TECHNICAL DOCUMENTS

Identity and Access Management/Governance

Practical guide – Implementation

February 2017

FRENCH INFORMATION SECURITY CLUB

11 rue de Mogador - 75009 Paris
Tel.: +33 1 53 25 08 80 – Fax: +33 1 53 25 08 88
clusif@clusif.fr – www.clusif.fr

Table of contents

Acknowledgements

CLUSIF would like to take this opportunity to thank the people who made this document possible, and in particular:

The head of the working group:

Olivier	Morel	***ILEX International***

The people who helped to write this document:

Stéphane	Camous	***ICF Habitat***
Delphine	de Saint Cyr	***BOURSE DIRECT***
Zahi	Dib	***IDENTO***
Rémi	Fournier	***SYNETIS***
Benoît	Fuzeau	***CASDEN BANQUE POPULAIRE***
Patrick	Marache	***WAVESTONE***

And all members who took part in the many sessions of the working group.

In particular:

Mohamed Bakkali (***ANSSI***); Valérie Chassaing (***PSA Groupe***); Rachid Elouarghani (***MODIS***); Florence Hanczakowski (***CLUSIF***); Astrid Lang (***AP-HP***); Alice Milanova (***MAIF***); Sylvain Moreau (***DEXIA***); Sven Neubert Pajadon (***BETA SYSTEMS***); Christiane Payan (***ORANGE***); Manuel Prieur (***Hewlett Packard Enterprise***); Emmanuelle Selosse (***IMPRIMERIE NATIONALE***); Eric Thierry (***MANUTAN International***); André Sonnois (***EDENRED***)

CLUSIF would also like to thank the members who helped to proofread this document.

I. Introduction

I.1. Description of the subject

In July 2007, CLUSIF published a technical document entitled “Identity management”, available to download on its website. While the functional and technical concepts expressed in this document clearly remain valid, there are now a number of gaps in it as a result of developments in the IT security market as a whole, and in the identity and access management market in particular:

- changing uses and technologies: Cloud/SaaS, Mobility, etc.
- changing approaches to implementation: a risk-based approach or an approach based on identity and access governance, an iterative approach, etc.
- changing constraints: legislation, cybercrime, etc.
- And so on.

In 2015, CLUSIF decided to produce a new document on Identity & Access Management (IAM)/Identity & Access Governance (IAG), drawing on plentiful feedback from its members. The aim was not to revise or correct the 2007 document, but rather to prepare a new one, organised differently, with a greater focus on concrete “use cases”.

The new working group (WG) initially aimed to produce a document addressing all concepts associated with Identity and Access Management/Governance and for a wide audience: technical or functional interlocutors, decision makers or users.

At many workshops, the WG shared lots of information relating to real use cases, implementation feedback, and IAM/IAG best practice.

The decision was made to deliver a “**practical guide to the implementation of IAM/IAG projects**”, identifying, for all the functional and technical domains that come under IAM/IAG, all the technical and organisational prerequisites, practical tips and points to bear in mind before, during or after such a project.

Our ambition is to be as pragmatic as possible, and to transfer to this deliverable the experiences and advice of parties who have already implemented this type of project.

I.2. Who is this document aimed at?

This document is aimed at anyone responsible for kicking off or implementing all or part of an IAM/IAG project in their organisation: CIO, CISO, project manager, architect, business owner, main contractor, consultant, etc.

I.3. Profile of WG participants

Over the course of around two years, the WG met on average once a month for a discussion and work seminar. Thirty people took part at least once, with varying levels of activity, and were split as follows:

- 2/3 “users”: all business sectors, all company sizes;
- 1/3 “providers”: consultancy firms, integrators, software vendors.

I.4. Aims of the document

The main aim of this document is to help you take ownership of and implement an identity and access management/governance project. It aims to present simple, pragmatic information so that you get a better grip on your project and thus reduce the risk of failure.

The WG thus decided to present a document in the form of a methodological guide supplemented by best practices, and to make it as pragmatic as possible, drawing on its members’ experience.

We wanted to organise the document according to the phases in the life cycle of an IAM project, with information on the following stages:

- before the project;
- during the project;
- after the project.

Based on the observation that IAM projects are no longer implemented in one fell swoop, but rather in a succession of iterations or batches, we also decided to regard a “global” IAM project as a series of “IAM component” implementation sub-projects.

The document is thus made up of different functional modules that can be taken separately depending on the type of subject to be addressed or the concerns encountered.

I.5. What is not addressed in this document

In this spirit, we had to make choices to deliver an effective and useful document. Some subjects were deliberately ruled out, for different reasons: either these subjects were too recent or not mature enough in the French market, and so there was little feedback available, or they were subjects that can be addressed completely separately from IAM/IAG.

The WG therefore barely addressed or ignored subjects such as IAM for the Internet of Things, “Customer IAM”, “IAM as a Service”, Physical Access Control and privileged account management.

The WG focused on the most commonly encountered IAM subjects, favouring a pragmatic implementation approach over a theoretical or dogmatic one.

Lastly, this document presents no market solution because of the existence of numerous analysts’ reports on this very subject.

I.6. Acronyms

The various acronyms used in the document are presented below. A glossary in the appendices to this document also gives definitions for all the concepts discussed in the document.

Acronyms	Meaning
2FA	Two Factor Authentication
ABAC	Attribute Based Access Control
ACL	Access Control List
AD	Active Directory
ADFS	Active Directory Federation Services
ANSSI	National Cybersecurity Agency of France
API	Application Programming Interface
BYOD	Bring Your Own Device
B2B	Business To Business
B2C	Business To Consumer
CAPEX	Capital Expenditure
CAS	Central Authentication Service
CIAM	Customer Identity & Access Management or Consumer Identity & Access Management
CMS	Card Management System
COPE	Corporate Owned, Personally Enabled
CPE	Carte de Personnel d’Établissement [card for non-professional healthcare staff]
CPS	Carte de Professionnel de Santé [card for healthcare professionals]
CLUSIF	French Information Security Club
CNIL	Commission Nationale de l'Informatique et des Libertés [French data protection agency]
CYOD	Choose Your Own Device
CIO	Chief Information Officer
GDPR	General Data Protection Regulation
GRC	Governance, Risk management & Compliance

IAG	Identity & Access Governance
IAI	Identity Analytics & Intelligence
IAM	Identity & Access Management
IAMaaS	Identity & Access Management as a Service
IDaaS	Identity as a Service
IdP	Identity Provider
IGA	Identity Governance and Administration
UI	User Interface
IoT	Internet of Things
IRM	Identity Relationship Management
ITSM	Information Technology Service Management
eIDAS	electronic IDentification And trust Services
eSSO	enterprise Single Sign-On
FAQ	Frequently Asked Questions
FIDO	Fast IDentity Online
WG	Working Group
LDAP	Lightweight Directory Access Protocol
LPM	Loi de Programmation Militaire [French military planning act]
LSF	Loi de Sécurité Financière [French financial security act]
MCO	Maintien en Condition Opérationnelle [maintenance in operational condition]
MFA	Multi-Factor Authentication
MOA	Maîtrise d'OuvrAge [business owner]
MOE	Maîtrise d'Œuvre [main contractor]
NFC	Near Field Communication
OIDC	OpenID Connect
OCI	Operator of Critical Infrastructure
OOB	Out-Of-Band
OPEX	Operational Expenditure
ORBAC	Organisation Role Based Access Control
OTP	One-Time Password

PaaS	Platform as a Service
PAM	Privileged Account Management
PIM	Privileged Identity Management
PUM	Privileged User Management
PCI DSS	Payment Card Industry Data Security Standard
PKI	Public Key Infrastructure
POC	Proof-Of-Concept
ISSP	Information Systems Security Policy
RBAC	Role Based Access Control
RFID	Radio Frequency IDentification
RGS	Référentiel Général de Sécurité [General Security Reference Base]
ROI	Return On Investment
CISO	Chief Information Security Officer
SAAS	Software As A Service
SAML	Security Assertion Markup Language
IS	Information System
SIEM	Security Information and Event Management
SP	Service Provider
SPOF	Single Point of Failure
SoD	Segregation of Duty
SOX	Sarbanes-OXley
SLO	Single Log Out
SSO	Single Sign-On
TPAM	Third-Party Application Maintenance
UBA	User Behaviour Analytics
UEBA	User & Entity Behaviour Analytics
WAM	Web Access Management

II. Fundamental Principles of IAM and IAG

This chapter aims to give a simplified definition of the fundamental principles covered by Identity and Access Management/Governance. So many different terms are used (IAM, IAG, IGA, IRM, IAI, IDaaS, and so on) and they do not all give a clear picture of what they refer to.

We therefore aim to present a simple – and simplified – picture of IAM/IAG by grouping the fundamental principles into 6 concrete issue areas:

1. improving and simplifying the management of identities, rights and accounts;
2. steering, auditing and checking identities, rights and accesses;
3. authenticating users;
4. checking and simplifying accesses to applications;
5. extending IAM/IAG and IAI services;
6. capitalising on the cloud.

II.1. Improving and simplifying the management of identities, rights and accounts

The aim here is to simplify and automate everyday actions linked to the management of identities and their rights.

II.1.1. Identity lifecycle management

Identity lifecycle management consists in modelling and providing the tools for managing events in the life of an identity within a company.

It also covers:

- all populations having to log into a company's IS: employees, service providers on- and off-site, suppliers, partners, clients, and in the future perhaps connected objects, machines, robots, etc.;
- all events affecting an identity during the course of its lifecycle, and which might vary depending on the population and the business activity: arrival, change of job, departure, arrival/return of seasonal staff, posting, long absence, suspension, additional assignment, etc.

Accordingly, it is necessary to:

- take account of the master reference bases already used by the company (IS-HR for internal staff in general, specific databases or purchasing applications for service providers or partners, organisational reference bases, etc.) via regular data updates;
- offer UIs and management processes (approval workflows) for populations or events having no master reference base, such as service providers;
- make it possible to configure management constraints for some populations, including:
    - the option to limit authorised persons and create service providers;
    - the mandatory entry of the assignment end date for service providers or staff on fixed-term contracts, with automatic suspension of their accounts in the IS on that date;
    - regular access certification to confirm, for example, the presence of service providers or an employee's assignment.

II.1.2. Entitlement management

Identities need to be managed, and so do their entitlements in the IS, i.e. their application account(s) and their rights in applications.

The management of entitlements is generally based on:

- an **entitlements model**, i.e. the consistent modelling of rights in the IS;
- a **back office organisation** responsible for defining and updating this model;
- **approval processes** in the event that a right is requested, modified or withdrawn;
- a **front office organisation** responsible for approving, rejecting or completing submitted requests.

Lastly, in order to simplify the user experience and make IAM the main tool for managing requests, the management of entitlements may be extended to other resources, such as:

- logical or physical access badges: catering, coffee machines, etc.;
- IT equipment: mobile phones, tablets, etc.;
- physical access rights: access to buildings, to some premises, etc.

II.1.2.a. The entitlements model

The entitlements model must be understandable to the people requesting them. To this end it must be “business-oriented” and consistent with the company's maturity. There is therefore no “single correct model” for entitlements, even though there are modelling principles or theories such as the ABAC, RBAC, ORBAC models, etc.

The simplest models will be limited to a handful of application profiles, or even simply to a (yes/no) authorisation to access an application.

More commonly, more elaborate entitlements models combine, depending on necessity and the organisation's maturity, the following concepts:

- **job profiles** describing a responsibility in the company's processes. They encompass one or more application profiles. As an example, in a hospital, the “radiologist” job profile will encompass the application profiles “doctor” for access to medical records, and “radiologist” for access to images and the entry of reports in the medical imaging system;
- **application profiles** associated with an application, in the business and non-technical sense of the term. As an example, an ERP module can be regarded as an application in its own right because it represents a coherent set of privileges in this application for the purposes of performing a task;
- the idea of a **scope** describing a data perimeter delimiting a job or application profile. Scopes can be constructed on the basis of a tree structure such as a country, a region, a site, a building or a department.

Lastly, the most mature models have advanced functionalities such as:

- **automatic profile attribution** on the basis of the beneficiary's attributes. Nevertheless, this type of automation remains, without exception, the preserve of very mature and relatively stable organisations such as: points of sale or warehouses in the retailing and distribution industry, or bank branches;
- **profile suggestion** on the basis of the beneficiary's attributes. Suggestion remains an indication to help applicants with their requests. For example, when 90% of people have a profile that can be calculated from their job or qualifications, validation of automatic suggestion – with possible modification if necessary – is quick and avoids mistakes;
- **conflict rules,** or an incompatibility matrix, between different profiles (SoD), or between a profile and the beneficiary's attributes. These rules make it impossible, for example, for one person to create and validate a sensitive action like making a bank transfer;
- a start and end date for profile attribution.

II.1.2.b. The back office organisation

It is responsible for operating the entitlements model over time:

- monitoring uses: unattributed profiles, profiles attributed routinely in a way that could potentially be automated, frequently added profiles, etc.;
- alignment with changes in the IS: new applications, new functionalities within an application, new deployments, etc.;
- alignment with changes in the organisation.

To this end, it might draw on decision-making functionalities applied to IAM/IAG, namely on the principles of IAI (Identity Analytics & Intelligence) described below.

II.1.2.c. Approval processes

Approval processes must make it possible to validate – or otherwise – the legitimacy of the attribution or modification of rights. They are triggered when a right is requested, extended or removed, but also if the beneficiary transfers internally, requests a sensitive right, etc.

Four types of approvals are generally used in these processes:

- **hierarchical**: by the line manager, the entity manager;
- **functional**: by a gatekeeper for the requested profile or application;
- **security**: for a right having a significant impact in terms of risk;
- **budget**: in the context of controlling or reducing the cost of licenses.

To aim for effective processes, it is best to avoid having more than two approval steps in most situations.

Setting a finite and limited number of approval processes ensures that the solution can be maintained. Ideally, the use of job or application profiles automates the choice of processes to be followed.

II.1.2.d. The front office organisation

The front office organisation is responsible for submitting rights requests, and approving or blocking them. This organisation must be:

- coherent with the company organisation;
- as close as possible to users so that it can assess the legitimacy of requests.

The current trend is to enable users to submit requests on their own behalf in self-service mode, or even on behalf of any other user. This model means greater attention needs to be paid to the ergonomics of the solution and to defining job and application profiles.

Lastly, for specific populations, such as partners, part of this management can be delegated. Here too, delegation demands strong and contractually defined accountability.

II.1.3. Provisioning

After managing entitlements requests, it remains to create the ad hoc accounts and rights in the IS. That is the purpose of provisioning. It seeks to keep updated the major reference bases like the Active Directory and the LDAP directories, along with each application's reference bases.

Several levels of integration are possible.

Automatic provisioning aims to automatically create the necessary accounts and rights. Technically, it is necessary to implement connectors, web services or other solutions. Functionally, it must be ensured that the rules that led to automation remain valid over time. It is important to stress that application provisioning is possible only with the prior support of the application publisher, and that limits on provisioning may appear in this context.

Manual or **guided provisioning** requires that technical actions be performed manually by the administrator. To implement it, there are two main approaches:

- interface the IAM/IAG tool with the existing ITSM tool. Thus, IAM/IAG creates a ticket in the ITSM then tracks its processing so that the user can be shown a level of progress;
- directly implement in IAM the appropriate processes to notify task administrators in the meantime and enable them to report their actions.

Mixed or **semi-automatic provisioning** combines automatic tasks and manual actions. Depending on the context, it can combine several advantages such as:

- the automatic management of sensitive attributes such as the active or suspended status of an account, or the expiry date of passwords, to ensure a high level of security;
- the manual management of access rights for simple implementation.

“On the fly” provisioning has emerged more recently in tandem with federated identity management tools. It consists in providing, in the exchanged identity token, all the information needed to create and update the account. It is then up to the application that consumes the token to create the account when the user first logs in and then to update it on subsequent accesses.

II.2. Steering, auditing and checking identities, rights and accesses

The aim here is to have the capacity to steer, audit and check accesses to the IS. Conventionally, these functions were slightly underdeveloped in IAM solutions until the emergence of tools dedicated to this task, coming under the banner of IAG or IAI (Identity & Access Governance, Identity Analytics & Intelligence). Still now, IAM tools are seeking to extend their functional scope, sometimes leading to an overlap between IAM, IAG and IAI solutions.

IAM, IAG and IAI solutions are distinguished by:

- **the intrinsic design of the tools**: IAI tools are the Business Intelligence counterpart of IAM. They are built around a "data warehouse" and are designed to react after the event;
- **the granularity of the rights managed**: in the vast majority of cases, IAM and IAG tools deal only in the rights they need to attribute. In SAP for example, they will play composite roles. Taking things further, IAI tools are intended to recreate the full access chain, including the finest-grained right in applications. In SAP for example, this means transactions. The aim is to detect risks or non-conformities due to the definition of roles or profiles.
- **the sponsors and order givers targeted**: IAI solutions are aimed chiefly at managing the level of risk associated with access rights. In this sense, they are aimed primarily at risk and internal audit departments.

In a very schematic way, IAI aims to achieve 3 objectives:

- **improve data quality** using consistency checks and help with identifying sources of inconsistency;
- **manage risks associated with entitlements** by monitoring the attribution of risky rights, steering review campaigns and managing exceptions;
- **adjust the entitlement model** or role management by analysing the use of defined job and application profiles and comparing attributed rights with the transactions actually carried out.

IAI really comes into its own when risk and internal audit departments are closely involved in the project.

The remainder of this chapter provides a quick insight into the main functionalities of IAI.

II.2.1. Data warehouse

The data warehouse is very much central to the solution, and is designed to:

- store and archive all imported data;
- organise these data in a shared model (or pivot).

The advantage of this model is that it can extend the IAI solution to new resources without jeopardising the dashboards and other processing operations based on this shared model.

II.2.2. Data supply package

The data supply package populates the data warehouse. Accordingly it must:

- be compatible with a maximum number of sources and formats;
- offer data quality improvement functionalities: verification of format rules; detection of duplicates or similar records;
- factor in accounts with their rights just as much as access log files so that the attributed rights can then be compared with the rights actually used.

II.2.3. Analysis and alert functionalities

On the basis of the shared data warehouse model, analysis and alert functionalities make it possible to implement client context-specific indicators, alerts and dashboards. For example:

- data consistency rules: accounts attributed to employees not present in the HR IS, or present in several systems, users with application accounts but no AD account, etc.;
- access rights consistency rules: a Marketing Department user having access to transactions or a directory shared with the Finance Department, a hospital department user having access to other hospitals with a profile that does not match her job, etc.;
- segregation of duty (SoD) rules: a user having toxic roles, a job profile posing an intrinsic risk, etc.

