

# **Tivoli Nation Identity Management – The IAG Journey**

Heng Mok – Security Architect

Version 1

30th July, 2008

# Agenda

- About IAG
- Issues and Problems facing IAG
- IAG's Approach
- High Level Architecture and Solution
- Achievements and Benefits
- Key Learning's
- Conclusion and takeaway points

# About Insurance Australia Group (IAG)

## General Information

- Largest home and car insurer in Australia
- Core focus is general insurance
  - **Travel**
  - **Motor**
  - **Home**
  - **Commercial**
- Has offerings in both the intermediary and direct insurance markets
  - **Via a broker / agent mode**
  - **Direct to the customer**
- IAG is holding company for specific insurance lines and brands
- Brands across Australia, NZ, Asia and the UK

# About Insurance Australia Group (IAG) Brands

REGION	DIRECT INSURANCE	INTERMEDIATED INSURANCE
 AUSTRALIA	   	 
 NEW ZEALAND		
 EUROPE		 
 ASIA	 96% voting rights	 

\* Via a distribution relationship and underwriting joint venture with RACV Limited

\*\* Not IAG wholly owned

# About Insurance Australia Group (IAG)

## IT Perspective when we started IdM

- CGU and IAG had just merged
- Mixed and complex environment from various mergers and acquisitions
  - **No real technology standards – a bit of everything**
  - **Large amount of heavily customised core systems**
- Insourced the IT function 5 years ago from IBM
- Many new people to the organisation
- Steep learning curve to implement new processes and procedures
  - **Lack of governance**
  - **No formalised architecture functions**
- Some core insurance systems were in the process of being transformed

# Issues and Problems facing IAG

At time of journeying down the IdM Patch

- Large amount of manual processes inherited from insource
- System Access Request in the dark ages - paper and fax forms
  - **Processes were transitioned from the insource**
- Identity data inconsistent across the board
- Multiple user account formats
- Core application's security model complex
- High staff turnover rate in contact centre's
- Pain points around password resets
  - **Made up 30% of Help Desk Calls**
- External auditors raising issues around the system access request process
  - **Terminations**

# Identity Management Definition

## IAG's definition

- Identity Management is about managing the lifecycle of the identity
- Process
  - **Add / Remove / Modify**
- Attributes
  - **Data about the identity**
- Properties directly impacted and linked to identity
  - **Reduced sign on**
  - **Process automation**
  - **Single sign on**
  - **Access control**

