Proposed Table of Contents for the IDPro Body of Knowledge – Volume 2

(Updated 13 July 2022)

Table of Contents

[Access Control 2](#_Toc108602485)

[Access Governance 2](#_Toc108602486)

[Public Sector IAM 2](#_Toc108602487)

[Public sector vs private sector 2](#_Toc108602488)

[Strong identity proofing 2](#_Toc108602489)

[Financial services 3](#_Toc108602490)

[Integration with the legacy system 3](#_Toc108602491)

[High Level of Assurance on sensitive activities 3](#_Toc108602492)

[Identity Delegation - Fintech 3](#_Toc108602493)

[Financial regulations compliance and guidance from the government organizations 3](#_Toc108602494)

[Healthcare 4](#_Toc108602495)

[High Level of Assurance on sensitive data (LoA) 4](#_Toc108602496)

[Identities Delegation – Health Care 4](#_Toc108602497)

[Healthcare regulations compliance 4](#_Toc108602498)

[Gaming Industry 4](#_Toc108602499)

[Local game privacy compliance 4](#_Toc108602500)

[Scalability and availability 5](#_Toc108602501)

[Gaming and authentication 5](#_Toc108602502)

[Academic IAM 5](#_Toc108602503)

[Key Characteristics of Academic IAM 5](#_Toc108602504)

[K-12 IAM 5](#_Toc108602505)

[Higher Education IAM 5](#_Toc108602506)

[Risk Assessment for IAM in Academia 7](#_Toc108602507)

[Non-Human Entity 7](#_Toc108602508)

[Operational Technology (OT) 7](#_Toc108602509)

[Service Accounts 7](#_Toc108602510)

[IoT Devices 7](#_Toc108602511)

[IoT Sectors 7](#_Toc108602512)

[RPA / robotics 7](#_Toc108602513)

[Security requirements 7](#_Toc108602514)

[IAM Architecture and Solutions 7](#_Toc108602515)

[Identity Governance 7](#_Toc108602516)

[Elements of IGA Systems 7](#_Toc108602517)

[Business System 7](#_Toc108602518)

[Business Processes 7](#_Toc108602519)

[Recommended Practices 7](#_Toc108602520)

[Design for security 7](#_Toc108602521)

[Operational Considerations 8](#_Toc108602522)

[Account recovery 8](#_Toc108602523)

[Call centers 8](#_Toc108602524)

[Engagement of user for their own security 8](#_Toc108602525)

[Security events and operations 8](#_Toc108602526)

[Project Management 8](#_Toc108602527)

[Migration Projects 8](#_Toc108602528)

[Managing Business Mergers (Identity Systems) 8](#_Toc108602529)

# Access Control

## Access Governance

# Public Sector IAM

## Public sector vs private sector

The article explains the unique use cases and challenges in the public sector and private sector that should be considered by the IAM practitioners. The article also provides the best practices and tips to deal with the use cases and challenges. Almost every service requires a different identification method in public sectors. Each governmental agency has unique requirements for authentication. As an example registering with your General Practitioners (GP) in the UK requires a National Health Service number, while HMRC directs users to its Government Gateway scheme to sign up and pay self-assessment taxes. This net result is citizens need to have a variety of different identification methods to complete straight forward tasks. The section article explains tips and best practices for navigating this issue.

### Strong identity proofing

Identity proofing is essential to enable the digital government. But the extensive amount of data to prove the citizen identity has become one of the challenges. The section explains the tips on navigating some of the issues to create a strong yet consumer-friendly identity proofing.

# Financial services

The section explains the unique use cases and challenges in the financial industry that should be considered by IAM practitioners. The section also provides the best practices and tips to deal with the use cases and challenges.

## Integration with the legacy system

This should be considered given that most of the banks or financial services have had their own system for a long time ago. Things like how to let existing customers apply for new services easily should be considered.

## High Level of Assurance on sensitive activities

Most of the activities in the financial services industry involve action toward and accessing sensitive information, such as purchase goods, funds transfer, etc. Due to this, there must be a high LoA to make sure the right person performs the right activities. This article explores ways of having a higher level of assurance and protects consumers from fraud, e.g., perform step-up authentication, contextual authorization, pin validation, card validation, etc.

## Identity Delegation - Fintech

An example is a child managing a bank account on behalf of an elderly parent. There are several challenges to deal with the use case. Some of them are to deal with the power of attorney, and audit to make sure the child doing things based on court authorization on behalf of the parent and not just sharing the parent’s password with the child. The article explores the best practices to deal with the use case as it is becoming more common use cases across several sectors, such as financial and healthcare services.

