Experiences and best practice for Identity and Access Management

Colin Miles – Pirean Ltd

PCTY2011

Pulse Comes to You

Optimising the World's Infrastructure

PIREAN

Together We're Smarter.

Agenda

- Our experiences – IAM solution delivery
- Business Drivers / Scoping our solution
- Common challenges and approaches
- Solution examples & best practices
- Conclusions

About Pirean

As one of the world's leading IBM Premier Business Partners, Pirean are proud to have been recognised by IBM as the world's most certified IBM Tivoli Partner (as of March 2010).

Pirean holds 14 of IBM's A, AA and AAA Tivoli Accreditations spanning Security and IT Service delivery and is the first and only Partner to hold IBM Tivoli AAA status, the highest authorised level, across both IT Service and Security Management.

Pirean's Information Security practice delivers AAA accredited services for IBM Tivoli Software - we provide trusted counsel and industry leading solutions to shape our customer's security infrastructure into a valid business enabler.

Established in 2001, in September 2009 Pirean debuted as the highest placed IT Services Company on The Sunday Times Microsoft Tech Track 100 annual league table of Britain's fastest-growing private tech companies.

At Pirean we recognise that a broad base of skills and experience means little without the right approach to realising our customers ambition. Our approach crosses boundaries of consultancy, technology and outsourcing – providing a single support structure to partner our customers in the delivery of enterprise services.

Implementing IAM Solutions

Business drivers

Scoping our solution

IAM – The Business Drivers

If implemented in alignment with a clear, strategic vision IAM solutions will offer real benefit to the business. Some examples of business drivers:

Driver	What it means
Agility	Significant reductions in the time required to set up new users or change user access levels leads to dramatic increases in productivity. Automation speeds the processing of requests, freeing administrators to spend time on more productive activities. A standards based infrastructure allows for rapid expansion whether via natural enterprise evolution (employee growth), new ventures (mergers & acquisitions) or new markets (expanding customer base).
Security	Enhanced security through task automation, consistent policy application and enforcement, centralised audit and reporting capabilities and the timely creation, suspension and deletion of user accounts.
Cost	Reduced development costs by centralising identity information and making it consistently available to multiple applications instead of having each application store and maintain its own data in multiple locations. Save on software licensing costs by disabling dormant or inactive user accounts in a timely fashion. Support costs are reduced as a centralized, high-performance, and scalable identity repository reduce troubleshooting time and error correction demands. Also, with self-service password resets and single sign-on, users no longer have to call the help desk.
Compliance	Many compliance and regulatory concerns such as PCI-DSS, Sarbanes-Oxley (SOX) and the European Union Directive on Data Protection call for effective authentication, authorisation and audit controls.

Identity and Access Management – Getting started

Typical business challenges that demonstrate the need for Identity Management may be understood by asking some simple, basic questions. For example:

1. Do we know **who** is accessing our systems? Do we have a **consistent, consolidated view** of exactly **who** is accessing **what**? .

2. Do all our users have the **appropriate access** to systems when they need it (and how long does it take to set up all the correct access for a new user)?