# Approach to the Problem

## Strategy and Requirements

- Link business objectives to identity management services

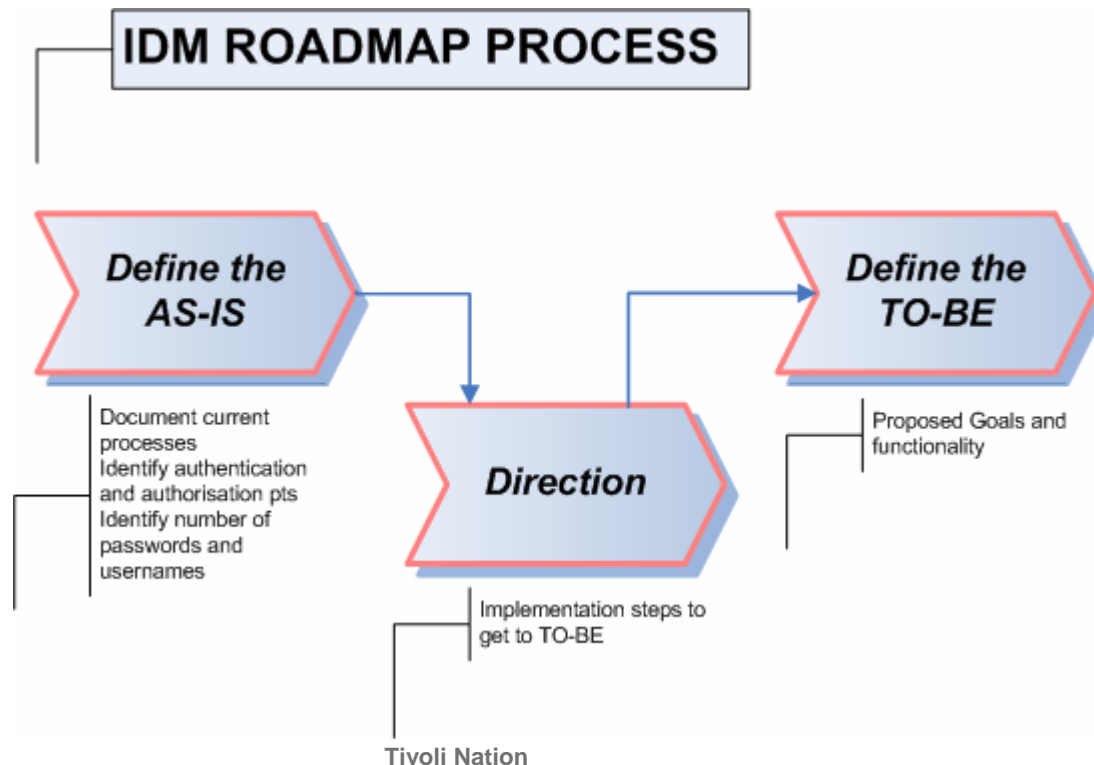
Business Objective	Identity Management Service										
	Identity administration (Delegated)	Identity provisioning	Authentication	Web access management	Workflow	Identity password management	Personalization / relevance (LDAP)	Password Synchronization	Work flow-Accountability	Self Service	Exception / compliance reporting
Reduce 'time to market' of new applications	✓	✓		✓					✓	✓	
Ease of use systems that help build market share	✓			✓		✓			✓	✓	
Migrate to a centralised security model		✓									
Reduce Helpdesk calls relating to passwords and accounts											
Expand services offered to brokers	✓			✓							
Self-service to Brokers	✓				✓	✓					

Map business objective to identity management service

# Approach to the Problem

## Strategy and Requirements

- Develop a strategy – Roadmap
  - **Know your AS-IS**
  - **Define your TO-BE**
  - **What are the steps required to get there**



# Approach to the Problem

## Strategy and Requirements

- Build the business case
  - **Ensure all facts are gathered and analyse data from ticketing systems**
  - **Determine your pain points**
- Use the 80 – 20 rule around functionality delivery
  - **Don't over analyse**
- What does the end user currently experience
- Don't over promise automation
- Stakeholder Management
  - **Applications**
  - **Infrastructure**
  - **Customers**