II.2.4. Entitlement review or Access certification package and user interface

The entitlement review or access certification package is designed to reconfigure and steer identity and account review campaigns. It is split into three phases:

- campaign organisation: scope, users concerned, campaign frequency, people responsible;
- campaign follow-up and steering: response monitoring, reminders, redirections to new actors;
- campaign closure and generation of evidence.

As well as this review package, the user interfaces enable users to track the configured indicators, search and perform checks.

II.3. Authenticating users

Authenticating a user means guaranteeing, with an appropriate level of confidence, the user's identity. The purpose of this chapter is to provide a snapshot of authentication methods other than the still very widespread "login/password" combination.

II.3.1. Strong authentication, step-up authentication, MFA

Although there is no single official definition, **strong authentication** can be defined as the combination of two principles:

- the combination of at least two different factors from the following list:
  - what I know and what I am the only person to know: e.g. a password or a PIN;
  - what I possess: e.g. a chip card, a certificate, a token or a smartphone;
  - what I am: e.g. a fingerprint, a vein network, a face.
- at least one of these factors must be one-time. This means that the data shared between user and server cannot be reused. So, even if intercepted, they are unusable.

Conventionally, the concept of **step-up authentication** is used when authentication methods are not one-time.

Recently, the term "**MFA**" or "2FA" has come to be used to refer to multi-factor authentication. However, despite the "strong" nature of this type of authentication, these methods are still vulnerable to some attacks, such as Man-In-The-Middle and Phishing attacks.

To make authentication more secure, additional mechanisms can be considered. The main ones are described in the remainder of this chapter.

II.3.2. OOB (Out-Of-Band) authentication

With OOB authentication, an authentication factor uses a different channel to that used to access the application.

- OOB example: access to a web application on a PC + application on a smartphone receiving a push notification in which you have to confirm your identity.
- Non-OOB example: access to a web application on a PC + SMS sent to a smartphone containing a code to be entered in the web application UI.

II.3.3. Behavioural biometrics

Behavioural biometrics means comparing the user's behaviour with his/her “behavioural fingerprint”. The latter can be generated during a registration phase or built up gradually, as the user uses his/her devices.

E.g. typing speed or pattern, mouse movements, touchscreen use habits.

II.3.4. Risk-based authentication, adaptive authentication

Risk-based authentication uses confidence “indices” to assess whether the recorded behaviour matches the user's “classic” behaviour or suggests a “risky situation”. As an illustration:

- the use of a new device, such as a new PC, is detected;
- an unusual access attempt is detected, e.g. from a foreign country, or in a noteworthy time slot;
- a non-compliant browsing action is detected in the application, e.g. an attempt to set up a bank transfer without first viewing the account balance;
- the use of behavioural biometrics.

On the basis of these risk factors, each application can implement a suitable behaviour. For example:

- ignore and continue browsing;
- continue browsing but notify the user by email or mark the transaction as “risky” in back office;
- request a new proof of ID, potentially a strong or different one;
- block the requested functionality.

II.4. Checking and simplifying accesses to applications

There are two aims here:

- to simplify access for the user by limiting authentication requests: this is the principle behind SSO, which after an initial authentication aims not to authenticate the user again for a given period;
- to check access to applications, i.e. check that the user is indeed authorised to access the requested application, and track that access.

To achieve this aim, there are various technical approaches aimed at different situations. The associated solutions use identity reference bases and audit and track authentications and entitlements. They also provide logical access control functionalities and are generally combined with strong authentication technologies.

II.4.1. eSSO or Enterprise SSO

eSSO is all about acting on the user's behalf. Its “core” component is the eSSO engine, which is tasked with:

- detecting application windows, such as authentication, authentication error and password change windows;
- on the user’s behalf, filling in the fields necessary for authentication, notably logins and passwords and potentially additional fields.

For this to operate:

- an administrator must first have configured the windows to be detected by the eSSO solution, and the various behaviours expected by the solution;
- the eSSO solution must know the user's “secondary credentials” for this application, i.e. his/her login/password combination. This can be ensured in two different ways:
  - by self-learning: when the user first logs in, the eSSO solution asks him/her to enter, for the last time, his/her login and password;
  - by provisioning, via an IAM/IAG tool capable of automatically populating the eSSO solution, which must, for example, provide an API capable of this.

eSSO solutions can also offer advanced functionalities like:

- automatic password change in the application;
- consolidated access tracking;
- detection of passwords shared by multiple users;
- delegation to one user or another.

eSSO solutions have benefits:

- they are non-intrusive in the applications they cover and do not require modifications to the applications;
- they are compatible with a very large number of thick or thin client applications.

However, they also have drawbacks:

- they are usually affiliated with the workstation by installing the eSSO engine and can therefore only be deployed on managed workstations;
- they run on the workstation side and not on the application server side, which can generate additional deployment and support workload;
- they might require reconfiguration when in-scope applications are upgraded.

II.4.2. WebSSO, or Web Access Management (WAM)

WebSSO/WAM solutions emerged with the huge rise in the number of thin client applications. They use session tickets, like Kerberos in the Microsoft universe.

A WebSSO/WAM solution must therefore:

- generate session tickets, which requires implementation of a central infrastructure tasked with this operation;
- check the validity of the ticket when the user accesses a WebSSO/WAM-protected resource. A control component must therefore be installed in the access chain between the user and the application, either directly on the application server – as an "agent" – or on a reverse proxy upstream of the application.

As they are positioned so as to block the flow of data between user and application, WebSSO/WAM solutions provide a higher level of security than eSSO solutions. They offer the following advantages:

- passwords are potentially no longer stored in the application reference bases, except for some applications that require it;
- access control rules can be implemented centrally. For example: prevent access to a resource outside business hours, require strong or additional authentication;
- finer-grained access profiles can be defined for a given user, making it possible to limit the functionalities or transactions available to that user;
- traceability, notably of authentications and authorisations, is ensured;
- they are non-intrusive on the workstation and can be deployed in environments in which workstations are not managed;
- they run on the infrastructure side, which generally ensures a higher level of reliability.

However, these solutions have the following drawbacks:

- they are only compatible with web applications and might be intrusive in these applications if adaptations are needed to ensure compatibility;
- they are a SPOF, which requires the deployment of a highly available infrastructure and an appropriate organisation and processes.

However, Federated Identity Management standards are beginning to be extended to WebSSO/WAM solutions too, and are therefore simplifying integration with modern applications.

II.4.3. Federated Identity Management

Federated Identity Management can be seen as an upgraded version of WebSSO/WAM addressing two major IS changes:

- the opening-up of the IS to external populations not managed directly by the company;
- cloud computing and access to external resources not managed directly by the company.

To address these two changes, Federated Identity Management uses the exchange of identity tokens and has two founding principles:

- use shared and recognised standards such as *SAMLv2*, *OAuth2*, *OpenIDConnect*, *WS-Federation*;
- standardise and separate the responsibilities of Identity Providers (IdP) from those of Service Providers (SP).

As an illustration:

The case of a company accessing a cloud service:

- the company manages identities: it plays the role of Identity Provider;
- it accesses an external service: it plays the role of Service Provider.

Case of a company making a partner portal available to its suppliers or customers:

- the company plays the role of Service Provider for its suppliers;
- the suppliers play the role of Identity Providers.

Federated Identity Management can also offer advanced functionalities such as:

- on-the-fly provisioning to create and update users' accounts. However, account removal is not always offered;
- "impersonalisation", i.e. sharing information between IdP and SP while also guaranteeing the person accessing it a degree of anonymity.

For example, a company connecting to a supplier portal may provide the following information:

- the company's ID;
- the user's access profile.

Thus the company does not communicate users' personal data.

Federated Identity Management solutions have the following benefits:

- they are a de facto standard in the internet world and extend to web applications in general;
- they suit a huge number of use cases;
- they make it possible to deactivate access to federated applications centrally.

However, they also have drawbacks:

- they require a relationship of trust, which is generally contractually defined, between the IdP and SP;
- they have a weakness when it comes to managing access traceability. On the other hand, IAI remedies this shortcoming.

II.4.4. Mobile SSO

Mobile SSO aims to offer an SSO service for mobile devices like smartphones and tablets. This is the area into which SSO has moved most recently. For this reason, the standards are still young and the solutions fairly rare. However, it is worth highlighting the emergence of the OAuth2 for Native Apps standard, which aims to provide SSO functionalities between mobile applications.

It differs depending on the mobile OS:

- BrowserView for iOS;
- Custom Tab for Android.

The purpose of this standard is to ask native applications, equivalent to thick clients, to use the system's browser to manage authentication and SSO. It is even possible to use this principle to deliver SSO on a conventional workstation between web applications and thick clients.

II.5. Extending IAM/IAG and IAI services

II.5.1. Protecting highly privileged administrator accounts

Highly privileged IS administrator accounts have specific technical characteristics: non-personal accounts, like “root” accounts, specific functionalities, like “sudo” commands, etc. Protecting them therefore requires a particular approach and methods.

That is the aim of specific tools sometimes called PIM, PUM or PAM. These tools are usually found “outside” the IAM/IAG solution, but are coupled with it, or at least AD. For example, they adopt the security bastion principle by blocking the data flow between the administrator and the system to be administered:

- the administrator authenticates and accesses this security bastion;
- he/she performs administrative actions via this bastion.

The bastion offers advanced functionalities: administrator access management, access tracking, session recording, updating of privileged account passwords, etc.

II.5.2. Protecting unstructured data

The protection of unstructured data, such as shared directories, raises specific technical issues. These include:

- it is often the data item itself that carries authorisations. For example, ACLs relate to a file or a directory. Authorisations are not therefore centralised, or carried by access accounts, but are distributed to each unstructured item of data to be protected: shared directory, file, cloud storage space, SharePoint drive, etc.;
- the volume of unstructured data in a company is gigantic, even for modestly sized companies. Studies estimate that 80% of a company's data is unstructured;
- the nature of unstructured data varies hugely: personal, financial, commercial, R&D, health-related, related to payment methods, etc. This means a larger number of regulations to be obeyed;
- unstructured data are extremely volatile, and created in “real time".

Thus, to cope with unstructured data, the essential first step is to define a framework – a policy – governing access to them.

In many cases, this policy:

- standardises best practice and therefore limits the permitted granularity and the extent to which authorisations can be fine-grained;
- seeks to disallow direct authorisations in favour of authorisations granted to groups of accounts for more centralised management: it is not accounts but rather groups of accounts that have authorisations to access data.

Once this framework is in place, and to aid its deployment, the solutions must offer the following capabilities, among others:

- reconstruct, from end to end, the authorisation chain from the item of data to the access account;
- explain reasons for an authorised or unauthorised access. For example, membership of a group or business division, or one-off authorisation;
- analyse uses, shed light on uses that diverge from the most commonly observed uses and raise an alert if necessary;
- automatically remedy an illegitimate use or access, etc.

When it comes to tools, there are two potential approaches.

- Use solutions designed to cope with unstructured resources: these may be additional IAM/IAG modules or stand-alone solutions. They generally have the advantage of offering a very advanced level of integration with the technologies they cover. However, they are generally limited to a handful of technologies or resource types and can therefore create a silo effect that prevents a cross-functional, company-level analysis.
- Use IAM/IAG and IAI modules that are already deployed. These two modules share responsibilities: the IAM/IAG module manages access requests and provisioning to an access group. It offers analytics functionalities to reconstruct the authorisation chain from end to end and ensure that only the access groups are authorised to access unstructured data, without managing one-off authorisations.

  Without requiring additional modules, this approach has the advantage of offering a cross-functional overview of authorisations to applications and unstructured data, whatever the underlying technology. This makes it possible to perform analyses without being constrained by silos.

  However, it requires strict implementation of the policy, including the systematic creation of an access group. In addition, if a non-conformity is detected in a resource, for example the attribution of a direct authorisation without the intermediary of a group, the IAI solution may raise an alert. However, in most cases, it will not be able to correct this discrepancy and a further – often manual – action will be needed.

II.5.3. Analysing behaviours

The most innovative IAI solutions are starting to offer behaviour analytics functionalities. They are often called UBA (*User Behaviour Analytics*) or UEBA (*User & Entity Behaviour Analytics*).

They promise to detect risky behaviours or at least behaviours that diverge from the observed “common” use. To do this, they do not rely on *a priori* rules or pre-defined patterns. On the contrary, they bring to bear innovative big data or machine learning technologies to:

- consolidate the application log files produced by each application;
- analyse and correlate these log files with each other and in relation to the characteristics of identities;
- identify, on the basis of mathematical models, behaviours that differ from the “average of observed behaviours”.

Each detected divergence then has to be analysed individually to separate the truly inappropriate uses from the false positives.

These advanced functionalities can be used, in particular, to combat fraud. They can also offer help in understanding actual real-life uses, and thus help adapt and improve IAM functionalities, such as processes, the entitlements model, etc. Secondly, they might also be linked with SIEM services, which are still often limited to network and IT events and have little to do with application and business strategies.

II.6. Capitalising on the cloud

IDaaS/IAMaaS services aim to offer IAM functionalities in the cloud, i.e. in SaaS mode.

As with other IT services, many customers are wondering whether they should use the cloud for IAM services. At the time of writing this document, use of these services remains limited because not all IAM packages offer the same level of maturity:

- cloud services associated with access management, such as multi-factor authentication, SSO and federated identity management, already offer an attractive level of maturity;
- Cloud services associated with identity management are lagging behind “on-premises” offerings. It is worth noting that the functional coverage of a publisher offering its solution in on-premises mode and cloud mode is not necessarily identical;
- Cloud services associated with IAI are the least well represented in cloud offerings.

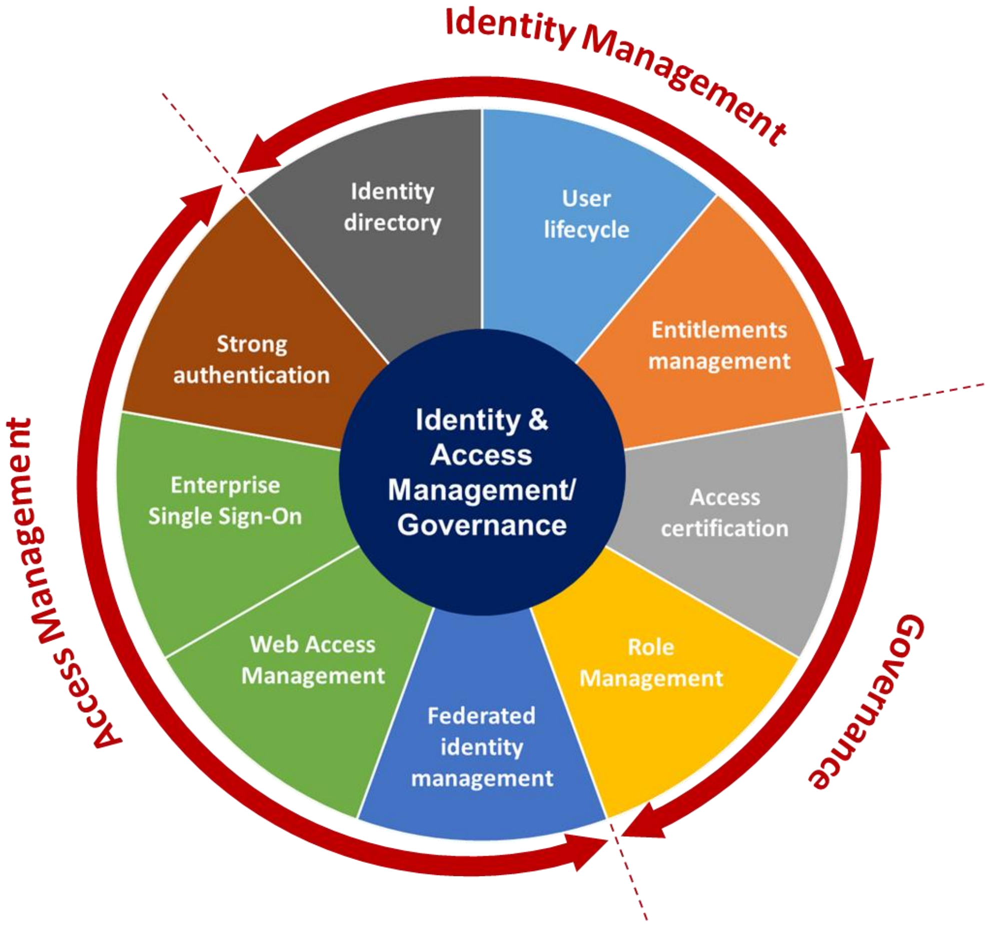
The most common current approaches are at best hybrid, combining an on-premises infrastructure with some cloud services.

Lastly, to make up for the lack of cloud offerings, some integrators are beginning to deliver on-premises implementations of solutions with cloud hosting (PaaS). This delivery method is still quite new and does not offer an identical level of service to a fully-fledged cloud offering.

III. Why green-light an IAM/IAG project?

In the previous chapter we suggested grouping together the principles underpinning IAM/IAG into 6 concrete issue areas which highlight a number of components or modules. Having said that, in this document, and as specified in chapter 1.5, we have deliberately not addressed in detail all of the functional components of IAM/IAG, favouring the most basic, widespread and mature modules currently on the market, grouped into "major families".

As the graphical depiction of Identity and Access Management/Governance could be presented in various forms, we chose a conventional representation corresponding to the structure of this document.



NB:

We could have made other choices: the "Access Management" and "Identity Management" arrows could very well join in the middle of the "Identities directory" section, since an identity reference base is needed for both areas.

Similarly, not overlapping the "Governance" arrow with the "Identity Management" arrow might suggest that there is no business dimension to governance, which is of course not the case.

There are also access certification functions in identity management, and we could equally have only used two arrows: one for "Access Management" and one encompassing "Identity Management" and "Governance", which we could perhaps have named "Identity Administration & Governance".

There are many reasons for starting all or part of an Identity and Access Management/Governance project. That is why the aim of this chapter is not to exhaustively list them but rather to identify numerous concrete use cases or objectives that amount to arguments justifying launching an IAM/IAG project.

The table below presents a number of these use cases, organised by functional area and issue area, alongside which we have set out the most directly related IAM/IAG components.

The list is not exhaustive; other use cases are provided in the remainder of the document, notably in the factsheets in chapter VI.