3. Have we **revoked** access for those users who no longer require access?

4. Can we **demonstrate** exactly who has access to what to our auditors?

5. If a user has forgotten his / her password – how does he/she get it reset (and how long does it take)?

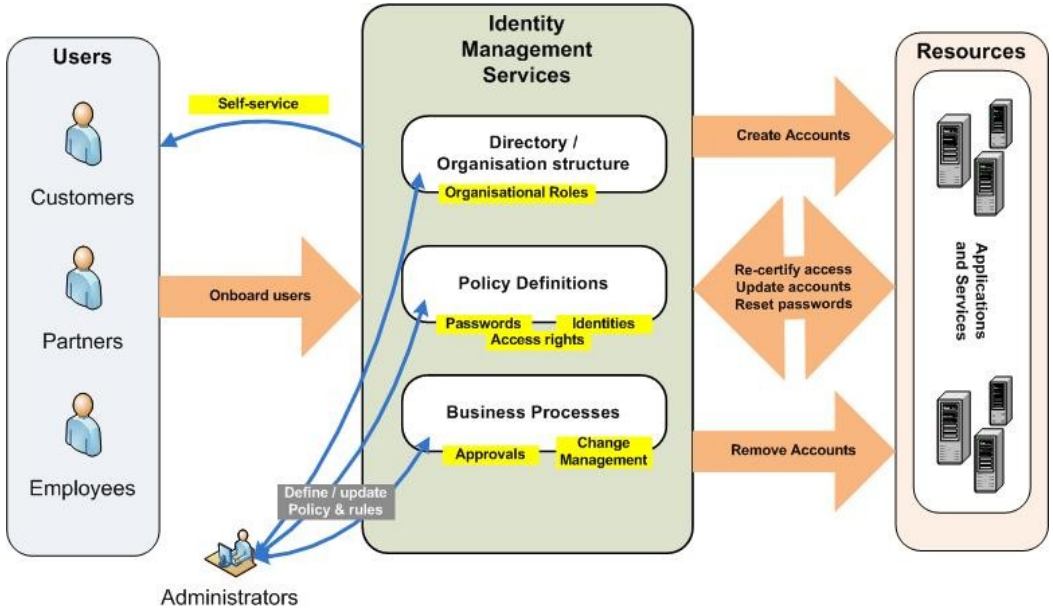
6. How long does it take for us to **onboard** new applications and services?

7. Do we understand what the costs of managing user access across the organisation are?

8. Are user management or security issues preventing us from on-boarding new applications or moving into new markets quickly?

Identity Management – Solution basics

Identity Management brings support for **User Lifecycle Management**. This means establishing control over the identities of employees, partners, customers and trial participants throughout their entire period of interaction with the organisation.



User Lifecycle Management:

Onboard	Provide users with access quickly. Ensure appropriate levels of access for all users.
Manage	Add / remove rights as requirements change. Enforce policies. Integrate with business processes.
Support	Track and maintain privileges. Provide user self-service. Monitor, audit & report.
Deactivate	Identify and action terminations automatically.

Common themes and topics:

User Management
Identity Aggregation (due to mergers/acquisitions or enterprise evln)
Credential Management
Entitlement Management
Provisioning & De-Provisioning
Password Synchronisation
Self Service
Attestation / Recertification
Separation of Duties

Identity Management – understanding requirements & defining a solution approach

Our approach for the implementation of the **core functions** of IdM builds upon an understanding of some basic requirements:

Question	Typical Identity Management functions	Meeting the requirements
Who are our users?	Establishing an **authoritative data source** (directory) for identity information. **On boarding and maintaining user information** based on changes in other directories.	Understand **user types & volumes.** Understand **common activities / pain points.** Understand and **business processes.**
What access is required for our users?	Determine **access rights** and **entitlements**. Define and apply policies that govern access rights either through automated role based or request based provisioning.	Understanding coverage required – i.e.: • Automated feeds • Self-service • Manual input • Role Based Access Control - Readiness today - Analysis needed - Common approaches
How do we set up access?	**Provision** users and access rights automatically. Create and manage (modify, suspend, restore) user accounts for systems and applications.	

