENT

ASSET ONBOARDING

AUTHORITATIVE SOURCE MANAGEMENT

PLATFORM CONSULTANCY

**IAM PLATFORM MANAGEMENT**

SERVICE MGT & OPERATIONS

SERVICE DELIVERY

OPERATIONAL SUPPLIER MANAGEMENT

**IAM MANAGEMENT**

PERFORMANCE & CONTROL

KNOWLEDGE MANAGEMENT

INSIGHTS & ANALYTICS

VALUE MANAGEMENT

IAM SUPPLIERS

Responsible

Involved

### Implementation Controls

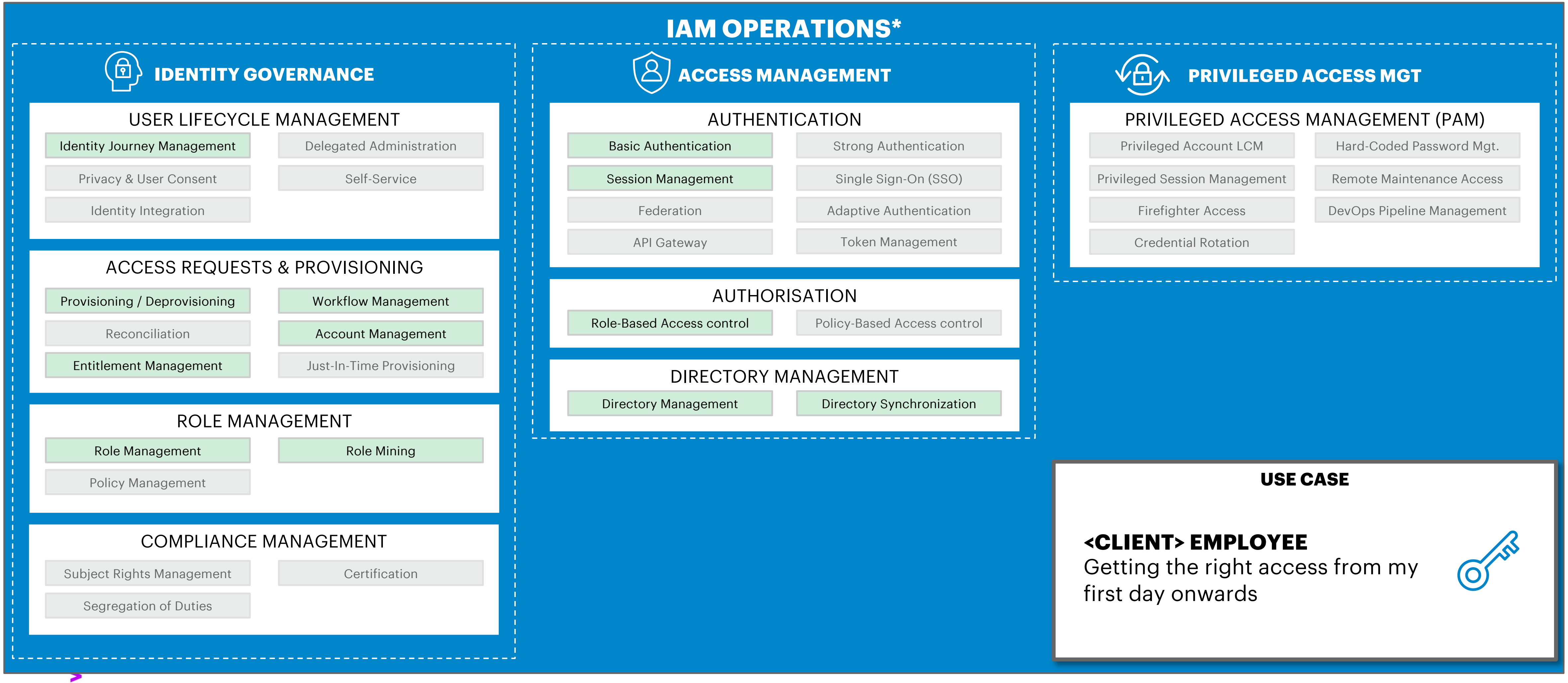
### Responsible Supervisor/Manager

Manager of the employee

- **Defining and maintaining the roles and policies, which can be of different levels, depending on the required access of the respective teams**
- **Request access for new employees in his/her team**
- **Validation of (additional) access to the platform and take part in the audit cycles (certification)**
- **Supports in defining the roles and policies**