Areas	Examples of issues and use cases	Strong auth.	SSO	Federation	Directory	Lifecycle	Entitlements	Certification	Roles
Security	Know who can access what				■	■	■	■	■
	Know who actually accesses what	■	■	■	■				
	Eliminate the use of commonplace passwords and adapt the level of authentication to the context	■	■						
	Control and track accesses to applications from any entry point	■	■	■					
	Enhance the authentication mechanisms in applications and/or on workstations	■	■						
	Control the openness of your IS and the outsourcing of services	■		■					
	Have a central directory to manage identities and accesses				■	■	■		
	Control and track the allocation, modification and removal of user rights in the IS				■	■	■		
	Delete orphan accounts, ensure that individuals do not hold multiple toxic rights					■	■	■	
	Check that accounts are actually closed for people who have left the company					■	■	■	
Ergonomics & User satisfaction	Implement one-time, ergonomic authentication for all applications	■	■	■	■				
	Give users the freedom to reset their own passwords		■						
	Delegate authentication to third-party identity management providers			■					
	Make the user journey uniform whatever access is used: internal, mobile, remote, etc.		■	■					
	Offer a self-service portal for IS application access requests				■	■	■		■
	Simplify the rights allocation and removal process					■	■		
	Simplify operational access certification tasks						■	■	■
Costs/ROI	Streamline password management and renewal	■	■	■					
	Standardise and pool authentication and authorisation infrastructures		■		■				
	Simplify the integration and connection of new services to the IS		■	■	■				
	Reduce administrative tasks					■			
	Improve the effectiveness and reliability of entry, mobility, exit and rights allocation processes				■	■	■	■	■
	Automate the provisioning of accounts and rights in IS applications				■	■	■		■
	Eliminate processes using “paper” forms				■	■	■		

Areas	Examples of issues and use cases	Strong auth.	SSO	Federation	Directory	Lifecycle	Entitlements	Access	Roles
Infrastructure architecture, Standards	Define an authentication platform that is separate from specific implementations			■	■				
	Simplify the integration of new applications and make the IS flexible and agile			■	■				
	Have a single, reliable, central reference base of identities and rights				■	■	■	■	■
	Make overall security policies within the IS consistent	■	■	■					
Business	Follow the major trends towards opening up your IS to third parties or to the cloud			■					
	Facilitate accesses to applications in corporate change contexts			■					
Compliance	Satisfy regulatory requirements demanding the implementation of strong authentication	■			■				
	Satisfy the constraints imposed by internal control, regulators and auditors					■	■	■	■
	Facilitate access certification and the performance of audits and controls						■	■	■
	Enable checks on compliance with the principle of SoD						■	■	■

0

IV. Before getting started: pre-conceived ideas, pitfalls to avoid...

An IAM/IAG project is not confined to the deployment of a technical product installed in plug & play mode. It is a more iconic, functional and organisational project, implementation of which can fail if insufficient attention is paid to a series of points.

The aim of this chapter is to list several subjects that relate either to pre-conceived ideas to be dispelled quickly, or to easily avoidable pitfalls, or quite simply to practical tips.

The remainder of this document will focus on each phase of the project in more detail. The “prerequisites” section of “factsheets” provides more specific insight into a given context.

IV.1. Some pre-conceived ideas...

“IAM is a magic bullet”

Unfortunately, there is nothing magical about IAM. You can’t use it as a magic wand to deal with blurred organisational lines, the inconsistent definition of job profiles or technical obsolescence that makes applications incompatible with current standards.

So, to prevent disappointment, you will need to:

- evaluate your “IAM maturity”;
- set out a roadmap to increase this maturity;
- specify the prerequisites for each step in order to get the very most out of IAM.

For example, an IAM project will not integrate all IS applications into its scope, at least in the first phases of the project, especially in the “accounts and rights provisioning strand”.

You therefore need to pay attention to disappointments such as “IAM stops where the IS starts”. You need to be realistic, communicate clearly about the scope of your project, or even an initial scope, to avoid these disappointments. You also need to be prepared if necessary to adapt to market technologies, internal processes, the budget, etc.

“Manage the project yourself to save time and have fewer headaches”

Implementation of this type of project very often impacts on your whole organisation. IAM is a cross-functional project that can disrupt the organisation. For this reason, it is essential to communicate and involve all stakeholders. This applies to business lines, HR, general management, the IT department, management controllers, auditors, and so on. The best approach is naturally to make allies, by finding arguments that concern them and by reaching out to the people with something at stake from the outset. (See factsheets later in the document.)

IV.2. Some pitfalls to avoid...

“Buying the software package before you have even defined your need”

This is certainly one of the biggest mistakes you can make. While IAM packages do what they are designed to do, they do not all do it in the same way, and they do not necessarily all have the same functional coverage.

Just as you should never “put the cart before the horse”, you should not go all in on this or that solution as a group choice, for example, or because it is discounted, or on the strength of an overly subjective piece of advice, before you have a good overview of what is expected in the short, medium and long terms from IAM.

It is easy to understand why, for instance, a small subsidiary would not necessarily want to use and deploy group solutions that are unsuited to it functionally and technically. If the IS is of a reasonable size, it may be preferable to consider manual procedures to begin with and to meet the project’s priorities.

However, once you have chosen your solution, the approach needs to switch. It is essential that you investigate exactly how the solution functions, perhaps seeking help from a partner, so that your plans match the general capabilities of the solution. This will limit special developments. In addition, functionalities not envisaged at the outset may be available and make it easier to accommodate some use cases.

“Wanting to do everything at once”

Pay close attention to the initial scope. You should forget about implementing your IAM project in one fell swoop. An iterative approach is by far the best approach: break it down into functional modules, geographical or organisational units, user populations or application scopes, etc.

You need to make step-by-step progress, starting with a reduced, controlled scope so that you understand the nuts and bolts of the software packages you’re using. The “blitz” approach has given way to the batch approach once and for all. Here too, you need to communicate this to stakeholders, to avoid disappointment.

⚠ **“Short-term thinking”**

IAM never stops. Once the project is implemented, it continues. It is a very dynamic system which long outlasts the initial build. It is crucial you know who will be managing the project once this initial phase is complete, who will operate it, who will upgrade it, etc. This means having a service continuity guarantee; without one it is best not to start at all.

⚠ **“Thinking you know how people work day to day”**

You know how your company is organised, its main business lines, its key specific features, how it has changed in the past and perhaps how it might evolve in the future.

But do you know enough about how each member of staff operates and the working demands they face? Do you know about the constraints on office-bound and roaming staff? Those that have a desk and those you don’t? Those that have low-bandwidth network access, are remote from support teams or work antisocial hours? What about how organisations operate during the holidays? Etc.

An IAM project will necessarily have to address the operational reality on the ground, and will only be welcomed if it makes everyday uses simpler and takes account of legitimate specific differences. You therefore need to look beyond organisational principles in order to:

- understand how the company functions operationally;
- compare these uses with the theoretical organisational model;
- separate “operational biases” that need not be factored into IAM from “actual specific characteristics” that IAM must adapt to.

IV.3. A few tips before getting started...

“Know your IS”

An IS will very often be long-established, and encompass a variety of systems, all of which makes it more complex to implement an IAM project. To keep nasty surprises to a minimum, it is very advisable to identify clearly, and as soon as possible, the people responsible for the functional and technical aspects of the application fleet, so that they can be involved very early in the preliminary scoping phase.

“Define your need clearly”

It is essential to delimit your needs clearly in the short term, and in the medium and long terms if known. This allows you to plot your roadmap and identify the steps in your project. There is a strong temptation to keep adding functionalities, but you should not give into it, or you may never get started on the project. It is better to split the project into batches and iterations, and anticipate upgrades, as far as possible, while also considering the consistency of the user population.

“Do not mix genres”

In an attempt to oversimplify, some shortcuts can prove ill-advised.

For example, lifecycle management cannot be addressed in the same way for internal IS users as for external clients. The constraints and volumes are different. You might have a thousand internal staff but millions of client identities to manage, so the processes are different. This logic also applies to applications to manage in an SSO or federated identity management project, or a strong authentication project, etc.

Get away from ambiguous names: IAM, IAG, IAI

Talking about IAM, IAG, IGA, IRM, IAI, IDaaS, etc. can be a major source of confusion, including for suppliers. This is especially true when each step in the project might only overlap partially with these concepts.

As an illustration:

- identity recertification functionalities might greatly improve the quality of data in a step centred on identity management and the creation of an identity reference base;
- a rights recertification step might greatly help in defining job profiles and upgrading the entitlements model.

“Master the vocabulary”

The vocabulary used seems easy and understandable to all, but do not be mistaken. Within the same organisation, does everyone know the difference between a credential and an authorisation? Authentication and identification? What is the definition of an account, a role and a profile?

It is vital to master the terms used in this type of project to avoid misinterpretations. Putting together a presentation and an internal glossary, illustrated with relevant examples, is very often a good way of ensuring everyone speaks the same language.

“Get a grip on communication”

Getting a grip on communication means first identifying the impacts of deploying your project. You will then be able to plan, target and control how it is communicated. It means identifying the actors concerned, when and how to involve them, how to assess the gains, etc.

V. Pre-project: the questions to ask yourself...

The aim of this chapter, laid out in the form of an “FAQ”, is to provide some important recommendations and tips to consider in the pre-project phase. These concern in particular the preparatory work needed, the content of your specifications, and the choice of solutions.

The following questions are covered below:

Q1: Should I seek support before starting my project?

Q2: What link should there be between functional teams and technical teams?

Q3: Should I first analyse the IAM solutions on the market? Which ones? How many? And how should I assess analysts’ reports?

Q4: What do I need to prepare ahead of my project?

Q5: What organisation do I need before starting my project?

Q6: What legal constraints do I need to take into account?

Q7: Should I involve procurement from the start of the project?

Q8: Which elements must not be overlooked in my specifications?”

Q9: Who should I send my tender documents to?

Q1 Should I seek support before starting my project?

Another way of framing this question might be: “Do I have the expertise and experience in-house to implement my project?” ».

There are numerous IAM experts in the security industry. It might therefore be a good idea to call on them, although their services may come in various forms, and cost various amounts.

Naturally, the volume of support in terms of days will depend on the assignment, the size of the company, the scope of the future project, the organisation in place in the company, and the capacity to commission such services. For example:

- For low-cost services requiring several dozen person-days: initial scoping, awareness-raising, macroscopic analysis to “get the project on track”, budgeting – a vital element in deciding whether the company has the resources to match its ambitions – and production of the roadmap.
- For wider-ranging services:
  - help drafting the statement of needs and the specifications document, with data processing, and with production and follow-up of the PoC;
  - help with the detailed description of entry/mobility/exit processes, with mapping applications, with the definition of roles and profiles within the organisation, etc.

However, one provider will not be able to implement the project alone. It will have to call on an in-house team, which has legitimacy within the organisation. Indeed, one provider may be able to offer insights but will not be able to stand in for the client and decide which priorities to adopt or make the necessary judgement calls.

It is therefore very important to define what is expected of the provider and what the client will undertake to do, which does not release the client from acquiring the minimum expertise before beginning; reading this guide is a good start.

Q2 What link should there be between functional teams and technical teams?

IAM/IAG projects are simultaneously functional, organisational and technical. The question of the link between functional teams and technical teams therefore arises naturally. For companies that separate project ownership and project management, it is essential that teams work very closely, understand each other and trust each other so that they can make the best decisions together. Indeed, it is always preferable to get the most from the native functionalities offered by solutions to be deployed, even if this means slightly adapting how the stated needs are met.

For example, rather than implementing very complex checks and request workflows, it may be better to keep a minimum number of simple checks on requests and to apply checks after the event in the most complex cases. This allows you to offer responsive request processes and use native functionalities while also keeping the desired level of security. This applies, for instance, to internal mobility, with a handover period. In this case, a review of old rights is easy to carry out, is in line with the “reality on the ground”, and is often sufficient from a security standpoint.

Ideally, if the project owner cannot also be the project manager, being able to rely on a single partner is an ideal solution, and should at least be considered.

Q3 Should I first analyse the IAM solutions on the market?

And how should I assess analysts' reports?

Clearly, not all IAM solutions address all needs, or even in the same way. Thus you are strongly advised to take the time to analyse a number of solutions first.

In addition, while one of the main benefits of analysing market solutions is that it helps frame your needs and estimate your budget, it can reveal other needs or highlight sticking points or factors that might have been overlooked.

Several methods of analysis are possible:

- When support is chosen (see previous question Q1), a survey to determine the state-of-the-art solutions that meet your needs may form part of the support service. In this case, you must make sure of the impartiality of your provider, which must of course be skilled in integrating a number of solutions so that it can present their pros and cons depending on the client context.
- Even without obtaining support, it is possible to find out more by taking part in a number of events: specialist trade fairs, usually attended by a large number of IAM/IAG industry figures, conferences, working groups, etc. Doing this helps you to acquire "general IAM knowledge", and to ensure you at least have an opinion on the issue.
- The big consultants (Gartner, Forrester, KuppingerCole, etc.) also offer a number of tools and reports on market solutions. Make sure you regard them as influences but do not follow them blindly because the assessment criteria and rankings used in analysts' reports can differ.
- Visiting clients listed by selected publishers is also a very good way of checking the quality of implementations, in a very hands-on way.
- Lastly, the best approach, when it is possible to implement it because it demands more work than the others, is often a PoC. This needs to be applied to a reduced but representative sample of short- and medium-term needs. Be careful not to assess too many solutions, a maximum of three in general, so that you don't spend too long on it, and use one of the methods above to produce a shortlist of favourite solutions to assess.

It is also advisable to take a long-term view of the investment. A first short-term project, for example a password reset self-service module, can form part of a larger long-term project, for example an enterprise SSO or federated identity management project. This preliminary analysis phase allows you to ensure – on paper at least – that the chosen solution will also meet your long-term needs.

Lastly, some people will choose not to make any enquiries or assessments before putting out their calls for tenders, so as not to have differing influences. This introduces a considerable risk, namely that of stating requirements which no market solution will meet, and thus of being out of step with the market.

Q4 What do I need to prepare ahead of my project?

This depends directly on the type of project: the prerequisites differ for a federated identity management project and an entitlements governance project, for example.

However, and as a general rule, it is essential to measure your level of IAM maturity in respect of the desired goal. In other words: do I have the means – i.e. the legitimacy, the organisation, the processes, the technical wherewithal, the budget, the timetable, etc. – to match my ambitions?

The "project factsheets" in the next chapter (sections 3 and 4 of each factsheet in particular) give a more detailed answer to this question.

Q5 What organisation do I need before starting my project?

The answer here is similar to the answer to Q4: it depends on the desired IAM/IAG components. The "project factsheets" cover each component of the subject, to determine:

- Who is financing the project?
- Who is steering the project?
- Who is responsible for acceptance-testing and accepting the solution?
- Who will be responsible for the platform once it is implemented?
- Etc.

Q6 What legal constraints do I need to take into account?

They depend on various parameters, such as the nature of the IAM/IAG project being undertaken and the company's business sector.

For example, for a strong authentication project based on electronic certificates, RGS certificates will have to be used in government departments and CPS/CPE cards in the healthcare sector. You will also, once an identity reference base is set up, have to check the CNIL's personal data protection obligations and the new European eIDAS and GDPR regulations. The finance and insurance sectors are not to be outdone in this area, imposing numerous standards and regulations that may have an impact on the project, including SOX, PCI DSS, etc.

In some situations, legal obligations can be fairly simple and be limited to a few clarifications in the IT guidelines or in the ISSP. In others, they might be more binding, including, for example, the retention of logs and accreditation data, supplier contracts, etc.

In any case, the legal department will need to be involved so that you know, from the start of the project, the legal requirements to be taken into account.

Q7 Should I involve procurement from the start of the project?

In some organisations, procurement needs to be involved at quite an early stage. In this case, the question no longer arises. In other cases, it is most important to know which constraints are procurement-related in order to anticipate them: for example, relating to the minimum turnover or the listing of software publishers or integrators bound by the commitment to results.

Q8 Which elements must not be overlooked in my specifications?"

As a general rule, any measure that might save time when scoping or starting the project is worth taking. Similarly, the more precise the description of objectives and requirements is, the easier it will make the comparison of the technical and financial aspects of the various offerings.

A few simple tips:

- provide all the information needed to ensure you do not have to compare very different offerings. For example:
    - a precise scope inside which the tenderers have to operate: users, applications, processes, requirements, constraints, etc.:
        - Identity management: which populations are targeted? Using which processes? Inside which scopes?
        - SSO: what are the applications' features? What are the use cases? Internal/external access, type of workstation, types of users?
        - Provisioning: which objects? Which targets? Which sources? Type, underlying technologies, versions, content, accounts/profiles/rights, use cases?
        - Entitlement governance: existing arrangements and surveys of roles/profiles identified in the organisation? Role management? At what granular level should rights be managed? For which targets?
    - the quantity and level of expected deliverables; this will have an impact on the proposed project management;
- avoid all unnecessary questions or requirements, which instead of helping will tend to "muddy" the clarity of publishers and/or integrators' responses, or make analysis more complex. It is not the volume or number of pages in the specifications document that counts, but rather its level of precision and the clarity of the information provided and the requirements stated. For example, do not request 24/7 international support if it is not necessary;
- in the same vein, you might get a "letter to Father Christmas" back from tenderers if you give them too much freedom to suggest what they want. The risk is once again that you will have to analyse wildly differing commercial and technical proposals, with large price discrepancies. If you do go down this road, you should attach priorities to the most important items, and suggest a precise and relatively "closed" response framework;
- indicate which evaluation and selection criteria are the most important, without necessarily providing your full assessment grid, at the risk of influencing responses; at least supply a weighting of these criteria.

Some pitfalls to avoid when drafting your specifications document:

- confusing the capacity of technical solutions with the scope of the service: technical solutions offer a wide range of functionalities so it is crucial to define your priorities and the context in which the solution needs to be implemented;
- requesting that all functionalities be in production in less than 6 months. As IAM projects are often keenly anticipated, a certain time pressure is often applied. Bear in mind that before any IAM project, of whatever kind, you first have to define the organisation, use cases and processes. It is fanciful to put a technical solution into production without having spent time on the preparatory phase;
- not describing existing arrangements in detail. The more information tenderers have on existing arrangements, the more precise and consistent their answers will be. As some functionalities or applications are particularly important in this type of project, every oversight or imprecision will inevitably lead to misunderstandings and therefore to implementation difficulties later on.

Appendix 2 provides a possible “template” structure for an IAM/IAG specifications document.

Q9 Who should I send my tender documents to?

There are several schools of thought: you might seek a contribution from the publisher, from the integrator, or from both. In practice, several approaches are used:

- an “integrated solution”-oriented call for tenders: in this case a complete solution is requested, encompassing one or more solutions, integrated by one or more integrators, with a single point of entry;
- solution chosen in phase 1, then integrator chosen in phase 2 to integrate the solution, in line with the desire to integrate it internally after training;
- integrator chosen in phase 1, then solution chosen in phase 2 according to its analyses, advice and skills.