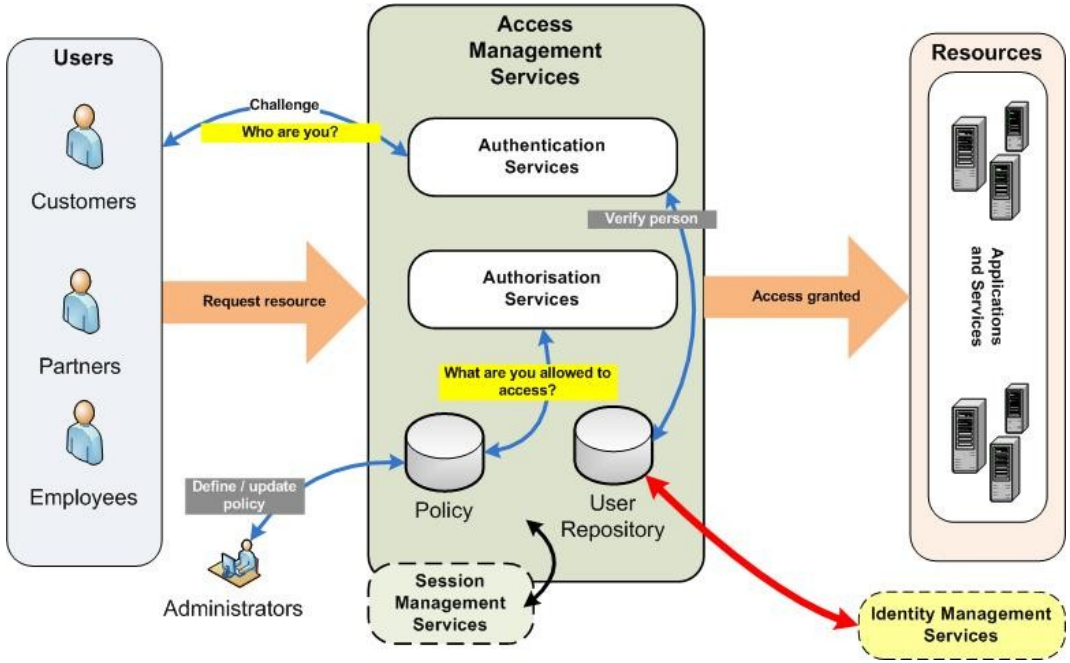
Identity Management – understanding requirements & defining a solution approach

More core functions...

Question	Typical Identity Management functions	Meeting the requirements
How do we manage and track access?	Continually track and assess access privileges for users – attesting to their continued accuracy and validity.	User access can be controlled and audited through native functionality of the IDM toolset. Clarify requirements for **re-certification** of access rights periodically (to ensure compliance and observance of **separation of duty** controls).
How do we remove access?	**Automatically** suspend (or "mark" – see notes) all access privileges based on rules and automatically delete accounts during leaver processing / trial completion.	Native functionality of the toolset allows us to ensure that dormant accounts are removed as speedily as possible (helping prevent any potential malicious re-use of accounts and as well as helping manage software license costs). Typical approaches will adopt a "**soft**" stance on highlighting and managing dormant accounts in the early phases – allowing investigation of account status where needed. A move to automated de-provisioning of non-compliant accounts will come with further IDM process maturity.

Access Management – Solution Basics

Focusing on Access Management for **web based resources** (i.e.. resources accessed by a user through a browser, or other web based services).



Key functions:

- Define **policy**
- **Identify** user (who are you?)
- **Authenticate** user (prove it!)
- **Authorise** user (what can you access?)
- **Single sign-on** (logon only once to access multiple services and applications)

Access Management – understanding requirements & defining a solution approach

In a similar fashion, we can start to understand the basic requirements for our AM solution by asking :