# EXAMPLE USE CASE: THE RIGHT ACCESS FROM DAY 1

## USE CASE



### IAM OPERATIONS*

#### IDENTITY GOVERNANCE

**USER LIFECYCLE MANAGEMENT**
- 🟩 Identity Journey Management
- ⬜ Delegated Administration
- ⬜ Privacy & User Consent
- ⬜ Self-Service
- ⬜ Identity Integration

**ACCESS REQUESTS & PROVISIONING**
- 🟩 Provisioning / Deprovisioning
- 🟩 Workflow Management
- ⬜ Reconciliation
- 🟩 Account Management
- 🟩 Entitlement Management
- ⬜ Just-In-Time Provisioning

**ROLE MANAGEMENT**
- 🟩 Role Management
- 🟩 Role Mining
- ⬜ Policy Management

**COMPLIANCE MANAGEMENT**
- ⬜ Subject Rights Management
- ⬜ Certification
- ⬜ Segregation of Duties

#### ACCESS MANAGEMENT

**AUTHENTICATION**
- 🟩 Basic Authentication
- ⬜ Strong Authentication
- 🟩 Session Management
- ⬜ Single Sign-On (SSO)
- ⬜ Federation
- ⬜ Adaptive Authentication
- ⬜ API Gateway
- ⬜ Token Management

**AUTHORISATION**
- 🟩 Role-Based Access control
- ⬜ Policy-Based Access control

**DIRECTORY MANAGEMENT**
- 🟩 Directory Management
- 🟩 Directory Synchronization

#### PRIVILEGED ACCESS MGT

**PRIVILEGED ACCESS MANAGEMENT (PAM)**
- ⬜ Privileged Account LCM
- ⬜ Hard-Coded Password Mgt.
- ⬜ Privileged Session Management
- ⬜ Remote Maintenance Access
- ⬜ Firefighter Access
- ⬜ DevOps Pipeline Management
- ⬜ Credential Rotation