Each approach has its benefits and drawbacks, and whether it is used clearly depends on the company’s maturity and expertise in the subject, and on the organisation's internal processes. As with the previous points, it is possible to offer a few simple tips:

- clearly state who will be asked to contribute to integration of your project;
- do not send your specifications to the whole publisher/integrator market, or you risk having a huge analysis and bid selection job on your hands; the exception to this rule is in the public sector, which requires open competition;
- seek contributions from specialists, with demonstrable positive experience in the field of IAM/IAG. When you choose to work with a generalist integrator, e.g. on listing suppliers, you need to ensure that you require it to subcontract the expertise of the publisher of the proposed solution, or an integrator specialising in this solution, and demand to have direct access to the expert without intermediary in the event of difficulties;
- take the step of meeting market players – integrators and publishers – prior to the call for tenders to get your own idea of their skills and how they operate;
- think long term: the product(s) that will be installed as part of the project will be in place for several years. You need to clearly identify who will provide level 1 and 2 support,

given that level 3 support is necessarily provided by the product developer, so the publisher.

In addition, here are a few important ideas to bear in mind:

- there is no such thing as an integrator who specialises and is expert in all market solutions. Similarly, few publishers offer a full list of the software packages available in the IAM/IAG sector;
- publishers do not necessarily offer local professional services and local support, and certainly not in all languages. This point can be an obstacle in some cases;
- the integrator's added value rises with the number of solutions to implement as part of the project: it is the sole point of entry and has skills in all the components to be implemented, which may be published by different companies.

VI. Implementation of an IAM project – Factsheets

VI.1. Introduction

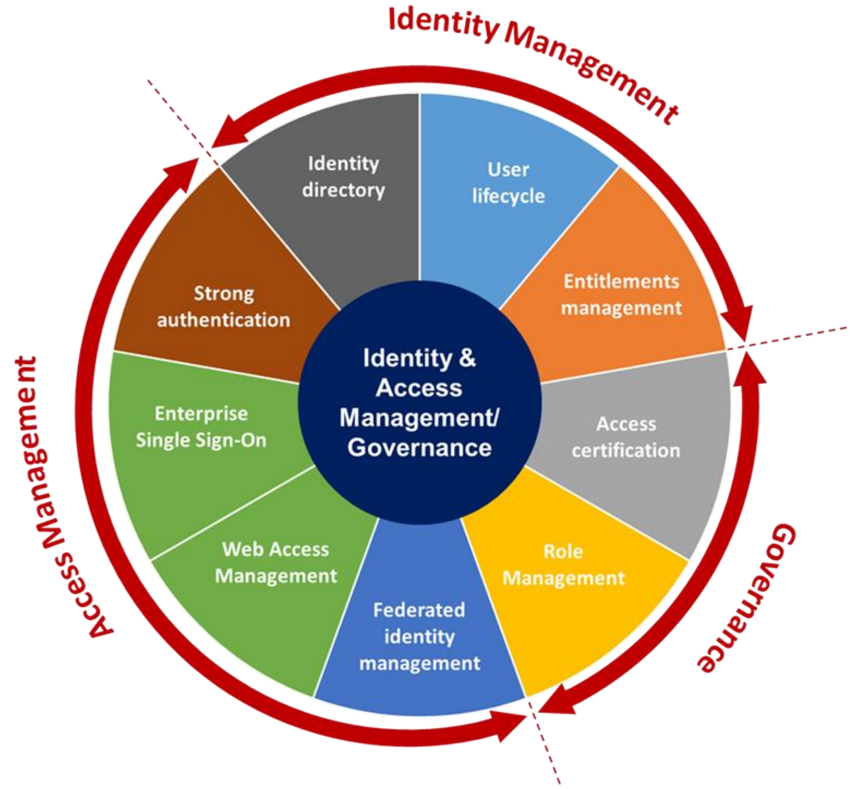
This section comprises a number of factsheets, presented in the form of "recipes", which break IAM/IAG down into functional modules. These factsheets can of course be combined.

The aim is to list a maximum number of key points, so that the following questions are answered for each functional module:

- Why a project like this? What are the advantages and who are the priority beneficiaries? Which arguments to use to convince senior decision-makers to start a project like this?
- How to sell the project internally?
- Which specific elements need to be taken into account in the project budget?
- What are the key steps in deployment? Which questions do you need to ask yourself and the points not to be overlooked?
- What are the key points for successful implementation of a project like this?

We also aimed to produce a "digest" document. Consequently, we focused mainly on the most specific elements of each module presented in the context of a conventional project approach.

Lastly, as stated at the start of the document, we deliberately did not cover all the functional components of IAM/IAG, choosing instead to limit ourselves to the following modules:

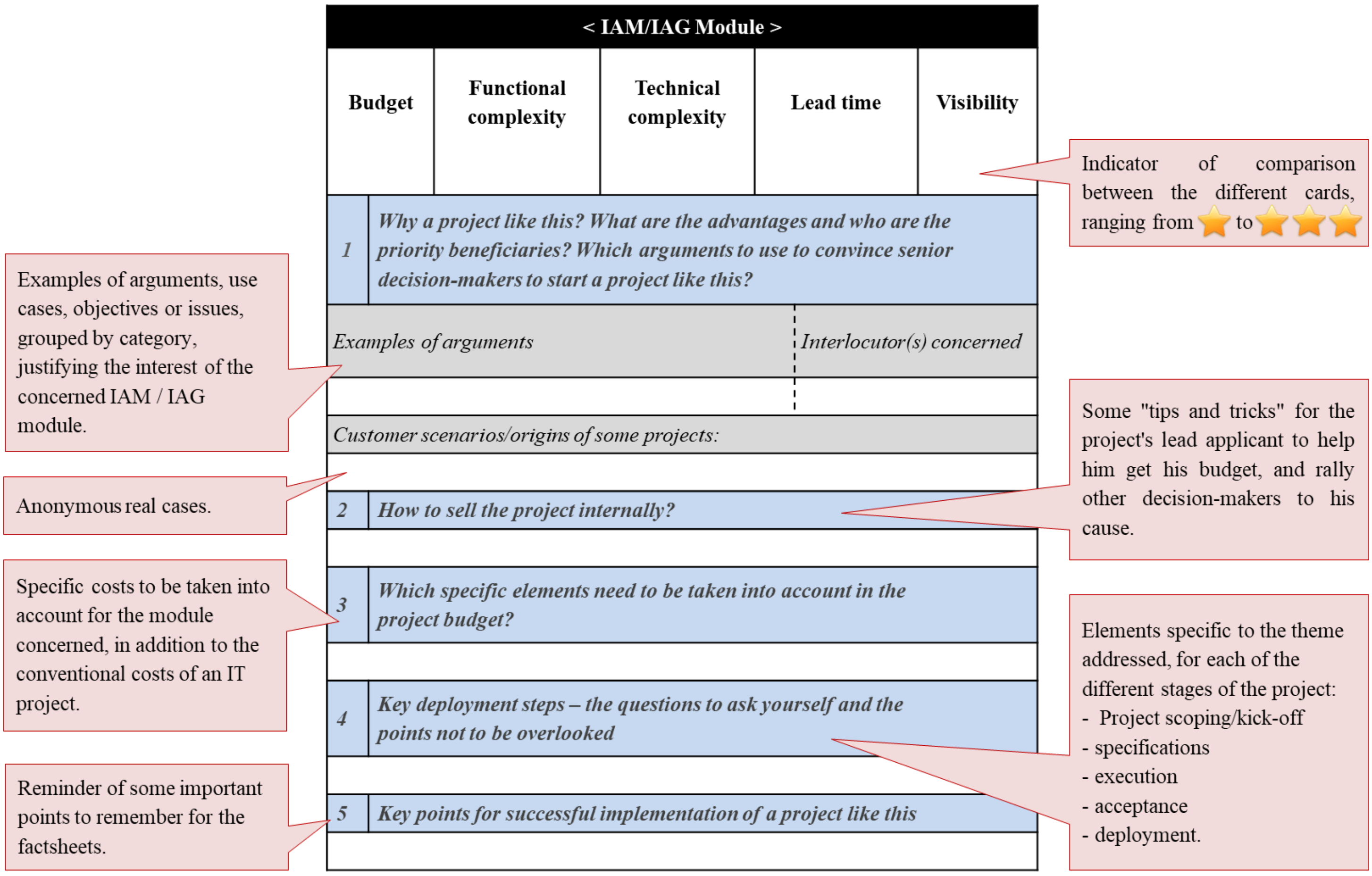


The following factsheets are presented below:

- "Access" factsheets
  - **SSO – Single Sign-On**, encompassing eSSO and WAM modules
  - **Federated Identity Management**
  - **Strong authentication**
- "Identities" factsheets
  - **Identity directory**
  - **User lifecycle**
  - **Entitlement** management
- "Governance" factsheets
  - **Entitlements review / Access certification**
  - **Role management**

VI.1.1. How to? Reader's guide to the factsheets

The factsheets are all presented in the following format:



< IAM/IAG Module >

Budget	Functional complexity	Technical complexity	Lead time	Visibility

1 *Why a project like this? What are the advantages and who are the priority beneficiaries? Which arguments to use to convince senior decision-makers to start a project like this?*

Examples of arguments	*Interlocutor(s) concerned*

Customer scenarios/origins of some projects:

2 *How to sell the project internally?*

3 *Which specific elements need to be taken into account in the project budget?*

4 *Key deployment steps – the questions to ask yourself and the points not to be overlooked*

5 *Key points for successful implementation of a project like this*

Indicator of comparison between the different cards, ranging from ★ to ★★★

Examples of arguments, use cases, objectives or issues, grouped by category, justifying the interest of the concerned IAM / IAG module.

Anonymous real cases.

Some "tips and tricks" for the project's lead applicant to help him get his budget, and rally other decision-makers to his cause.

Specific costs to be taken into account for the module concerned, in addition to the conventional costs of an IT project.

Elements specific to the theme addressed, for each of the different stages of the project:
- Project scoping/kick-off
- specifications
- execution
- acceptance
- deployment.

Reminder of some important points to remember for the factsheets.

The stars awarded to the five criteria in the top section of the sheet are level comparison indicators ranging from one to three. The scores below have been set consensually by the members of the IAM WG on the basis of their experience.

The idea is therefore:

- to rank the different IAM/IAG modules in relation to each other;
- to get a simple overview of the major characteristics of each sheet.

This analysis assumes that the prerequisites are in place, and readers are invited to compare their organisational and technical contexts to adjust the scale.

Lastly, the customer scenarios are real and anonymised for confidentiality reasons.

VI.1.2. Overview

The table below summarises the "scores" from each factsheet presented in detail in the following paragraphs.

	Budget	Functional complexity	Technical complexity	Lead time	Visibility
SSO **Single Sign-On**	★	★	★	★	★★★
Federated Identity Management	★	★	★	★	★★★
Strong authentication	★★★	★	★	★	★★★
Identity directory	★★	★★	★	★	★★★
User lifecycle	★★	★★	★★	★★	★★
Entitlement management	★★★	★★★	★★	★★	★★
Access certification	★★	★★	★	★★	★
Role management	★★★	★★★	★★	★★★	★★

VI.2. Access Management

VI.2.1. “SSO – Single Sign-On” factsheet

“SSO – Single Sign-On”				
Budget	**Functional complexity**	**Technical complexity**	**Lead time**	**Visibility**
★	★	★	★	★★★

1	***Why a project like this? What are the advantages and who are the priority beneficiaries? Which arguments to use to convince senior decision-makers to start a project like this?***

Examples of arguments	*Interlocutor(s) concerned*
• **Security** • eliminate the need for people to use post-it notes for passwords everyone knows, or the use of commonplace passwords; • control accesses to applications from any entry point; • make overall security policies within the IS consistent; • strengthen password strategies for applications; • put in place account delegation mechanisms; • track accesses to applications: authentications and authorisations; • audit security and have at your disposal IS access statistics, including for workstations or applications shared by multiple users.	CISO
• **Ergonomics/User comfort and satisfaction** • make life easier for users by simplifying access to IS applications; • implement one-time authentication for all applications; • give users the freedom to reset their own passwords or their authentication methods; • access services such as an “SSO portal” or “account delegation”;	Users
• **Administration costs** • streamline password management and renewal; • standardise and pool authentication and authorisation infrastructures; • simplify the integration and connection of new services to the IS; • check the correspondence between licenses paid for and those actually used, in SaaS for example, by using application usage reports.	Finance Department Management control

Customer scenarios/origins of some projects:

Customer scenario 1: #Finance #Security #150kUsers

- Trigger: Anti-fraud.
- Main objectives: Delegate the authentication function for several hundred internal and external web applications to a dedicated service; step up access control; put in place strong authentication functionalities for “sensitive” applications; roll out SSO for web applications; provide an SAMLv2 federated identity management service to B2B partners.
- Solution: Deployment of a central Web Access Management & Federated Identity Management solution providing several methods of 1, 2 or 3-factor authentication depending on the individual case, and SSO for several hundred group web applications.

Customer scenario 2: #Retail #MobileVendors #Roaming #Virtualisation #20kUsers

- Trigger: Migration of more than 120 IS, i.e. one per store, to a centralised IS, including implementation of virtualisation.
- Main objectives: Cut the costs of the helpdesk, updates, etc.; modernise the IT access system; integrate new devices like tablets; facilitate login via an access method; guarantee security and confidentiality.
- Solution: Virtualisation of workstations on thin clients including deployment of an eSSO solution adding strong authentication functionalities using RFID Badge, fast login/logout, SSO in applications, and session mobility.

Customer scenario 3: #Service #ContactCentreAgents #ResetPassword #ROI #20kUsers

- Trigger: Regular losses of passwords leading to a loss of productivity.
- Main objectives: Call centre agents working on a different application per call centre, each necessitating dedicated authentication using application-specific login/password combinations. Forgotten passwords lead to frozen accounts and prevent users from logging in because of repeated erroneous attempts. The main objective is to reduce losses of productivity by ensuring that accounts are blocked less frequently, thereby cutting the associated downtime.
- Solution: Deployment of an eSSO solution ensuring a single password, the one used to open the Windows session, and transparent authentication in all business applications.

2 *How to sell the project internally?*

With the help of a PoC

- The establishment of a PoC is definitely the most effective way of selling a project internally. A PoC is a way of illustrating tangibly the integration of an SSO solution into its IS and of measuring the expected benefits. It is also a way of ensuring engagement, including of the businesses, and of scoping the target project in advance.
- If the PoC is convincing, the next step is often a pilot. It involves extending the scope of the PoC to a wider user population – e.g. all a department’s users – or to applications in production.
- Note that a PoC needs planning: it must be carried out in an environment representative of the intended target: applications, workstations, uses, etc.

By delivering quick wins

- One of the advantages of SSO projects is that they can be implemented relatively quickly, e.g. in several weeks depending on the initial scope, and can make life more comfortable for the company's users by making one-time authentication available.
- Examples of visible quick wins:
  - single web application access portal: "WebSSO portal";
  - password reset self-service;
  - SSO in a mobile environment;
  - strong authentication (see separate factsheet);
  - federated identity management (see separate factsheet).

3 *Which specific elements need to be taken into account in the project budget?*

An SSO project can give rise to specific costs if the project is combined with a strong authentication project. See separate "strong authentication" factsheet below.

Similarly, in some cases, integrating an application into the SSO project can require changes to that application – for example, if it needs to be "SAML-ready", linked to a CAS solution – or the implementation of an API for the chosen SSO solution.

4 *Key deployment steps – the questions to ask yourself and the points not to be overlooked*

During project scoping/kick-off

As is often the case, it is crucial to clearly define the project's organisational and functional scope. You first need to find out the answers to the following questions:

- Do I have an identity reference base to back up my SSO service? Is the quality of the data in it sufficient?
- Who will the SSO users be: everyone, some units only, head office, branches, some subsidiaries?
- Which applications will be included? Which "type" of SSO to implement: Enterprise SSO? Web Access Management? Federated Identity Management? Mobile SSO? All of the above?
- Who will be involved in the project: CISO, application managers, operators, publishers, etc.?
- Are there existing authentication methods to take into account? Are there any use, technology, legal or other constraints to take into account for authentication?
- Are the applications concerned by the project managed? Ditto the workstations?
- Will users still need to know their passwords? What is the expected level of security of the project?
- What are the expected degraded modes, and the lead times associated with this type of situation?

During the functional and technical specifications

It is advisable to proceed by “topical workshops”:

- functional workshops: user use cases, processes of authentication, application access, registration, delegation and password reset, end-to-end business processes (login, application access, functional validation, user switching, etc.);
- technical workshops: overall architecture, critical architectural elements such as login peaks, load increases, authentication reference bases, types of workstation, location of equipment for access;
- applications: proceed by “application description sheets” – see examples in appendix IX.3.

Implementation of a mock-up or a PoC, if not done in an early phase of the project, gives you concrete evidence to fall back on in the design phase.

During the execution phase

Do not neglect organising scale-up tests if this criterion is important for the forthcoming project.

During the acceptance-testing phase

It is advisable to test degraded/alternative login modes and procedures. The risk that they do not function when needed is real if they weren’t acceptance tested.

During the deployment phase

An effective approach is often to start with a pilot scope, then to roll out deployment iteratively, batch after batch, each batch perhaps relating:

- in the case of an eSSO project, to a new user or workstation scope, for example a department, site, branch or subsidiary;
- in the case of a WebSSO project, to new applications attached to the project;

During this phase, knowledge is transferred and the teams responsible for deployment and operations are trained in the tools.

5 Key points for successful implementation of a project like this

Some key points:

- clearly scope your project and manage your goals: the statement of needs and aims of the project must be clear. The need must be defined before choosing the solution, and not vice versa;
- make sure you have a quality identity reference base, the means of checking the quality of these data and the legitimacy to request any data upgrades/corrections;
- choose a solution adapted to your needs: it is essential to have a short-term vision and a long-term vision so that you do not have to invest in another solution one or two years later;
- be proactive: everything you plan and prepare early on in the project will not have to be redone, for example analysis of the applications and identification of the associated decision-makers;

- anticipate all possible degraded modes: for example, if the main password or authentication token is lost or stolen, or the SSO system is unavailable, remembering that, in this latter case, an SSO system rolled out to almost all a large group's applications demands a very high availability architecture;
- batch the project: start with a basic platform which makes sense to users, with a limited number of applications linked to it: the most sensitive applications, the most critical or the most used, for example. Next roll out the deployment in "packs" of applications or users;
- define a strategy and methodology for integrating existing and future applications into the SSO project;
- do not overlook change management and internal project costs.