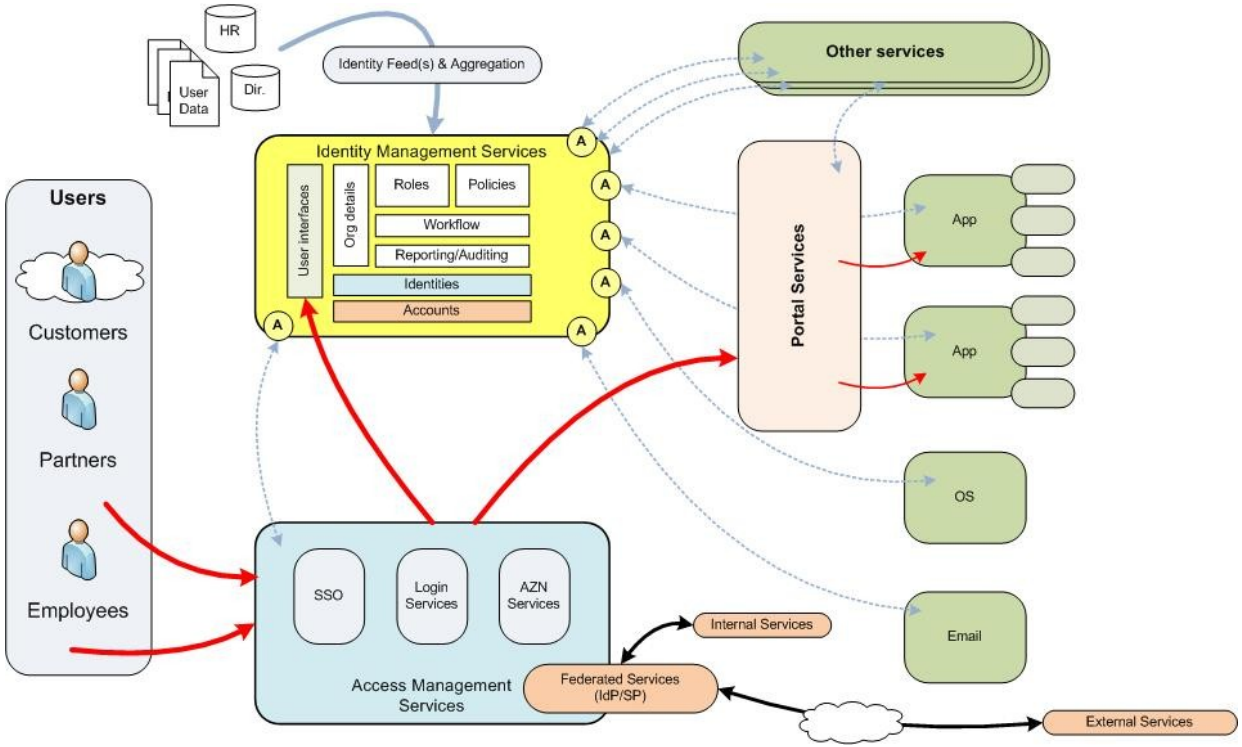
Question	Typical Access Management functions	Meeting the requirements
How can we be sure only the right people are accessing our systems? **How do we define and enforce security policies?**	Provide a means for the user to identify themselves via an appropriate **authentication mechanism** (i.e.. username / password or use of strong authentication mechanisms such as smartcards, tokens or biometrics).	Are initial requirements for **username / password** authentication only? All protected applications can have a single interface for authentication services which can evolve to provide **stronger authentication** mechanisms: User ID & Password, Two-Factor, etc.
	Provide **authorisation policies** and **enforcement**. Once authenticated, a user should only be able to access a service for which they are authorised to do so via their entitlements.	Only permitted users with the appropriate credentials can access protected applications. Furthermore, policies can be defined to restrict access to known IP addresses, to certain times of the day and to users who have authenticated using specified mechanisms.

Access Management – understanding requirements & defining a solution approach

Further questions...

Question	Typical Access Management functions	Meeting the requirements
How do we make user access to our systems simpler?	Provide **single sign-on** to allow the user access to multiple applications and services while only having to login once.	Reduce authentication challenges and increase productivity. Improve the user experience and perception of services. Native functionality of the Access Management toolset provides the facility for Web SSO. Many configuration options are available to integrate with backend systems (credential management – IDM). Federated Identity (Access) solutions make the access proposition even simpler – and increase the scope for simplified integration with other user repositories.
How can we monitor access and make informed business decisions based on usage?	**Centralised auditing** - as access is performed centrally, all accesses can be logged and audited centrally.	Access to web resources can be audited and reported on centrally. Other options / extensions are available.

Integrated Identity and Access Management solutions



Implementing IAM Solutions

Common challenges

PIREAN
Together We're Smarter.

Common obstacles for successful IAM deployments

Common Issues	Reasons
Large/Cumbersome Projects	IAM is a discipline that touches virtually every individual end user and user group in the organisation, as well as some fundamental IT infrastructure and business processes.
Stakeholder Expectations Not Met	Stakeholders need to be sure that the solution that will be provided meets their business requirements and processes. Stakeholders should be made aware of exactly what the Identity Management system will provide and how applications will be secured by the Access Management system.
Fear	Automating processes can lead people to believe that their jobs are at risk. System Administrators can become uncooperative unless they are assured that their role will evolve.
Perception	IAM solutions are business enablers rather than "necessary evils" – the perception of the project needs to be right in order to realise value
Technology Only View	IAM solutions impact on business process and are not merely IT projects. Business process must be considered (or reconsidered) as part of the programme of work rather than merely automating flawed processes.