## Financial regulations compliance and guidance from the government organizations

There are specific regulations and organizational guidance in the financial industry that help security and convenience to the consumer, for example, Payment Service Directives 2 (PSD2), Open Banking, Financial Ask Task Force organization. The article explains about those and provides tips on how to comply with the regulation or follow the organizational guidance.

# Healthcare

The section explains the unique use cases and challenges in the financial industry that should be considered by IAM practitioners. The section also provides the best practices and tips to deal with those use cases and challenges.

## High Level of Assurance on sensitive data (LoA)

Most data in the healthcare industry are sensitive data, e.g., a patient's profile, disease history, medical records, etc., and so a high level of assurance is required for making sure only the right person accesses the right data. There are several exceptions though. For example, a homeless person who doesn’t have a fixed address and no form of authentication wants to access their data. The person deserves to access their data but they can’t prove themself. The section explains ways and best practices for achieving the high LoA, e.g., step-authentication and to deal with the unique use case such as the homeless person case, e.g., implements “known to the practitioners” or in other words the ability of a practitioner (doctor) to vouch for the patient’s identity

## Identities Delegation – Health Care

An example is the parent and child relationship where the parent has access to their child’s medical records (provided consent was given). There are several challenges to deal with the use case. Some of them are to deal with the power of attorney and audit. The article explores the best practices to deal with the use case as it is becoming more common use cases across several sectors, such as financial and healthcare services.

## Healthcare regulations compliance

The section explains the regulations in the healthcare industry such as the Health Insurance Portability and Accountability Act (HIPAA) and the tips to comply with those.

# Gaming Industry

The section explains unique use cases and challenges faced in the gaming industry that should be considered for IAM practitioners. The section also explains the tips and best practices to deal with those use cases and challenges.

## Local game privacy compliance

The section explains the regulations in the game industry that should be considered while building CIAM such as General Data Protection Regulation (GDPR) for EU players, and Shutdown Law for Korean players and the tips to comply with those.

## Scalability and availability

There are around 1.2 billion players in the world. Knowing this, the scalability and the high availability are important factors for having a successful CIAM. The article explains the tips and best practices to handle the load and keep the game services online at all times.

## Gaming and authentication

Most mobile games do not require authentication at the start so the player could start playing immediately thus increasing the player engagement. This could be achieved by creating an anonymous account at the start of the game. The article explores the tips to deal with this “expectation”, anonymous account implementation, and account upgrade implementation to help players secure their account.

# Academic IAM

## Key Characteristics of Academic IAM

### K-12 IAM

This article will describe the context and critical drivers for IAM in the world of K-12.

### Higher Education IAM

This article will describe the context and critical drivers for IAM in higher education.

#### Institutional Dynamics

Discuss some of the major stakeholders in higher education and how they interact with an IAM system. Stakeholders include students (undergraduate and graduate), faculty (research, teaching, emeritus, adjuct, etc), staff (including retirees), and general administration.

#### Campus Libraries and IAM

Campus libraries often have unique requirements of an IAM system. This article describes those considerations, touching on specific expectations around user privacy, subscription requirements, and business models.

#### Research Collaborations and IAM

Researchers often collaborate with other researchers from different campuses. Large-scale collaborations may have dozens or even hundreds of different institutions involved. This drives a need for federated identity beyond what most other campus stakeholder groups required. This article will explore the IAM requirements for this stakeholder group.

#### Academic Hospital Considerations

Many schools have academic medical centers with significantly different risk tolerances, requirements, modes of operation that cause them to have to act as a more-or-less separate entity with regard to IAM. This can cause issues for faculty, staff, students with dual roles.

#### Considerations for IAM for Small, Medium, and Large Campuses

The IAM requirements for a small liberal college are likely to be very different from that of a large research university. This article will explore the IAM requirements that are driven by the size and focus of different types of higher ed institutions.

## Risk Assessment for IAM in Academia

# Non-Human Entity

## Operational Technology (OT)

## Service Accounts

## IoT Devices

### IoT Sectors

#### Home Automation

#### Personal (wearables)

#### Implants

#### Plant Automation

#### Vehicle

#### Smart Cities

#### Agriculture

#### Building/Industrial

#### Utilities

## RPA / robotics

## Security requirements

# IAM Architecture and Solutions

### Identity Governance

### Elements of IGA Systems

## Business System

### Business Processes

#### Recertification of accounts

## Recommended Practices

### Design for security

# Operational Considerations

## Account recovery

## Call centers

## Engagement of user for their own security

## Security events and operations

# Project Management

## Migration Projects

## Managing Business Mergers (Identity Systems)