**USE CASE**

**<CLIENT> EMPLOYEE**
Getting the right access from my first day onwards

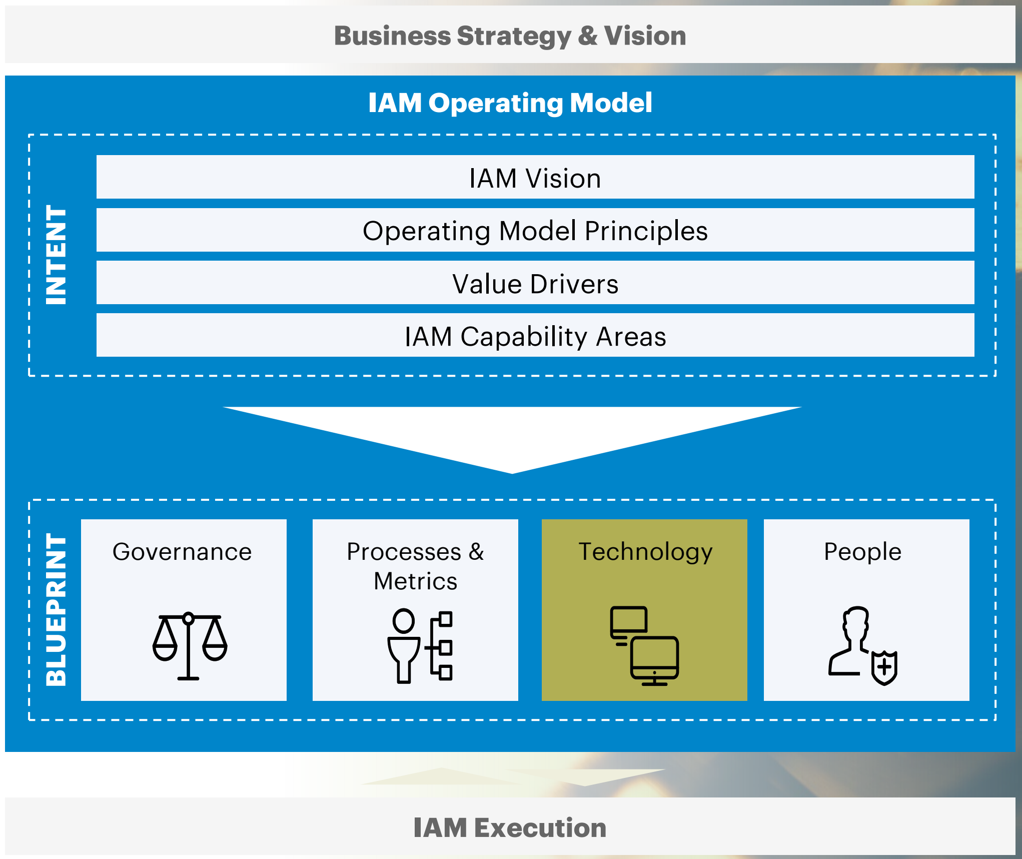
🟩 Relevant for this use case ⬜ Not relevant for this use case

# CONTENTS

## IAM CAPABILITY MODEL

### Contents

1. IAM Vison
2. Operating Model Principles
3. Value drivers
4. IAM Capability Areas
5. Metrics
6. Governance & Processes
7. **Technology & Vendors**
8. People (Roles and sourcing)



# TO ENABLE REQUIRED IAM CAPABILITIES, DIFFERENT TECHNOLOGIES ARE NEEDED AND DIVIDED INTO FIVE FUNCTIONAL AREAS

## RELEVANT IAM TECHNOLOGIES OUTLINED

### Identity Governance (IGA)

Management of user lifecycle and roles, assigning/removing access by providing an **overview of who has access to what and for what reason**

### Access Management (AM)

Services to provide internal and external identities with **seamless and secure access to resources**

### Policy-Based Access Control (PBAC)

A form of externalized and fine-grained authorization, in which one or more **attributes and/or roles of the user are used to determine access** rights based on predefined policies

### Customer Identity & Access Mgt (CIAM)

Managing authentication and authorization for **external identities** of consumers, for example. Key CIAM features include **self-service for registration, password and consent management**

### Privileged Access Management (PAM)

Services to manage the lifecycle of **non-personal and privileged accounts**, including for the DevOps pipeline

# THERE IS A WIDE RANGE OF VENDORS THAT ARE A POTENTIAL FIT FOR <CLIENT>

## MAPPING FUNCTIONAL DOMAIN

| | | |
|---|---|---|
| IAM CAPABILITY MODEL | Identity Governance & Administration | Active Directory<br>Azure<br>okta<br>PingIdentity<br>WSO2<br>ForgeRock<br>ONE IDENTITY<br>SailPoint |
| | Customer IAM | Active Directory<br>Azure<br>ForgeRock<br>PingIdentity<br>okta<br>WSO2 |
| | Policy-Based Access Control | NEXTLABS<br>PingIdentity<br>ForgeRock<br>AXIOMATICS<br>plainID AUTHORIZATION MADE SIMPLE<br>styra |
| | Access Management | Active Directory<br>Azure<br>CYBERARK<br>ForgeRock<br>okta<br>PingIdentity |
| | Privileged Access Management | aws<br>BeyondTrust<br>CYBERARK<br>thycotic |