Some key challenges - Business

Some of the most significant Business Challenges likely to impact our IAM project include:

Strategic Objectives Alignment	How do we aligning IAM to strategic business objectives?
Stakeholder Buy-in	How do we get stakeholder buy-in across the organisation? Can we agree a common view of goals, risks, timescales etc?
Centralisation	How do we translate the existing "distributed" methods of identity and access management for a centralised approach?
Ownership	Who "owns" identity data?

Some key challenges - Technical

A number of Technical Challenges are also likely to arise – our design will need to address these concerns early on:

Application Integration for Provisioning	For applications that have their own credential repository, it may be that there is no interface available for making updates (or perhaps support would be invalidated if data was written directly into the credential store). Having readily available "adapters" for the majority of enterprise applications can help but it is likely that customer-built adapters will be required for proprietary applications.
Application Integration for Access Control	Not all applications can be easily tailored to integrate with an Access Management solution. As such, techniques for performing Single Sign On may need to be configured on an application by application basis. Also, not all applications are written in a manner which makes the deployment of a Access Management services (where intermediary servers become part of the process flow) easy process.
Standards	While many standards exist in the IAM space, not all standards have been adopted by application vendors.

Implementing IAM Solutions

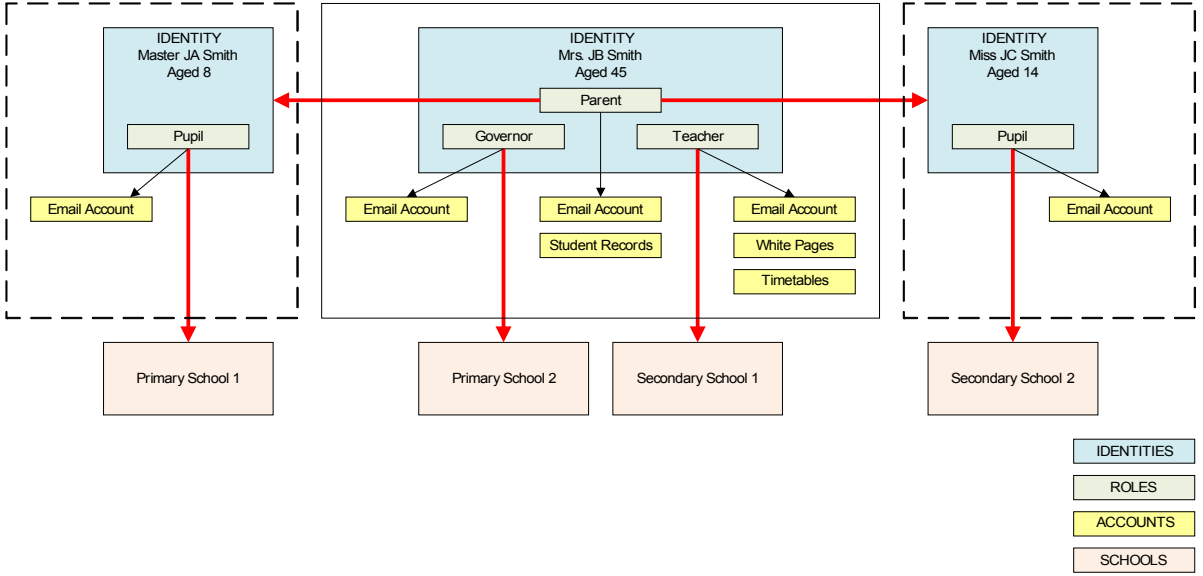
Solution examples – challenges faced

Best practices

PIREAN
Together We're Smarter.

