# IDPro Body of Knowledge Table of Contents
# Working DRAFT

September 12, 2019

# Contents

# Chapter 1

# Introduction

## 1.1 Ethics

## 1.2 Information security

### 1.2.1 Trust (say more - what is this?)

## 1.3 Privacy

## 1.4 Identification and authentication

### 1.4.1 Context and Identity

### 1.4.2 Levels of Assurance

## 1.5 The Business Case for IAM

### 1.5.1 Workforce IAM

### 1.5.2 Consumer/Citizen IAM

# Chapter 2

# Digital Identity

## 2.1 Definition

### 2.1.1 Reputation

### 2.1.2 Laws of Identity (this sounds like jurisdictions and real laws - is that the intent?)

## 2.2 Identifiers

## 2.3 Digital Identity Lifecycle (?)

## 2.4 Mapping to human or device

## 2.5 Proofing, Binding or Registration (?)

### 2.5.1 Verification/Validation

## 2.6 Credentials

# Chapter 3

# Access Control

## 3.1 Authentication

### 3.1.1 Dynamic Authentication (risk-based)

### 3.1.2 Multi-Factor Authentication

### 3.1.3 Single Sign-on Within a Domain

### 3.1.4 Centralised Authentication Service

### 3.1.5 Federated Authentication (between domains)

### 3.1.6 Device Identity for Corroboration

### 3.1.7 Fast Identity Online (FIDO) and its cousins

### 3.1.8 Session Management

## 3.2 Authorization

### 3.2.1 Resources to Protect

### 3.2.2 Authorisation

#### 3.2.2.1 ACL's

#### 3.2.2.2 RBAC

#### 3.2.2.3 ABAC / Dynamic Access Management

**Policy Management solutions**

### 3.2.3 Privileged Access Management

#### 3.2.3.1 Alignment to Risk Management

#### 3.2.3.2 System Accounts

# Chapter 4

# Laws, Regulations, and Standards

Abstract: This chapter provides information about the externally defined environment in which Identity and Access management professionals operate. The laws are documents that define duties and consequences in legal jurisdictions, such as countries. Regulations are more specific and detailed requirements. Standards may also be mandatory; government entities often require compliance with standards produced by certain standards bodies. We also include *de facto* standards and recommended practices here.

## 4.1 Framework to Understand Legal Environment

Abstract: Identity systems and its participants are governed by a myriad and complex set of laws, regulations, and contractual requirements, and the obligations they impose are not always clear. This article focuses on the legal environment that governs identity systems. The emphasis is on United States, but references are made to other countries' laws and efforts to coordinate rules underway in the UN Commission on International Trade Law (UNCITRAL) regarding identity management legislation.

## 4.2 Highlights of Selected Laws

Abstract: This section is organized by jurisdiction. It is intended to provide at a minimum a reference to known laws and regulations in jurisdictions likely to be encountered by our membership. At present this includes Europe, United States, and Canada will likely also include Australia in the short term.

### 4.2.1 Europe

#### 4.2.1.1 GDPR

Abstract: This article provides a basic understanding of how the *General Data Protection Regulation (GDPR)* applies when processing 'any information relating to an identified or identifiable natural person'.

### 4.2.2 United States

Abstract: This article explains how identity and access management supports the requirements of prominent U.S. laws.

#### 4.2.2.1 Sarbanes-Oxley Section 404

#### 4.2.2.2 Health Insurance Portability and Accountability Act (HIPAA)

#### 4.2.2.3 Health Information Technology for Economic and Clinical Health Act (HITECH)

#### 4.2.2.4 Family Educational Rights and Privacy Act of 1974 (FERPA)

#### 4.2.2.5 Children's Online Privacy Protection Act (COPPA)

#### 4.2.2.6 Fair and Accurate Credit Transaction Act (FACTA)

### 4.2.3 Canada

Abstract: This article explains how identity and access management support the requirements of prominent Canadian laws.

#### 4.2.3.1 Personal Information Protection and Electronic Documents Act (PIPED Act, or PIPEDA)

## 4.3 Regulations

Abstract: This article explains how identity and access management supports the requirements of prominent regulations.

## 4.4 Standards

Abstract: There are many standards. Standards may be mandatory such as when government entities require compliance with standards produced by certain standards bodies. We also include *de facto* standards and recommended practices here. This is a curated set of standards that have been deemed to be useful to identity professionals. They are organized topically, not by their source. Standards that span more than one topic are possible. In this case cross references may be used.

### 4.4.1 Architecture

Abstract: This article surveys the known standards concerning architecture for identity systems.

#### 4.4.1.1 ISO/IEC 24760-2:2015 Information technology -- Security techniques -- A framework for identity management -- Part 2: Reference architecture and requirements

### 4.4.2 Assurance

Abstract: This article surveys the known standards concerning risk and assurance for identity systems.