Identity Governance | Access Management | Privileged Access Management

# WHICH VENDOR COVERS WHICH TECHNOLOGY?

## MAPPING FROM VENDOR PERSPECTIVE

| | IGA | CIAM | PBAC | AM | PAM |
|---|---|---|---|---|---|
| aws | | | | | + |
| AXIOMATICS | | | ++ | | |
| BeyondTrust | | | | | ++ |
| CYBERARK | | | | + | ++ |
| ForgeRock | + | ++ | + | ++ | |
| Active Directory Azure | + | + | | ++ | |
| NEXTLABS | | | ++ | | |
| okta | + | ++ | | ++ | |
| ONE IDENTITY | ++ | | | | |
| PingIdentity | + | ++ | ++ | ++ | |
| plainID AUTHORIZATION MADE SIMPLE | | | ++ | | |
| SailPoint | ++ | | | | |
| styra | | | ++ | | |
| thycotic | | | | | ++ |
| WSO2 | + | ++ | | | |

+ Technology coverage by vendor ++ Leader in the field

### Observations

- No vendor covers all the required functional domains for <CLIENT>
- From a vendor perspective, **ForgeRock**, **Okta** & **Ping** cover the most domains
- However, it is recommended that based on the relevant use-cases and architectural principles, to evaluate which **combination of vendors** would be the best fit for <CLIENT>

# IDENTITY GOVERNANCE AND ADMINISTRATION (IGA)

## OVERVIEW

| Vendor (A-Z) | Description | Leader in the field | User lifecycle Management | Identity Integration | Delegated Administration | Self-service | Workflow Management | Role Management / Mining Policy | Policy Management | Reporting | SoD | Certification | Usability (intuitive / user-centric) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ForgeRock | Relatively new cloud solution<br>Strong standard-based integration patterns<br>Managed service in place |  | +/- | ++ | + | + | +/- | + | + | +/- | - | - | - |
| Azure Active Directory | Cloud-native: Azure<br>Works well with Microsoft services, less with other ones<br>Large partner ecosystem |  | + | +/- | + | - | - | - | - | + | - | - | +/- |
| okta | Cloud-native<br>Strong ecosystem with many out of the box connectors/integrations<br>Managed service in place |  | + | ++ | + | + | +/- | - | - | + | - | - | ++ |
| ONE IDENTITY | Strong cloud solution<br>Out of the box integration patterns (applications): simple configurations instead of custom code<br>Managed service in place | ✓ | ++ | - | + | ++ | ++ | ++ | - | + | + | + | ++ |
| PingIdentity | Cloud solution & on-premise<br>Managed service in place |  | + | ++ | + | + | + | - | - | + | - | - | +/- |
| SailPoint | New focus on cloud - traditional on-premise<br>Vendor integration: Okta, CyberArk & ServiceNow<br>Standard connectors for target applications<br>Managed service in place | ✓ | ++ | - | ++ | ++ | + | ++ | - | + | + | + | + |

# CUSTOMER IAM

## OVERVIEW

| Vendor (A-Z) | Description | Leader in the field | User Lifecycle Management | Integration | Policy Management | Token Management | Consent Management | Reporting | Self-service | Usability (intuitive / user-centric) |
|---|---|---|---|---|---|---|---|---|---|---|
| ForgeRock | • Supports the following standards: JWT, SAML, OIDC, Oauth 2.0, UMA<br>• Co-founder of User Managed Access (UMA)<br>• Flexible provisioning for self-registration, LDAP and SCIM.<br>• ForgeRock recently launched a SaaS-implementation model | ✓ | ++ | ++ | +/- | ++ | ++ | ++ | + | + |
| Azure Active Directory | • Cloud-native<br>• Supports the following standards: JWT, Oauth, OIDC & SAML tokens<br>• Works well with Microsoft services, less with other ones<br>• Lags behind with authentication, SDK, support for modern standards, privacy management & IoT integration |  | + | + | +/- |  | +/- | + | + | + |
| okta | • Cloud-native (SaaS)<br>• Supports the following standards : JWT, Oauth, OIDC and SAML<br>• Strong ecosystem with many out of the box connectors/integrations | ✓ | + | ++ | +/- | ++ | + | ++ | ++ | ++ |
| PingIdentity | • On-premise & cloud deployment<br>• Supports IAM standards<br>• PingIntelligence (separate product) supports interoperability | ✓ | + | ++ | - | + | + | ++ | ++ | ++ |
| WSO2 | • Cloud-native<br>• Open-source<br>• Supports the follow standards: JWT, Oauth 2.0, UMA, OpenID, OIDC, SAML and WS-Fed/Trust. | ✓ |  | ++ | + | + | + | + | + | + |