VI.2.2. "Federated Identity Management" Factsheet

Federated identity management can be viewed from two main perspectives:

- From a "business" perspective: it facilitates B2B or B2C exchanges and gets around a number of constraints linked to identities and authentication mechanisms in particular.
- From a "technical" perspective: it is becoming increasingly necessary as a tool for implementing WebSSO architectures, via the use of standard and standardised protocols such as SAML, Oauth and OpenIDConnect. This is particularly true of applications available in SaaS and cloud modes, and increasingly for mobile applications.

In fact, it is often worth specifying which perspective federated identity management is approached from, even though these two positionings are clearly not incompatible.

Note that, in those cases where federated identity management is regarded as a way of doing WebSSO with federation-compliant or federation-ready applications, you can refer to the SSO factsheet presented above, and to appendix *"IX.3.3. Questions specific to WebSSO and federated identity management*".

“Federated Identity Management”

Budget	Functional complexity	Technical complexity	Lead time	Visibility
★	★	★	★	★★★

1	***Why a project like this? What are the advantages and who are the priority beneficiaries?*** ***Which arguments to use to convince senior decision-makers to start a project like this?***

Examples of arguments	*Interlocutor(s) concerned*
• **Business** • follow the major trend into the cloud; • support the opening-up of your IS to third parties: partners, clients, etc. • facilitate accesses to applications in corporate change contexts: restructuring, joint ventures, M&A, spin-offs, etc.; • facilitate the management of accesses to shared services within complex organisations or partner networks.	General Management CIO CISO
• **Ergonomics, user services** • facilitate and standardise the registration and authentication journeys for the services available to external users; • delegate authentication to third-party identity management providers: France Connect, Google, Facebook, etc.; • simplify access to external services: SaaS or cloud services, such as O365, GoogleApps, etc., or to services offered by B2B partners; • standardise user journeys on all platforms, whether web or mobile.	General Management Marketing Digital
• **Infrastructure architecture, standardisation** • define an authentication platform that is separate from specific implementations; • simplify the integration of new services into the IS; • make the IS flexible and agile; • benefit from federation standards guaranteeing the security and traceability of accesses in a relationship of trust between partners.	CIO CISO IS infrastructure designers Architects
• **Security** • avoid duplicating directories in SaaS infrastructures or providing external access to your identity or authentication directories; • do not have to manage “others’ identities”; • control the openness of your IS and the outsourcing of services.	CISO

Customer scenarios/origins of some projects:

Customer scenario 1: #Media #B2B #B2C #8Musers

- Trigger: Redesign and standardisation of the access control platform for all the group’s websites.
- Main objectives: Secure and improve management of authentication and access to services; standardise registration and authentication journeys for web platforms; implement interfacing with social networks and enable the use of third-party digital identities; become a hub for authentication with suppliers of third-party identities; facilitate the integration of journeys into all federated portals and on all devices.
- Solution: Deployment of a central platform for authentication and access to group services, acting as a multi-protocol federated identity management hub, and making it possible to simultaneously play the role of service provider and identity provider to commercial partners.

Customer scenario 2: #Retail #Stores #Cloud #3kUsers

- Trigger: Make IS users comfortable while also ensuring a good level of security and availability. This should accommodate uses that differ widely depending on whether users are at head office or in store, and roaming or otherwise.
- Main objectives: Provide access to GoogleApps using a single authentication which varies depending on whether the user is at head office on their own workstation, a shared workstation or roaming, or in store on their own or a shared workstation, or even roaming in the case of sales staff.
- Solution: Deployment of an access control solution implementing several authentication methods depending on the individual case, such as Kerberos, a certificate, login/password linked to SAMLv2 federation, in order to reach the GoogleApps suite securely and ergonomically, whatever the entry point.

Customer scenario 3: #Bank #B2B #SAMLv2 #9kUsers

- Trigger: Open up access to e-money applications hosted by the “Bank1” client to internal users and to the external users of its subcontractor client “Bank2”.
- Main objectives: Open up its IS to partners securely; control external accesses; simplify authentication procedures and standardise the connection of services to a federated identity management platform.
- Solution: Implementation of an SAMLv2 federated identity management solution, thanks to which the users and clients of “Bank2” can access the e-money services hosted by “Bank1”.

2 *How to sell the project internally?*

There are numerous potentially convincing arguments for kicking off a federated identity management project: ergonomics and the user experience, security, infrastructure architecture or simplification. It is often quite simple to identify a “trigger” to highlight in order to justify kicking off a project, at lease in an initial “quick win” scope. For example, access to new cloud services, a sales agreement with a new B2B partner, opening up a service for external users, renewal or replacement of an existing WAM solution that is incompatible with the latest standards, etc.

3 *Which specific elements need to be taken into account in the project budget?*

In a federated identity management project, drawing up a legal “federation contract” between the different partner entities is a cost centre. In a B2B context, it requires at the very least legal experts from the different parties. In a B2C context, the declarations relating to personal data protection also need to be factored in.

In a “technical” federated identity management project, it is possible that you might have to modify some applications to make them compatible with the desired technical federation protocols. The integration of standards such as SAMLv2, OAUth2 and OpenID Connect may necessitate specific developments, or even the acquisition or development of federation “kits”, which will then need to be maintained. This may involve different development languages and frameworks, such as Java, .Net, or Spring. You will therefore have to ensure that you have a good level of skills to avoid any nasty surprises later.
Lastly, to avoid having to re-explain each time how to connect such or such an application to your future federation platform, you will have to educate in-house development teams about federation and the application of the associated best development practice.

4 *Key deployment steps – the questions to ask yourself and the points not to be overlooked*

During scoping/kick-off

Depending on the nature and type of federated identity management to be deployed, you will have to anticipate any necessary legal aspects: legal federation contract in a B2B context, responses to CNIL’s five key principles (purpose, relevance, retention, law, security), GDPR conformity and analyses of impacts on users’ privacy. Similarly, depending on the nature and visibility of the project, you will have to plan the involvement of general management and marketing and/or digital teams.

From a technical standpoint, it is important to ensure mastery of the management of the electronic signatures needed for functions such as signature, encryption and SSL which will be used in the technical implementation of the project. The risk of using this or that technical solution and its impact on applications should also be evaluated at this stage: compatibility with this or that federation protocol, necessary adaptations, etc.

During the functional and technical specifications

You will have to define the following elements in particular in detail:

- the federation roles to be played – identity provider, service provider – and by whom;
- the federation technology the company wants to use:
    - the federation protocols: SAMLv2, OAUth2;
    - the applications to integrate;
    - the connection kits: Java, .Net, Spring, etc.
- the procedures to be implemented: “IdP Initiated”, “SP Initiated”, etc.;
- the technical elements to take into account: federation profiles;
- the information that will be transmitted from one partner to the other, in the SAML, for example;
- in the case of federation with O365, for example, the method used to transfer users from O365;

In addition, see appendix “IX.3.3. Questions specific to WebSSO and federated identity management”, section “Specific case: SAMLv2-compatible application”.

During the execution phase

In the case of B2B federation, requiring operations by the federation partner(s), you will have to put in place monitoring of the associated technical operations, notably of the application of prerequisites by partners, interoperability tests, etc.

During the acceptance-testing phase

No particular special characteristic.

During the deployment phase

Monitoring of the production platform when the service opens will make it possible to endure that users buy into this new service and to plan any corrective actions.

5 Key points for successful implementation of a project like this

The recommendations are the same as those in the “SSO” sheet in chapter VI.2.1.

VI.2.3. “Strong authentication” Factsheet

> *NB: At the date of writing this document, a certain number of concepts are not sufficiently mature or deployed to be discussed here. They may be covered in an update or extension of this document. They include “Risk-based authentication”, “Adaptive authentication” and everything related to the FIDO, Windows Hello and Apple TouchID initiatives.*

“Strong authentication”				
Budget	**Functional complexity**	**Technical complexity**	**Lead time**	**Visibility**
★★★	★	★	★	★★★

1	***Why a project like this? What are the advantages and who are the priority beneficiaries? Which arguments to use to convince senior decision-makers to start a project like this?***

Examples of arguments	*Interlocutor(s) concerned*
• **Security** • enhance the authentication mechanisms in applications and/or on workstations, especially the most sensitive ones; • adapt the level of authentication to the user context, for example if it is in the company’s network or outside this network; • ensure a good level of authentication on mobile devices or for remote accesses; • identify the users who access shared workstations, or “kiosks”, started in a generic Windows session.	CISO
• **Compliance** • for a healthcare player, comply with the confidentiality ruling and roll out the “CPS” card for healthcare professionals; • for a banking player, meet the requirements of the PCI DSS standard, encompassing two-factor authentication for remote accesses to the network by employees, administrators and third parties, and for local access for administrators from version 3.2 (2016); • for an OCI, adhere to the LPM’s security rules, notably those relating to system protection: rules 11 to 19, including authentication.	CISO Head of compliance
• **Administration costs** • streamline password management and renewal;	Finance Department
• **Ergonomics**	Users

- replace passwords with a more ergonomic authentication method suited to users' uses;
- put in place fast locking/unlocking mechanisms on workstations along with fast user switching, on shared or "kiosk" workstations, in particular;
- factor in the latest standards integrating the use of biometrics, including Microsoft Windows Hello, Apple TouchID.

Customer scenarios/origins of some projects (real-life examples):

Customer scenario 1: #Media #SharedWorkstations #GenericAccounts #300Users

- Trigger: Protection against sensitive data theft on shared workstations.
- Main objectives: Check and audit accesses by external providers who temporarily use shared workstations started in a generic Windows session and may handle information of varying levels of sensitivity.
- Solution: Deployment of a strong authentication and eSSO solution on shared workstations; RFID/password authentication on the workstation using the premises access badge and contactless readers installed on the workstations concerned. The Windows session continues to be generic.

Customer scenario 2: #Healthcare #Roaming #Biometrics #5000Users

- Trigger: Improving security and ergonomics in some strategic services: emergencies, operating theatres, intensive care, paediatrics, medical secretaries.
- Main objectives: Increase security on self-service medical workstations; make users' journeys smoother; waste no more time entering passwords or resetting forgotten passwords, whether on personal, shared or mobile workstations, or in the institution's critical internal or external applications.
- Solution: Deployment of a "MatchOnServer"-type biometric authentication solution combined with a general SSO solution delivering eSSO functions on "kiosk" medical laptops, with roaming sessions, WebSSO and an SAML federation solution for external accesses or applications.

Customer scenario 3: #Energy #Web #OTP #55kUsers

- Trigger: Modernisation of the IS with the introduction of new technologies and new uses: mobile, personal devices; external accesses; cloud applications.
- Main objectives: Reduce risks linked to uneven access management, simplify the user experience, cut costs.
- Solution: Deployment of an "authentication broker" made up of a strong authentication service based on a multi-device software token in SaaS mode and a WebSSO and Federated Identity Management solution in on-premises mode.

2 *How to sell the project internally?*

With the help of a PoC, or a pilot

- As in the previous scenario – see SSO sheet – the establishment of a PoC is a way of introducing solutions, evaluating them and checking they are compatible with your own uses in terms of ergonomics, security, robustness, etc.
- If the choice of the technology to be evaluated is not final, you can take the opportunity to evaluate several authentication methods. Similarly, it may be necessary, in some instances, to evaluate solutions in web mode, workstation (credential provider) mode or mobile mode for smartphones and/or tablets.
- This PoC approach may generate a “Wow” factor among project decision-makers and financiers, which will make it easier to get funding. It may also lead smoothly on to a pilot, in real conditions, in a reduced user population, before a general, managed roll-out.

By using components already used or deployed internally

- It is not rare to be able to pool solutions. For example, when contactless badges are already used for physical access control, for access to the canteen or car park, for instance, it is often possible to use them for authentication on the workstations, in applications, and for logical access control. This might combine contactless identification with a PIN. In this case, the logistics, i.e. the badges, the CMS or the generation and delivery process, is already managed and the only hardware you usually need to acquire are contactless readers.
- It is also possible to assume that everyone has a smartphone; they may or may not come under a company management policy, but solutions using this hardware will be simple to deploy.

By coupling the strong authentication project with an SSO project

- These two projects are very often combined, the first delivering security, the second, ergonomics. See the previous “SSO” sheet for more details.

3 *Which elements need to be taken into account in the project budget?*

Acquisition and recurrent costs differ depending on the authentication technology being deployed. Here are a few examples:

- To deploy chip cards with certificates, you need cards, readers, middleware, a CMS, printers if personalisation is required, a PKI, etc.
- A turnkey SaaS-type solution may be an alternative depending on your capacity to absorb the costs involved, especially operating costs. In the case of RFID or NFC cards, without certificate, you should consider reusing an existing logistics structure: Are badges already used in the company? Does it have a CMS? Etc.
- For a technology relying on an OTP sent by SMS, you need to pay attention to the cost of SMS.
- For biometrics-based solutions, the user registration process can be costly, before you even start to think about sensors. Similarly, some users may not have usable fingerprints. This is true of people working in a medical environment who have been handling corrosive substances for a long time, for example. Alternative solutions may be required.

In fact, whenever you choose to implement a physical medium-based technology, you need to have in place a backup or replacement stock in the event that the hardware proves faulty, or is lost or left at home. Generally speaking, you also need to plan, from the outset, for degraded modes in the event that the main authentication method is unavailable.

Next, you should also bear in mind that a strong authentication project often goes hand in hand with an SSO project. You should therefore clearly set your project's boundaries and ensure that the chosen solutions are compatible with the defined scope (see previous "SSO" sheet).

Lastly, change management should absolutely not be overlooked for users such as administrators.

Appendix 4 presents a summary of the factors to take into account when evaluating one or more authentication technologies.

4 *Key deployment steps – the questions to ask yourself and the points not to be overlooked*

During scoping/kick-off

Particular attention should be paid to a number of points from the outset:

- ensure that the chosen authentication technology or technologies is/are compatible with the different uses within the organisation, i.e. with all use cases for all users;
- ensure that the chosen authentication technology or technologies is/are compatible with the original project trigger: security, ergonomics, cost reduction, or other;
- check that there is no major obstacle, such as statutory data protection constraints, if using biometric authentication;
- plan for degraded modes, in the event of e.g. a lost card, a forgotten PIN or password, a defective network meaning SMS or emails cannot be sent or received, broken or missing hardware, flat phone batteries, etc.
- restate the project scope:
  - in terms of users: all? Just a sub-set? How are they differentiated? Which identity reference bases can be used? *Pay attention to this last point, because if there is no authentication reference base, it may be necessary to create one. See the "Directory" sheet below;*
  - in terms of applications, workstations, and accesses: internal/external?
  - in terms of deployment: establish a restricted scope for the pilot then extend it for example.

During the functional and technical specifications

The following elements need to be defined in particular:

- the process of registering and delivering authentication methods to users;
- the definition of authentication procedures and associated degraded modes.

During the execution phase

No particular special characteristic.

During the acceptance-testing phase

No particular special characteristic.

During the deployment phase

It is preferable to deploy a strong authentication solution iteratively, starting with a pilot phase, on the scale of a department, a unit, or a sub-set of users for instance, taking account of their application scope.

It is also advisable to put in place steering indicators:

- feedback from users: adoption? Rejection? Level of satisfaction?
- helpdesk statistics: assistance, troubleshooting, renewals, etc.

5 *Key points for successful implementation of a project like this*

Some key points:

- bear in mind security AND ergonomics: it is not easy to strike the balance between these two areas, but it is nonetheless essential to do so;
- consider degraded modes and backup solutions in the event of a breakdown of the main authentication method;
- consider all users' uses and ensure that the chosen strong authentication methods are not counter-productive;
- beware of bandwagons and make sure that some apparently very attractive solutions will be sustainable and deliver the required functional and technical coverage;
- pay attention to the hidden costs of strong authentication solutions. Refer back to project budget-related factors above;
- do not overlook user registration phases, or change management, because they can be costly and difficult to manage;
- deploy the solution iteratively, and measure this deployment, adjusting it if necessary.

VI.3. Identity Management

VI.3.1. “Identity Directory” factsheet

“Identity directory”

Budget	Functional complexity	Technical complexity	Lead time	Visibility
★★	★★	★	★	★★★

1 ***Why a project like this? What are the advantages and who are the priority beneficiaries? Which arguments to use to convince senior decision-makers to start a project like this?***

Examples of arguments	*Interlocutor(s) concerned*
• **Architecture of the information system** • build up a single, central and reliable reference base for all other reference bases or applications in the IS; • meet the prerequisites for the implementation of identity-related services: identity and entitlement management – see following factsheets.	CIO IS infrastructure designers Architects
• **Security** • have a central directory to federate identities; • prepare your centralised management of accesses and your authentication directory. See the “Entitlement Management” factsheet and “Access Management” sheets.	CISO CIO
• **User services** • provide users with services like a company white pages directory, organisation flow charts, and the geographical location of employees.	All

Customer scenarios/origins of some projects:

Customer scenario 1: #Federation #Social #GroupIS #20kUsers

- Trigger: Information consolidation needs and necessity to deploy an overarching and consistent service for the various member organisations of the federation.
- Main objectives: Provide unified identity management for all applications in the group IS and common to all entities in the federation, each having between several hundred and several thousand users in their local IS; streamline the directories linked to the group IS.
- Solution: Creation of a central identity reference base providing an authentication service for the national applications in the group IS, and level one entitlement management, delegated administration, automatic population and “white pages” directory functions for the federation.

Customer scenario 2: #Energy #Intranet #300subsidiaries #90kUsers

- Trigger: Activation of the new Group intranet platform.
- Main objectives: Synchronise the data in the Group's directories; manage users' access to the Group SAP project; enable the construction of a Group intranet and an exhaustive Group white pages/yellow pages directory that is accessible to all. This encompasses a broad network of 300 companies and 90,000 employees.
- Solution: Implementation of a consolidated network and single authentication base for Group applications, including the Group intranet portal. This encompasses provisioning, reconciliation, white pages and yellow pages functions.

Customer scenario 3: #PublicInterest #Profession #Regulated #55kUsers

- Trigger: Provision of a unique identifier to the profession, but also to its partners and internet users, and creation of a centralised portal for access to the profession's applications.
- Main objectives: Unify and secure access to application services; have a full reference base of members of the profession; break the existing IS out from its silos; federate and modernise the profession's IT and eventually reach the general public.
- Solution: Implementation of a central identity directory of the profession's users, partners and the general public; a platform for a system of identification and authentication; and a centralised portal for access to the profession's applications.

2 *How to sell the project internally?*

By rapidly developing a suite of value-added services for users or business lines: intranet directory, organisation chart with or without photographs, self-service, etc.

By illustrating with use cases serving a key one-off need or linked to a strategic project.

3 *Which specific elements need to be taken into account in the project budget?*

An identity directory project may come with indirect or peripheral costs depending on the scope of the project and the context in which it is to be installed, as a result of:

- the development of interfaces with the other reference bases for upstream and downstream data population;
- the workload involved in upgrading the data, which may be quite large, demand lots of preliminary actions, and make heavy demands on project owners;
- change management, potentially including abandoning existing reference bases and/or processes;
- rewriting applications to use the new directory rather than existing reference bases.