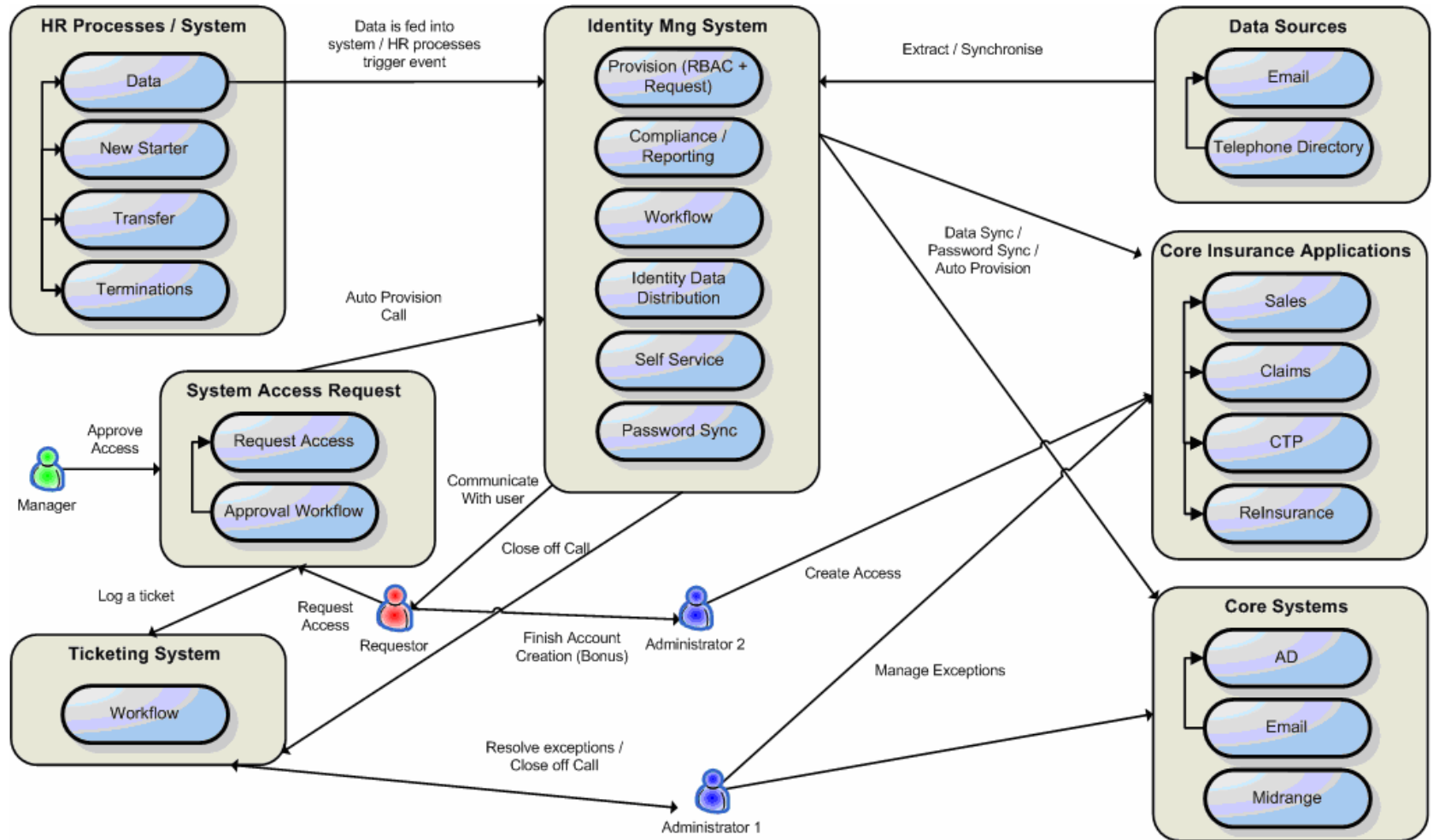
# Approach to the Problem

## Execution

- Take an organic approach based on quick wins
  - **Build an architecture foundation that can be built upon**
  - **Demonstrated tangible and ongoing value, high impact wins**
  - **Continuously evolve and improve**
  - **Utilise new functions in new versions of products**
- Utilise a hub / spoke model for identity data propagation
  - **Know all your sources of data truth**
  - **Be the broker**
  - **Accurate information enables other channels**

# High Level Architecture

## IdM HLA



# Key Technical Architecture Components - TIM

## Identity Management System

- TIM Server – Web Server, App Server, Messaging
  - **Main engine**
  - **Performs all the processing i.e workflow engine**
- TIM Backend – LDAP and relational DB
  - **Stores all the TIM data – reconciled accounts, identity data etc**
  - **Transaction data**
- Management Console – App management
  - **Used to manage and deploy applications**
- Forward Agents
  - **Perform account related requests to the end point**
  - **Password Sync / Account provisioning / de-provisioning**
- Reverse Password Sync Agents
  - **Detect a password change and make request to sync passwords**