If UMA needs to be supported, it is advisable to also consider Red Hat and Gluu

# ACCESS MANAGEMENT

## OVERVIEW

| Vendor (A-Z) | Description | Leader in the field | User lifecycle Management | Single Sign-On | Federation | API Gateway | Token Management | Usability (intuitive / user-centric) |
|---|---|---|---|---|---|---|---|---|
| CYBERARK | • Recently entered the access management domain with the acquisition of Idaptive, which offers SSO and strong authentication | □ | +/- | + | + | - | - | □ |
| ForgeRock | • Beginning cloud solution<br>• Strong standard-based integration patterns<br>• Managed service in place | ✓ | + | ++ | ++ | ++ | ++ | +/- |
| Azure Active Directory | • Cloud-native<br>• Works well with Microsoft services, less with other ones<br>• Large partner ecosystem<br>• Managed service in place | ✓ | +/- | + | + | + | + | +/- |
| okta | • Cloud-native<br>• Strong ecosystem with many out of the box connectors/integrations<br>• Managed service in place | ✓ | + | + | + | ++ | + | ++ |
| PingIdentity | • Cloud solution and strong on-premise<br>• Managed service in place | ✓ | + | + | ++ | ++ | ++ | + |

# POLICY-BASED ACCESS CONTROL (ABAC/EAM)

## OVERVIEW

| Vendor (A-Z) | Description | Leader in the field | Usability (Authoring policy in graphical UI) | Decentralised Policy Enforcement * | Policy as code | XACML based (in principle) |
|---|---|---|---|---|---|---|
| AXIOMATICS | • Cloud-native: SaaS available<br>• Vendor integrations: Java Software Development Kit for PEP integration<br>• Standards conform XACML, reputable with loyal customer base | ✓ | +/- | o | Alpha | ✓ |
| ForgeRock | • Cloud-native: SaaS available<br>• Broad vendor integration<br>• Standards conform XACML, reputable with loyal customer base<br>• Managed service in place |  | +/- | o | no | ✓ |
| NEXTLABS | • Cloud-native<br>• Vendor integration: SAP, Microsoft, Siemens, IBM, Oracle, AWS, Google, Salesforce, Workday and Okta.<br>• Strong focus on PEP like SAP | ✓ | + | o | no | ✓ |
| plainID AUTHORIZATION MADE SIMPLE | • Cloud-native: SaaS available<br>• Known for user-friendliness - UX enables business to manage policies<br>• Vendor integration: Sailpoint, Forgerock, Ping and Okta.<br>• Covers many integration modules for broader IAM-domain such as IGA | ✓ | + | o | no | ✓ |
| styra | • Cloud-native<br>• Relatively new company with strong support for cloud, k8s, & infra scenarios<br>• Vendor integration: particularly orchestration for OPA<br>• Emerging challenger in broader app space (microservices); strong tech customers e.g. Netflix |  | - | S | Rigor | ** |
| SYMPHONIC | • Part of PingIdentity<br>• Cloud native: currently not but is on the roadmap for 2021 | ✓ | +/- | o | no | ✓ |

*O = Optional S = Standard

* *Styra is not XACML-based (in principle), but can be linked with Open Policy Agent (OPA)