4 *Key deployment steps – the questions to ask yourself and the points not to be overlooked*

During scoping/kick-off

At this stage it is vital to:

- clearly delimit the target scope in terms of the identities and attributes to be managed in the directory;

- focus on defining the identity identifier with a primary key;
- determine how the identity will be populated and updated: automation, transactions input manually, or other.

On these bases, it is important to identify the component elements of the initial set-up:

- take stock of the various existing reference bases and their use;
- analyse data in terms of quality and meaning;
- identify the authoritative sources for each data item;
- identify processes that consume and produce data;
- identify data owners.

During the functional and technical specifications

Work on data is crucial:

- determine the identifier that will be adopted;
- define and approve the data catalogue, and the attributes;
- define authoritative sources;
- identify owners and stakeholders;
- identify processes;
- define management rules with the stakeholders concerned.

During the execution phase

It is advisable to progress in successive iterations and after each iteration to present mock-ups of data management or publication screens. This allows you to gradually approve development of the solution with the client or the user, and to avoid any tunnel effects.

During the acceptance-testing phase

As we have seen, data are central to this type of project. It is important to work with real-life quality and volumes, to avoid any nasty surprises in these areas during live release.

During the deployment phase

You are advised to start with a restricted scope, or the most visible part of the intended scope, and then to enlarge it later.

It is also important to communicate clearly about the services introduced in the project.

5 Key points for successful implementation of a project like this

Analysis of data, notably their quality and sources, is a critical plank of a directory project. It enables you to determine the scope of data to collect or adjust, and the authoritative sources for these data.

The quality of the data population interfaces is also important, to ensure the integrity of the collected data. Pay attention to the different lifecycles of data over time.

VI.3.2. “User Lifecycle” factsheet

“User Lifecycle”

Budget	**Functional complexity**	**Technical complexity**	**Lead time**	**Visibility**
★★	★★	★★	★★	★★

1 ***Why a project like this? What are the advantages and who are the priority beneficiaries? Which arguments to use to convince senior decision-makers to start a project like this?***

Examples of arguments	*Interlocutor(s) concerned*
• **Security** • provision the identities: create new recruits’ identities, take account of people’s movements and job changes, harmonise data in the various reference bases; • compliance: take account of transfers and departures; • make it easier to perform audits and controls.	CIO Risk and auditing Business lines CISO
• **Return on investment** • reduce administration as a proportion of the overall workload; • replace “paper” forms.	HRM, CFO CIO
• **Infrastructure architecture** • have an updated user directory for reference.	CIO Business lines

Customer scenarios/origins of some projects:

Customer scenario 1: #Housing #HRIS #2000Users

- Trigger: Need to put an end to duplicate HRIS/IS entries.
- Main objectives: Retrieval of HRIS data to take account of events associated with employee lifecycles; automation of network, email and HRIS account creation.
- Solution: Deployment of an identity management solution, with data exchange to retrieve HR events and create user accounts in the HRIS.

Customer scenario 2: #Service #SaaS #5000Users

- Trigger: Upgrades of the IS with a growth in the number of SaaS applications and HR management applications as recruitment and contract termination procedures have gone paperless.
- Main objectives: Elimination of Excel forms; reduction of users’ administrative tasks in several systems; centralisation and improvement of oversight; preparation for entitlement management in a preliminary step.
- Solution: Implementation of a user lifecycle management solution.

Customer scenario 3: #Distribution #3000Users

- Trigger: Modernisation of the IS and automation of staff movements.
- Main objectives: Optimise management of employees' movements within the organisation, a function previously managed using a Notes application; create a unique identifier and put in place an ORBAC model to prepare for entitlement management; put in place automatic provisioning in the main IS reference bases.
- Solution: Implementation of a user lifecycle management solution with a centralised reference base, a process for managing entry/mobility/exit flows, and upstream and downstream provisioning.

2 *How to sell the project internally?*

By highlighting:

- the effective and responsive way in which HR events are accounted for: recruitment, transfer, departure, etc.;
- the reuse of HR data: no entry of the same items of information in different parts of the IS;
- the reduction in input errors, and consequent improvement in data reliability.

3 *Which specific elements need to be taken into account in the project budget?*

Management of the user lifecycle consumes information from the HRIS and other reference bases. Work is needed on data quality to ensure you have a reliable database and that you know the nature, use and meaning of each item of data in the upstream reference bases.

There may be indirect costs as a result of:

- cleaning up data and ensuring it is compatible;
- developing connectors for data extraction with the possible involvement of publishers;
- the supervision of data exchanges and recovery following incidents, particularly if part of the IS is outsourced;
- adjustments to entry/exit/transfer business processes that might not have been covered exhaustively in the first version of the project.

4 *Key deployment steps – the questions to ask yourself and the points not to be overlooked*

During scoping/kick-off

- Examine user lifecycle-related HR processes from all angles. They all need to be listed, even if they are not necessarily all implemented immediately:
  - arrival of internal and external staff, on fixed-term and permanent contracts, of service providers, trainees, temporary staff, or other;
  - change: change of role, structure, name, management, etc.;
  - departure: long-term leave, sick leave, end of assignment, end of service provision, end of procurement contract, etc.
- Analyse the quality of HRIS data: the value of the same data item may vary depending on the meaning attached to it and the context of use: HR, business, etc.

- Construct a reference base or catalogue of process-related data.

During the functional and technical specifications

- Involve human resources in analysis and steering.
- Approve the different processes and flows linked to HR events and identify which players are involved.
- Approve, with the business departments, the catalogue of data items linked to the identities and attributes of the people in the organisation.
- Identify the different possible statuses of the identity – inactive, active, archived – and make arrangements for managing status changes.
- Identify the borderline cases: contract renewals, replacement of staff on sick leave, staff on dual contracts, handover periods, dual registrations, etc.

During the execution phase

- Proceed by iteration as soon as possible to approve the processes.

During the acceptance-testing phase

- Proceed with the processes and scenarios identified during upstream phases, using data identical (in terms of data and volume) to those to be used in production.

During the deployment phase

- If possible, implement a pilot before rolling out deployment, bearing in mind that not all solutions and/or configurations allow this.
- Organise the transfer of information from the field to identify specific scenarios.

5 *Key points for successful implementation of a project like this*

Some key points:

- work with HR on data and processes;
- draw up a data catalogue, and a process map;
- demonstrate the effectiveness, reliability and resource gains;
- acquire the means to steer the delivered service and measure the quality of data provided by the various sources.

VI.3.3. “Entitlement Management” factsheet

“Entitlement Management”				
Budget	**Functional complexity**	**Technical complexity**	**Lead time**	**Visibility**
★★★	★★★	★★	★★	★★

1	***Why a project like this? What are the advantages and who are the priority beneficiaries? Which arguments to use to convince senior decision-makers to start a project like this?***

Examples of arguments	*Interlocutor(s) concerned*
• **Security** • control and track the allocation, modification and removal of user rights in the IS; • produce reports on entitlements showing who has access to what; • monitor the withdrawal of rights and automatically deactivate accounts after the date of the user’s departure; • educate the figures tasked with approving the attribution of rights; • reduce the operational risk associated with using manual processes; • maintain industrial secrecy thanks to the control of rights.	CISO Risk Compliance CIO
• **Audit/Compliance** • satisfy the constraints imposed by internal control, regulators, auditors or other supervisory authorities; • facilitate access certification. See the “Access Certification” factsheet; • enable checks on compliance with the principle of SoD.	CISO Risk Compliance Finance/CFO
• **Infrastructure architecture** • have an up-to-date directory and user reference base; • have a central entitlement reference base for the applications.	CIO IS infrastructure designers Architects
• **Comfort/functionalities/services** • make users comfortable thanks to automated procedures; • manage entitlement for cloud/external applications; • offer a self-service portal for IS application access requests.	CIO Users
• **Return on investment** • improve the effectiveness and reliability of entitlement processes; • automate the provisioning of accounts and rights in the IS; • eliminate processes using “paper” forms.	CFO HRM CIO

Customer scenarios/origins of some projects:

Customer scenario 1: #Finance #Regulation #5kUsers

- Trigger: Overhaul of entitlements management procedures.
- Main objectives: Formalise the entitlements process; appoint IS owners; adhere to the least privilege principle; get a consolidated overview of a person's entitlements; effectively manage employee mobility; ensure the traceability of entitlement management; monitor entitlements; raise the awareness of users and the people involved in entitlement management.
- Solution: Deployment of a central entitlement reference base and application systems; appointment of actors, namely owners and delegates, entitlements coordinators, etc.; definition of procedures and automation; introduction of the rights review.

Customer scenario 2: #Media #Turnover #10kUsers

- Trigger: Need to manage the entitlements of the Group's various users: staff on fixed-term and permanent contracts, temporary staff, occasional workers, interns, external providers, some of which have high staff turnover.
- Main objectives: Make the process of attributing rights to the whole IS simpler and securer; save substantial time administering these tasks; offer new services to users, including self-service; comply with current regulations.
- Solution: Implementation of a solution to manage the user lifecycle and users' entitlements in the IS based on a rights model, with a rights allocation flows process and automatic provisioning to IS applications.

Customer scenario 3: #Housing #HRIS #2000Users

- Trigger: A specific entitlement management tool which is hard to maintain or upgrade.
- Main objectives: Replicate the existing entitlement management scope; abandon forms sent by email; reduce processing times.
- Solution: Deployment of an entitlement management solution in which requests are directly stated and processed, with information retrieved from the HRIS and secondary reference bases.

Customer scenario 4: #Healthcare #Audit #40kUsers

- Trigger: Security audit by the ANSSI.
- Main objectives: Respond to the difficulty of making it possible to audit users' accesses; guarantee that only doctors access patients' records; be able to inform patients reliably of accesses to their records; be alerted in the event of an illicit access to a record.
- Solution: Updating of an entitlements matrix; automation of checks on the consistency of rights allocated based on job; sntitlements matrix management processes; monthly account checks to ensure the system is reliable.

2 *How to sell the project internally?*

Demonstrate the need: carry out an audit of entitlements, even within a limited scope, such as sensitive applications, to show the gaps and the risks.

Demonstrate the return on investment: it generally takes a handful of use cases to identify the cost, lead time and quality drivers.

3 *Which specific elements need to be taken into account in the project budget?*

You need to factor in the following specific costs:

- cost of redesigning applications: for example, for an entitlement management project encompassing implementation of the SoD, if the rights model that operates within applications does not itself comply with the SoD;
- mapping of applications and review of application profiles and job roles;
- change management, notably for figures in the entitlements team or managers who allocate rights;
- costs of a PoC.

4 *Key deployment steps – the questions to ask yourself and the points not to be overlooked*

During scoping/kick-off

- Identify the project sponsor: the project must be led at a high level and must have cross-functional influence: EXCOM, CFO, etc.
- Define the project scope and the deployment roadmap:
    - Which applications? The most sensitive? The most used?
    - Which business lines?
- Identify who will be involved in the project:
    - HR, with a view to raising their awareness;
    - Application owners/managers, the people responsible for allocating rights, the people involved in the allocation process. They are indispensable in data analysis.

During the functional and technical specifications

- To define roles, identify all sources:
    - application managers;
    - process managers;
    - people who play a role in an organisation;
    - people “who know”.
- Use an iterative approach to compare reality with the simulation. At this stage a tool may help you.
- Mix top-down and bottom-up approaches in the analysis.
- Use a mock-up for concrete aspects.

- Carry out a detailed analysis of:
  - data: quality, relations, lifecycle;
  - processes: identify possible cases, even borderline cases, with application managers and businesses.

During the execution phase

Proceed by iteration as soon as possible to approve the processes.

During the acceptance-testing phase

No particular special characteristic.

During the deployment phase

- Implement the model, then deploy in waves or batches: beware of the limitations of some solutions in this respect (see advantages of the PoC).
- Arrange in-depth training for the people tasked with rights allocation and provide support.
- Have a steering committee monitor the progress of deployment.
- Organise the feedback of information from the field to identify special cases that might not have been reported in the analysis and anomalies or stumbling blocks to correct them.

5 *Key points for successful implementation of a project like this*

When managing the project, you need to:

- have a good project sponsor and pilot;
- involve business lines from the start of the project;
- involve HR as part of an awareness-raising campaign;
- work quickly on actual/field data;
- validate the quality of data, their consistency, the links between the various existing reference bases.

Remember to batch and deploy your project in waves, and in so doing:

- prioritise applications according to the maturity of the business line and the uniform use of the application scope;
- emphasise applications that are strategic from the point of view of visibility or high entitlement management activity in order to achieve quick wins.

Lastly, when choosing a solution, you are advised to:

- establish a PoC first to validate the operating principles, and the intrinsic possibilities of the solution: connectors, deployment procedures, process personalisation, etc.;
- agree to be supported to avoid pitfalls.

VI.4. Identity and Access Governance

VI.4.1. “Entitlements Reviews / Access Certification” factsheet

“Entitlements Reviews / Access Certification”				
Budget	**Functional complexity**	**Technical complexity**	**Lead time**	**Visibility**
★★	★★	★	★★	★

1	***Why a project like this? What are the advantages and who are the priority beneficiaries?*** ***Which arguments to use to convince senior decision-makers to start a project like this?***

Examples of arguments	*Interlocutor(s) concerned*
• **Security/reduction of operational risks** • remove orphan accounts; • check that the accounts of people who have left the company are actually closed; • check that each person does have the minimum rights needed for the IS; • check rights to generic accounts and that they are matched with physical people; • check, for each application and each resource, that only authorised people can access them, in accordance with their jobs.	CISO Internal control Risk
• **Audits by regulators or other supervisory authorities** • provide evidence of Access certification; • provide evidence of follow-up of the post-review action plan.	CFO CEO
• **Anti-fraud** • ensure that individuals do not hold multiple toxic rights.	CFO Risk
• **Costs** • reduce the cost of application licenses by ensuring that unnecessary accounts are removed.	CIO CFO

Customer scenarios/origins of some projects:

Customer scenario 1: #finance #security #>5kUsers

- Trigger: Regular audits of the parent company.
- Main objectives: Save time on Access certification and responses to audits, manage entitlements.
- Solution: Kick-off of a full IAG project including the review / certification of identity and access management processes, but also implementation of an entitlements review module.

Customer scenario 2: #energy #compliance # >40kUsers

- Trigger: Audit by official auditors.

- Main objectives: Manage entitlements and avoid combinations of toxic rights (SoD - Segregation of Duty) in the finance IS.
- Solution: Deployment of a system for checking entitlements and toxic rights in the finance IS.

Customer scenario 3: #insurance #security #>5kUsers

- Trigger: ISO 27001 certification.
- Main objectives: Produce reports on Access certification of the identified sensitive assets scope and follow up the corrections actions plans.
- Solution: Deployment of a system for checking entitlements for accessing all sensitive assets with Access certification conducted both on an organisational level and in terms of assets; acquisition of a market solution to perform the Access certification.

Customer scenario 4: #bank #security #>2kUsers

- Trigger: Audit by official auditors and audits of the parent company.
- Main objectives: Manage entitlements; avoid combinations of toxic rights to access all sensitive assets; enforce the SoD.
- Solution: Deployment of a system for checking entitlements across the whole organisation for the most sensitive assets; acquisition of a market solution to perform the Access certification.

Customer scenario 5: #service #security #>20kUsers

- Trigger: Analysis of risks and decision to reduce operational risks.
- Main objectives: Carry out Access certification of privileged accounts, across all organisations and of assets regarded as sensitive.
- Solution: Deployment of a system for checking entitlements for accessing all sensitive assets with Access certification conducted both on an organisational level and in terms of assets. Acquisition of a tool for part of the Access certification with the eventual aim of replacing manual Access certification.

2 How to sell the project internally?

By carrying out a flash audit

- Demonstrate in a handful of days that it is possible to quickly produce the list of orphan accounts, of people who have the most rights, or of people in finance who have privileged rights. This will raise awareness among the main stakeholders.
- In the context of such a flash audit, it is vital to have raw extractions from the entitlements bases and from an identity reference base – an HR file, external staff file, etc. – so that the results are significant and speak for themselves.
- The flash audit also provides ready-to-use reports for the various populations: auditors, asset managers, company managers, etc.

By highlighting the operational gains

- The Access certification and the follow-up of action plans are often time-consuming for the people involved: managers, asset managers, review leaders, the person responsible for corrective actions. Highlighting the operational gains made by the new tools is one of the most widely used arguments.
- Market tools can offer users an intuitive interface which reduces the time it takes to carry out Access certification and also improves their quality.
- Sometimes, by organising Access certification carried out manually here or there and improving the “manual tools” available, e.g. Excel or Access, you can also achieve significant operational savings.
- Providing a 360° overview of all entitlements belonging to all users can also enable operations teams covering the helpdesk, infrastructures or applications to troubleshoot more effectively.

By calculating the ROI from the licenses saved

- Very often, audits of licenses held with IT departments reveal that solutions are more heavily used than they should be because access privileges are too widely held or not removed. In some cases, putting in place a system for checking assets with high license costs can lead to a financial saving in the medium term. However, this is not true in most cases.

3 Which specific elements need to be taken into account in the project budget?

As well as implementing processes and any tools, which will usually generate project CAPEX and OPEX when operating the service, this type of project can give rise to very specific costs:

- Entitlements documentation: there is no point asking to review accesses that are not comprehensible to company managers or asset managers;
- constructing and maintaining an SoD matrix: SoD is not always within the scope of this type of project. But if it is, this activity demands considerable resources to implement and keep in an operational condition;
- standardisation of extractions: the regular generation, whether manually or with tools, of extractions to populate the solution can be a significant cost centre. The reproducibility and integrity of the extractions are two crucial points. The complexity of the extractions varies depending on the type of review system: AD, Mainframe, RACF, SAP, etc.;
- appointment of business managers or asset managers: there can be no certification campaign without a review manager, whether the review is of an organisation or of assets. Depending on the maturity of the organisation, it can be difficult to identify some actors in order to carry out an effective review;
- change management: deployment of a review system means having people perform activities linked to these Access certification. These people need to be trained, whether for the Access certification themselves, or for the ensuing corrective actions.

4 *Key deployment steps – the questions to ask yourself and the points not to be overlooked*

During scoping/kick-off

It is crucial to define a limited scope, especially for a first iteration, so that you have the means to start the project, see it through, and be able to deal with the resulting action plans and corrective actions.

Scoping should define:

- the scope of applications and resources;
- the scope of organisations and users;
- the desired level of granularity for the Access certification: accounts, profiles, fine-grained rights;
- the people involved in the Access certification;
- the consumers of review-related activities.