#### 4.4.2.1 *Standard on Identity and Credential Assurance*

[Canada] Government of Canada February 2013 https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776. Archived - Need successors

#### 4.4.2.2 *Digital Identity Guidelines*

[SP 800-63-3] NIST Special Publication 800-63-3 June 2017 https://doi.org/10.6028/NIST.SP.800-63-3

#### 4.4.2.3 *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*

[SP-800-37] NIST Special Publication 800-37r1 June 2014 https://doi.org/10.6028/NIST.SP.800-37r1

### 4.4.3 Authentication

Abstract: This article surveys the known standards concerning methods of authenticating principals.

#### 4.4.3.1 *Digital Identity Guidelines: Authentication and Lifecycle Management*

[SP 800-63B] NIST Special Publication 800-63C December 2017 https://doi.org/10.6028/NIST.SP.800-63b

#### 4.4.3.2 *Introduction to Public Key Technology and the Federal PKI Infrastructure*

[SP 800-32] NIST Special Publication 800-32 February 2001. https://tsapps.nist.gov/publication/get_p

#### 4.4.3.3 *Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map*

[IETF RFC 4510] RFC 4510 June 2006 https://tools.ietf.org/html/rfc4510

#### 4.4.3.4 *OpenID Connect Core 1.0 incorporating errata set 1*

[OIDC] Sakimura, N., Bradley, B., Jones, M., de Medeiros, B., and C. Mortimore November 2014 https://openid.net/specs/openid-connect-core-1_0.html.

#### 4.4.3.5 *Personal Identity Verification (PIV) of Federal Employees and Contractors*

[FIPS 201-2] NIST FIPS Publication 201-2 September 2013 https://doi.org/10.6028/NIST.FIPS.201-2

#### 4.4.3.6 *Biometric Data Specification for Personal Identity Verification*

[SP 800-76-2] NIST Special Publication 800-76-2 July 2013 https://doi.org/10.6028/NIST.SP.800-76-2

### 4.4.4 Authorization

Abstract: This article surveys the known standards concerning methods of access control. These standards involve protecting resources. This is sometimes called authorization.

#### 4.4.4.1 *The OAuth 2.0 Authorization Framework*

[IETF RFC 6749] RFC 6749 October 2012 https://tools.ietf.org/html/rfc6749

#### 4.4.4.2 *User-Managed Access (UMA) Profile of OAuth 2.0*

Abstract: The weaknesses of many notice-and-consent paradigms of data privacy are clear. This article notes the social, legal and regulatory drivers and examines some approaches to satisfy them.

[KI UMA] Kantara Initiative UMA Recommendation December 2015 https://docs.kantarainitiative.uma-core.html

### 4.4.5 Federation

Abstract: This article surveys the known standards concerning methods of allowing authentication from one domain to be honored in another.

#### 4.4.5.1 *OpenID Connect Core 1.0 incorporating errata set 1*

[OIDC] Sakimura, N., Bradley, B., Jones, M., de Medeiros, B., and C. Mortimore November 2014 https://openid.net/specs/openid-connect-core-1_0.html.

#### 4.4.5.2 *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*

[OASIS SAML 2] SAML 2.0 March 2005 http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

#### 4.4.5.3 *Digital Identity Guidelines: Federation and Assertions*

[SP 800-63C] NIST Special Publication 800-63C December 2017 https://doi.org/10.6028/NIST.SP.800-63c

### 4.4.6 Lifecycle

Abstract: This article surveys the known standards concerning the creation and registration of identities and subsequent changes to the characteristics of those identities and the eventual removal of the same.

#### 4.4.6.1 *Standard on Identity and Credential Assurance*

[Canada] Government of Canada February 2013 https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776. Archived - Need successors

#### 4.4.6.2 *Digital Identity Guidelines: Enrollment and Identity Proofing Requirements*

[SP 800-63A] NIST Special Publication 800-63A December 2017 https://doi.org/10.6028/NIST.SP.800-63a

#### 4.4.6.3 *Digital Identity Guidelines: Authentication and Lifecycle Management*

[SP 800-63B] NIST Special Publication 800-63C December 2017 https://doi.org/10.6028/NIST.SP.800-63b

### 4.4.7 Operations

Abstract: This article surveys the known standards concerning the operation of identity systems.

#### 4.4.7.1 *Information technology -- Security techniques -- A framework for identity management -- Part 3: Practice*

[ISO 24760-3] ISO/IEC 24760-3:2016 2016 https://webstore.ansi.org/Standards/ISO/ISOIEC2476020

### 4.4.8 Terminology

Abstract: This article surveys the known standards for the purpose of collating and contrasting terminology defined.