# PRIVILEGED ACCESS MANAGEMENT

## OVERVIEW

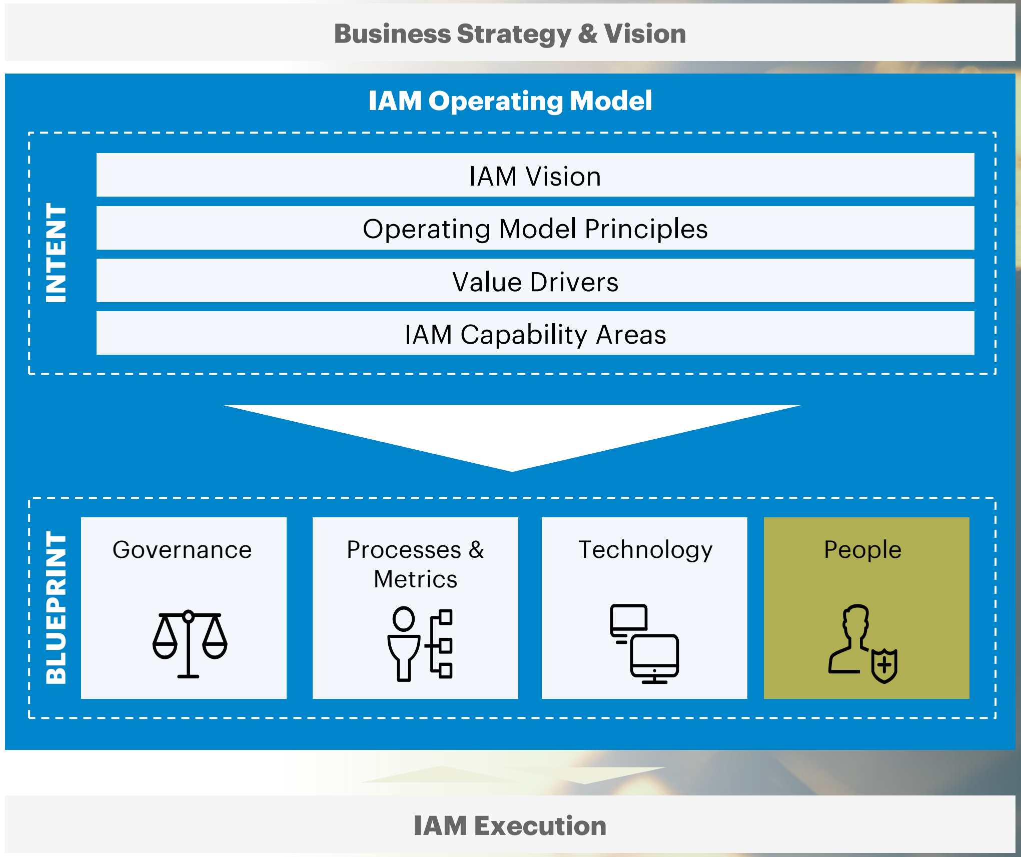
| Vendor (A-Z) | Description | Leader in the field | Password management | Session isolation | Hardcoded credential management | DevOps Pipeline Management | Usability (intuitive / user-centric) |
|---|---|---|---|---|---|---|---|
| aws | • Cloud-native<br>• Focuses mainly on PAM within the Amazon environment | □ | + | - | ++ | ++ | - |
| BeyondTrust | • Focus on local administrator account and privileged escalation | ✓ | + | + | - | - | + |
| CYBERARK | • Leader in the field<br>• CyberArk has options for standard integration with many tools<br>• Great flexibility in available protocols<br>• Available as a managed service | ✓ | ++ | ++ | ++ | ++ | ++ |
| thycotic | • Cloud-native<br>• Thycotic has standard integration patterns for most standard tools/platforms<br>• Cost-effective tool for standard use cases | ✓ | ++ | ++ | □ | □ | ++ |