In addition, it is important to distinguish between regular checks and surveillance, against fraud at a moment in time T for example, in the scoping phase to avoid any project creep.

During the functional and technical specifications

It is advisable to arrange workshops focusing on specific topics, and then on application types and resource types:

- functional workshops: user use cases, data access procedures, visible reports, review procedures, types of Access certification, quality controls, compliance checks, etc.;
- technical workshops: overall architecture, storage, backup, archiving, etc.;
- identity and organisation reference bases: sources of data, processing and reconciliation rules;
- applications and resources: connection type, via file or connector, automatic or manual corrections, data model, reconciliation rules, etc.

During the execution phase

It is essential that these key steps are a success during the execution phase:

- quality of the identity reference base: the cornerstone of account and credential Access certification;
- quality of the organisation reference base: essential for Access certification from an organisational perspective;
- quality of the asset manager reference base: essential for Access certification of individual assets or asset types;
- quality of reports, before getting started on compliance reports;
- quality of reconciliation rules and manual finalisation;
- addressing SoD only when the “basic” quality and compliance reports are validated.

And also:

- work in order: quality of identities, of applications, of accounts, of fine-grained rights;
- bear in mind that the sensitivity level of applications varies;
- anticipate rejection levels and reconciliation difficulties, and the time that this takes;
- work on improving data quality;
- work in batches and iteratively.

During the acceptance-testing phase

The acceptance-testing phase often entails checking hundreds or thousands of items of data. It is therefore essential to carry out an acceptance test per batch:

- verification of identity data;
- verification of asset data: at least one report per asset to be validated;
- verification of reconciliation rules: bad reconciliation rules will give rise to erroneous Access certification;
- verification of quality reports;
- verification of compliance reports;
- verification of data accesses.

During the deployment phase

During the deployment phase it is often necessary to reuse manual reconciliations carried out during the execution or acceptance-testing phases in order to avoid discrepancies and double workloads.

Deployment as such does not require any special attention, with the exception of rights to data. Implementation of an initial review, however, should be handled carefully, taking account of change management and the involvement of a range of actors.

5 Key points for successful implementation of a project like this

Start “small and simple”: once the model and basic system are constructed, the application scope will be enlarged, as will the number of reports. Each report entails work on correcting data when it is used.

VI.4.2. “Role Management” factsheet

“Role Management”				
Budget	**Functional complexity**	**Technical complexity**	**Lead time**	**Visibility**
★★★	★★★	★★	★★★	★★

1	***Why a project like this? What are the advantages and who are the priority beneficiaries? Which arguments to use to convince senior decision-makers to start a project like this?***

Examples of arguments	*Interlocutor(s) concerned*
• **Security and reduction of operational risks** • ensure simply that, for a given function, only the necessary rights are attributed: addition of one or more roles corresponding to the function; • ensure that old rights are withdrawn in the event of a transfer.	CISO Internal control Risk
• **Audits by regulators or other supervisory authorities** • have well-argued documents presenting existing roles: validators, content; • comply with some audits that simply specify “put in place role-based management”, which can be arguable because it amounts to more of a means than an end.	CFO CEO
• **Anti-fraud** • an SoD matrix based on roles is generally easier to maintain than a matrix based on fine-grained rights.	CFO Risk
• **User experience** • simplify the rights allocation and removal process; • simplify operational access certification / review tasks; • avoid operators and users having to know all roles.	Users

Customer scenarios/origins of some projects:

Customer scenario 1: #insurance #security #>5kUsers

- Trigger: Audit by a regulatory authority.
- Main objectives: Improve the entitlement management.
- Solution: Design of roles based on interviews with the businesses and supported by the acquisition of relevant tools, then integration of roles into the tool-based entitlement management processes. A pilot phase in one department is carried out before organisation-wide deployment. The roles are managed by the IT department.

Customer scenario 2: #bank #security #>2kUsers

- Trigger: "P1" recommendation in an audit.
- Main objectives: Improve the entitlement management.
- Solution: Design of roles based on interviews with the businesses and modelling aided by an IAG tool; deployment of the IAG solution with the following functionalities: role management, Access certification, SoD, then extension to provisioning and identity management. The roles are managed by the IT department.

Customer scenario 3: #service #security #>20kUsers

- Trigger: Make it easier to process entitlements requests.
- Main objectives: Reduce the time taken to process entitlements: additions, changes and withdrawals.
- Solution: Design of roles based on interviews with the businesses and modelling aided by an Excel tool; deployment of the IAM solution with personalisation of interfaces to handle role management. The roles are managed by the businesses.

Customer scenario 4: #bank #security #>3kUsers

- Trigger: Make it easier to process entitlements requests.
- Main objectives: Compliance of entitlements and operational effectiveness.
- Solution: Design of roles on the basis of interviews with the businesses and modelling aided by an Excel tool. Deployment of the IAM solution with personalisation of interfaces to handle role management. The roles are managed by the businesses.

Customer scenario 5: #healthcare #security #40kUsers

- Trigger: Certification of accounts.
- Main objectives: Prove that roles are well founded and get project owners to validate content.
- Solution: Design business need-based roles with standard construction and structures; make it easier for all actors to understand and change them; Excel tool, process of validation by the businesses.

2 How to sell the project internally?

The deployment of role management is definitely the hardest IAM subject to sell. Its ROI is always a matter for debate.

The question to ask yourself is: "Will the time wasted managing and maintaining roles really save time and improve the quality of the attribution of entitlements?"

The answer depends on various factors, including the type of organisation concerned, the governance implemented and the chosen roles model. In practice, the real ROI can only be calculated after several years in operation.

When deployment of role management proves genuinely necessary, the key factors may include:

- highlighting of the contribution made by role management to businesses for the adoption of an IAM/IAG solution;
- easy scalability and understanding of rights;
- demonstration of user interfaces and management of entitlements made easier by the use of roles;
- demonstration of the simplification of the SoD matrix;

- identification of operational gains and calculation of ROI: time saved managing attributions compared with time spent managing roles.

3 Which specific elements need to be taken into account in the project budget?

The initial modelling of roles across an entire scope is usually costly and requires numerous contacts with the business. It necessitates wide-ranging knowledge of the organisation.

Implementation of role management without tools is generally doomed to failure because it is complex to maintain. A specific set of tools should therefore be identified.

Roles should be reviewed regularly so that they fit the businesses and adapt to restructurings. This “remodelling” may be time-consuming, but it is essential. It often means reviewing roles with the businesses and involving people who have experience in this type of exercise and cutting-edge expertise.

4 Key deployment steps – the questions to ask yourself and the points not to be overlooked

During scoping/kick-off

Scoping of role management must answer the following questions:

- Which modelling of roles to carry out? RBAC? ABAC? OrBAC? etc.
- What organisation and which processes should be used for role management?
- What are the organisational and application scopes to be covered? What is the roadmap?
- Should IT staff be involved in role management?
- Which tool(s) to use and which ones are impacted?
- Modelling of roles often reveals anomalies in the applications to be integrated. In this case, what is the plan for addressing them?

During the functional and technical specifications

It is advisable to work entity-by-entity when modelling roles. For each one, a set of roles must be defined and compared with the reality of the entitlements reference bases.

All processes and user interfaces relating to roles must be meticulously described.

During the execution phase

For each scope, it is a good idea to adopt an iterative approach to modelling roles:

- interviews with the businesses;
- identification of theoretical roles based on analysis of the organisation and of functions;
- identification of operational roles through the analysis of entitlements data relating to each situation;
- modelling of a first version of the roles;
- validation with the businesses and any adjustments.

Once the roles models are defined, documented and instantiated, they must be integrated into the operational workflow processes of a technical solution.

During the acceptance-testing phase

The acceptance-testing phase must be as close as possible to production, using a real volume of data in order to assess the impacts on production. Acceptance-testing based on a partial dataset would be catastrophic.

You should therefore put in place an acceptance-testing environment that is identical to production in terms of the population scope and the entitlements to be covered.

During the deployment phase

Deployment of role management must be carried out in batches so as not to disturb users. Otherwise, you need to provide a completely new solution equipped with entitlements management.

5 Key points for successful implementation of a project like this

Some key points:

- work iteratively;
- provide strong support;
- do not underestimate the internal and external costs of implementing role management and maintaining it in operational condition.

VII. After the project

While a well-executed IAM project is often underpinned by high quality specifications, an IAM project “in good health” generally reflects faultless organisation and segregation of duties. Indeed, such a project does not stop the day after live release. Overlooking the importance of the post-project phase will hinder the success of the project and undermine user satisfaction with the implemented solution.

While the solution is in place, it must be maintained and adapted to the various changes in the company, whether technical or organisational changes. This is a new step in the lifecycle of the solution: “recurrent mode”. The transition from project mode to recurrent mode poses new challenges for the company. We will summarise these changes in the remainder of this section, and then focus on the question of the ROI of IAM projects.

VII.1. The challenges of recurrent mode

After the live release of an IAM solution, a number of events may make it necessary to modify it.

Changing application scope

In recurrent mode, you should consider the constant addition of applications to the scope of the IAM project. In the initial phase, a number of applications were integrated. If the solution deployed provides satisfaction, other applications may be integrated thereafter. It is essential to describe the application management process, and, ideally, appoint an in-house manager to oversee this process.

Changing accreditations

An application's fine-grained roles may be amended, and job roles may change. These changes need to be adapted to. Keeping the roles and accreditations matrix updated ensures, at any given moment, that the theoretical access model matches the practice.

Corporate restructuring

Companies are always evolving. A restructuring, whether in-house or as the result of a merger, means adapting the IAM solution. For example, the reorganisation of business units or the addition of new sites can make it necessary to update roles and the rights matrix. In some cases, these changes can be wide-ranging. If the organisation is very agile in this respect, the scalability criterion should be a key factor when selecting the solution.

Changes to the HR IS

As the HR IS is very often the main reference base underpinning the IAM solution, changes like technology upgrades, the activation of additional modules or the management of an additional population of users in the HR IS must be accompanied by suitable changes in the IAM solution.

Changes to applications within the scope

If an application within the scope migrates to the SaaS/Cloud or a new version is integrated, this will have an impact on the IAM solution deployed. Changes will be necessary, especially to adapt provisioning of the application or to adapt the SSO solution.

Version upgrades of the solution

The publisher of the solution releases regular version upgrades to correct the application's limitations, factor in the latest security recommendations, or update the application's components. A version upgrade plan must be drawn up taking account of who does what and at what intervals. The cost of doing this can be evaluated ahead of time.

OS migration

The IS infrastructure may also evolve, in part or more comprehensively. This can raise various questions: can the server(s) on which the solution is installed be migrated? How will the solution be impacted by the OS migration? Are inter-machine flows maintained? This does not necessarily and only concern server infrastructures: in the case of an eSSO project, for example, it is the migration of the OS running on workstations that can have an impact on the solution.

Operating incidents

Whatever the quality of the work carried out during the project phase, the risk of an operating incident can never be completely ruled out. Once the origin of the incident is diagnosed, the necessary corrective actions need to be taken. In general, this aspect of the post-project phase is relatively well prepared for and handled in the context of MCO.

In summary

Recurrent mode can raise several questions. During the project phase, a team was put in place, generally made up of in-house staff and providers, including integrators.

During the post-project phase, new responsibilities need to be defined: which in-house team manages recurrent mode? If it is not the project team, skills transfer will have to be addressed. What changes can be managed in-house? What changes require the intervention of experts in the solution? What are the respective roles of the integrator and the publisher in recurrent mode?

Ideally, recurrent mode should be prepared for during the project phase. It is particularly crucial to consider, from the outset, which types of changes might happen in the post-project phase. During the integration phase, this helps to make the solution more flexible, at a time when future changes are being considered. Sometimes, if the possible changes are substantial, it may even be worthwhile considering these issues as early as the solution selection phase.

VII.2. What is the ROI of an IAM project?

When an organisation green-lights an identity and access management project, its goals are usually to secure its information system or to improve the user experience for its staff. The project is viewed as a cost centre, to be balanced against the expected benefits. However, an identity and access management project also helps to cut some of the company's operating costs and the initial investment can be turned to profit quickly. In the remainder of this chapter, we will expand on the answer to the following question: **What savings does an IAM project deliver and how do you calculate the return on investment (ROI) of an IAM project?**

VII.2.1. ROI of an IAM project

Return on investment is defined as the ratio expressing the net benefit of an initial investment in a project relative to its initial cost:

$$ROI = \frac{(Investment\ gains - Investment\ costs)}{Investment\ costs}$$

NB: It is also possible to seek to estimate the return on investment period, before a project begins, i.e. the time needed for the gains from the project to exceed the initial investment.

In the context of an IAM project, the costs comprise mainly:

- the costs of buying software and integration costs, which are one-off costs at the outset of the project: BUILD phase;
- the annual infrastructure and software maintenance costs, support costs and the project upgrade costs: RUN phase.

Because of the automation of some processes, it is legitimate to expect an IAM project to generate savings.

- Identity management project – automated management of IS user transfers:
  - reduction in the number of manual actions needed;
  - reduction in the number of errors during execution of the various processes.
- Access management project – one-time authentication:
  - reduction in the number of manual entries of passwords;
  - reduction in the number of passwords staff need to know, so reduction in the number of password resets.

VII.2.2. Automated management of arrivals/departures/transfers

The automation of management of staff arrivals, departures and transfers helps to reduce the time taken to process requests and therefore to cut the associated operating costs.

The arrival, transfer and departure of a member of staff requires a certain number of operations: for example, his/her account needs to be created, amended or deleted in the central HR software, or in the company's directory or directories. His/her email account needs to be created or deleted, rights need to be given to him/her or removed from him/her in the company's applications, etc.

Without identity management, most of these actions have to be performed manually. IAM aims to automate these actions as far as possible. In an ideal scenario, when a member of staff joins, HR will still manually create his/her account in its HR software, but then the user's accounts and rights will be managed automatically[1].

The gains expected from deploying an identity management project will thus depend on the degree of process automation on the reduction in the number of actions to perform when a member of staff joins, leaves or transfers, in the average time per action, in the hourly cost of work, but also in the number of procedures needed, in other words those relating to staff turnover, internal mobility, the external provider usage policy, and the company's growth.

Moreover, each manual action carries a risk of error. By automating processes with an identity management project, the number of manual actions to perform falls, and with it the number of potential errors and the costs that these actions entail.

Finally, the automation of procedures reduces the time needed for staff to obtain accreditations and therefore boosts their productivity when they join or transfer.

[1] *In practice, it is not uncommon to still have some manual actions to carry out, in the case of applications that do not lend themselves to automatic provisioning for technical or functional reasons. Project managers will therefore have to make a judgement between the cost of implementing automatic provisioning and the cost of retaining manual provisioning.*

VII.2.3. One-time authentication (SSO)

Deploying a one-time authentication solution allows you to reduce the number of passwords users have to remember, and therefore reduces the number of password reset requests. According to a *Forrester* study *("Use Commercial IAM Solutions to Achieve More Than 100% ROI Over Manual Processes",* by Andras Cser, October 1, 2012*)*, users forget their passwords on average four times a year. When a password is reset, this entails not only costs for the helpdesk responsible for resetting it, but also a loss of productivity for the member of staff waiting for his/her new password.

One-time authentication also means that users no longer have to enter their login and password in each application, and can instead enter them only once. This generates an average daily time saving of 9.51 minutes per user, according to a *Ponemon Institute* study *("How Single Sign-On Is Changing Healthcare - A Study of IT Practitioners in Acute Care Hospitals in the United States*" - June 2011)

VII.2.4. Overview and limits on ROI

When a company considers implementing an IAM project, it weighs up the benefits it will gain from it in terms of security and the user experience. Financially, it estimates the cost of the project depending on the chosen solution, in terms of the cost of licenses, support and integration. But it will often forget to take account of the financial gains that the project will help to generate. Factoring in these gains, the ROI period looks much shorter. Depending on the company's characteristics, the project will potentially be profitable in the years immediately following implementation.

But there are limits on calculating ROI:

- From an economic perspective, the costs and benefits do not generally come in the same period, and it may be a good idea to convert the different values to present worth. This updating reflects a preference for the present and risk aversion. To convert to present worth, you can calculate the project's Net Present Value (NPV).

- ROI is a decision-support tool. It is calculated before the project begins, based on estimated gains – reduction in the number of calls to the helpdesk, reduction in the number of manual actions needed when a member of staff joins – and on the cost of licenses and integration days. But there is always a difference between the anticipated solution and the implemented solution: the number of applications may change, as may the integration time, depending on difficulties encountered, the project's specific features, the client's environment, etc.

- Few organisations will actually know the cost to them of all the manual actions they need to perform when a member of staff joins or when somebody calls the helpdesk, except perhaps when they have outsourced the helpdesk. Not knowing the initial cost of these operations, they might not be receptive to the argument that savings can be made in these cost items.

- Little data is available on the costs that the actions described above account for. Estimates can vary significantly from one source to the next. This has an impact on the evaluation of ROI, and can undermine its credibility in the eyes of some. It may be worthwhile gathering data and putting in place indicators to estimate the time it takes to process an arrival (user lifecycle management), the frequency of calls to the helpdesk associated with password reset requests (self-service SSO), the number of password entries per day and the time spent (SSO), the number of accesses to particular applications (access control), and so on.

Lastly, you should bear in mind that ROI is only meaningful if your audience is receptive to it, and that the ROI tool many only be worthwhile using if the gains, or “non-expenses”, are very precise, including the saving made on licenses for particular applications, the reduction in helpdesk costs in the event that this service is outsourced, etc. Similarly, and looking beyond productivity, we should not forget that IAM solutions are also a means of improving security, and therefore of limiting the financial risks that might arise.

VIII. Conclusion

The members of the CLUSIF working Group wanted to make their contribution to the world of IAM by providing, with this document, help implementing all or part of an identity and access management/governance project.

While the arguments in favour of IAM are widely accepted, implementation still remains a complex process. This document thus aims to provide support in this area, asking the right questions and providing broad responses.

Naturally, we had to make choices. One of these was to focus on the fundamentals and not to cover some technical or related subjects.

Once these fundamentals are implemented, it will probably be easier to address other subjects, such as managing identities and accesses for clients, or the management of connected objects.

"The most solid stone in the structure is the lowest one in the foundation"

Khalil Gibran, poet, 1883-1931

IX. Appendices

IX.1. Glossary

The glossary below supplements chapter “*II. Fundamental Principles of IAM and IAG*”, and is designed to shed light on a number of concepts used in this document.

It may also provide the basis for an internal glossary when launching an IAM/IAG project (see chapter “*IV.3 A few tips before getting started*”).