#### 4.4.8.1 *Digital Identity Guidelines*

[SP 800-63-3] NIST Special Publication 800-63-3 June 2017 https://doi.org/10.6028/NIST.SP.800-63-3

#### 4.4.8.2 *An Ontology of Identity Credentials Part I: Background and Formulation*

[SP 800-103] NIST Special Publication 800-103 (Draft) October 2006. https://tsapps.nist.gov/publicati

**4.4.8.3** *Security and Privacy -- A Framework For Identity Management -- Part 1: Terminology And Concepts*

[ISO 24760-1] ISO/IEC 24760-1:2019 IT 2019 https://webstore.ansi.org/Standards/ISO/ISOIEC247602

**4.4.8.4 ISO/IEC 24760-1:2019 IT Security and Privacy -- A Framework For Identity Management -- Part 1: Terminology And Concepts**

# Chapter 5

# Workforce IAM / Internal IAM

## 5.1 IAM Processes

### 5.1.1 Joiner-Mover-Leaver

### 5.1.2 HR Ownership

### 5.1.3 Provisioning (On-boarding and Off-boarding)

### 5.1.4 Role Management

### 5.1.5 Re-certification

## 5.2 Compliance

## 5.3 Analytics and Intelligence

## 5.4 Handling Business Partners' People

# Chapter 6

# Consumer/Citizen IAM

## 6.1 Consumer Journey (identification to loyal customer)

### 6.1.1 Registration of Consumers

### 6.1.2 Authentication Assurance (meeting LoA requirements)

## 6.2 Industry Considerations

### 6.2.1 Public Sector vs. Private Sector

### 6.2.2 Financial Services

### 6.2.3 Healthcare

## 6.3 Social Sign-up and Sign-on

# Chapter 7

# Non-Human Entity

## 7.1 Operational Technology (OT)

## 7.2 IoT Devices

### 7.2.1 IoT Sectors

#### 7.2.1.1 Home Automation

#### 7.2.1.2 Personal (wearables)

#### 7.2.1.3 Implants

#### 7.2.1.4 Plant Automation

#### 7.2.1.5 Vehicle

#### 7.2.1.6 Smart Cities

#### 7.2.1.7 Agriculture

#### 7.2.1.8 Building/Industrial

#### 7.2.1.9 Utilities

## 7.3 RPA / robotics

## 7.4 Security requirements

# Chapter 8

# IAM Architecture and Solutions

## 8.1 Business System

### 8.1.1 Business Processes

#### 8.1.1.1 Recertification of accounts

## 8.2 Information/Data Architecture

## 8.3 Application Portfolio

### 8.3.1 APIs

#### 8.3.1.1 HTTP

#### 8.3.1.2 S/LDAP

#### 8.3.1.3 RACF

#### 8.3.1.4 XACML

## 8.4 Technical

### 8.4.1 Repositories

#### 8.4.1.1 Relational Database

**Query optimization**

**Replication limitations**

#### 8.4.1.2 Directories

**Historical note - X.500**

**SLAPD and its descendants**

#### 8.4.1.3 NoSQL databases

**Graph Databases**

#### 8.4.1.4 Identity Provider (IdP) Trends

**Distributed Ledger (Blockchain)**

### 8.4.2 Identity Provider Services

### 8.4.3 Protocols

#### 8.4.3.1 Kerberos

#### 8.4.3.2 Lightweight Directory Access Protocol (LDAP)

#### 8.4.3.3 SCIM

#### 8.4.3.4 SAML

**SP Initiated vs IDP Initiated**

**Bindings**

#### 8.4.3.5 OIDC

**Authentications Flows**

#### 8.4.3.6 OAuth

#### 8.4.3.7 WS-Fed

#### 8.4.3.8 FIDO U2F and UAF

### 8.4.4 Enterprise control of “Cloud”

#### 8.4.4.1 Public Cloud vs Private Cloud

#### 8.4.4.2 Local Connectors and Gateways

#### 8.4.4.3 IPSec VPN

## 8.5 Recommended Practices

### 8.5.1 Design for security

## 8.6 Governance and Administration

### 8.6.1 Audit

### 8.6.2 Monitoring

# Chapter 9

# Operational Considerations

## 9.1 Account recovery

## 9.2 Call centers

## 9.3 Engagement of user for their own security

## 9.4 Security events and operations

# Chapter 10

# Project Management

Many Identity and Access Management (IAM) projects proceed without a project manager. In these cases the IT group in charge of identity management are left to deploy the required solution in the absence of any overarching management. While this is sometimes seen as the most expedient way to get a system installed or updated, it is short-sighted and likely to cost the organisation more money in the longer term. An IAM solution touches so many systems within an organisation and is dependent on the current and planned condition of so many applications that to deploy a solution without properly considering the impact, managing the required resources and keeping management advised of progress, will result in a substandard deployment.

Here we look at two ways to manage a project – "Classic", sometimes called Waterfall, and "Agile, a way to manage projects that accommodates changes that inevitably arise during the course of a project.

Reference is made to the Project Management Institute (PMI) Framework. This document in no way seeks to replicate the PMI's methodology or replace the project management training that the PMI provides. The reader is referred to the PMI Body of Knowledge for further information.

## 10.1 Project Management Institute Framework

## 10.2 New Implementation Projects

## 10.3 Migration Projects

## 10.4 Project Management Office Issues

# Chapter 11

# IAM Knowledge Sharing

## 11.1 Independent Organizations

## 11.2 Standards Bodies

## 11.3 Analyst Organizations

## 11.4 Conferences

# Chapter 12

# Advanced Topics – Parking Lot

## 12.1 Digital Legacy - handling deceased persons’ digital ID (Advanced Topic)

## 12.2 Self-Sovereign Identity

### 12.2.1 Blockchain ID