# Achievements

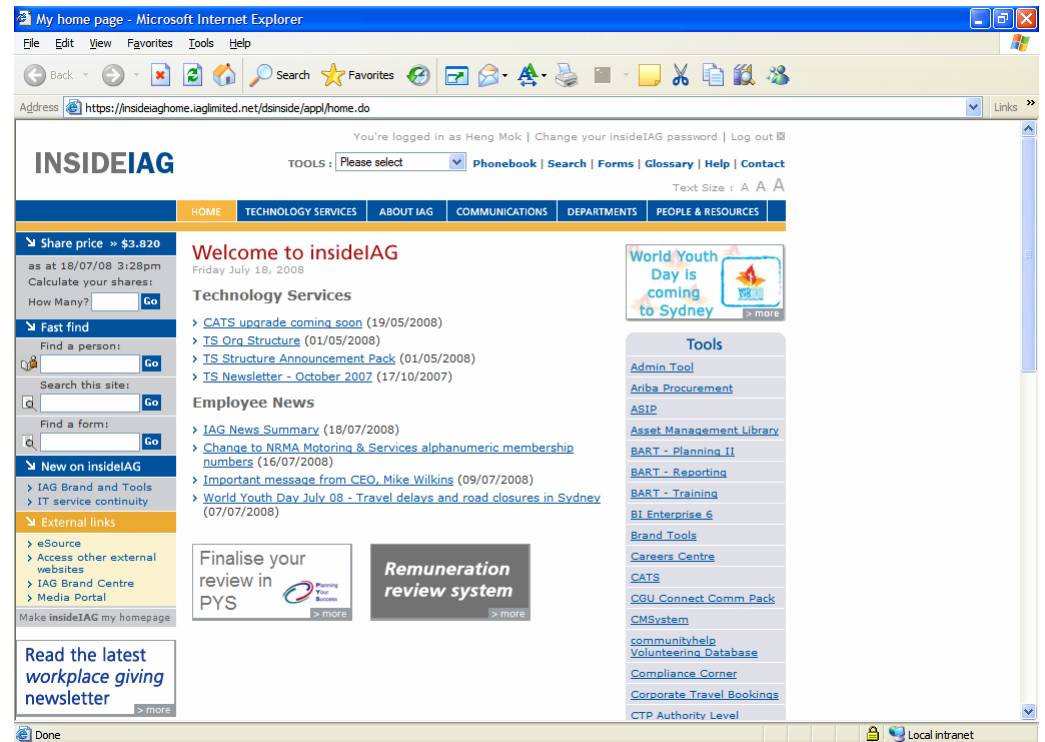
## Password Synchronisation

- Implemented 2 reverse password synchronisation points
  - **Intranet**
  - **Active Directory**
- Integrated with ~16 different end points including wintel, midrange, mainframe and applications
- The average IAG user has 5 – 6 usernames and passwords
- Majority of core passwords are synchronised with network password
- Focused on the core applications and systems
  - **Number of users were greater than 500 users**
- Significant reduction in number of password related issues to the help desk 20% decrease in overall related calls
  - **Today password resets only make up less than 10% of Help Desk calls**

# Achievements

## Base Provisioning

- Intranet is automatically provisioned into with a base level of access
- Provides users with day one access
- Look at policies and begin training



# Achievements

## Request Based Role Provisioning

- Exposed TIM service interface via TDI
- Core insurance applications are provisioned to once approval workflows have completed
- Role model Relies on 5 pieces of information to provision access
  - **Business Area, Business Unit, Business Role, State / Territory and work location**
  - **These attributes will determine the authorization access across each required end point**
- Targeted applications that have general use and high turnover
- Improved the accuracy of provisioning
  - **Manual Errors**
  - **Identity data inconsistencies**
- Reduce the time to provision from 5 end points manually to an automated request
- Repeatable framework that can be used with other systems