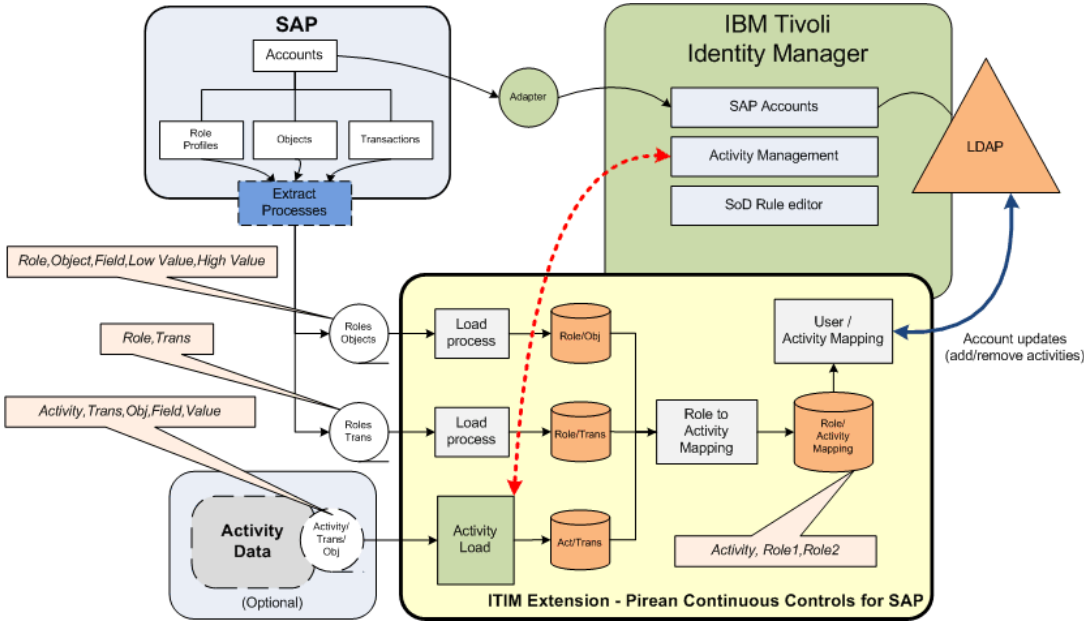
Identity Management – integration challenges

- Identity Feeds
  - Is a single authoritative source of identity data available?
  - What relationships apply?
  - Is identity data duplicated?
  - What alternate mechanisms for loading identity data need to be supported?
    - Automated
    - Aggregated
    - Manual
    - Self-service



Identity Management – integration challenges

- Integration challenges – ITIM adapters
  - Will an “OOTB” approach apply for each target system?
  - Can we understand application entitlements in a business context?
  - Experiences – adapters & adapter development
    - Flexible approaches required
    - Example enhancements delivered
      - SAP
      - RACF
      - TAM Combo



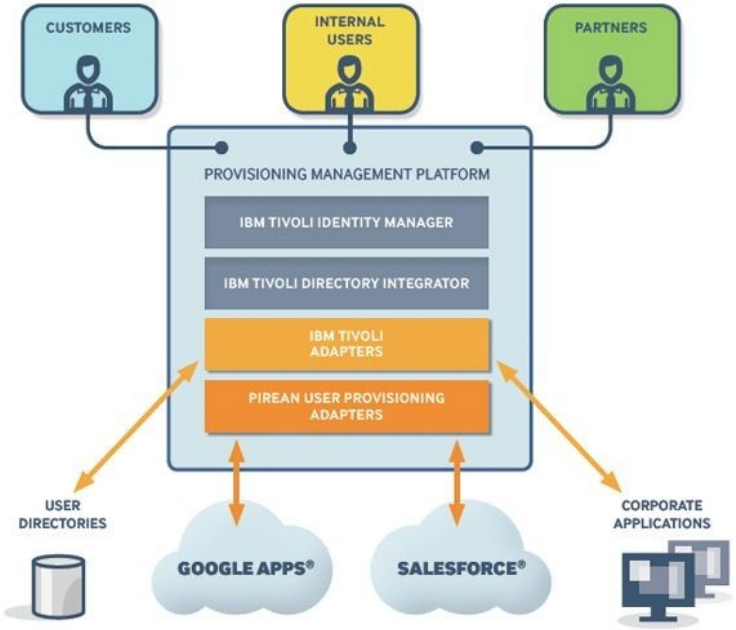
Access Management – integration challenges

- Meeting complex authentication requirements
  - Enhanced security and dynamic request routing
  - Branding and internationalisation of content
  - Non standard credential entry methods / workflows
  - Authentication against multiple foreign registries

- SSO integration techniques
  - Is credential management on backend system still required?
  - How do we effect an SSO to the backend system?
  - How do we establish trust?
  - Examples...