# CONTENTS

## IAM CAPABILITY MODEL

### Contents

1. IAM Vison
2. Operating Model Principles
3. Value drivers
4. IAM Capability Areas
5. Metrics
6. Governance & Processes
7. Technology & Vendors
8. **People (Roles and sourcing)**



accenture

# FOR <CLIENT>, THE QUESTION IS HOW TO FILL THE ROLES WITHIN THE IAM PLATFORM TEAM

## THREE SCENARIOS FOR STAFFING THE IAM PLATFORM TEAM

|  | A: Mixed Vendor and <CLIENT> |  |  |  |  | B: Vendor provides specific skill |  |  |  |  | C: Vendor provides service/product |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *Role BaU (estimated FTE)* | IGA | PAM | AM | PBAC | CIAM | IGA | PAM | AM | PBAC | CIAM | IGA | PAM | AM | PBAC | CIAM |
| **Product Owner (0.5 FTE)** | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ● |
| **Technical Specialist* (4 FTE)** | ● | ○ | ● | ● | ● | ● | ● | ● | ● | ● | ○ | ● | ○ | ○ | ● |
| **System Architect (0.2 FTE)** | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ● |
| **Business Analyst (1 FTE)** | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ● |
| **Scrum Master (0.5 FTE)** | ○ | ○ | ● | ● | ● | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ● |

*Illustrative*

○ **>CLIENT<**

● **Vendor**

- Mixed teams where resources from vendors are interspersed based on availability
- No overall accountability and limited control to ensure stability of team
- Slows formation of team and time to maturity
- Easier to slot in resources to fill near-term needs

- Vendor provides a particular skill set that is common across a set of Teams (e.g., business systems analyst)
- Improved team performance relative to a mixed set of skills
- Can support development of <CLIENT> colleagues in that role
- Potential confusion on team accountability

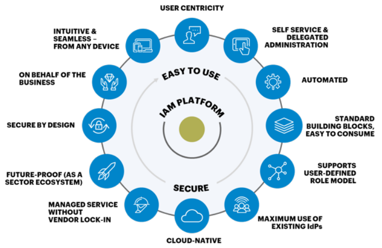
- Vendor provides complete Teams that augment the domain
- Clearer accountability for ownership of outcomes relative to the product area
- Provides flex capacity if planned demand for effort fluctuates
- Potential over-reliance of vendors when a strategic capability is required
- Information sharing across product teams within domain could be negatively impacted

*Illustrative Technical Specialist (Developer / Tester) estimation breakdown:
**IGA**: 1,0 FTE,  **PAM**: 1,0 FTE , **AM**: 1.0 FTE
**PBAC**: 0,5 FTE. **CIAM**: 0,5 FTE

accenture

# APPENDIX

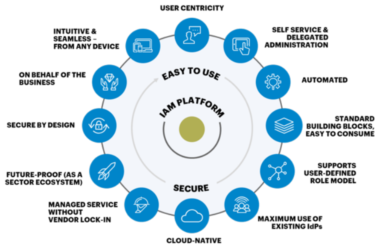
# GENERAL PRINCIPLES FOR IAM BLUEPRINT (2/2)


USER CENTRICITY
SELF SERVICE & DELEGATED ADMINISTRATION
AUTOMATED
STANDARD BUILDING BLOCKS, EASY TO CONSUME
SUPPORTS USER-DEFINED ROLE MODEL
MAXIMUM USE OF EXISTING IdPs
CLOUD-NATIVE
MANAGED SERVICE WITHOUT VENDOR LOCK-IN
FUTURE-PROOF (AS A SECTOR ECOSYSTEM)
SECURE BY DESIGN
ON BEHALF OF THE BUSINESS
INTUITIVE & SEAMLESS – FROM ANY DEVICE
EASY TO USE
IAM PLATFORM
SECURE