# Achievements

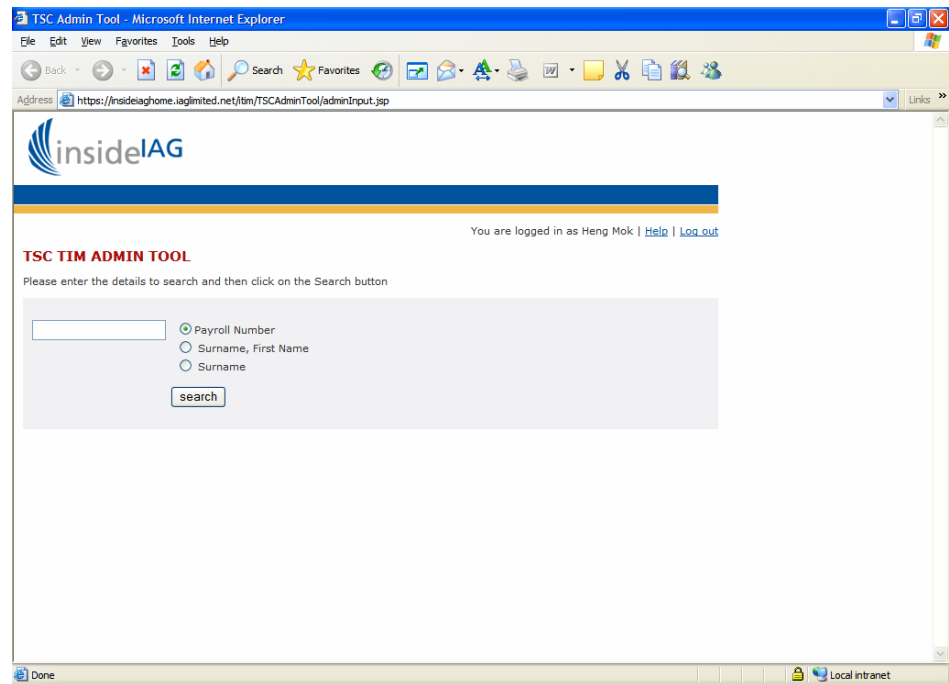
## Deprovisioning

- Implemented workflow to terminate users
  - **Take the termination date established by HR to disable accounts**
  - **Performed 3 times a day as per new HR data coming to the system**
- Able to better comply with our regulators around system access and the processes supporting terminations
- External auditors have not raised any more issues surrounding the controls in place for deprovisioning
- Provides an audit log of when people were terminated corresponding back to the HR date
  - **Audit evidence**
- Provides the option for quick termination remove all core access with one button if the staff member is being walked.

# Achievements

## Centralised Help Desk Tools

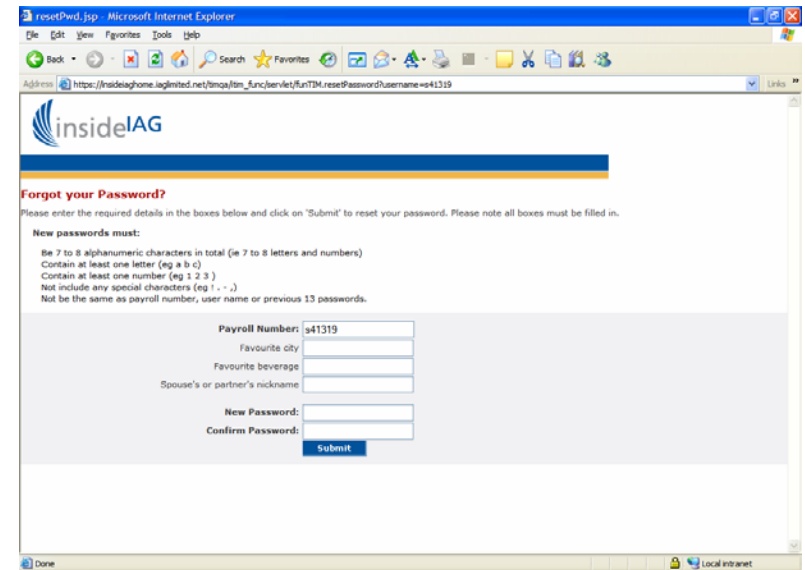
- Developed customised WAS applications utilising the TIM API's
- Reduce the requirement to have multiple tools for resetting passwords
  - **Centralise and control access for help desk staff**
- Value add's to improve productivity and assist other areas
- Keep the auditors happy by reducing level of privileged access across systems