Approaches for new challenges

- Federated Identity
  - FSSO models
  - Significant challenges remain for account management, login & user registration orchestration
- Identity and Access Management in the Cloud
  - Security should not inhibit cloud adoption
  - ITIM adapters for cloud based services
- Other options / experiences for extending the Tivoli Security Solution Portfolio

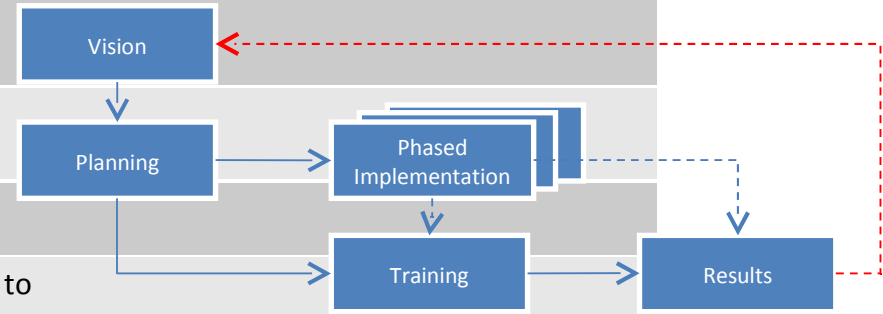


Conclusions: Successful IAM implementations

Our Recommendations	
Know your business	Those organisations who knew what their organisation looked like and what they wanted it to look like were able to articulate their requirements and business processes accurately from the start.
Involve the right people	Those organisations who ran their IAM implementation as a programme of work which involved everyone from end users to IT, marketing and business executives were more successful than those organisation who ran their IAM programme in a silo.
Phased implementations	Phased approaches that deliver value early and often gain better support from end users.
Education	Organisations who communicate the potential business process changes early and educate their end users, business and IT staff gain better buy-in to the programme and less resistance when the changes are applied.
Recognise evolution	IAM solutions need routine attention – it's a programme of work that will help deliver business benefit by evolving with business processes. Successful programmes recognise the on-going process rather than deploy and forget.

Conclusions: Successful IAM implementations

Steps for success	
Vision	Identify goals for the project
Planning	Establish the most appropriate engagement approach. Who does the work? Where? How do we engage with impacted users? When does the project start and when does it start to show tangible results?
Pilot	Start with a small user base to validate the approach
Rollout	Rollout to a larger user base adding value incrementally
Results	Validate results against the goals at every stage
Transition Management	From systems design, development and delivery to an ongoing BAU operational model



A final note: Managing Risks and Issues

Risk/Issue	Description
Poor Pre-Project Preparation	Setting false expectations, indecisiveness (resulting in engineers defining business requirements) and not realising business value quickly enough can undermine confidence in a major IAM deployment. This can be alleviated with executive sponsorship, well defined business requirements, a project team that extends beyond the engineers and good change control.
Poor Requirements Definition	Requirements must meet business requirements and the requirements should not be defined beyond the scope of what can be economically delivered. Defining requirements outside the framework of the toolset may be difficult and expensive to implement and support.
Large Initial Scope	IAM projects can have broad impact on users and business processes. Trying to “boil the ocean” may not just challenge the technology but may have a major impact on the organisation and will certainly delay perceived system value. The project should be implemented in phases with maximum value returned in the shortest timeframe in order to establish a foundation for further enhancement.
Inexperienced Resources	An inexperienced team will make poor design/implementation decisions or choose a customised approach rather than leverage the strength of the relevant toolsets. Qualified & experienced systems integrators should be used to help build, train and mentor others.
Poor Project Methodology	Partner with a systems integrator with a proven track record of IAM delivery.
Scope Creep	Requirements gathering and change management can mitigate against scope creep but, with a system that spans almost all areas of an enterprise, it is easy for functionality to be added to an IAM project. Keep in mind the phased approach and maximising ROI.

Any Questions?