## GENERAL PRINCIPLES FOR IAM BLUEPRINT - EXPLANATION

| PRINCIPLES | EXPLANATION | Rational |
|---|---|---|
| **Users centricity** | IAM will be designed around the requirements of end-users (e.g. employees of <CLIENT>) | • Increases user experience and employee productivity |
| **Intuitive & seamless - from any device** | The IAM solution must be easy to use and provide easy access to all <CLIENT> applications, from all devices. Whether BYOD is allowed depends on the policy to be defined. | • Increases user experience and employee productivity |
| **Self service & delegated administration** | The IAM solution must be self-sufficient and facilitate users as much as possible in solving their own problems such as password resets and rights requests. Delegated administration should be included. | • Increases user experience and employee productivity<br>• Contributes to more efficient operations and reduced costs. |
| **On behalf of the business** | The IAM solution serves The IAM solution contributes to the business goals and overall success of <CLIENT>. Value is also tracked and reported to the business. | • Contributes to convincing the business of the importance of ongoing investment in an IAM program<br>• Ensures focus on realizing value through the IAM related initiatives |
| **Automated** | The IAM solution uses automation wherever possible to simplify processes and increase efficiency. | • Contributes to (cost) efficient implementation, with fewer manual errors. |
| **Secure by design** | The security of the IAM solution and its processes must be in line with the <CLIENT> security policy | • Identity is the new perimeter, contributing to lowering the risk profile by effectively deploying control mechanisms. |
| **Standard building blocks, easy to consume** | IAM consists of standard building blocks, which are easily consumed by the development teams. This also means that standard protocols are used as much as possible and configuration is preferred over customization. | • Enables developers to focus on development<br>• Reduces the risk of complications if components need to be replaced in the future |

# GENERAL PRINCIPLES FOR IAM BLUEPRINT (2/2)


USER CENTRICITY
SELF SERVICE & DELEGATED ADMINISTRATION
AUTOMATED
STANDARD BUILDING BLOCKS, EASY TO CONSUME
SUPPORTS USER-DEFINED ROLE MODEL
MAXIMUM USE OF EXISTING IdPs
CLOUD-NATIVE
MANAGED SERVICE WITHOUT VENDOR LOCK-IN
FUTURE-PROOF (AS A SECTOR ECOSYSTEM)
SECURE BY DESIGN
ON BEHALF OF THE BUSINESS
INTUITIVE & SEAMLESS – FROM ANY DEVICE
EASY TO USE
IAM PLATFORM
SECURE

## DETAILED EXPLANATION

| PRINCIPLES | EXPLANATION | Rational |
|---|---|---|
| **Future-proof as an ecosystem** | The IAM platform will be developed to support a future ecosystem within the sector.<br>This means that current and future innovations in the market (of both identities, IAM, Applications and underlying infrastructure) will be used as much as possible and that this will also be secured in the development of the roadmap. | • Facilitates central role within the digitization of the energy sector and ensures sustainable development of IAM platforms. |
| **Supports user-defined role model** | IAM must be able to identify both the identity of the acting entity (organization, person, system) and the capacity in which it is acting, taking into account that a user may be acting in another capacity at another point in time. | • Contributes to compliance.<br>• There may be requirements (e.g. license or accreditation) for assuming capacities. |
| **Managed Service without vendor lock-in** | Where possible, services surrounding IAM are arranged as a managed service.<br>A vendor-agnostic design ensures that in the future certain components can be (relatively) easily disconnected. | • Contributes to more efficient operations.<br>• Ensures that <CLIENT> can focus on its core business, as devising and implementing solutions itself requires a lot of <CLIENT> capacity. |
| **Making maximum use of existing IdPs** | IAM should support integration with IdPs that are, or appear to be, market standards in order to facilitate its end users as much as possible. | • Contributes to cost-efficiency and digital enablement<br>• Should prevent additional work of self-maintenance and/or development. |
| **Cloud – Native** | The IAM solution must enable cloud services (IaaS, PaaS, SaaS, BPaaS) and be cloud-based itself. | • Contributes to cost elasticity and scalability - ability to scale up or down cloud services depending on demand<br>• Contributes to agility - ability to quickly and safely integrate (new) cloud services. |