# Achievements

## Self Service

- Built custom applications to handle self service components
- The ability for users to reset their own passwords through self service mechanisms
- Processes to fill in questions and answers when they first login to the Intranet
- Move password resets back to the user



The screenshot shows a web browser window titled "resetPwd.jsp - Microsoft Internet Explorer". The address bar displays the URL: "https://insideaghome.iaglimited.net/bmqal/m\_func/servlet/RunTDM.resetPassword?username=041319". The page features the "insideIAG" logo at the top. Below the logo, the heading "Forgot your Password?" is displayed in red. A message instructs the user to enter details in the boxes below and click "Submit" to reset their password. The "New passwords must:" section lists requirements: 7 to 8 alphanumeric characters, at least one letter and one number, no special characters, and not the same as previous passwords. The form includes input fields for "Payroll Number" (pre-filled with "041319"), "Favourite city", "Favourite beverage", "Spouse's or partner's nickname", "New Password", and "Confirm Password". A blue "Submit" button is located at the bottom right of the form area.

# Achievements

## Centralised Policy Enforcement

- Configured a common policy on TIM
  - **Reverse password sync checks policy before password sync occurs**
- Security enforcement point to ensure that the password comply to a common password standard
- Practical means of enforcing the password management policies
- Because of password sync, will need to go to lowest common denominator of end points

# Key Learning's

## Technology

- New versions of technology can be flaky
  - **Early editions of the software were difficult to deploy**
  - **Troubleshooting problems were extremely hard**
- LDAP architecture is still not a “low cost” resilient architecture
  - **Mitigate risk through some LDAP proxying**
- TDI is a Swiss Army Knife
  - **Can solve a number of problems**
  - **Identity feed / custom agents**
- Customisation is needed to get the required result especially in workflow / specific functions
- Ensure flexibility in the architecture for scale and future requirements
- Build a services interface

# Key Learning's

## Process

- Know your requirements and what you are trying to solve scope creep can kill you
- Ensure strong linkages between detailed designers and architecture strategy
- Ensure development teams and solution architect's have standards which aligns to strategy
- Where possible align to HR onboarding process
- Don't try and reengineer all the people processes (some business processes are difficult to change)
- Pilot new functionality on smaller sites if possible
- There is always going to be a mix between request vs fully automated provisioning

# Key Learning's

## People

- When looking to operationalise your identity management deployment look for skills early on
  - **Hard to find people to fill positions**
- Try to involve your production support people as part of the design process
  - **Ensures they have the history**
  - **Upskilling**
  - **Know why specific decisions were made**
- Get a lab buddy / advocate
  - **IBM has a security development lab in the Gold Coast**
  - **Strong identity management skills and experience**
- Utilise the Tivoli User Groups for knowledge sharing