It does not provide definitions in the academic or literary sense, the aim being instead to explain simply and pragmatically the terms used in this document. The explanations given are deliberately concise, as readers can find out much more at their leisure about any of the concepts rapidly outlined here.

Please also note that this glossary only contains descriptions of terms used in IAM/IAG. This is to try to limit the size of the document. Similarly, we did not redefine concepts already explained in the document, notably those already defined in chapter “*II. Fundamental Principles of IAM and IAG*”.

The following concepts are described:

Terminology	Description
ABAC	*(Attribute-based access control)* An access rights model whereby rights are granted based on the person's attributes.
Access certification (process of)	Process which aims to revalidate or reconfirm an item of information. There are several recertification processes: • team certification, designed to confirm the links between managers and their reports; • certification of providers, designed to confirm the presence of providers; • certification of entitlements, designed to confirm the relevance of attributed Entitlements. Access certifications are usually conducted in the form of campaigns, with an opening, a period of review, and a closure. These campaigns may be one-offs, or conducted at regular intervals.
Access control	Process whereby an applicant's access to a resource is authorised or blocked based on that person's identification, authentication and entitlements. Several levels of access control can be identified: • logical access control: yes/no access to an application involving no check of rights; • logical authorisation control: finer-grained control checking that the user has the necessary rights for the requested action; "physical" access control: to buildings, car parks, secure rooms, etc. (This aspect is not covered in this document).
Account	Digital definition of a digital identity in an application or system within the IS. This account is often associated with an authenticator and a set of rights and technical data. It is therefore a technical concept. Generally speaking, there are several types of account: user account, test account, generic account, service account, training account, etc.
Application role (or profile)	Usually corresponds to a group of rights to a single application. An application role (or profile) has a set of attributes specifying the definition of the application role. A context can be defined to specify the remit of the role, such as a scope or a validity period. An application role is often

	attributed to login profiles, and an application role can belong to several business roles (or profiles).
Attribute	Defines a property of an object. For example, a person has a first name and a surname. An organisation is defined by a code, a display name, a description, etc.
Business role (or profile)	Corresponds to a group of application roles. A business role (or profile) has a set of attributes specifying the definition of the role. A context can be defined to specify the remit of the role, such as a scope or a validity period.
CAS	(*Central Authentication Service*) Denotes both an open source software package and protocol which provide an SSO service for the web.
Circle of trust	In the context of federated identity management, defines a space in which several providers ("identity providers" (IdP), "service providers" (SP)) have agreed on operating rules for federated identity management.
Credentials (secondary)	For an eSSO solution, defines the users' login/password combinations that will be authenticated by the eSSO engine in the application windows covered by the solution. The term "accreditation" is also used.
Delegation	Action whereby a task is entrusted to one (or more) other person(s) – the delegate(s) – although this does not absolve the delegator of his/her responsibility. In general, a delegation has a start date and an end date.
Dormant account	Account existing within an application but not used by its owner. Generally, an IAM policy rule specifies the criteria defining a dormant account. For example: any account associated with an identity that has not been used for over 6 months. This concept of "dormant" may also be extended to the concept of a right: a dormant right is thus a right held by an account but unused by its owner.
Entitlement	Right to access a resource.
Exceptional right	Right granted to a user outside the rights model. Exceptional rights can be granted temporarily and can be deactivated.
FIDO	*(Fast IDentity Online)* International alliance of organisations defining strong authentication standards.

HR reference number	This is an employee's “HR” identifier in the HR IS. Therefore, only employees have an HR reference number. In some specific cases, a person’s HR reference number may change. This happens when legal entities merge, for example. A person may also have several HR reference numbers when s/he has several employment contracts. It is therefore not recommended to use a person’s HR reference number as his/her unique identifier or login, even within the employee population. Nonetheless, as HR systems are very often authoritative sources for IAM systems, the HR reference number may be used as a reconciliation key between IAM and the HR IS.
Identification (process of)	Process whereby the identity of a resource is recognised.
Identity (digital)	Digital representation of a (natural or legal) entity in the IAM reference base, and more broadly in the IS. In general, a digital identity is made up of: • a unique identifier; • all the attributes that characterise that identity; • all the technical information needed for the proper use of that identity in the digital world. Except in exceptional cases, a single person or thing has a single identity, and one identity corresponds to a single person or thing.
Identity Provider	(In the context of federated identity management – see chapter II.4.3.) An Identity Provider (IdP): • guarantees the user authentication solutions used to grant access to the services available within the circle of trust; • transmits identity information as defined in an initial agreement; manages and supervises outbound accesses to available resources.
LDAP	*(Lightweight Directory Access Protocol)* Originally designated a directory query protocol. By extension, an LDAP is a technical component enabling data to be stored in a hierarchical and standardised way.

Least privilege	Principle whereby only those privileges that are strictly necessary are granted, and no more.
Login profile	Represents the digital identity and enables access to the Information System. It has a unique identifier which may serve as a login. • one login profile corresponds to a single digital identity; • one digital identity may correspond to several login profiles; • different roles may be attributed to each login profile. For example, an identity may have a standard login profile for everyday activities, and an administrator login profile for more sensitive activities.
OAuth	Designates one of the standards used in federated identity management.
OpenID Connect	Designates one of the standards used in federated identity management.
OrBAC	*(Organization-Based Access Control)* Access rights model in which rights are granted on the basis of roles and on the basis of belonging to one or more organisations.
Orphan account	Account no longer attached to a company identity. An orphan account may result from an accreditation process that has not yet begun or a process of removing all its entitlements.
OTP	*(One-Time Password)* Single-use password which is generated dynamically based on a temporal or sequential reference, and which is renewed after each authentication.
Permission	Fine-grained right to a resource, which may be “read”, “write”, etc.
Person	Digital definition of a human entity in an authoritative business reference base other than the IAM reference base, such as the human resources database for employees, the customer database, etc. The definition given in the old CLUSIF document makes no distinction between a “person” and an “IS user”, or between a “person” and an “identity”. Given that a person has to have a human and natural character, “person” here refers to an individual. And given that behind a legal person there must

	always be at least one natural person, such as suppliers or partners, the notion of a legal person does not apply in the context of IAM. It therefore falls outside the scope of this document.
Privileged account	Account having entitlements to access sensitive information or enabling the account to perform sensitive technical and/or functional operations. For example: administrator account, "root" account, server operator, etc. Usually, this concept refers to technical accounts, in IT infrastructure components, and excludes accounts in applications having a very high level of authorisation, such as "SAP_ALL".
RBAC	*(Role-Based Access Control)* An access rights model whereby rights are granted on the basis of roles.
Reconciliation	Operation whereby information, such as accounts or rights, relating to a resource, is read and reconciled with information in the IAM system, such as identities or entitlements.
Resource	Hardware or software element of an information system that can be used by different users. It corresponds to the type of target: a resource is usually software (AD, SAP, Google, etc.) but can also be hardware (means of authentication, telephone, access badge, etc.).
Right	Corresponds to an entitlement or disentitlement to access/use a resourceor a component of a resource. Usually, although this definition does not apply in all cases, a right denotes the finest-level authorisations in applications. A right may therefore belong to several roles or application profiles in general.
SAML	*(Security Assertion Markup Language)* Designates one of the standards used in federated identity management.
Service account	Account used on a system so that a process or an application can be run. A service account is not intended to be used by a human being with the exception of some administration actions.
Service Provider	(In the context of federated identity management – see chapter II.4.3.) A Service Provider (SP):

	• makes resources or Web services available; • validates the information transmitted by the IdP and manages the federated identities: privileges and authorisations, attribute updates; • propagates information to target services; supervises the actions performed in the accessed services.
SoD	*(Segregation Of Duty)* The SoD specifies the incompatibility of roles. Roles may have several levels of incompatibility, such as: • it is not possible to apply for two incompatible roles: either they are not visible together, or the application is automatically rejected; • the application for two incompatible roles triggers a specific validation process; the application for two incompatible roles is approved but it is labelled as needing specific monitoring, such as recertification at regular intervals.
Thing (IoT)	Digital definition of a non-human entity in an authoritative business reference base, other than the IAM reference base, such as the vehicle reference base.
Unique identifier	Unique code which references an object unambiguously. Best practice stipulates that a unique identifier must also: • be invariable over time; • not carry information; • fall under a single responsibility or authority, or at least within a defined scope. The primary purpose of a unique identifier is to be a join identifier, known at least to IAM. Ideally, it should also be entered in an attribute of each user account. By extension, and without obligation, it can also use serve as a login.
User account	Account attributed to any IS user. Unlike a service account, a user account is attributed to a person.
WS-Federation	Designates one of the standards used in federated identity management.

IX.2. "IAM specifications" document

This appendix supplements question "Q7: Which elements must not be overlooked in my specifications?" and proposes an example of a possible "standard table of contents" for a specifications document. The idea here is to stress all the sections to be included.

1. Introduction
    a. Purpose of the document
    b. Context of the document
    c. Project challenges
2. Existing arrangements
    a. Organisation and process
    b. IS
        i. Users and uses
        ii. Infrastructures
        iii. Applications
3. Needs
    a. Functional requirements
        i. Identity management
        ii. Entitlement management
        iii. Authentication
        iv. SSO
        v. Access control
    b. Technical requirements
        i. Security
        ii. Infrastructure
        iii. Quality of service
    c. Target functional architecture
    d. Constraints/Specific features of the context
4. Documents to be delivered
    a. Services
    b. Tools
    c. Deliverables
    d. Timetable
5. Response options

IX.3. SSO datasheets

The elements below can be used during the SSO project scoping and planning phase, or during specifications workshops. They enable you to identify all the information needed to integrate applications into the project, and make this integration easier during the execution phase. Ideally, you should fill in, get others to fill in, or seek help filling in one sheet per application. As the information will differ depending on the nature of the project (eSSO/WebSSO/Federated Identity Management), these sheets address general information and then information specific to each of these SSO methods.

IX.3.1. General information

Question	Answer
Application name/reference	
Description of the application	
Publisher of the application + contacts	
Date sheet was created	
Date sheet was edited	
Sheet author	
Type of application (Thick Client/Thin Client/Web)	
Level of availability?	
Does technical documentation exist for this application?	
Availability of a test environment for this application?	
Availability of test accounts for this application?	

IX.3.2. Questions specific to eSSO (enterprise SSO)

Question	Answer
Type of application: • Windows • DotNet or Accessible or Console • Web (+ browsers used) • AS400/ehllapi (Emulator) • Java • Other?	
Type of window to be registered: • Authentication • Authentication error • Change of password • Change of password error	

• Other?	
Attributes to be managed (+ type): • Login (“simple text” syntax) • Password (“password” syntax) • Others: domain, email, role (e.g. list, boolean, etc.)	
Does the application have a particular password policy? Does this policy need to be overloaded by the eSSO solution?	
Is the application's user reference base identical to the main reference base (e.g. AD, Primary LDAP)? If not, what is it?	
Can users have several accounts in the application (multi-account: user, administrator, etc.)?	
Does the application include a password change interface?	
Does the application have to be run automatically upon the user's arrival?	
Does the application have to be interrupted when there is a change of user? (This is true in “kiosk” or “shared” mode.) Does it have “fast user switching”?	
Can the application be run several times in a single Windows session? (This is true of “multi-desktop” mode.)	
Can the user start the application from the eSSO client?	
Does the application require primary reauthentication? (Sensitive application.) Using which authentication method?	
Does access to running the application need to be protected? Does the eSSO solution have to prevent the application from starting if the user is not authorised to use it?	
Can users delegate their application account?	
Do some users have shared accounts in the application?	
Can users log out? (In which case the solution must not automatically reauthenticate users.)	
Is the application integrated into the internal credential management solution? If so, are the application’s entitlements provisioned automatically to the eSSO solution?	

IX.3.3. Questions specific to WebSSO and federated identity management

In WebSSO, the approach is generally more complex and often requires a more in-depth analysis of the applications to be integrated by SSO experts, integrators and publishers. The specifications must make it possible to define the main trends, namely whether it is possible to use federated identity management, and which type, whether it is possible to use SSO methods via API, Web Services or valve applications, or whether the subject is addressed by other Web SSO methods: HTTP headers, form completion, URL rewriting, etc. The choice of SSO method to use is therefore highly dependent on the application and some questions cannot be answered by the application manager, but instead the SSO project manager, or even other technical managers of LDAP or AD directories, etc.

Question	Answer
Technical information	
Server platform (OS)	
Web server (type/version/options)	
Application technology (ASP, JSP, etc.)	
Access criticality (strong security?)	
Level of availability implemented at server level	
Application access protocol? (HTTP/HTTPS)	
Application delivered on the network? (Intranet, DMZ, SaaS, etc.)	
Is it possible to install an agent on the application server? (Apache module, ISAPI filter, Tomcat valve, etc.)	
Do users access the application via a reverse proxy? If so, is it possible to install an SSO agent on the reverse proxy?	
User processes	
What are the application access processes? • Link in a portal? • Links in emails? • Bookmarks?	
Are these links always static (e.g. application homepage) or can they be dynamic (e.g. page with a file ID)?	
How do users currently authenticate in the application?	
Should it still be possible to access the application without using SSO?	
What URL is entered by users to access the application? (To be confirmed for each environment: production, pre-production, etc.)	

SSO method	
Which authentication (or SSO) mechanisms are supported by the application? • HTML form • Basic HTTP • HTTP header • Kerberos/NTML • SAMLv2 • OAuth2/OpenID Connect • X509 certificate • Other?	
Is the application modifiable? (e.g. can the application's authentication mechanism be overloaded?)	
Specific case: SAMLv2-compatible application	
Federation partner name/Contacts	
Technology used by the partner (ADFS, OpenSSO, OpenSAML, etc.)?	
Version of SAML protocol to be used (1.1, 2.0)?	
Role played by the internal solution in this Federation: • IdP: identity provider • SP: service provider/identity consumer	
What is the initiator of the federation sequence? (“IdP Initiated” mode or “SP Initiated” mode)	
SAML Profiles	
SAML Binding	
Do SAML assertions have to be signed?	
Do authentication requests (AuthNRequest) have to be signed?	
Federation mode (temporary or permanent?)	
Name of the SAML attribute carrying the user's identity (only if temporary federation)	
User identifier	
Necessary attributes (list the attributes sent by IdP or needed by the SP)	
Other information?	

IX.4. “Strong authentication” appendix

The purpose of this appendix is to provide some information about the different authentication technologies, simple or strong, deployed on the market. To help any readers who are currently selecting such a technology to choose depending on their constraints, we suggest some advantages and drawbacks of the various options.

To begin with, remember that chapter “II.3. Authenticating users” of this document introduces the main authentication concepts.

IX.4.1. Simple identification

Username + Password	*Advantages*	• Easy to implement
	Drawbacks	• Requires a complex password policy • Passwords can be cracked, by brute force for example • Management of forgotten passwords
	Ergonomics	• Management of multiple passwords • Users write usernames on post-its • “Irritant” for users
	Security	• Weak
	Cost	• Average
RFID	*Advantages*	• Easy to implement • No passwords to remember • Various RFID tag formats
	Drawbacks	• Requires RFID readers • Weak card-reader transaction security • Risk of the tag being lost/stolen/broken
	Ergonomics	• No PIN to protect access to the tag • Multi-service support: coupling with physical access control, for example
	Security	• Weak
	Cost	• Weak

IX.4.2. Strong two-factor authentication

RFID/Password	*Advantages*	• No certificate management • No wear, long system lifespan • Varied RFID tag formats: USB key, smartphone, card, etc. • Graphic personalisation possible
	Drawbacks	• Requires RFID card readers • Weak card-reader transaction security • Risk of the tag being lost/stolen • No PIN to protect access to the tag
	Ergonomics	• Multi-service support • Ease of use, contactless mode • Rapid staff identification
	Security	• Average
	Cost	• Weak
Chip card **+ PIN**	*Advantages*	• Security: requires a PIN to authorise access to the card • Use of certificates: signature, encryption, authentication • No passwords to manage • Theft: no direct access to the certificate because it is PIN-protected • Graphic personalisation possible
	Drawbacks	• Risk of the card being lost/stolen • Requires a contact card reader and deployment of middleware • Certificates need to be managed: PKI, CMS, etc.
	Ergonomics	• Reliable, robust system • Ease of use • Rapid staff identification • Multi-service support possible thanks to RFID
	Security	• High
	Cost	• High
USB token **+ PIN**	*Advantages*	• Security: requires a PIN to authorise access to the token • Use of certificates: signature, encryption, authentication • No passwords to manage • Theft: no direct access to the certificate because it is PIN-protected • No need for a card reader • Data storage possible

	Drawbacks	• Risk of the card being lost/stolen • Certificates need to be managed • Requires access to USB ports
	Ergonomics	• Reliable, robust system • Ease of use • Multi-service support possible thanks to RFID • Storage of encrypted personal files
	Security	• High
	Cost	• High
Biometrics (Match on Card)	*Advantages*	• Security: what I am • CNIL compliance of “Match on Card”, unlike “Match on Server”, for instance
	Drawbacks	• High price • Specific readers
	Ergonomics	• Need to register fingerprints • No passwords to remember
	Security	• High
	Cost	• High

IX.4.3. Strong two-factor authentication [Out-of-Band]

OTP SMS	*Advantages*	• Nothing to install • Ease of use, for example the user copies a code • Nothing to remember
	Drawbacks	• Cost of the SMS-sending platform • Need to have your phone with you • Need to have access to the GSM network • Users’ phone numbers need to be known
	Ergonomics	• Very easy to access: compatible with all types of phone • Conventional, widespread use, including for 3DSecure payment
	Security	• Average
	Cost	• High
OTP Mail	*Advantages*	• Nothing to install • Ease of use, for example the user copies a code • Nothing to remember

	Drawbacks	• Need to have a mobile phone connected to the network • Requires an email address • Low email security: interception
	Ergonomics	• Conventional use of mobile phones
	Security	• Average
	Cost	• Average
OTP Smartphone (PUSH)	*Advantages*	• OTP code generation platform protected by password or PIN • Operates in offline mode
	Drawbacks	• Requires an application on a smartphone • The external device needs to be registered beforehand
	Ergonomics	• Easy to install on a business smartphone
	Security	• High
	Cost	• Average
Electronic/soft tokens	*Advantages*	• Single authentication token
	Drawbacks	• Requires a server infrastructure • Risk of loss or theft
	Ergonomics	• Need to have your token with you
	Security	• Average
	Cost	• Average

L'ESPRIT DE L'ÉCHANGE

FRENCH INFORMATION SECURITY CLUB

11 rue de Mogador
75009 Paris
France
☎ +33 1 53 25 08 80
clusif@clusif.fr

Download all CLUSIF documents at
www.clusif.fr