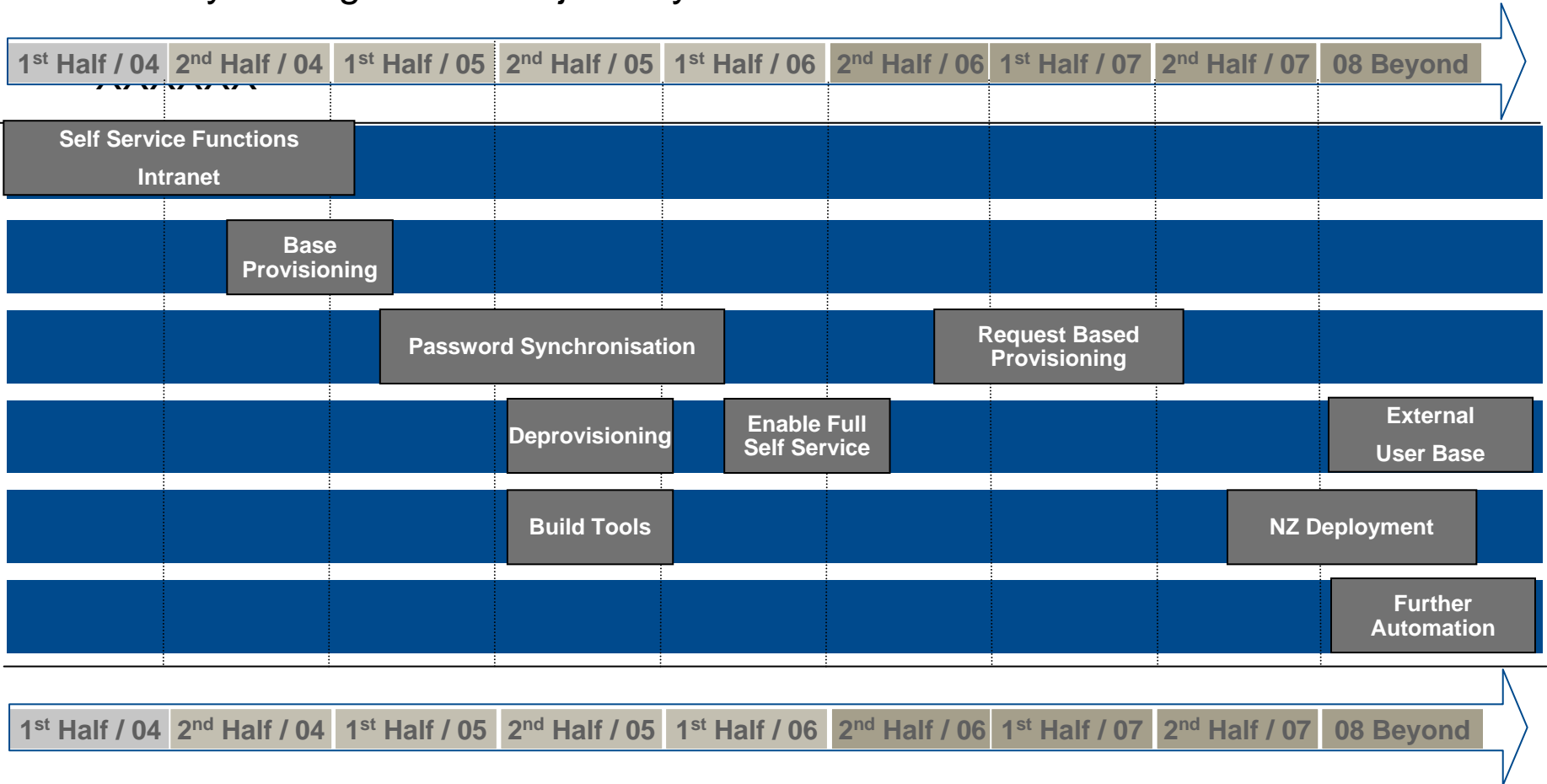
# Where to From Here

## Further Automation

- Focus has been primarily on internal users
  - **Continue to automate internal provisioning processes**
  - **Network level, email systems, high turnover systems**
- A greater need to expose services in legacy and multiple systems
  - **External user provisioning processes need to be automated**
  - **Offer different challenges**
- Focus on reporting capability and self validation functions

# Key Takeaway Points

- Identity Management is a journey



## Key Takeaway Points

- IdM shows and demonstrates tangible and intangible security value
  - **Process improvement**
  - **Automate repeatable processes**
- IdM improves the risk and compliance posture
- IdM is never set and forget, it is a continual process to improve
- Once a framework has been established it is easy to continually plug more applications and resources into the framework
- IdM is 70% process and 20% stakeholder management (politics) and 10% technology

# End of Slide Group

Questions?????